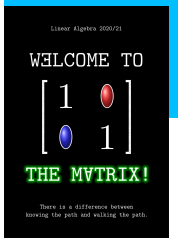
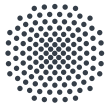


Lineare Algebra

freundlich und gründlich

erkennen.
beweisen.
anwenden.

Prof. Dr. Michael Eisermann
eiserm.de/lehre/LinA



Universität Stuttgart
WiSe 2020/21 und SoSe 2021
Stand 5. März 2022

Habe Mut, dich deines eigenen Verstandes zu bedienen!

Much to learn, you still have.
This is just the beginning.

Für die Mitteilung von Unklarheiten und Fehlern aller Art sowie für Verbesserungsvorschläge bin ich stets dankbar!

Urheberrecht und Haftungsausschluss

Diese Unterlagen werden genutzt zur Vorlesung *Lineare Algebra*. Sie sind für das Grundstudium der Mathematik konzipiert und vermitteln einschlägiges mathematisches Basiswissen.

Die Inhalte wurden vom Autor mit größter Sorgfalt für die Präsentation in der Lehre erstellt. Sie werden allein zu Lehrzwecken zur Verfügung gestellt, in der Hoffnung, dass sie zum Lernen und Üben nützen mögen, ohne jeden Anspruch auf Eignung zu irgendeinem anderen Zweck. Sie sind keine Handlungsanweisung oder Empfehlung. Nur eigenständiges Denken hilft!

Kunst und Wissenschaft, Forschung und Lehre sind frei. (GG Art. 5.3.1) Der Autor übernimmt keinerlei Gewähr für die angebotenen Informationen und Daten, deren Aktualität, Korrektheit, Vollständigkeit, Qualität oder irgendeine Nutzbarkeit außerhalb der Lehre. Haftungsansprüche für mögliche Schäden, materieller oder immaterieller Art, sind grundsätzlich ausgeschlossen.

Für Inhalte externer Quellen, insb. verlinkter Webseiten, ist stets deren Anbieter verantwortlich.

Herzlich willkommen zur Linearen Algebra!

Alles Wichtige zur *Organisation* und alle Angebote der diesjährigen Linearen Algebra finden Sie in unserem liebevoll gestalteten Ilias-Kurs. Dieses Skript dient als Grundlage meiner Vorlesung, derzeit als Videos. Es wird während des Semesters fortgeschrieben und vervollständigt.

Die *Vortragsfolien* sind dabei durch blaue Titelbalken leicht zu erkennen. Hier finden Sie alles Wesentliche, darauf sollten Sie sich konzentrieren. Die *Hintergrundfolien* bieten Erläuterungen, Übungen, Vertiefungen, etc. Diese sollten sie überfliegen und sich heraussuchen, was Ihnen hilft.

In der Vorlesung entwickle ich für Sie die zentralen Ideen und führe die wesentlichen Definitionen, Sätze, Beweise und Techniken präzise aus. Diese Darstellung ist so ausführlich wie nötig und so knapp wie möglich; einiges verstehen Sie sofort, für anderes benötigen Sie Zeit und Muße.

Um diese Ideen und Werkzeuge wirklich zu begreifen, müssen Sie alles selbst in die Hand nehmen, erproben, anwenden, vertiefen, kurz: üben! Das Skript bietet Ihnen hierzu passende Übungen mit Lösungen sowie zahlreiche weitere Illustrationen, Erläuterungen und Ergänzungen.

Herzlich willkommen zur Linearen Algebra!

Diese Vorlesung ist eine Einführung, zwar gründlich doch begrenzt. Sie ist in sich geschlossen und zugleich offen, ein solider Anfang, sie soll Ihnen später insbesondere eine Brücke zur Literatur bieten. Bitte lesen Sie Lehrbücher, sobald Sie sich sicher genug fühlen!

Zur Linearen Algebra gibt es viele gute Lehrbücher. Alle behandeln als Kernprogramm die klassischen Themen, die in den ersten Semestern eines Mathematikstudiums erworben werden müssen und anschließend die Grundlage für alles Weitere bilden. Lehrbücher unterscheiden sich jedoch in Breite oder Kürze der Darstellung, in zusätzlichen Themen, Anwendungen oder historischen Einschüben, sowie in der Menge an Beispielen und Aufgaben. Eine kurze Liste an Empfehlungen finden Sie auf der öffentlichen Vorlesungswebseite `eiserm.de/lehre/2020/LinA`.

Nur durch eigenständige Lektüre lernen Sie verschiedene Sichtweisen kennen in mathematischem Stil und Inhalt, Auswahl und Aufbau, ... Selbst wenn Sie manche Lehrbücher zunächst nur anlesen, sind dies doch wichtige Kondensationskeime, um später darauf zurückzukommen.

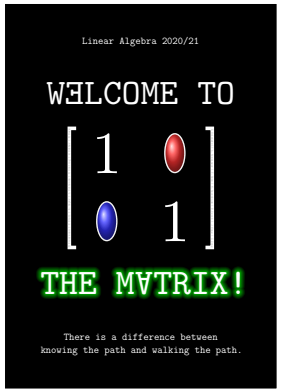
Herzlich willkommen zur Linearen Algebra!

Studieren bereitet Freude und erfordert Disziplin!

- Erstellen Sie einen realistischen Zeitplan.
- Führen Sie ein ehrliches Logbuch.
- Arbeiten Sie gewissenhaft mit.

Wir unterstützen Sie dabei!

- Lehrvideos mit Skript, ergänzend Lehrbücher
- Gut abgestimmte Vorlesung und Übungen
- Ein erfahrenes und hochmotiviertes Team



Dieses weitgehend digitale Semester ist eine immense Herausforderung für uns alle, Lernende und Lehrend-Lernende, insbesondere in Fragen der umsichtigen Organisation und vorausschauenden Kommunikation.

Gemeinsam wird dieses Vorhaben gelingen, indem wir uns gegenseitig stützen und motivieren, aktiv und konstruktiv aufeinander zugehen. Sprechen Sie mit uns! Nutzen Sie die vielfältigen Kontaktmöglichkeiten!

Wie lernen und studieren Sie erfolgreich?

Die Distanzlehre verschiebt die Kommunikationsformen und -medien, ändert jedoch nicht die Ziele und Inhalte Ihrer universitären Ausbildung. Die Universität Stuttgart sichert die hohe Qualität ihrer Studiengänge.

Speziell wir im Fachbereich Mathematik, Dozenten und Studierende, tun gemeinsam alles, um dieses Semester erfolgreich zu gestalten, sodass Sie trotz der widrigen Umstände regulär studieren können.

Für die Vorlesungen in der Mathematik ist das relativ gut möglich: Abgesehen von medientechnischen Änderungen ist unsere Lehrform weiterhin bewährt und robust gegen die meisten äußeren Änderung: Was zählt ist Ihre dauerhafte Aktivierung und hochwertige Anregung.

Für Sie als Studierende gelten dieselben Hinweise und Regeln wie immer: Arbeiten Sie engagiert mit! Mehr denn je sind Ihr Engagement und Ihre individuelle Lernfreude der Schlüssel zu Ihrem Studienerfolg.

Die Universität lehrt kritisches Denken und eigenständiges Arbeiten. Genau diese Grundtugenden fordert (und fördert) die aktuelle Krise. Nehmen Sie, und wir gemeinsam, diese Herausforderungen an!

Wo finden Sie Materialien und Unterstützung?

Alle Angebote finden Sie in unserem liebevoll gestalteten Ilias-Kurs.

Wo finden Sie Materialien und Unterstützung?

Bitte machen Sie sich früh und gründlich mit dem Ilias-Kurs vertraut, sodass Sie ab der ersten Vorlesungswoche voll mitarbeiten können. Manche gehen es halbherzig an, vertrödeln den Einstieg, können dies nicht mehr aufholen und geben frustriert auf. Machen Sie es besser!

Der Ilias-Kurs bündelt alle Angebote und wird für die gesamte Lineare Algebra Ihre zentrale Anlaufstelle sein. Nutzen Sie die gut durchdachte Struktur und die zahlreichen Hilfestellungen der Linearen Algebra. So erleichtern Sie sich spürbar den Einstieg in Ihr Studium.

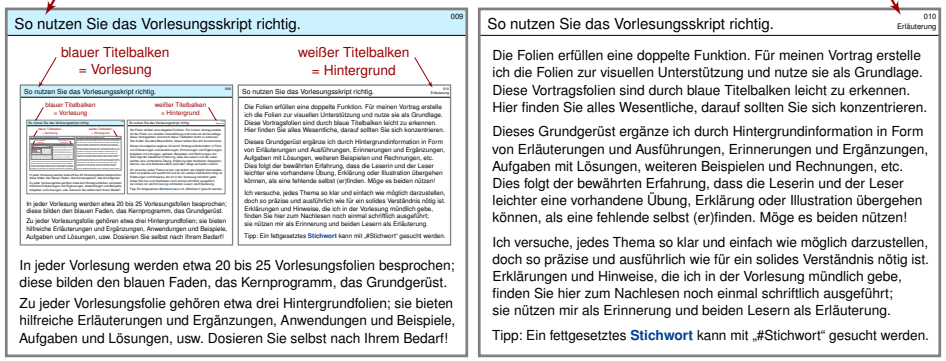
Zunächst einmal finden Sie im Kurs alle Materialien zur Vorlesung. Bitte nutzen Sie vor allem die vielfältigen Kontaktmöglichkeiten, um untereinander und mit Ihrem LinA-Team ins Gespräch zu kommen. Sich alleine durchzukämpfen ist schwer bis unmöglich.

Der Übergang von der Schule zur Hochschule ist ein enormer Sprung. Viele Ihrer bisherigen Gewohnheiten genügen nun nicht mehr, und Sie müssen sich an neue Situationen und Herausforderungen anpassen. Das ist gut und richtig so, und wir unterstützen Sie dabei.

So nutzen Sie das Vorlesungsskript richtig.

blauer Titelbalken = Vorlesung

weißer Titelbalken = Hintergrund



In jeder Vorlesung werden etwa 20 bis 25 Vorlesungsfolien besprochen; diese bilden den blauen Faden, das Kernprogramm, unser Grundgerüst.

Zu jeder Vorlesungsfolie gehören etwa drei Hintergrundfolien; sie bieten hilfreiche Erläuterungen und Ergänzungen, Anwendungen und Beispiele, Aufgaben und Lösungen, usw. Dosieren Sie selbst nach Ihrem Bedarf!

So nutzen Sie das Vorlesungsskript richtig.

Die Folien erfüllen eine doppelte Funktion. Für meinen Vortrag erstelle ich die Folien zur visuellen Unterstützung und nutze sie als Grundlage. Diese Vortragsfolien sind durch blaue Titelbalken leicht zu erkennen. Hier finden Sie alles Wesentliche, darauf sollten Sie sich konzentrieren.

Dieses Grundgerüst ergänze ich durch Hintergrundinformation in Form von Erläuterungen und Ausführungen, Erinnerungen und Ergänzungen, Aufgaben mit Lösungen, weiteren Beispielen und Rechnungen, etc. Dies folgt der bewährten Erfahrung, dass die Leserin und der Leser leichter eine vorhandene Übung, Erklärung oder Illustration übergehen können, als eine fehlende selbst (er)finden. Möge es beiden nützen!

Ich versuche, jedes Thema so klar und einfach wie möglich darzustellen, doch so präzise und ausführlich wie für ein solides Verständnis nötig ist. Erklärungen und Hinweise, die ich in der Vorlesung mündlich gebe, finden Sie hier zum Nachlesen noch einmal schriftlich ausgeführt; sie nützen mir als Erinnerung und beiden Lesern als Erläuterung.

Tipp: Ein fettgesetztes **Stichwort** kann mit „#Stichwort“ gesucht werden.

Wie nutzen Sie Vorlesung, Videos und Folien?

Bei einer Tafelvorlesung schreibe ich nur das Nötigste, alles Weitere wird mündlich erklärt. Mitschreiben ist eine knifflige, aber gute Übung. Ein Skript hingegen kann ich ausführen, ich muss es sogar, da manche TeilnehmerInnen sich dann vorrangig oder gänzlich darauf stützen.

Die Vorlesungsfolien erfüllen, wie oben erklärt, eine doppelte Funktion. Für das Mitschreiben bzw. Abschreiben sind sie eher nicht gedacht, da neben dem absolut nötigen Kern auch freundliche Erläuterungen angefügt sind, und da ist der individuelle Bedarf sehr verschieden.

Die Folien dienen Ihnen sehr gut als Unterlage parallel zur Vorlesung. Die hilfreiche Aktivität des Mitschreibens verlagert sich dabei wie folgt:

1. Markieren Sie wichtige oder noch unklare Stellen zur Nacharbeit.
2. Exzerpieren Sie das Wichtigste als Ihre eigene Zusammenfassung.

Speziell für die Arbeit mit Vorlesungsvideos gilt:

3. Pausieren und wiederholen Sie das Video nach Ihrem Bedarf.
4. Halten Sie immer Stift und Papier für Nebenrechnungen parat.

Wie nutzen Sie Vorlesung, Videos und Folien?

Ich führe eine ungewöhnlich große Zahl von Nebenrechnungen aus, gemäß dem Motto "freundlich und gründlich". Manche Rechnungen überlasse ich Ihnen. Die allermeisten davon sind leichte Routine, das sehen und verstehen Sie aber erst, wenn Sie sie selbst ausführen.

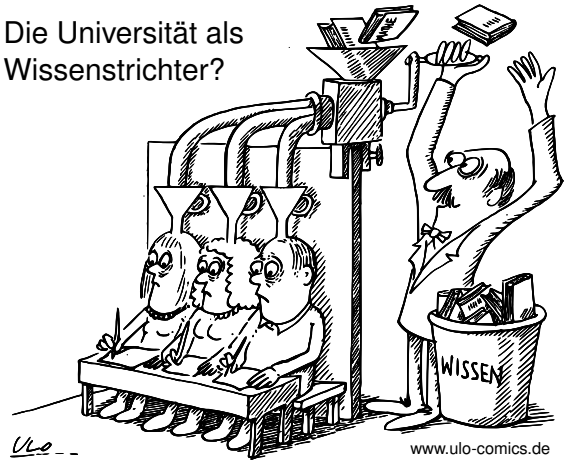
Sie werden vorerst nicht alles durchrechnen können / wollen / müssen, aber möglichst viele Stichproben sollten Sie dennoch selbst versuchen, um sicher zu gehen, dass Sie das Prinzip wirklich verstanden haben. Auch in der Mathematik gilt: Rechnen reinigt die Seele.

Es ist unmöglich, im ersten Durchgang alles zu 100% zu verstehen. Lernen ist iterativ, mit mehreren Ansätzen und Wiederholungen. Die Vorlesung bietet Ihnen dazu gute Anleitung und viel Anregung, doch Ihren Bedarf kennen nur Sie, hier ist Ihre Eigenarbeit gefragt!

Mit der Vorlesung verschaffen Sie sich zunächst einen guten Überblick, anschließend verfestigen Sie Ihr Verständnis und vertiefen es im Detail. Hierbei helfen Quizze und Übungen. Arbeiten Sie die Vorlesung nach, tauschen Sie sich aus, stellen Sie sich und uns Fragen!

Aktives vs passives Lernen

Die Universität als Wissenstrichter?



Erwarten Sie nicht, dass irgendjemand Ihnen irgendetwas beibringen könnte — ohne Ihr Zutun.
Ich kann Ihnen viel Spannendes erzählen, doch nur Sie selbst können sich Verständnis erarbeiten.
Letztlich müssen Sie selbst dieses Material eigenständig durcharbeiten, um es zu beherrschen.
Zwei Faktoren bestimmen Ihren Lernerfolg: extrinsische Anregung und intrisische Motivation!

Weniger ist mehr? Ignorant ist klug?

Sie haben sich in der Schule bereits gut auf Ihr Studium vorbereitet, und zwar auf zwei Ebenen: erstens inhaltlich, zweitens methodisch. Sie wissen aus eigener Erfahrung, das passives (Auswendig)Lernen nur sehr kurzfristig hilft. Für komplexe Zusammenhänge ist es nutzlos. Sie studieren an einer Universität, weil Sie *verstehen* wollen, und dies gelingt allein durch aktives, selbständiges, erarbeitendes Lernen.

Manch eine/r wünscht sich Vorlesung und Skript möglichst kurz, oft verbunden mit der verzweifelt-naiven Forderung, sich allein auf klausurrelevantes Material zu konzentrieren, am besten nur Beispiele, notfalls eine Liste von auswendig zu lernenden Formeln und Rezepten.

Das ist Bulimie-Lernen, von Studierenden zurecht angeprangert, doch zugleich von einigen implizit gefordert und explizit praktiziert: Stoff auswendig lernen, zur Klausur reproduzieren, dann vergessen. Schon als kurzfristige Notlösung ist dies eine freudlose Schinderei, und als langfristige Vermeidungsstrategie ist es unerträglich.
Bitte, tun Sie sich das nicht an, es ist der falsche Weg.

Besser mehr als weniger

Versöhnen Sie kurzfristigen und langfristigen Nutzen!
Ihr Studium ist nicht nur Konsum, sondern auch Investition.
Dabei kommt es wesentlich auf die richtige Balance an.
Ihre Investition von heute ist Ihr Ertrag von morgen!

Das erste Studienjahr ist entscheidend für die soliden Grundlagen, auf denen Sie anschließend Ihr weiteres Studium aufbauen können. Die Lineare Algebra bietet hierzu eine breite und solide Fundierung. Daher das obige Motto dieser Vorlesung: *freundlich und gründlich*.

In dieser Vorlesung nehme ich mir die Zeit für anschauliche Motivation, für mathematische Präzision sowie einige Beispiele und Anwendungen. Das alles kostet viel Mühe, für Sie wie für mich, doch es lohnt sich! Betrachten Sie es nicht als Belastung, sondern als Bereicherung.

Vertrauen und Zusammenarbeit

Diese Lehr-und-Lern-Veranstaltung zur Linearen Algebra macht Ihnen ein gut durchdachtes und reichhaltiges Angebot. Bitte nutzen Sie es!
Wir vertrauen Ihnen, dass Sie Mathematik lernen wollen und können.
Bitte vertrauen Sie uns, dass wir Sie dazu anleiten und Ihnen helfen.

Wo dieses Grundvertrauen fehlt, wird die Universität zu einem müßigen Gegeneinander. Wir brauchen dagegen ein konstruktives Miteinander! Wir vermitteln Ideen, Verständnis und Begeisterung der Mathematik, dazu die handwerklichen Grundlagen und Methoden. Beides wirkt!

Tatsächlich springt dieser Funke oft über. Dazu muss ich voraussetzen, dass Sie bewusst und umsichtig ein Studium gewählt haben, für das Sie Neugier, Ernst und Freude empfinden und bereit sind hart zu arbeiten. Das sind die unabdingbaren Grundlagen, nur so kann es gelingen.

Freiheit und Verantwortung

In Ihrem Studium sind Sie frei und eigenverantwortlich. Das ist etwas Wunderbares, aber erfahrungsgemäß auch eine große Schwierigkeit!

With great power comes great responsibility.

Anders als in der Schule prüft an der Uni zunächst niemand nach, ob Sie zur Vorlesung gehen und aufmerksam mitdenken, die Inhalte gründlich nacharbeiten und Ihre Hausaufgaben sorgfältig machen. Hierfür sind Sie selbst verantwortlich – mit allen Konsequenzen!

Ihre Leistung beweisen Sie in der Klausur am Ende des Semesters. Dieser weite Zeithorizont überfordert viele Studierende: Wissen und Können wachsen nur langsam. Wer nicht kontinuierlich mitarbeitet, kann seine Fehlplanung kurz vor Schluss nicht mehr korrigieren.

Als hilfreiche Zwischenetappen gibt es daher (je nach Veranstaltung) Quizze oder Hausaufgaben oder auch ein bis zwei Scheinklausuren. Manche Studierende empfinden kontinuierliche Kontrolle als Gängelung, andere sind für diese Strukturierung und Rückmeldung sehr dankbar.

Realistisches Zeitbudget

Ein typische Vorlesung mit Übung entspricht 9 LP: insgesamt 270h

- **Präsenz:** 15 Wochen à 2h Übung + 4h Vorlesung = 90h
- **Individuelle Arbeit:** ein weiterer Tag (8h) pro Woche = 120h
- **Wiederholung** zur Prüfungsvorbereitung: zwei Wochen = 60h

Das sind Erfahrungswerte der letzten Jahrzehnte. Ihr individueller Bedarf kann davon etwas abweichen, aber die Größenordnung ist realistisch: Sie benötigen mindestens doppelt soviel Eigenarbeit wie Präsenzzeit!

Sie können Ihre Zeit anders aufteilen, aber viel Spielraum bleibt nicht. Es gilt die Erhaltung der Arbeit: Die 270 Stunden werden Sie brauchen!

Beispiel: Wer beschließt, Vorlesung und Übung zu schwänzen, und jeweils nur das Übungsblatt in 2h abzuschreiben, der muss zur Klausur etwa 240h in Eigenregie nachholen, alleine! Das sind sechs Wochen konzentrierte Eigenarbeit . . . und wird erfahrungsgemäß scheitern.

Qui va lentement, va sûrement, et qui va sûrement, va loin.

Gemeinsames Arbeiten

Ein typisches Semester hat etwa 15 Wochen, das klingt zunächst viel, vergeht aber andererseits sehr schnell. Wir müssen die Zeit gut nutzen! Dabei zeigt sich immer wieder, dass es für die meisten Studierenden viel besser ist, in Gemeinschaft zu arbeiten und zu lernen, als alleine.

Naiv könnte sich jede/r das Skript oder ein Buch nehmen, nach eigenem Rhythmus durchlesen, und so zur Klausur antreten. Doch weit gefehlt! Ein oft unterschätzter, aber erster zentraler Faktor ist die Interaktion! Gerade bei einem anspruchsvollen Studium wird dies entscheidend.

Wir Menschen lernen schrittweise, fragen, diskutieren, probieren, entwerfen vage Ideen, behalten die guten, verfestigen und vertiefen. Davon ausgehend entwickeln wir neue Ideen und Fragen, diskutieren, probieren, schreiten voran. Wissen und Können wachsen nur langsam!

Als Einzelkämpfer/in ist das unnötig schwer, meist sogar unmöglich. Es gelingt am besten in Gemeinschaft: Genau das bietet die Universität! Gut angeleitet durch Vorlesungen und Übungen, eingebettet in eine motivierte Arbeitsgruppe, nutzen Sie dieses produktive Umfeld!

Eigenständiges Arbeiten

Universität bedeutet Gemeinschaft der Lehrenden und Lernenden.

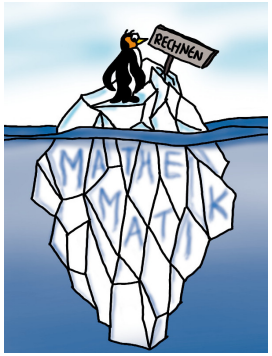
Der zweite entscheidende Faktor für den Erfolg Ihres Studiums ist die eigenständige, intensive Auseinandersetzung mit den Inhalten. Sie werden insbesondere mit Ihren Übungsblättern viel Zeit verbringen. Das ist gut und richtig so, im Idealfall macht es Ihnen auch Freude.

Sie können nicht erwarten, dass Sie ein Übungsblatt in zwei Stunden lösen. Manche Aufgaben sind Routine, aber auch das erfordert zunächst Einarbeitung. Dabei entstehen Fragen, denen Sie nachgehen sollten, denn nur so verstehen und verfestigen Sie den Stoff der Vorlesung.

Andere Aufgaben sind kniffliger und erfordern eigenes Nachdenken und Ausprobieren und durchaus mehrere Anläufe. Insofern unterscheiden sich die Übungsaufgaben an der Uni von Hausaufgaben in der Schule. Das ist keine böswillige Schikane, sondern das unabdingbare Training!

Rechnen in der Schule ist Breitensport.
Mathematik an der Uni ist Spitzensport.

Mathematik ist mehr als Rechnen!



Aus der Schule kennen Sie ein Fach namens „Mathematik“. Manche hatten das Glück, dort sorgfältiges Rechnen zu lernen, andere nicht.

Derzeit sollte das Schulfach tatsächlich eher „Rechnen“ heißen, um falsche Versprechungen, Enttäuschungen und Kummer zu vermeiden.

Lehrpläne kaschieren mangelnde Inhalte gerne mit großspurigen Buzzwords. Zubereitet wird daraus zwangsläufig ein dünnes Süppchen mit wenig Geschmack und geringem Nährwert. Schade!

Schulmathematik besteht leider allzu oft nur aus sturem Anwenden von fertigen Rezepten und stupidem Auswendiglernen von Formeln. Im Extrem wird sinnentleerte Formelgläubigkeit gelehrt und gedrillt: „Hier sind Zahlen x und y, setze sie in die magische x-y-Formel ein!“

Handwerkliche Routine ist wichtig und nützlich, aber eben nur ein sehr kleiner Teil der Wahrheit. **Mathematik ist viel mehr als Rechnen!**

Warum genügt Auswendiglernen nicht?

Zu vielen Problemen sind noch gar keine Lösungen bekannt!
Stur auswendiggelernte Rezepte helfen hier also kein Stück weiter. Gefragt sind im Gegenteil Kreativität, Umsicht und Einfallsreichtum, um überhaupt erst geeignete Methoden zu finden, maßgeschneiderte Algorithmen zu entwickeln, oder bekannte Methoden anzupassen.

Echte Mathematik ist viel umfassender und interessanter!
Meist geht es nicht nur um einzelne Beispiele, das wäre hoffnungslos ineffizient! Konkrete Daten und Problemstellungen ändern sich ständig, daher benötigen wir allgemeine Methoden, die möglichst universell einsetzbar sind. Dieser Werkzeugkasten erlaubt effizientes Arbeiten.

Abstraktion hilft und vereinfacht! Die Mathematik versucht, Ergebnisse zu bündeln, Muster zu erkennen, Gemeinsamkeiten zu nutzen, und so eine möglichst universelle Beschreibung von Problemen und Lösungen bereitzustellen. Das erhöht spürbar die Effizienz. Über Fallbeispiele hinaus wollen wir ein kohärentes Gesamtbild!

Warum sind Beweise so wichtig?

Wir wollen unsere **Resultate** sorgfältig erarbeiten und kritisch prüfen. Wie können wir sicher sein, dass neu gefundene Ergebnisse korrekt sind, also unsere Sätze, Methoden, Algorithmen, ... wirklich leisten, was sie versprechen? Natürlich können wir eine allgemeine Aussage anhand von konkreten Beispielen testen, und so eventuell Fehler finden.

Leider genügen noch so viele erfolgreiche Beispiele noch nicht, um zu garantieren, dass die Aussage wirklich immer gilt. Wie können wir die Wahrheit sicher erkennen und nachvollziehbar vermitteln? Anders als andere Wissenschaften besitzt die Mathematik hierzu eine Geheimwaffe, von manchen gefürchtet, von anderen gefeiert: **Beweise**!

Um als Satz zu gelten, muss die behauptete Aussage bewiesen werden. Andernfalls ist sie bloß eine Vermutung und sollte ehrlicherweise auch so genannt werden. So hat jede Aussage einen unmissverständlichen Status: Sie ist entweder bewiesen oder widerlegt oder noch offen. Auch das steigert die Effizienz: **Prove once, apply everywhere.**

Wie lernen Sie beweisen?

Ab Beginn Ihres Mathematikstudiums lernen Sie in Linearer Algebra und Analysis, wie Sie Beweise richtig ausführen. Erst kleine, dann größere.

Dazu benötigen Sie viel Übung und Erfahrung, zudem genaue Kenntnis erfolgreicher Beweismethoden. Als Ausblick nenne ich: direkter Beweis durch Rechnen oder Konstruktion, indirekter Beweis durch Widerspruch, Kontraposition, Fallunterscheidung, Ringschluss, vollständige Induktion, für Hartgesottene sogar die transfinite Induktion, ... und vieles mehr!

Wenn Sie diese bewährten Techniken kennen, dann fällt Ihnen das Beweisen viel leichter. Das Ziel sind zwei sich ergänzende Fähigkeiten:
Lesen: einen vorgelegten Beweis detailliert nachvollziehen und prüfen.
Schreiben: einen neuen Beweis selbst finden und korrekt ausführen.

Im ersten Semester beginnen Sie dazu mit der **Logik**, aus der Sie alle nötigen Beweismethoden ableiten können. Sie lernen dabei, logisch schlüssig zu argumentieren, Behauptungen und Beweise genau zu formulieren, typische Fehler und Trugschlüsse zu vermeiden.

Wie schreibt man griechische Buchstaben?

Zur Übersicht hier die 24 Buchstaben des griechischen Alphabets:

A	α	Alpha	I	ι	Iota	P	ρ, ϱ	Rho
B	β	Beta	K	κ	Kappa	Σ	σ	Sigma
Γ	γ	Gamma	Λ	λ	Lambda	T	τ	Tau
Δ	δ	Delta	M	μ	Mü	Υ	υ	Ypsilon
E	ε, ϵ	Epsilon	N	ν	Nü	Φ	φ, ϕ	Phi
Z	ζ	Zeta	Ξ	ξ	Xi	X	χ	Chi
H	η	Eta	O	o	Omikron	Ψ	ψ	Psi
Θ	ϑ, θ	Theta	Π	π	Pi	Ω	ω	Omega

Die Variante ε (statt ϵ) unterscheidet sich besser vom Elementzeichen $\in$, ebenso ϑ (statt θ) und φ (statt ϕ) von ihren Großbuchstaben Θ und Φ. Unterscheide ζ und ξ: Wie Z hat ζ zwei Querzüge, wie Ξ hat ξ drei.

Weitere Schriften (wie Skript $\mathscr{A}, \mathscr{B}, \mathscr{C}, \ldots$ oder Fraktur $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$) sind oft nützlich, selten auch weitere Alphabete (wie hebräisch $\aleph, \beth, \gimel, \ldots$).

Wie schreibt man griechische Buchstaben?

Mathematische Notation nutzt über das lateinische Alphabet hinaus auch das griechische. Bitte üben Sie die griechischen Buchstaben, so dass Sie diese fehlerfrei lesen und sauber schreiben können. Das lohnt sich für diese und alle weiteren Vorlesungen!

Übung: Die griechische Bezeichnung für ‘Mathematik’ lautet:

μαθηματική τέχνη

Versuchen Sie dies fehlerfrei zu buchstabieren. Sie können dies sogar laut vorzulesen, wenn Sie die Lautwerte erraten oder nachschlagen.

Übung: Schreiben Sie das griechische Alphabet in Kleinbuchstaben mindestens einmal ab, besser mehrmals für eine fluide Handschrift.

Vielleicht erstaunt es Sie, dass Ihre erste Übung in dieser Vorlesung so etwas banales ist wie das Alphabet abzuschreiben. Es ist wie mit allen handwerklichen Übungen: früher oder später werden sie nötig. *Just do it.* Wann, wenn nicht jetzt? Wo, wenn nicht hier?

Worum geht es in der Mathematik?

Mathematik (gr. μαθηματική τέχνη) ist die ‘Kunst des Erkennens’; sie ist ein systematisch-schöpferischer Prozess zum **Lösen von Problemen**.

Mathematik ist zugleich abstrakte **Theorie** und konkrete **Anwendung**. Diese beiden Pole begründen ihren Reiz, aber auch ihre Schwierigkeit.

Sie ist schön und nützlich, ästhetische Kunst und praktisches Handwerk, rechnen und begründen, kritisch und korrekt, sorgfältig und effizient.

Sie erklärt und quantifiziert Zusammenhänge: Das ist ihr Nutzen! Dank Abstraktion ist sie universell anwendbar: Das ist ihre Stärke!

Mathematik verbindet **Anschauung** und **Formalisierung**:

1. Intuition / Anschauung / Motivation / Ziel: Was wollen wir?
2. Präzision / formale Ausführung / Weg: Wie erreichen wir dies?

Intuition ist hilfreich zur Motivation und wichtig zur Orientierung. Wir benötigen ebenso Präzision, also die detaillierte Ausführung.

C’est par la logique que l’on prouve, et par l’intuition que l’on découvre.
[Mit der Logik beweisen wir, mit der Intuition entdecken wir.]
Henri Poincaré (1854–1912)

Wozu dient die Mathematik?

High Technology is essentially mathematical technology.
Enquete Commission of the American Academy of Science

Verständnis und Beherrschung komplexer Zusammenhänge benötigen neben Empirie auch Theorie, insbesondere quantitative Modelle und sorgfältige Planung. Diese beruhen im Wesentlichen auf Mathematik.

Sie ist die **Sprache** des systematischen logischen Denkens und damit unverzichtbare **Grundlage** für Naturwissenschaft und Technik. Sie ist

- **Werkzeugkasten**, um relevante Probleme eigenständig zu lösen,
- **Wissensgebiet**, allgemeine Kulturtechnik, Schlüsseltechnologie,
- **Wissenschaft**, Ideenschmiede, lebendiges Forschungsgebiet.

Mathematische Methoden sind häufig Voraussetzung für den Erfolg technischer Entwicklungen; das gilt auch, wenn sie beim Endprodukt im Inneren wirken und oberflächlich nicht offen sichtbar sind.

Mathematik ist spannend, herausfordernd, anstrengend doch lohnend. Sie ist eine natürliche menschliche Tätigkeit: Wir folgen unserer Neugier!

Mathematik ist universelle Sprache.

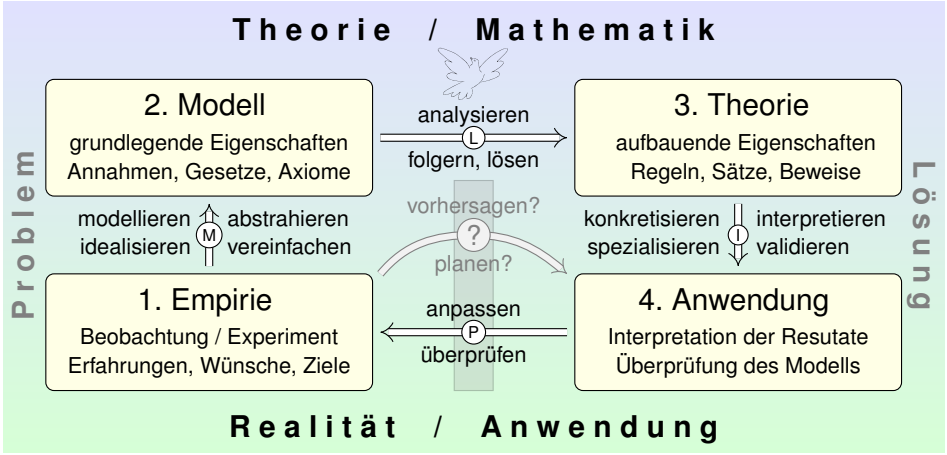
Jahrhunderte naturwissenschaftlicher und technischer Erfahrung lehren uns eindrücklich: **Mathematik ist die Sprache des Universums!**

Wir können diese Sprache verstehen und sprechen lernen.
Wir können sie anwenden und damit gezielt Probleme lösen.
Wie jede Sprache lernt man Mathematik durch Üben! Üben! Üben!

Die Grenzen meiner Sprache bedeuten die Grenzen meiner Welt.
Ludwig Wittgenstein, 1889–1951, *Tractatus Logico-Philosophicus*

Als eindringliches Beispiel unter vielen nenne ich die Elektrodynamik. Faradays empirische Beobachtungen fasste Maxwell 1865 in knappen Formeln zusammen; diese sind elegant und zudem überaus nützlich: Maxwells einheitliche **Theorie** der Elektrodynamik eröffnete auch in der **Praxis** völlig neue Anwendungen. Dank seiner Gleichungen konnte er insbesondere die Möglichkeit elektromagnetischer Wellen vorhersagen. Diese waren 1865 noch unbekannt und experimentell nicht zugänglich; ihr Nachweis gelang Heinrich Hertz erst 1886. Wir nutzen sie bis heute!

Alles Leben ist Problemlösen. (Karl Popper)



Konkrete Anwendung benötigt abstrakte Kenntnisse; je anspruchsvoller, desto mathematischer!
Alles Denken beruht auf Modellen; diese können *deskriptiv* oder *normativ* eingesetzt werden.
Deskriptiv: beschreibend (Kettenlinie), erklärend (Planetenbewegung), vorhersagend (Wetter).
Normativ: vorschreibend (Bauplan), planend (Raumsonde), gesetzgebend (Klimaschutz).
Sie wollen beides. Hierzu benötigen Sie ausreichend starke mathematische Werkzeuge.

Mathematik ist effizientes Werkzeug.

Dieselben mathematischen Strukturen und Techniken treten in immer neuen Zusammenhängen auf, sie beschreiben augenscheinlich völlig unterschiedliche Phänomene und lösen die verschiedensten Probleme.
Der Kontext ändert sich, aber die Rechnung ist immer dieselbe!

Abstraktion ist die Kunst, Wesentliches von Unwesentlichem zu trennen.

Mathematische Modelle haben somit ihre eigenständige Bedeutung und ihre Wichtigkeit, daher lohnt es sich, sie eigenständig und allgemein zu untersuchen. Genau dies wollen wir in dieser Vorlesung tun, damit Sie für alle Fälle gewappnet sind, auch für zukünftige Anwendungen!

The enormous usefulness of mathematics in the natural sciences is something bordering on the mysterious and there is no rational explanation for it. […]
The miracle of the appropriateness of the language of mathematics […]
is a wonderful gift which we neither understand nor deserve. We should be grateful for it and hope that it will remain valid in future research.
(Eugene Wigner, 1902–1995,
The unreasonable effectiveness of mathematics in the natural sciences)

Mathematik ist Schlüsseltechnologie.

Mathematische Modelle und Methoden erlernen Sie zunächst unter vereinfachten *Laborbedingungen*, in kleinem Maßstab, sozusagen unter dem Mikroskop. Unter *Industriebedingungen* ist ihre Vielfalt oft nur mit Computerhilfe voll auszuschöpfen. Umso wichtiger ist es, die Zusammenhänge und Mechanismen grundlegend zu verstehen:
Algorithmen und Programme übersetzen mathematische Modelle!

Meist können Sie nicht in ein laufendes Programm eingreifen, um ad hoc mit „Intuition“, „Anschauung“ oder „gesundem Menschenverstand“ zu korrigieren, was die „dumme Maschine“ alleine nicht richtig macht.
Im Gegenteil müssen Sie vorhersehen, wie ein Verfahren im Detail funktioniert, um korrekte Anweisungen zu formulieren. Hierzu müssen Sie sorgfältig arbeiten, akribisch jeden möglichen Fall berücksichtigen.

Sie müssen dem Computer genau sagen, was er tun soll, oft auch wie. Das Ergebnis müssen Sie kritisch prüfen, verstehen und interpretieren. Die Mathematik stellt hierzu alles Nötige zur Verfügung. — Sie wollen Computer korrekt und effizient nutzen? Dazu brauchen Sie Mathematik!

Worum geht es in der Linearen Algebra?

033
Erläuterung

In der Linearen Algebra geht es zunächst um Zahlen und Vektoren, Matrizen und lineare Abbildungen. Diese Begriffe und die zugehörigen Techniken sind für die gesamte Mathematik grundlegend und werden Ihnen überall nützen, in der Mathematik und ihren Anwendungen.

Aus der Schule können Sie bereits lineare Gleichungssysteme lösen, zunächst mit wenigen Gleichungen und Unbekannten (meist bis drei). Lineare Gleichungssysteme sind überaus nützlich und interessant! Sie sind direkter Zugang und solide Grundlage der Linearen Algebra.

Als erstes werden wir die allgemeine Fragestellung systematisieren und zum Matrixkalkül ausbauen: Was sind Zahlen, vor allem: wie rechnen wir mit ihnen? (Kapitel A: Körper) Wie lösen wir strukturiert und effizient lineare Gleichungssysteme? (Kapitel B: Matrizen)

Auf dieser ganz handwerklichen Grundlage entwickeln wir die Theorie der Vektorräume und der linearen Abbildungen (Kapitel I: lineare Räume, J: Basis und Dimension, K: Matrixdarstellung, L: Determinanten. Daran schließt die Lineare Algebra 2 im Sommersemester an.)

Worum geht es in der Linearen Algebra?

034
Überblick

Bei dieser Entwicklung geht es einerseits um konkretes Rechnen und effiziente Algorithmen, für Sie selbst und für Computer. Darüber hinaus geht es um das Erlernen der zugehörigen Theorie: Die abstrakte Denkweise erweist sich als ebenso wichtig und nützlich!

Mit dem Studium der Mathematik verbinden Sie beides: praktische Anwendungen und theoretische Grundlagen.

Sie wollen hoch hinaus, daher handeln wir mit angemessener Weitsicht: Um Ihrem Vorhaben ein solides Fundament zu sichern, nehmen wir uns von Anfang an die nötige Zeit für die mathematischen Grundlagen. (Kapitel C: Logik und Beweistechniken, D: Mengen und Abbildungen, E: Kombinatorik und Quotienten, F: Ordnungen und Mächtigkeit)

Diese allgemeinen Grundlagen lohnen sich, denn sie klären und ordnen. Diese Werkzeuge der Logik und Mengenlehre bilden die Grundlage für die gesamte Mathematik. Damit ausgerüstet können wir insbesondere unser Programm der Linearen Algebra nun getrost ausführen. (G: Ringe und Körper, anschließend lineare Räume und lineare Abbildungen, etc.)

Worum geht es in der Linearen Algebra?

035
Überblick

Solide Fundamente: Ein hoher Turm braucht eine breite Basis!

Worum geht es in der Linearen Algebra?

036
Überblick

Die Abstraktion ist wesentlich für das mathematische Arbeiten: Wir wollen Gemeinsamkeiten erkennen und zusammenfassen, über Fallbeispiele hinaus wollen wir ein kohärentes Gesamtbild. Erst die abstrakte Theorie öffnet den Weg zu neuen Anwendungen!

Diese Abstraktion bereitet erfahrungsgemäß gerade in den ersten Semestern große Schwierigkeiten. Als langfristige Investition kostet sie am Anfang viel Kraft und Durchhaltewillen, doch sie zahlt sich aus: Ihre Vorbereitung von heute ist Ihr Nutzen von morgen!

Haben Sie also die nötige Geduld mit sich und der Mathematik. Das Studium fördert Beharrlichkeit und Frustrationstoleranz. Sie werden schrittweise immer mehr sehen und verstehen: Die Mathematik ist wunderschön und nützlich. Bleiben Sie dran!

Dazu bieten wir Ihnen Hilfestellungen und einen schrittweisen Aufbau: Der Stoff wird hier vollständig für Sie entwickelt. Ganz wichtig ist daher die lückenlose Teilnahme an der Vorlesung und die ausdauernde Bearbeitung der Übungen: Arbeiten Sie mit, fragen Sie nach!

Ziele und Inhalte der Linearen Algebra

Die Lineare Algebra gehört zum Beginn der Mathematikstudiums wie das Erlernen der Buchstaben zum Anfang der Grundschule.

Sie behandelt das bewährte Kernprogramm klassischer Themen, die im ersten Jahr jedes Mathematikstudiums erworben werden müssen und die Grundlage für alles Weitere bilden.

- Aufbau des Zahlensystems und Matrizenkalkül
- Mathematische Logik und Beweistechniken
- Mengen, Relationen und Abbildungen
- Monoide und Gruppen, Ringe und Körper
- Vektorräume und lineare Abbildungen
- Determinanten und Eigenwerte
- Diagonalisierung und Jordanisierung
- Bilineare Algebra und euklidische Geometrie

Ich beginne mit dem Aufbau des Zahlensystems und Matrizenrechnung. Wir haben noch nicht alle Hilfsmittel (Logik, Mengen, Abbildungen, etc.), doch gewinnen schon reichlich Erfahrung, Anschauung und Motivation.

Das Ziel und der Weg

Mathematik ist schön und nützlich, zwar anstrengend doch lohnend!

Five percent of the people think; ten percent of the people think they think; and the other eighty-five percent would rather die than think.“
Thomas A. Edison (1847–1931)

„Because in the end, you won’t remember the time you spent working in the office or mowing your lawn. Climb that goddamn mountain!“
Jack Kerouac (1922–1969)

Das Ziel und der Weg

Vor uns liegt ein langer Weg, manchmal steinig und steil, doch überall voller nützlicher Erkenntnisse, tiefer Einsichten und schöner Ausblicke. Ich erkläre Ihnen einmal alles Nötige, freundlich und gründlich. Danach sind Sie dran, den Stoff nachzuarbeiten und die Techniken einzuüben.

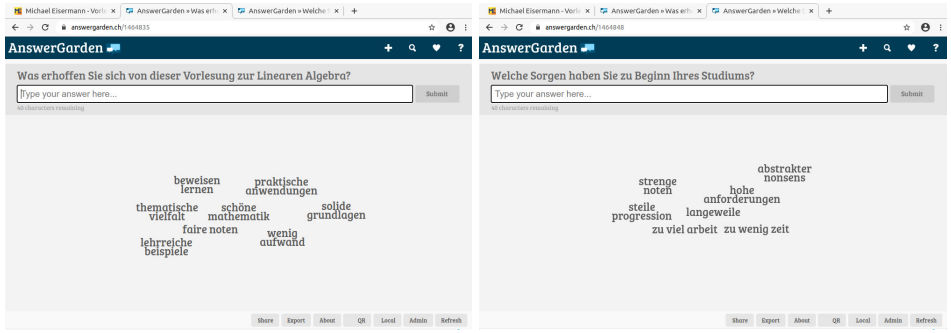
Die Vorlesung ist voll gepackt mit schöner und nützlicher Mathematik: Sie müssen voll konzentriert und fokussiert mitarbeiten. Dann haben Sie schon mal die Ideen verstanden. Für das Verständnis im Detail müssen Sie die Themen anschließend selbständig und gründlich durcharbeiten.

Dabei unterstützen wir Sie umfassend mit wöchentlichen Quizzen, gut abgestimmten Übungsaufgaben, Übungsgruppen und Vortragsübung. Das Café Matrice, Forum und Umfrage runden das Gesamtpaket ab. Wir sind für Sie da und freuen uns über Ihr Engagement.

Unser Vorhaben gleicht einer ambitionierten Wanderung:
Jeder einzelne Schritt ist leicht, doch sehr viele sind nötig.
Es ist Ihr Studium, engagieren Sie sich, bleiben Sie dran!

Was sind Ihre Erwartungen?

Was erhoffen Sie sich von dieser Vorlesung zur Linearen Algebra?
Welche Sorgen haben Sie zu Beginn Ihres Studiums?



Siehe Ilias, verlinkt zu `answergarden.ch/1464835` und `1464848`.
Wir laden Sie ein zum Austausch über Mathematik und drumherum!

Mathematik und Schule

Manche/r Lehramtsstudierende beklagt und behauptet:
„Die Mathematik an der Uni ist nicht relevant für die Schule.“
Das ist ein oft wiederholter und schwerwiegender Vorwurf.
Ich nehme die Klage ernst und muss dazu einiges klarstellen:

1. Verstehen Sie Ihr Mathematikstudium richtig?
2. Verstehen Sie wirklich die Schulmathematik?
3. Warum ist Ihr Mathematikstudium relevant?
4. Was brauchen Sie als zukünftige/r Lehrer/in?

Das sind wichtige Fragen, und hierzu gibt es klare Antworten!
Allzu viele Studierende verrennen sich in unrealistische Vorstellungen, entfremden sich von ihrem Studium und blockieren sich damit selbst.
Ich möchte Ihnen helfen und Sie vor den typischen Fehlern bewahren.

(Meine nachfolgenden Erläuterungen sind wie immer gänzlich unnütz:
Wer sie liest, ist wohl nicht betroffen. Wer betroffen ist, liest sie nicht.
Engagierte Hochschullehrer/innen sind verflucht wie einst Kassandra, die das drohende Unheil zwar voraussieht, aber kein Gehör findet.)

Mathematik und Schule

1. Es ist richtig und wichtig, die Anliegen der Studierenden zu verstehen, konstruktiv über das Studium zu diskutieren und Inhalte zu entwickeln.
Andererseits sind „die Studierenden“ gerade im Lehramt eine reichlich heterogene Gruppe, mit unterschiedlichen Ansichten und Bedürfnissen:

Manche studieren Mathematik aus ehrlichem Interesse, persönlicher Neigung, gar Leidenschaft, andere aus Not und irregeleitetem Kalkül.
Letztere folgen keiner Berufung, suchen weder Wissen noch Können, sondern einen sicheren und vermeintlich ruhigen Job. Und scheitern!

Der pauschale Vorwurf der Irrelevanz wird oft erhoben von Studierenden, die ihr Fach eigentlich kaum kennen und daher nicht wirklich verstehen, daher ist ihr Urteil wenig aussagekräftig. Das gilt auch und gerade in der Mathematik, findet sich aber ebenso in vielen anderen Studiengängen.

Pauschale Vorwürfe entspringen daher meist nicht der kritischen Auseinandersetzung mit dem Studium, sondern der Flucht davor.
Sie sind keine Aussage über die Studieninhalte, sondern Ausdruck der eigenen Hilflosigkeit und Überforderung. Das ist hart, aber ehrlich.

Mathematik und Schule

2. Zu den Bildungszielen der Universität gehören wissenschaftliche Neugier und Sorgfalt sowie intellektuelle Offenheit und Ehrlichkeit.
Leider fördert unser Schulsystem oft nicht Neugier und Lernfreude, sondern erzwingt Auswendiglernen und Nachbeten. Das ist fatal.

Wer mit solch falsch geprägten Vorstellungen an die Universität kommt, wird zurecht gründlich enttäuscht. In der Wissenschaft, insbesondere der Mathematik, geht es nicht nur ums Auswendiglernen, sondern vielmehr ums Verstehen, nicht um Nachbeten, sondern um eigenes Denken.

Wenn Sie also glauben „Die Uni macht die Lehrerausbildung falsch.“, dann sollten Sie sich zuerst fragen: „Verstehe ich die Schule richtig?“
Sie sollten sich klar werden, was die Schule soll und was ein/e Lehrer/in dazu braucht. Daraus folgen die Ansprüche an das Lehramtsstudium.

Wenn Ihre Wünsche und Vorstellungen unvereinbar bleiben mit den Angeboten und Anforderungen Ihrer Studienwahl, dann werden Sie an Ihrem Studium leiden und letztlich scheitern. Bringen Sie daher beides schnell in Einklang: Ändern Sie Ihre Einstellung oder Ihr Studienfach!

Mathematik und Schule

Schule und Universität handeln zwar auf verschiedenen Ebenen, doch sie verfolgen grundsätzlich dieselben, gemeinsamen Lernziele!

So wie in der Schule ist auf höherem Niveau auch im Studium Ihr Ziel, Mathematik zu verstehen und die behandelten Methoden selbstständig, sicher, kritisch, korrekt und kreativ anzuwenden. Das heißt ausführlich:

- **Selbstständig:** Es geht nicht nur um Auswendiglernen, sondern um Verstehen und unabhängige Urteilsfähigkeit.
- **Sicher:** Es geht nicht nur um Intuition oder Spekulieren, sondern um nachvollziehbare Argumente und Rechnungen.
- **Kritisch:** Es geht nicht nur um Glauben oder (Auto)Suggestion, sondern um (selbst)kritische Fragen und sorgfältige Antworten.
- **Korrekt:** Sie beherrschen Definitionen, Sätze, Methoden, Proben. Gegenbeispiele zeigen Fehlerquellen, die es zu vermeiden gilt.
- **Kreativ:** Es geht nicht nur um fertige Rezepte, sondern um eigenständige Anwendung.

Mathematik und Schule

3. Ich bin zutiefst überzeugt: Die Mathematik, wie Sie sie bei uns an der Universität lernen, ist absolut relevant für Sie als zukünftige/r Lehrer/in! (Über die Dosierung einzelner Themen können wir gerne diskutieren, wenn Sie wollen auch streiten, doch am Grundsatz besteht kein Zweifel.)

Mathematische Erkenntnis kommt nicht durch Propheten vom Berg, sondern sie wird erklärt und begründet, erarbeitet und gepflegt.
Sie ist keine Sammlung einzelner zusammenhangloser Fakten, sondern ein kohärentes Gebäude von Ideen und Methoden.

Genau diese logischen Zusammenhänge lernen Sie im Studium!
Hier verstehen Sie, wie Sie Mathematik aufbauen, Erkenntnisse finden, präzise formulieren und sorgsam begründen. Das nützt ein Leben lang, insbesondere als Lehrer/in bei der Strukturierung und Vermittlung.

Wenn Sie immer noch glauben, stupides Auswendiglernen genügt, dann bedeutet das nur, dass die Schule es falsch gemacht hat und Ihre Sichtweise völlig falsch geprägt wurde. Nochmal, bringen Sie beides in Einklang: Ändern Sie Ihre Einstellung oder Ihr Studienfach!

Mathematik und Schule

Zur Illustration nenne ich einige einfache, aber grundlegende Fragen. Sie stellen sich bereits in der Schule, und zwar ganz konkret und dringend, doch meist werden sie erfolgreich verdrängt. Das ist fatal, denn so gewöhnen sich Schüler/innen ans Glauben statt ans Fragen!

Was sind natürliche, ganze, rationale, reelle (und komplexe) Zahlen? Welche Rechenregeln gelten, welche nicht? Woher kommen diese Regeln? Was ist Definition, was ist Folgerung? Wie erkennen wir wahr und falsch? Was ist der Nenner von $\frac{4}{6}$? Warum ist $0.99999\ldots$ gleich 1?

Wie löst man Gleichungen? Wie nutzt man Äquivalenzumformungen? Wie prüft man eine vermeintliche Lösung? Was ist die Lösungsmenge? Wie garantiert man ihre Vollständigkeit? Was bedeuten Existenz und Eindeutigkeit? Wie lässt sich die Folge $1, 2, 4, 8, 16, 32$ fortsetzen?

Was ist eine Funktion? Warum ist der Definitionsbereich so wichtig? Was ist die Zielmenge? Wie beschreiben wir die Zuordnung $f : x \mapsto y$? Wann erlaubt die Gleichung $f(x) = y$ eine Lösung? mindestens eine? höchstens eine? Wie lösen wir lineare Gleichungssysteme $Ax = y$?

Mathematik und Schule

4. Hoffentlich hatten Sie in Ihrer Schulzeit das Glück, begeisternde Lehrer/innen und guten Unterricht kennen zu lernen, auch und gerade in Mathematik. Vermutlich haben Sie davon profitiert, und vielleicht hat dies Ihre Entscheidung geformt, nun selbst Mathematik zu studieren.

Vermutlich kennen Sie auch Gegenbeispiele, sicherlich haben Sie sich geärgert über manch uninspirierte Lehrer/innen, die weder anschaulich motivieren noch präzise erklären, weder begeistern noch vermitteln, und die insgesamt mehr verwirren als helfen. Leider gibt es auch das.

Das drängt uns die Frage auf: Warum gibt es schlechte Lehrer/innen? Wenn das Studium so irrelevant ist, wie behauptet, dann sollte doch das Verstehen und das Vermitteln ohne langwierige Mühen möglich sein. So leicht ist es aber nicht! Das Studium wirkt. Langsam aber sicher.

Provokant gesagt: Wenn Sie ein/e schlechte/r Lehrer/in werden wollen, dann ist das Mathematikstudium für Sie wohl tatsächlich irrelevant. Wir wollen jedoch dafür sorgen, dass Sie es wesentlich besser machen! Hierzu legt Ihr Studium die fachlich-didaktischen Grundlagen.

Mathematik und Schule

Zu Ihrem Erfolg als Lehrer/in tragen mehrere Faktoren bei:

1. Inhalte erfordern umfassendes und sicheres Fachwissen:
   Nur wer sein Fach wirklich versteht, kann es gut vermitteln.
2. Vermittlung benötigt umfassende didaktische Fähigkeiten:
   Kommunikation, Verständnis, Aktivierung sind die Schlüssel.
3. Ebenso hilfreich sind eine wirksame Lehrpersönlichkeit, interessierte Schüler/innen, ein konstruktives Kollegium, ein positives Umfeld, etc.

Diese Faktoren interagieren miteinander auf höchst komplexe Weise. Klar ist, dass Sie alle drei benötigen werden, auch wenn das genaue Verhältnis schwer zu präzisieren ist und sicherlich nicht für alle gleich. Das ist genau die Schwierigkeit: Keiner dieser drei Faktoren darf fehlen!

Als Lehrer/in wird man nicht geboren, es ist ein Beruf, den man erlernen muss und kann! In Ihrem Studium erwerben Sie dazu zunächst und vor allem (1) mathematische Inhalte und (2) didaktische Grundlagen, später komplettieren Sie diese durch Referendariat und Berufserfahrung.

Der Weg ist lang, doch das Ziel ist hehr!

Legende / Leseanleitung: Folien zur Linearen Algebra

Vortrag und Skript haben verschiedene Ziele und ergänzen sich:
Der Vortrag gibt einen Überblick, das Skript dient zur Vertiefung.
Die Vortragsfolien sind durch blaue Titelbalken leicht zu erkennen;
dies kennzeichnet die Folien, die in der Vorlesung behandelt werden.

Ich möchte Vortrag und Skript synchron halten, soweit dies möglich ist.
Die Nummerierung der Folien, Abschnitte, Definitionen, Sätze usw.
ist daher dieselbe, auch wenn dadurch im Video der Zähler springt.
Der Übergang zwischen Vortrag und Skript wird dadurch nahtlos.

Aufbau der Vorlesung

Ich präsentiere hier Ideen, Techniken und Anwendungen, Definitionen und Sätze, Aufgaben und Lösungen. Dabei versuche ich, jedes Thema so einfach wie möglich darzustellen, doch so präzise und ausführlich wie es für ein solides Verständnis nötig ist. Möge es nützen!

Wir beginnen diese Vorlesung mit zwei Kapiteln zur Vorschau; diese geben einen Einblick in zentrale Themen der Linearen Algebra und dienen somit zur frühen Orientierung, als Ausblick und Motivation. Diese Versprechen werde ich in den nächsten Wochen einlösen.

Kapitel A: Aufbau des Zahlensystems

A1 Natürliche, ganze und rationale Zahlen
- A1.1 Was sind und was sollen die Zahlen?
- A1.2 Der Halbring $(\mathbb{N}, +, \cdot)$ der natürlichen Zahlen
- A1.3 Der Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen
- A1.4 Der Körper $(\mathbb{Q}, +, \cdot)$ der rationalen Zahlen
- A1.5 Die Körpererweiterungen $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{Q}[\mathrm{i}]$
- A1.6 Der Ring $K[X]$ der Polynome über K

A2 Arithmetik in $\mathbb{Z}$ und der Restklassenring $\mathbb{Z}_n$
- A2.1 Division mit Rest und euklidischer Algorithmus
- A2.2 Der Fundamentalsatz der Arithmetik
- A2.3 Der Restklassenring $(\mathbb{Z}_n, +_n, \cdot_n)$

A3 Reelle und komplexe Zahlen
- A3.1 Der Körper $(\mathbb{R}, +, \cdot)$ der reellen Zahlen
- A3.2 Der Körper $(\mathbb{C}, +, \cdot)$ der komplexen Zahlen
- A3.3 Der Schiefkörper $(\mathbb{H}, +, \cdot)$ der Quaternionen

Kapitel B: Matrixkalkül und Gauß–Algorithmus

B1 Der Matrixkalkül
- B1.1 Vom Gleichungssystem zur Matrix
- B1.2 Matrixaddition und Skalarmultiplikation
- B1.3 Multiplikation von Matrizen passender Größe
- B1.4 Invertierbare Matrizen und ihre Inversen
- B1.5 Inversion im Ring der 2×2–Matrizen
- B1.6 Komplexe Zahlen und Quaternionen als Matrizen

B2 Der Gauß–Algorithmus
- B2.1 Zeilenstufenform
- B2.2 Der Gauß–Algorithmus
- B2.3 Zeilenoperation als Matrixmultiplikation
- B2.4 Invertierbarkeitskriterien für Matrizen

B3 Erste Anwendungen: drei schöne Beispiele
- B3.1 Es werde Licht! . . . mit Linearer Algebra
- B3.2 Lagrange–Interpolation und Vandermonde–Matrix
- B3.3 Zufällige Irrfahrt und harmonische Gewinnerwartung

Kapitel C: Mathematische Logik und Beweistechniken

C1 Aussagenlogik
- C1.1 Aussagen und Wahrheitswerte
- C1.2 Aussagenlogische Formeln und Tautologien
- C1.3 Nützliche Rechenregeln der Aussagenlogik
- C1.4 Aussagenlogische Formeln und Junktoren

C2 Schlussregeln und Beweisverfahren
- C2.1 Schnittregel, Kettenschluss, Fallunterscheidung
- C2.2 Kontraposition und Beweis durch Widerspruch

C3 Prädikate und Quantoren
- C3.1 Rechenregeln für Existenz- und Allquantor
- C3.2 Existenz und Eindeutigkeit

C4 Induktion: the road to infinity!
- C4.1 Das Prinzip der vollständigen Induktion
- C4.2 Starke Induktion als nützliche Variante

Kapitel D: Mengen, Abbildungen und Relationen

D1 Die Sprache der Mengen
- D1.1 Elemente, Teilmengen und Potenzmenge
- D1.2 Aussonderung und Ersetzungsmenge
- D1.3 Schnittmenge und Vereinigungsmenge
- D1.4 Zerlegungen und Repräsentantensysteme
- D1.5 Tupel und kartesische Produktmenge

D2 Relationen und Abbildungen
- D2.1 Motivation und erste Beispiele
- D2.2 Relationen und Abbildungen
- D2.3 Bildmenge und Urbildmenge

D3 Invertierbarkeit von Abbildungen
- D3.1 Komposition und Einschränkung
- D3.2 Invertierbarkeit von Abbildungen
- D3.3 Beispiele und erste Anwendungen

Kapitel E: Kombinatorik und Quotienten

E1 Endliche Mengen und Elementezahl
- E1.1 Permutationen und Zykelzerlegung
- E1.2 Der Zählsatz: Wie messen wir Mengen?
- E1.3 Invarianzsatz und Dirichlets Schubfachprinzip

E2 Kombinatorische Abzählformeln
- E2.1 Grundrechenarten für endliche Mengen
- E2.2 Teilmengen und Binomialkoeffizienten
- E2.3 Zerlegungen und Stirling–Zahlen

E3 Zerlegungen, Äquivalenzrelationen und Quotienten
- E3.1 Zerlegung und Quotient, die Klassengleichung
- E3.2 Äquivalenzrelationen und Faktorisierung
- E3.3 Konstruktion der rationalen Zahlen $\mathbb{Q}$
- E3.4 Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Kapitel F: Ordnungsrelationen und Mächtigkeit

F1 Ordnungsrelationen
- F1.1 Grundbegriffe zu Ordnungsrelationen
- F1.2 Kleine Beispiele, Warnung vor Intransitivität
- F1.3 Kleinstes / größtes Element versus Minima / Maxima
- F1.4 Infimum und Supremum, untere und obere Grenze
- F1.5 Monotone Abbildungen und Isomorphismen
- F1.6 Wohlordnungssatz und Lemma von Zorn

F2 Die Mächtigkeit von Mengen
- F2.1 Dedekinds Rekursionssatz, un/endliche Mengen
- F2.2 Die Mächtigkeit von Mengen, erste Beispiele
- F2.3 Abzählbare Vereinigungen, Hilberts Hotel
- F2.4 Der Äquivalenzsatz von Cantor–Bernstein
- F2.5 Die Mächtigkeit der reellen Zahlen

Kapitel G: Ringe und Körper

G1 Monoide und Gruppen
- G1.1 Verknüpfungen
- G1.2 Monoide und Gruppen
- G1.3 Lösung von Gleichungen
- G1.4 Untergruppen und -monoide
- G1.5 Homomorphismen
- G1.6 Erzeugte Untergruppen
- G1.7 Kartesische Produkte

G2 Ringe und Körper
- G2.1 Definition und erste Rechenregeln
- G2.2 Homomorphismen und Unterringe
- G2.3 Matrixringe und Funktionenringe

G3 Polynomringe
- G3.1 Definition und erste Rechenregeln
- G3.2 Die universelle Abbildungseigenschaft
- G3.3 Euklidische Division und Nullstellen von Polynomen
- G3.4 Arithmetik in $\mathbb{Z}$ und $K[X]$ und euklidischen Ringen

Kapitel H: Halbzeit

H1 Halbzeit geschafft.

H2 Frohe Weihnachten!

Kapitel I: Lineare Räume und lineare Abbildungen

I1 Grundbegriffe
- I1.1 Lineare Räume
- I1.2 Lineare Abbildungen
- I1.3 Lineare Räume über $\mathbb{Z}$, $\mathbb{Z}/p$ und $\mathbb{Q}$
- I1.4 Lineare Unterräume
- I1.5 Bild und Kern einer linearen Abbildung
- I1.6 Beispiele aus der Analysis
- I1.7 Erzeugte Unterräume

I2 Universelle Werkzeuge
- I2.1 Quotientenraum und kanonische Faktorisierung
- I2.2 Korrespondenzsatz und Isomorphiesatz
- I2.3 Exakte Sequenzen, Anwendungsbeispiele
- I2.4 Direkte Summen, extern und intern

Kapitel J: Basis und Dimension

J1 Basis und Dimension
- J1.1 Basis, erzeugend und linear unabhängig
- J1.2 Anwendung des Gauß–Algorithmus
- J1.3 Invarianz der Dimension über Divisionsringen
- J1.4 Bild und Kern und Dimensionsformel

J2 Konstruktion von Basen
- J2.1 Existenz von Basen
- J2.2 Erste Anwendungen
- J2.3 Exakte Sequenzen

J3 Aufgaben und Ergänzungen

Kapitel K: Darstellung linearer Abbildungen durch Matrizen

K1 Lineare Abbildungen und Matrizen
- K1.1 Das Prinzip der linearen Fortsetzung
- K1.2 Darstellung linearer Abbildungen durch Matrizen
- K1.3 Anwendungsbeispiel: Ableitung von Polynomen
- K1.4 Anwendungsbeispiel: Ableitung von $\cos, \sin, \exp$
- K1.5 Verträglichkeit mit Addition und Komposition

K2 Kanonische Darstellung und Basiswechsel
- K2.1 Kanonische Darstellung einer linearen Abbildung
- K2.2 Matrixdualität: Zeilenrang gleich Spaltenrang
- K2.3 Basiswechsel und Koordinatentransformation
- K2.4 Anwendungsbeispiele, erste Diagonalisierungen

K3 Aufgaben und Ergänzungen

Kapitel L: Signatur und Determinante

L1 Die Signatur
- L1.1 Permutationen, Inversionen und Parität
- L1.2 Die Signatur einer Selbstabbildung
- L1.3 Die alternierende Gruppe

L2 Die Determinante
- L2.1 Geometrische Motivation als orientiertes Volumen
- L2.2 Die drei Axiome: multilinear, alternierend, normiert
- L2.3 Der Hauptsatz zu Determinanten und erste Beispiele
- L2.4 Existenz und Eindeutigkeit und Multiplikativität
- L2.5 Cramersche Regel, Adjunkte und Inverse
- L2.6 Effiziente Berechnung der Determinante
- L2.7 Die rekursive Laplace–Entwicklung

L3 Erste Anwendungen
- L3.1 Invarianz der Dimension über kommutativen Ringen
- L3.2 Die Determinante eines Endomorphismus
- L3.3 Die spezielle lineare Gruppe
- L3.4 Volumen und Orientierung

Kapitel M: Eigenvektoren und Diagonalisierung

M1 Einführung und Grundbegriffe
- M1.1 Kanonische Darstellung eines Homomorphismus
- M1.2 Diagonalisierung eines Endomorphismus
- M1.3 Eigenwerte, Eigenräume, Eigenvektoren, Eigenbasen
- M1.4 Erste Beispiele zur Eigenraumzerlegung

M2 Determinante und charakteristisches Polynom
- M2.1 Das charakteristische Polynom einer Matrix
- M2.2 Eigenschaften des charakteristischen Polynoms
- M2.3 Das Standardverfahren zur Diagonalisierung
- M2.4 Anwendung auf Rekursionsgleichungen

M3 Trigonalisierung und Diagonalisierung
- M3.1 Trigonalisierung eines Endomorphismus
- M3.2 Lokales Minimalpolynom und Cayley–Hamilton
- M3.3 Minimalpolynom und charakteristisches Polynom
- M3.4 Äquivalente Kriterien zur Diagonalisierung

M4 Anwendungsbeispiele und Übungen

Kapitel N: Hauptvektoren und Jordanisierung

N1 Hauptvektoren und Jordanisierung
- N1.1 Die Jordan–Normalform: Existenz und Eindeutigkeit
- N1.2 Erste Beispiele und Anwendungen
- N1.3 Beweis des Satzes von Jordan

N2 Differenzengleichungen und Differentialgleichungen
- N2.1 Diskrete Ableitung und Verschiebeoperator
- N2.2 Ableitung und lineare Differentialgleichungen
- N2.3 Inhomogene lineare Differentialgleichungen
- N2.4 Freie und erzwungene harmonische Schwingung

N3 Lineare Differentialgleichungssysteme
- N3.1 Gekoppelte Oszillatoren und Eigenfrequenzen
- N3.2 Matrix-Exponentialfunktion und Jordanisierung
- N3.3 Linearisierung um Fixpunkte und In/Stabilität

Kapitel O: Bilinearformen und Quadriken

O1 Bilinearformen und darstellende Matrizen

O2 Diagonalisierung symmetrischer Bilinearformen
- O2.1 Zusammenfassung zur Klassifikation

O3 Quadriken und ihre affine Klassifikation
- O3.1 Zusammenfassung zur Klassifikation

Kapitel P: Vektorräume mit Skalarprodukt

P1 Skalarprodukte
- P1.1 Skalarprodukte über $\mathbb{R}$, euklidische Vektorräume
- P1.2 Skalarprodukte über $\mathbb{C}$, unitäre Vektorräume
- P1.3 Erste Anwendungen, von Pythagoras zu Fourier

P2 Orthonormalisierung
- P2.1 Gram–Schmidt–Verfahren und QR–Zerlegung
- P2.2 Bestapproximation und Methode der kleinsten Quadrate
- P2.3 Näherungslösung eines überbestimmten Gleichungssystems

P3 Orthogonale und unitäre Endomorphismen
- P3.1 Orthogonale und unitäre Endomorphismen
- P3.2 Orthogonale und unitäre Gruppen
- P3.3 Geometrie des dreidimensionalen Raumes

Kapitel Q: Spektralsatz und Anwendungen

Kapitel R: Linearformen und Dualität

R1 Dualräume
- R1.1 Der Dualraum V^* zu V
- R1.2 Duale Familien in V^* und V
- R1.3 Die duale Familie $(b_i^*)_{i\in I}$ einer Basis $(b_i)_{i\in I}$
- R1.4 Der natürliche Homomorphismus von V zum Bidual V^{**}

R2 Dualität und Bilinearformen
- R2.1 Der Annulator $X^\circ \leq V^*$ einer Teilmenge $X \subseteq V$
- R2.2 Bilinearformen und Dualität
- R2.3 Normen und Dualität

R3 Duale Homomorphismen
- R3.1 Der duale Homomorphismus $f^* : V^* \to U^*$ zu $f : U \to V$
- R3.2 Matrizen und duale Abbildungen $f : v \mapsto Av$ und $f^* : u \mapsto uA$
- R3.3 Bild und Kern und exakte Sequenzen

Kapitel S: Tensorprodukt

Kapitel A

Aufbau des Zahlensystems

Mathematics teaches us not so much
what to think, but how to think!

(anonyme Weisheit)

Inhalt dieses Kapitels A

Ein einführendes Beispiel

Aufgabe: (Tomatensalat, Aufgabe für Klasse 5, DIE ZEIT 15.10.2020)

Eine Gemüsehändlerin kauft im Großmarkt $150\mathrm{kg}$ *Tomaten für* $2€/\mathrm{kg}$. *In ihrem Laden verkauft sie Packungen zu* $500\mathrm{g}$, *am ersten Tag für* $2€$, *am zweiten Tag für* $1.60€$. *(a) Übrig bleiben* $12\mathrm{kg}$. *Wie viele Packungen hat die Händlerin verkauft? (b) Die Händlerin macht* $220€$ *Gewinn. Wie viele Packungen hat sie zu* $2€$ *verkauft, wie viele zu* $1.60€$*?*

Wie gehen Sie diese Frage an? Wie formulieren Sie Ihren Lösungsweg? Es gibt viele kreative Lösungsmöglichkeiten, probieren Sie es selbst! Mögliche Werte x, y raten und prüfen? als Schleife programmieren? Graphisch als Schnittpunkt von zwei Geraden in der x–y–Ebene?

Eine bewährte, universelle Methode sind lineare Gleichungssysteme:

$$\begin{cases} 0.5x & + & 0.5y & = & 138 \\ 2.0x & + & 1.6y & = & 520 \end{cases}$$

🙂 Mit einer guten Methode gelingt die Rechnung leicht und routiniert. Mathematische Abstraktion hilft, strukturiert und vereinfacht!

Ein einführendes Beispiel

Lösung mit einem allgemeinen Verfahren: der Gauß–Algorithmus!

$$\begin{cases} 0.5x & + & 0.5y & = & 138 \\ 2.0x & + & 1.6y & = & 520 \end{cases}$$

Zeilenoperation $R_1 \leftarrow 2R_1$, multipliziere Zeile 1 mit dem Faktor 2.

$$\begin{cases} x & + & y & = & 276 \\ 2.0x & + & 1.6y & = & 520 \end{cases}$$

Zeilenoperation $R_2 \leftarrow R_2 - 2R_1$, addiere (-2) mal Zeile 1 zu Zeile 2:

$$\begin{cases} x & + & y & = & 276 \\ & - & 0.4y & = & -32 \end{cases}$$

Zeilenoperation $R_2 \leftarrow (-0.4)^{-1}R_2$, multipliziere Zeile 2 mit -2.5.

$$\begin{cases} x & + & y & = & 276 \\ & & y & = & 80 \end{cases}$$

Zeilenoperation $R_1 \leftarrow R_1 - R_2$, addiere (-1) mal Zeile 2 zu Zeile 1:

$$\begin{cases} x & & & = & 196 \\ & & y & = & 80 \end{cases}$$

Motivation und Vorgehensweise

Wir wollen lineare Gleichungssysteme in voller Allgemeinheit verstehen, mit beliebigen, endlichen Anzahlen von Unbekannten und Gleichungen. Das ist der algebraische Ursprung der Linearen Algebra, zusammen mit der analytischen Geometrie: Wir rechnen systematisch in Koordinaten!

Dazu gehören zunächst die folgenden grundlegenden Fragen:

0. Wo liegen die Koeffizienten? Wo suchen wir die Lösungen?
   Welche arithmetischen Operationen stehen uns zur Verfügung?
1. Was genau ist ein lineares Gleichungssystem, ganz allgemein?
   Wie können wir es präzise definieren und effizient codieren?
2. Wie können wir systematisch alle Lösungen berechnen?
   Wie aufwändig ist diese algorithmische Berechnung?
3. Wie viele Lösungen gibt es? Welche Kriterien helfen uns hier?
   Gibt es mindestens eine Lösung? Gibt es höchstens eine Lösung?

Die Fragen 1,2,3 klären wir detailliert im nächsten Kapitel B.
In diesem ersten Kapitel A werden wir zunächst Frage 0 klären...

Motivation und Vorgehensweise

In praktischen Anwendungen sind Gleichungssysteme oft sehr groß.
Wir müssen dabei den Überblick behalten und systematisch vorgehen.

Es lohnt sich, Mathematik zu verstehen, statt planlos herumzurechnen.
Theoretische Grundlagen bereiten den Weg zur effizienten Anwendung.

Die nötigen Begriffe und Methoden werden uns schnell in luftige Höhen führen. Abstraktion ist hilfreich und effizient, gute Beispiele aber auch!

Aus der Erfahrung zahlreicher Beispiele wie dem obigen wissen wir:
Zur Formulierung eines linearen Gleichungssystems benötigen wir Addition und Multiplikation, zur Lösung zudem Subtraktion und Division.

Grundlage der Linearen Algebra sind daher die vier Grundrechenarten:
Addition $(a,b) \mapsto a+b$ und Multiplikation $(a,b) \mapsto a \cdot b$, sowie ihre Umkehrungen Negation $a \mapsto -a$ und Inversion $a \mapsto a^{-1}$.

Wir wollen daher zuerst diese vier Grundrechenarten klären!
Die mathematischen Begriffe hierzu sind **Ringe und Körper**.

Motivation und Vorgehensweise

Wir haben einen gemeinsamen Weg vor uns, steil doch wunderschön.
Bitte haben Sie Geduld (mit sich & uns) und Vertrauen (in uns & sich)!

Geben Sie sich zu Beginn Ihres Studiums eine faire Chance auf Erfolg:
kooperativ und kommunikativ, offen und neugierig, ehrlich und fleißig.

Es ist wie in der Grundschule, als Sie Lesen und Schreiben lernten.
Auch das benötigt Geduld und Vertrauen. Und nützt ein Leben lang!

☹ *„Bevor ich meine Zeit mit diesem sogenannten A verschwende, will ich erst mal wissen, wozu dieses A überall gebraucht wird!“*

☹ *„Dieses A ist nur ein theoretisches Detail für Spezialisten, in der Wirklichkeit da draußen benötigt das niemand.“*

Über das Lesen und Schreiben und seinen Nutzen hört man das selten, über das Mathematik-Lernen hingegen allzu oft. Das ist nicht recht.

☺ Widerstehen Sie engstirniger Ungeduld und ignoranten Vorurteilen.
Pflegen Sie Ihre angeborene Neugier und Ihre Freude am Lernen!

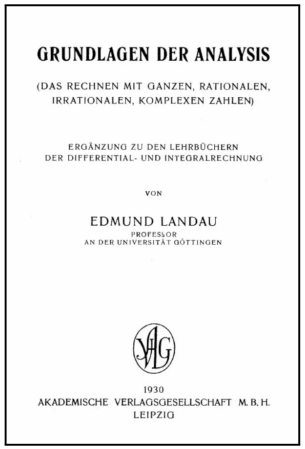
Motivation und Vorgehensweise

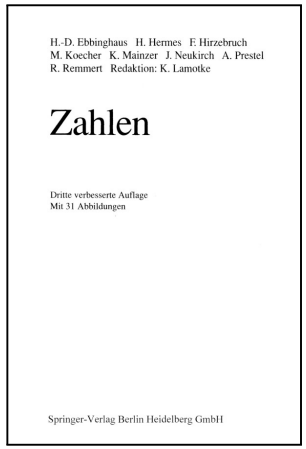
Wenn du ein Schiff bauen willst,
lehre deine Leute nicht nur ihr Handwerk,
sondern erwecke ihre Sehnsucht nach dem Meer!

Was sind und was sollen die Zahlen?

A101

Seit Urzeiten nutzen Menschen Zahlen und entwickeln das Rechnen.
Doch was genau sind Zahlen? Und woher kommen die Rechenregeln?





Bitte vergiss alles, was Du auf der Schule gelernt hast; denn Du hast es nicht gelernt. Bitte denke bei allem an die entsprechenden Stellen des Schulpensums; denn Du hast es doch nicht vergessen. (Landau, Vorwort für den Lernenden)

Was sind und was sollen die Zahlen?

A102
Erläuterung

Solide Grundlagen. Allen Studierenden der Mathematik empfehle ich, lieber früher als später, den Aufbau des Zahlensystems zu studieren.

Richard Dedekind hat sich schon 1888 sehr gründlich mit dem Aufbau der natürlichen Zahlen $\mathbb{N}$ und ihrer Arithmetik auseinandergesetzt. Als logische Grundlage für sein Unterfangen nutzte er gewinnbringend die damals gerade entstehende Mengenlehre. Diese trägt bis heute!

Edmund Landaus Lehrbuch von 1930 ist ein Klassiker. Hier wurde zum ersten Mal der Aufbau des Zahlensystems von den natürlichen Zahlen zu den rationalen, den reellen und schließlich den komplexen Zahlen systematisch und präzise ausgeführt. Es ist berühmt für Landaus (selbst so genannten) „unbarmherzigen Telegrammstil“ und oft zitiert dank seiner beiden prägnanten Vorworte „Vorwort für den Lernenden“ und „Vorwort für den Kenner“. Landaus Büchlein ist nach wie vor erhellend!

Beide Klassiker sind in kommentierten Neuauflagen gut zugänglich. Heutige Studierende finden vielleicht neuere Lehrbücher sympathischer. Ich empfehle das wunderschöne Buch *Zahlen* von Ebbinghaus *et al.*

Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

A103

Die Grundlage aller Mathematik ist das Zahlensystem:

natürliche Zahlen	$\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \}$
ganze Zahlen	$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$
rationale Zahlen	$\mathbb{Q} = \{ z/n \mid z, n \in \mathbb{Z},\ n \neq 0 \}$
reelle Zahlen	$\mathbb{R} =$ „$\mathbb{Q}$ und alle Grenzwerte“
komplexe Zahlen	$\mathbb{C} = \{ x + \mathrm{i}y \mid x, y \in \mathbb{R} \}$

Wie erklären / definieren / konstruieren wir diese Zahlbereiche?

P Pia, die pragmatische Physikerin: „Wie kann ich damit *rechnen*? Ich will Modelle und Werkzeuge, die meine Experimente beschreiben.“

I Ida, die innovative Informatikerin: „Wie *implementiere* ich Elemente und Operationen in jedem dieser Bereiche korrekt und effizient?“

L Lea, die lernbegeisterte Lehrerin: „Wie kann ich das gut *verstehen* und *vermitteln*, mathematisch korrekt und didaktisch geschickt?“

M Mia, die methodische Mathematikerin: „Wie kann ich diese Objekte definieren und konstruieren und ihre Eigenschaften *beweisen*?“

Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

A104
Erläuterung

Aller Anfang ist schwer! Das gilt besonders für Ihr Mathematikstudium. Glücklicherweise ist es nicht nur Anfang, sondern auch Fortsetzung: Sie haben Vorkenntnisse aus der Schule, darauf bauen wir auf.

In diesem Kapitel werden Sie viele alte Bekannte wiedertreffen, die Sie schon lange kennen, zum Teil seit der Grundschule: Zahlen, ihre Rechenregeln und die Lösung von Gleichungen.

Ausgehend von den natürlichen Zahlen $\mathbb{N}$ konstruieren wir die ganzen Zahlen $\mathbb{Z}$ und die rationalen Zahlen $\mathbb{Q}$. Wir erklären den Polynomring $\mathbb{Q}[X]$ und den Körper $\mathbb{Q}(X)$ der gebrochen-rationalen Funktionen.

Die Sichtweise ist jedoch neu und für Sie vermutlich ungewohnt: Wir verhandeln diese Objekte in mathematisch präziser Sprache. Insbesondere wollen wir Eigenschaften und Rechenregeln beweisen.

Das ist anfangs etwas mühsam, bietet aber wunderbar Lernmaterial. Zudem bietet es konkrete Anschauung für spätere Abstraktionen. Die Ideen, Begriffe und Techniken werden wir später erneut aufgreifen und vertiefen. Hier will ich die prominentesten Akteure vorstellen.

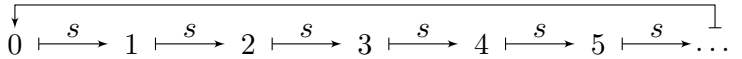
Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Anschaulich: Die natürlichen Zahlen $\mathbb{N}$ nutzen wir zum Zählen gemäß

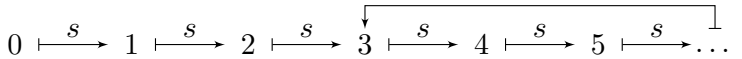
$$0 \overset{s}{\longmapsto} 1 \overset{s}{\longmapsto} 2 \overset{s}{\longmapsto} 3 \overset{s}{\longmapsto} 4 \overset{s}{\longmapsto} 5 \overset{s}{\longmapsto} \ldots$$

Die Abbildung $s : \mathbb{N} \to \mathbb{N}$ ordnet jeder Zahl n ihre Nachfolgerin $s(n)$ zu.
Ist damit alles klar? Aber nein, das Problem liegt in den drei Pünktchen!
Wir müssen unmissverständlich definieren, wie es weitergehen soll.

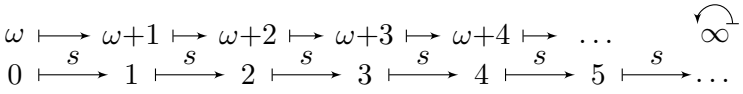
Der Zählprozess startet bei 0 und durchläuft jede Zahl genau einmal.
Situationen wie die folgenden wollen wir also ausschließen:



¬D0



¬D1



¬D2

Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Auf diese Weise können wir beliebig viele Beispiele vorführen, aber eben nur endlich viele! Wie beschreiben wir *alle* natürlichen Zahlen?

Drei kleine Pünktchen sind bequem und berüchtigt, gar gefährlich.
Sie haben eine völlig andere Bedeutung in folgenden Kontexten:

- „Die Jahreszeiten sind Frühling, Sommer, Herbst, Winter, . . . “
- „Die Wochentage sind Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, . . . “ und immer so weiter?!?

Vielleicht sagen Sie: „Das ist doch Haarspalterei! Ich weiß doch wie es weitergeht.“ Wirklich? Ich glaube nicht, dass wir Menschen weit blicken.

Auf 8-Bit-Computern gilt $s(255) = 0$, auf 16-Bit-Computern $s(65535) = 0$, auf 32-Bit-Computern $s(4294967295) = 0$. Das ist ein reales Problem.
Da die meisten Menschen nicht so weit zählen oder vorausschauen, würden sie keinen Unterschied vermuten. Doch wehe dem Überlauf!
Das ist keine Haarspalterei, sondern ein gefürchteter Programmierfehler.
Wir erinnern uns an das Jahr-2000-Problem oder das vermeintliche Weltende 2012 laut Maya-Kalender. Soviel zu den Pünktchen „. . . “.

Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Wir müssen also immer neue Zahlen generieren, ohne Wiederholung!
Das ist keineswegs selbstverständlich, wie Sie aus Kindertagen wissen.

Wie sehen konkrete Modelle aus? Am elegantesten ist das Binärsystem.
Wir nutzen die Ziffern $\mathtt{0}$ und $\mathtt{1}$ und bilden damit endliche Zeichenketten:

$$0 \mapsto 1 \mapsto 10 \mapsto 11 \mapsto 100 \mapsto 101 \mapsto 110 \mapsto 111 \mapsto 1000 \mapsto \ldots$$

Führende Nullen dürfen dabei beliebig ergänzt oder gelöscht werden.
Die Nachfolgerabbildung ist $s(*\mathtt{0}) = *\mathtt{1}$ und $s(*\mathtt{01 \ldots 1}) = *\mathtt{10 \ldots 0}$

Genauso gelingt dies im vertrauten Dezimalsystem, zur Basis Zehn:

$$\begin{aligned}
0 &\mapsto 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 6 \mapsto 7 \mapsto 8 \mapsto 9 \mapsto \\
10 &\mapsto 11 \mapsto 12 \mapsto 13 \mapsto 14 \mapsto 15 \mapsto 16 \mapsto 17 \mapsto 18 \mapsto 19 \mapsto \\
20 &\mapsto 21 \mapsto 22 \mapsto 23 \mapsto \quad \ldots \quad \mapsto 97 \mapsto 98 \mapsto 99 \mapsto \\
100 &\mapsto 101 \mapsto 102 \mapsto 103 \mapsto \ldots
\end{aligned}$$

Hier lautet die Regel entsprechend: Erhöhe die letzte Ziffer wie in der ersten Zeile gezeigt, bei Übertrag $*9 \mapsto *0$ erhöhe die Ziffer davor, usw.

Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

So können wir immer neue Zahlen generieren, ohne Wiederholung.
Beispiele und Gegenbeispiele wie die obigen illustrieren eindringlich:
Selbst bei einfachen Definitionen benötigen wir Sorgfalt und Präzision!

Die drei kleinen Pünktchen „. . . “ sind meist das extreme Gegenteil:
Sind sich Sender und Empfänger einig, so ist das kein Problem.
Aber diese Hoffnung ist oft keine belastbare Vereinbarung!

Die Auslassung ist oft bequem als erste Idee, das hilft manchmal, und so habe ich es oben genutzt. Oft jedoch stecken dahinter weniger edle Motive: An solchen Stellen hat der Autor die redliche Mühe gescheut und überlässt dies dem Leser oder der Phantasie jedes einzelnen.

In obigen Modellen habe ich daher den Zählprozess s explizit erklärt.
Auch über Ziffern und endliche Zeichenketten können wir noch genauer nachdenken, aber darin liegt keine grundsätzliche Schwierigkeit mehr.

Beide Modelle sind übrigens *isomorph*: Es gibt eine Übersetzung von Binär in Dezimal und zurück, sodass keine Information verloren geht:
Es genügt, beide Zählprozesse parallel laufen zu lassen. (Satz F2C)

Rechenoperationen für natürliche Zahlen

Logik Mengen Abbildungen

Die drei Daten $(\mathbb{N}, 0, s)$ erfüllen die **Dedekind–Peano–Axiome**:

D0: Null ist kein Nachfolger: $0 \notin s(\mathbb{N})$, also $\forall n \in \mathbb{N} : s(n) \neq 0$.

D1: Die Abbildung s ist injektiv: $\forall p, q \in \mathbb{N} : p \neq q \Rightarrow s(p) \neq s(q)$.
Äquivalent hierzu: $\forall p, q \in \mathbb{N} : s(p) = s(q) \Rightarrow p = q$.

D2: Prinzip der **vollständigen Induktion**: Vorgelegt sei $E \subseteq \mathbb{N}$ mit $0 \in E$, und für jedes $n \in E$ gilt $s(n) \in E$. Dann gilt bereits $E = \mathbb{N}$.

Dies definiert eindeutig, was wir unter dem Zählprozess verstehen.

Definition A1A: Rechenoperationen für natürliche Zahlen

Hieraus konstruieren wir rekursiv Addition, Multiplikation und Potenz:

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a, b) \mapsto a + b, \quad a + 0 := a, \quad a + s(n) := s(a + n)$$
$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a, b) \mapsto a \cdot b, \quad a \cdot 0 := 0, \quad a \cdot s(n) := (a \cdot n) + a$$
$$\hat{} : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a, b) \mapsto a^b, \quad a^0 := 1, \quad a^{s(n)} := a^n \cdot a$$

Damit gilt $s(n) = n + 1$, denn $n + 1 \overset{\text{Def}}{=} n + s(0) \overset{\text{Def}}{=} s(n + 0) \overset{\text{Def}}{=} s(n)$.

Rechenoperationen für natürliche Zahlen

Übung: Berechnen Sie so das kleine Einmaleins, zuvor Einspluseins.

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	10
2	2	3	4	5	6	7	8	9	10	11
3	3	4	5	6	7	8	9	10	11	12
4	4	5	6	7	8	9	10	11	12	13
5	5	6	7	8	9	10	11	12	13	14
6	6	7	8	9	10	11	12	13	14	15
7	7	8	9	10	11	12	13	14	15	16
8	8	9	10	11	12	13	14	15	16	17
9	9	10	11	12	13	14	15	16	17	18

·	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	10	12	14	16	18
3	0	3	6	9	12	15	18	21	24	27
4	0	4	8	12	16	20	24	28	32	36
5	0	5	10	15	20	25	30	35	40	45
6	0	6	12	18	24	30	36	42	48	54
7	0	7	14	21	28	35	42	49	56	63
8	0	8	16	24	32	40	48	56	64	72
9	0	9	18	27	36	45	54	63	72	81

Die rekursive Rechnung ist etwas gewöhnungsbedürftig, aber lehrreich. Genau so haben Sie es in der Grundschule gelernt! Dort natürlich an Beispielen ohne Definition. Hier sehen Sie, was genau dahinter steckt. Zudem erkennen wir erste Rechenregeln wie die Kommutativität. . .

Rechenregeln für natürliche Zahlen

Ringe und Körper

Die Addition erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{N}$:
Kommutativität, **Com**$(\mathbb{N}, +)$: $a + b = b + a$
Assoziativität, **Ass**$(\mathbb{N}, +)$: $(a + b) + c = a + (b + c)$
Neutrales, **Ntr**$(\mathbb{N}, +, 0)$: $0 + a = a$ und $a + 0 = a$
Wir sagen dazu: $(\mathbb{N}, +, 0)$ ist ein **kommutatives Monoid**.

Die Multiplikation erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{N}$:
Kommutativität, **Com**$(\mathbb{N}, \cdot)$: $a \cdot b = b \cdot a$
Assoziativität, **Ass**$(\mathbb{N}, \cdot)$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Neutrales, **Ntr**$(\mathbb{N}, \cdot, 1)$: $1 \cdot a = a$ und $a \cdot 1 = a$
Wir sagen dazu: $(\mathbb{N}, \cdot, 1)$ ist ein **kommutatives Monoid**.

Die Multiplikation ist distributiv über die Addition für alle $a, b, c \in \mathbb{N}$:
Distributivität links, **DL**$(\mathbb{N}, +, \cdot)$: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
Distributivität rechts, **DR**$(\mathbb{N}, +, \cdot)$: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

☺ Dies sind acht grundlegende und vertraute Rechenregeln.
Wir sagen dazu: $(\mathbb{N}, +, 0, \cdot, 1)$ ist ein **kommutativer Halbring**.

Rechenregeln für natürliche Zahlen

Erläuterung

Darauf beruhen alle Rechenverfahren, die Sie aus der Schule kennen. Solide Begründung und effiziente Handhabung der natürlichen Zahlen sind keineswegs leicht oder gar selbstverständlich. Stellenschreibweise und zugehörige Rechenverfahren sind monumentale Erfindungen; die Menschheit hat dafür ein paar Jahrtausende intellektuelle Entwicklung benötigt. Die erfreuliche Tatsache, dass Sie dies seit der Grundschule kennen und nutzen, darf Sie nicht über die Raffinesse hinwegtäuschen.

By relieving the brain of all unnecessary work, a good notation sets it free to concentrate on more advanced problems [. . .] Before the introduction of the Arabic notation, multiplication was difficult, and the division of integers called into play the highest mathematical faculties. Probably nothing in the modern world would have more astonished a Greek mathematician than to learn that, under the influence of compulsory education, a large proportion of the population of Western Europe could perform the operation of division for the largest numbers. Our modern power of easy reckoning with decimal fractions is the almost miraculous result of the gradual discovery of a perfect notation.
Alfred North Whitehead (1861–1947), *An Introduction to Mathematics* (1911)

Der Halbring $(\mathbb{N}, +, 0, \cdot, 1)$ der natürlichen Zahlen

Beweise Induktion

Satz A1B: Eigenschaften der natürlichen Zahlen

Die natürlichen Zahlen $(\mathbb{N}, +, 0, \cdot, 1)$ sind ein kommutativer Halbring.

Als charakteristische Eigenschaft erfüllt die Nachfolgerabbildung $s : n \mapsto n + 1$ die zugrundeliegenden **Dedekind–Peano–Axiome**:

- D0: Null ist kein Nachfolger: $0 \notin s(\mathbb{N})$, also $\forall n \in \mathbb{N} : n + 1 \neq 0$.
- D1: Die Abbildung s ist injektiv: $\forall p, q \in \mathbb{N} : p \neq q \Rightarrow p + 1 \neq q + 1$.
- D2: Prinzip der **vollständigen Induktion**: Vorgelegt sei $E \subseteq \mathbb{N}$ mit $0 \in E$, und für jedes $n \in E$ gilt $n + 1 \in E$. Dann gilt bereits $E = \mathbb{N}$.

Die Addition ist kürzbar, das heißt $a + c = b + c$ impliziert $a = b$.
Die Multiplikation ist kürzbar: $a \cdot c = b \cdot c$ und $c \neq 0$ implizieren $a = b$.

Die Potenz erfreut sich folgender Eigenschaften / Potenzgesetze:

$$a^0 = 1 \text{ und } a^1 = a \text{ sowie } a^{m+n} = a^m \cdot a^n \text{ und } a^{m \cdot n} = (a^m)^n.$$

Für alle $n \in \mathbb{N} \setminus \{0\}$ gilt: $a^n = b^n$ impliziert $a = b$.
Für alle $a \in \mathbb{N} \setminus \{0, 1\}$ gilt: $a^m = a^n$ impliziert $m = n$.

Nachweis der Eigenschaften durch vollständige Induktion

Beweis: Alle Behauptungen rechnen wir geduldig nach. Ich zeige dies ausführlich für die Addition, analog gelingen Multiplikation und Potenz.

(1) Zur Assoziativität **Ass**$(\mathbb{N}, +)$ betrachten wir die Erfüllungsmenge

$$E := \{\, n \in \mathbb{N} \mid a + (b + n) = (a + b) + n \text{ für alle } a, b \in \mathbb{N} \,\}.$$

Wir zeigen nun $E = \mathbb{N}$ durch vollständige Induktion.
Induktionsanfang: Es gilt $0 \in E$, denn

$$a + (b + 0) \overset{\text{Def}}{=} a + b \overset{\text{Def}}{=} (a + b) + 0.$$

Induktionsschritt: Gilt $n \in E$, dann auch $s(n) \in E$, denn

$$\begin{aligned} a + (b + s(n)) &\overset{\text{Def}}{=} a + s(b + n) \overset{\text{Def}}{=} s(a + (b + n)) \\ &\overset{n \in E}{=} s((a + b) + n) \overset{\text{Def}}{=} (a + b) + s(n). \end{aligned}$$

Per Induktion gilt $E = \mathbb{N}$. Die Addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ist also assoziativ.

Nachweis der Eigenschaften durch vollständige Induktion

(2) Nach Definition gilt $n + 0 = n$. Wir zeigen nun $0 + n = n$. Hierzu sei

$$E := \{\, n \in \mathbb{N} \mid 0 + n = n \,\}.$$

Wir haben $0 + 0 = 0$, also $0 \in E$. Gilt $n \in E$, dann auch $s(n) \in E$, denn

$$0 + s(n) \overset{\text{Def}}{=} s(0 + n) \overset{n \in E}{=} s(n).$$

Per Induktion gilt $E = \mathbb{N}$. Das Element 0 ist also beidseitig neutral.

(3) Nach Definition gilt $n + 1 = s(n)$. Wir zeigen $1 + n = s(n)$. Hierzu sei

$$E := \{\, n \in \mathbb{N} \mid 1 + n = s(n) \,\}.$$

Es gilt $0 \in E$, denn $1 + 0 = 1 = s(0)$. Gilt $n \in E$, dann auch $s(n) \in E$:

$$1 + s(n) \overset{\text{Def}}{=} s(1 + n) \overset{n \in E}{=} s(s(n)).$$

Per Induktion gilt $E = \mathbb{N}$. Also gilt $1 + n = n + 1$ für alle $n \in \mathbb{N}$.

Nachweis der Eigenschaften durch vollständige Induktion

(4) Zum Beweis der Kommutativität **Com**$(\mathbb{N}, +)$ betrachten wir

$$E := \{\, n \in \mathbb{N} \mid a + n = n + a \text{ für alle } a \in \mathbb{N} \,\}.$$

Induktionsanfang: In (2,3) haben wir bereits $0 \in E$ und $1 \in E$ gezeigt.
Induktionsschritt: Gilt $n \in E$, dann auch $s(n) \in E$, denn

$$\begin{aligned} a + s(n) &\overset{\text{Def}}{=} s(a + n) \overset{n \in E}{=} s(n + a) \overset{\text{Def}}{=} n + s(a) \\ &\overset{(3)}{=} n + (1 + a) \overset{(1)}{=} (n + 1) + a \overset{\text{Def}}{=} s(n) + a. \end{aligned}$$

Per Induktion gilt $E = \mathbb{N}$. Also ist die Addition kommutativ.

(5) Zur Kürzbarkeit schließlich betrachten wir

$$E := \{\, n \in \mathbb{N} \mid \text{für alle } a, b \in \mathbb{N} \text{ mit } a + n = b + n \text{ folgt } a = b \,\}$$

Es gilt $0 \in E$. Gilt $n \in E$, dann auch $s(n) \in E$, denn für alle $a, b \in \mathbb{N}$ gilt:

$$a + s(n) = b + s(n) \overset{\text{Def}}{\Longrightarrow} s(a + n) = s(b + n) \overset{\text{Inj}}{\Longrightarrow} a + n = b + n \overset{n \in E}{\Longrightarrow} a = b$$

Per Induktion gilt $E = \mathbb{N}$. Also ist die Addition kürzbar. QED

Von den natürlichen Zahlen $\mathbb{N}$ zu den ganzen Zahlen $\mathbb{Z}$

In $\mathbb{N}$ können wir Gleichungen wie $3 = 5 + x$ formulieren, aber nicht lösen.
Hierzu erweitern wir die natürlichen Zahlen $\mathbb{N}$ zu den ganzen Zahlen

$$\mathbb{Z} = \{\, z = [a-b] \mid a, b \in \mathbb{N} \,\}.$$

Auf dieser Menge $\mathbb{Z}$ vereinbaren wir die folgenden Operationen:

Vergleich:	$[a-b] = [c-d]$ in $\mathbb{Z}$	$\Leftrightarrow$	$a + d = c + b$ in $\mathbb{N}$
Addition:	$[a-b] + [c-d]$	$=$	$[(a+c) - (b+d)]$
Negation:	$-[a-b]$	$=$	$[b-a]$
Multiplikation:	$[a-b] \cdot [c-d]$	$=$	$[(ac+bd) - (ad+bc)]$

Wir haben die Einbettung $\mathbb{N} \hookrightarrow \mathbb{Z} : n \mapsto [n-0]$ und schreiben kurz $\mathbb{N} \subset \mathbb{Z}$.
Genauer gilt $(\mathbb{N}, +_{\mathbb{N}}, \cdot_{\mathbb{N}}) \subset (\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}})$; alles wird von $\mathbb{N}$ auf $\mathbb{Z}$ fortgesetzt.
Normalform: Für jedes $z \in \mathbb{Z}$ gilt $z = n$ oder $z = -n$ für ein $n \in \mathbb{N}$.

Beispiel: Die Gleichung $3 = 5 + x$ hat keine Lösung $x \in \mathbb{N}$.
In $\mathbb{Z}$ hingegen finden wir die Lösung $x = [3-5] = [0-2] = -2$.

Von den natürlichen Zahlen $\mathbb{N}$ zu den ganzen Zahlen $\mathbb{Z}$

Wir nutzen die Konvention **Punkt vor Strich**, um Klammern zu sparen.
Wo möglich lassen wir meist auch das Produktzeichen weg:

$$(a \cdot c) + (b \cdot d) = ac + bd$$

Die natürlichen Zahlen erweitern wir zu den ganzen Zahlen $\mathbb{Z}$: Addition und Multiplikation setzen wir fort und gewinnen zudem die Negation.

Dies definiert die Operationen, begründet oder motiviert sie aber nicht.
Genau so haben Sie es in der Schule gelernt und erfolgreich genutzt:
„Hier sind die Rechenregeln, damit können Sie arbeiten.“

P „Ok, damit bin ich zufrieden, damit kann ich konkret rechnen.“
I „Zur effizienten Implementierung muss ich noch genauer arbeiten.“
M „Sind unsere Konstruktionen einwandfrei und ohne Widersprüche?“
L „Warum vereinbaren wir diese Operationen? Woher kommen sie?“

Die Motivation erwächst erst aus den folgenden Rechenregeln und dem abschließenden Satz: Wir wollen den Halbring $\mathbb{N}$ zum Ring $\mathbb{Z}$ erweitern.
Dies gelingt auf genau eine Weise, nämlich wie hier gezeigt.

Der Ring $(\mathbb{Z}, +, 0, -, \cdot, 1)$ der ganzen Zahlen

Die Addition erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{Z}$:

Kommutativität,	**Com**$(\mathbb{Z}, +)$:	$a + b = b + a$
Assoziativität,	**Ass**$(\mathbb{Z}, +)$:	$(a + b) + c = a + (b + c)$
Neutrales,	**Ntr**$(\mathbb{Z}, +, 0)$:	$0 + a = a$ und $a + 0 = a$
Negatives,	**Inv**$(\mathbb{Z}, +, 0, -)$:	$(-a) + a = 0$ und $a + (-a) = 0$

Wir sagen dazu: $(\mathbb{Z}, +, 0, -)$ ist eine **kommutative Gruppe**.

Die Multiplikation erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{Z}$:

Kommutativität,	**Com**$(\mathbb{Z}, \cdot)$:	$a \cdot b = b \cdot a$
Assoziativität,	**Ass**$(\mathbb{Z}, \cdot)$:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Neutrales,	**Ntr**$(\mathbb{Z}, \cdot, 1)$:	$1 \cdot a = a$ und $a \cdot 1 = a$

Wir sagen dazu: $(\mathbb{Z}, \cdot, 1)$ ist ein **kommutatives Monoid**.

Die Multiplikation ist distributiv über die Addition für alle $a, b, c \in \mathbb{Z}$:

Distributivität links,	**DL**$(\mathbb{Z}, +, \cdot)$:	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
Distributivität rechts,	**DR**$(\mathbb{Z}, +, \cdot)$:	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

🙂 Dies sind neun grundlegende und vertraute Rechenregeln.
Wir sagen dazu: $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist ein **kommutativer Ring**.

Der Ring $(\mathbb{Z}, +, 0, -, \cdot, 1)$ der ganzen Zahlen

Jede Gleichung $a = x + b$ mit $a, b \in \mathbb{Z}$ hat genau eine Lösung $x \in \mathbb{Z}$, nämlich $x = a - b$. Zu $a \in \mathbb{Z}$ ist das Negative die Lösung zu $a + x = 0$; somit lässt sich die Negation $a \mapsto -a$ aus $(\mathbb{Z}, +, 0)$ rekonstruieren.

Statt $(\mathbb{Z}, +, 0, -)$ schreiben wir daher auch $(\mathbb{Z}, +, 0)$ oder kurz $(\mathbb{Z}, +)$.
Wie üblich nutzen wir die Abkürzung $a - b = a + (-b)$.

Zusammenfassung unserer Konstruktion:

Satz A1c: Die ganzen Zahlen erweitern die natürlichen Zahlen.

Die ganzen Zahlen $(\mathbb{Z}, +, 0, \cdot, 1)$ sind ein kommutativer Ring mit $\mathbb{Z} \supset \mathbb{N}$.

Genauer gesagt enthält der Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ den Halbring $(\mathbb{N}, +, 0, \cdot, 1)$ und jede ganze Zahl $z \in \mathbb{Z}$ ist eine Differenz $z = a - b$ mit $a, b \in \mathbb{N}$.

Dies ist der einzige Ring mit diesen Eigenschaften.

Die Multiplikation ist kürzbar: $a \cdot c = b \cdot c$ und $c \neq 0$ implizieren $a = b$.
Insbesondere ist $\mathbb{Z}$ nullteilerfrei: Aus $a \neq 0$ und $b \neq 0$ folgt $a \cdot b \neq 0$.

Von den ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen $\mathbb{Q}$

A121 Äquivalenz-relationen

In $\mathbb{Z}$ können wir Gleichungen wie $3 = 6 \cdot x$ formulieren, aber nicht lösen.
Hierzu erweitern wir die ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen

$$\mathbb{Q} = \{\, q = [a/b] \mid a, b \in \mathbb{Z},\ b \neq 0 \,\}.$$

Auf dieser Menge $\mathbb{Q}$ vereinbaren wir die folgenden Operationen:

Vergleich:	$[a/b] = [c/d]$ in $\mathbb{Q}$	$\Leftrightarrow$	$ad = cb$ in $\mathbb{Z}$
Addition:	$[a/b] + [c/d]$	$=$	$[(ad + cb)/(bd)]$
Negation:	$-[a/b]$	$=$	$[-a/b]$
Multiplikation:	$[a/b] \cdot [c/d]$	$=$	$[(ac)/(bd)]$
Inversion:	$[a/b]^{-1}$	$=$	$[b/a]$ falls $a \neq 0$

Wir haben die Einbettung $\mathbb{Z} \hookrightarrow \mathbb{Q} : z \mapsto [z/1]$ und schreiben kurz $\mathbb{Z} \subset \mathbb{Q}$.
Genauer gilt $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}) \subset (\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}})$; alles wird von $\mathbb{Z}$ auf $\mathbb{Q}$ fortgesetzt.

Normalform: Für $q \in \mathbb{Q}$ gilt $q = [a/b]$ mit $\operatorname{ggT}(a, b) = 1$ und $b \geq 1$;
dies nennen wir die Darstellung von q als gekürzten Bruch.

Beispiel: Die Gleichung $3 = 6 \cdot x$ hat keine Lösung $x \in \mathbb{Z}$.
In $\mathbb{Q}$ hingegen finden wir die Lösung $x = [3/6] = [1/2] = 2^{-1}$.

Von den ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen $\mathbb{Q}$

A122 Erläuterung

Die rationalen Zahlen $\mathbb{Q}$ erweitern die ganzen Zahlen $\mathbb{Z}$: Addition und Multiplikation setzen wir fort und gewinnen zudem die Inversion.

Dies definiert die Operationen, begründet oder motiviert sie aber nicht.
Genau so haben Sie es in der Schule gelernt und erfolgreich genutzt:
„Hier sind die Rechenregeln, damit können Sie arbeiten.“

P „Ok, damit bin ich zufrieden, damit kann ich konkret rechnen.“
I „Zur effizienten Implementierung muss ich noch genauer arbeiten.“
M „Sind unsere Konstruktionen einwandfrei und ohne Widersprüche?“
L „Warum vereinbaren wir diese Operationen? Woher kommen sie?“

Die Motivation erwächst erst aus den folgenden Rechenregeln und dem abschließenden Satz: Wir wollen den Ring $\mathbb{Z}$ zum Körper $\mathbb{Q}$ erweitern.
Dies gelingt auf genau eine Weise, nämlich die hier gezeigt.

🙂 *Fun fact:* Wir vergleichen die Erweiterungen $\mathbb{N} \hookrightarrow \mathbb{Z}$ und $\mathbb{Z} \hookrightarrow \mathbb{Q}$:
Für Differenzen $[a - b]$ ist die Addition leichter als die Multiplikation.
Für Brüche $[a/b]$ ist die Multiplikation leichter als die Addition.

Der Körper $(\mathbb{Q}, +, 0, -, \cdot, 1, ^{-1})$ der rationalen Zahlen

A123 Ringe und Körper

Die Addition erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{Q}$:

Kommutativität,	**Com**$(\mathbb{Q}, +)$:	$a + b = b + a$
Assoziativität,	**Ass**$(\mathbb{Q}, +)$:	$(a + b) + c = a + (b + c)$
Neutrales,	**Ntr**$(\mathbb{Q}, +, 0)$:	$0 + a = a$ und $a + 0 = a$
Negatives,	**Inv**$(\mathbb{Q}, +, 0, -)$:	$(-a) + a = 0$ und $a + (-a) = 0$

Wir sagen dazu: $(\mathbb{Q}, +, 0, -)$ ist eine **kommutative Gruppe**.

Die Multiplikation erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{Q}$:

Kommutativität,	**Com**$(\mathbb{Q}, \cdot)$:	$a \cdot b = b \cdot a$
Assoziativität,	**Ass**$(\mathbb{Q}, \cdot)$:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Neutrales,	**Ntr**$(\mathbb{Q}, \cdot, 1)$:	$1 \cdot a = a$ und $a \cdot 1 = a$
Inverses,	**Inv**$(\mathbb{Q}^*, \cdot, 1, ^{-1})$:	$a \cdot a^{-1} = 1$ und $a^{-1} \cdot a = 1$

Letzteres gilt nur für $a \neq 0$, also für alle $a \in \mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$.
Wir sagen dazu: $(\mathbb{Q}^*, \cdot, 1, ^{-1})$ ist eine **kommutative Gruppe**.

Die Multiplikation ist distributiv über die Addition, es gilt also **DL** und **DR**.

🙂 Dies sind zehn grundlegende und vertraute Rechenregeln.
Wir sagen dazu: $(\mathbb{Q}, +, 0, -, \cdot, 1, ^{-1})$ ist ein **Körper**.

Der Körper $(\mathbb{Q}, +, 0, -, \cdot, 1, ^{-1})$ der rationalen Zahlen

A124

Jede Gleichung $a = xb$ mit $a, b \in \mathbb{Q}$, $b \neq 0$ hat genau eine Lösung $x \in \mathbb{Q}$:

$$a = x \cdot b \implies a \cdot b^{-1} = (x \cdot b) \cdot b^{-1} = x \cdot (b \cdot b^{-1}) = x \cdot 1 = x$$
$$x = a \cdot b^{-1} \implies x \cdot b = (a \cdot b^{-1}) \cdot b = a \cdot (b \cdot b^{-1}) = a \cdot 1 = a$$

Zu jedem Element $a \in \mathbb{Q}^*$ ist das Inverse die Lösung zu $a \cdot x = 1$;
somit lässt sich die Inversion $a \mapsto a^{-1}$ aus $(\mathbb{Q}, \cdot, 1)$ rekonstruieren.

Statt $(\mathbb{Q}, \cdot, 1, ^{-1})$ schreiben wir daher auch $(\mathbb{Q}, \cdot, 1)$ oder kurz $(\mathbb{Q}, \cdot)$.
Wie üblich nutzen wir die Abkürzung $a/b = a \cdot b^{-1}$

Zusammenfassung unserer Konstruktion:

Satz A1D: Die rationalen Zahlen erweitern die ganzen Zahlen.

Die rationalen Zahlen $(\mathbb{Q}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Q} \supset \mathbb{Z}$.

Genauer gesagt enthält der Körper $(\mathbb{Q}, +, 0, \cdot, 1)$ den Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ und jede rationale Zahl $q \in \mathbb{Q}$ ist Quotient $q = z/n$ mit $z, n \in \mathbb{Z}$, $n \neq 0$.

Dies ist der einzige Körper mit den genannten Eigenschaften.

Die vier Grundrechenarten und ihre Rechenregeln

Definition A1E: Ringe und Körper

Wir nennen $(K,+,0,-,\cdot,1,^{-1})$ mit $0\neq 1$ einen **Körper**, wenn die obigen zehn Rechenregeln / Forderungen / Axiome gelten. Für abgeschwächte Forderungen vereinbaren und nutzen wir folgende Bezeichnungen:

Struktur $(K,+,\cdot)$		$(K,+)$				$(K,+,\cdot)$		$(K,\cdot)$			
Name	Beispiele	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	Inv*	Com
Körper	$\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_p$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CRing	$\mathbb{Z},\mathbb{Z}_n,\mathbb{Q}[X]$	✓	✓	✓	✓	✓	✓	✓	✓		✓
DRing	$\mathbb{H}\subset\mathbb{C}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Ring	$\mathbb{Z}^{2\times 2}$, $\mathbb{R}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓		
Rng	$\left(\begin{smallmatrix}\mathbb{R} & \mathbb{R}\\ 0 & 0\end{smallmatrix}\right)$	✓	✓	✓	✓	✓	✓	✓			
KRng	$2\mathbb{Z}$, $\mathscr{C}_c(\mathbb{R})$	✓	✓	✓	✓	✓	✓	✓			✓
Halbkörper	$\mathbb{Q}_{\geq 0}$, $\mathbb{R}_{\geq 0}$	✓	✓		✓	✓	✓	✓	✓	✓	✓
Halbring, Rig	$\mathbb{N}$, $[0,\infty]$	✓	✓		✓	✓	✓	✓	✓		

Die vier Grundrechenarten und ihre Rechenregeln

Körper sind die strengsten und schönsten dieser Strukturen: Hier gelten alle Rechenregeln. Für einen **Divisionsring**, kurz DRing, verzichten wir auf Kommutativität **Com**$(K,\cdot)$ der Multiplikation; auch das kommt vor. Einen nicht-kommutativen Divisionsring nennt man **Schiefkörper**.

Für einen **kommutativen Ring**, kurz CRing, verzichten wir stattdessen auf Invertierbarkeit **Inv**$(K^*,\cdot,1)$ der Multiplikation, noch allgemeiner für einen **Ring** auch auf Kommutativität **Com**$(K,\cdot)$. Ein (kommutativer) Ring $(R,+,0,-,\cdot,1)$ besteht also aus einer kommutativen Gruppe $(R,+,0,-)$ und einem (kommutativen) Monoid $(R,\cdot,1)$ und ist beidseitig distributiv.

Die untere Hälfte der Tabelle dient zur Abrundung nützlicher Begriffe. Uns begegnen öfters „Ringe ohne Eins“, engl. „ring without identity“, daher das Wortspiel **Rng**, für „Ringe ohne Negation“ entsprechend **Rig**.

Auch (nicht/kommutative) Halbkörper treten natürlich auf, etwa $\mathbb{Q}_{\geq 0}$: Hier ist zwar die Multiplikation invertierbar, aber nicht die Addition.

Halbringe sind mit die schwächsten dieser Strukturen. Allerdings sind die natürlichen Zahlen $\mathbb{N}$ sehr wichtig, daher stehen sie hier zu Recht.

Anordnung der ganzen Zahlen

Aufgabe: Wie erklären Sie die Anordnung $\leq$ der natürlichen Zahlen $\mathbb{N}$?

Lösung: Für $a,b\in\mathbb{N}$ definieren wir die Relation $a\leq b$ durch die Bedingung $a+x=b$ für ein $x\in\mathbb{N}$. Damit gilt für alle $a,b,c\in\mathbb{N}$:

Reflexivität, **Refl**$(\mathbb{N},\leq)$: $a\leq a$.
Antisymmetrie, **Asym**$(\mathbb{N},\leq)$: Aus $a\leq b$ und $b\leq a$ folgt $a=b$.
Transitivität, **Tran**$(\mathbb{N},\leq)$: Aus $a\leq b$ und $b\leq c$ folgt $a\leq c$.

Aufgabe: Wie erklären Sie die Anordnung $\leq$ der ganzen Zahlen $\mathbb{Z}$? Was sind die grundlegenden Rechenregeln? Wie beweist man sie?

Lösung: Für $a,b\in\mathbb{Z}$ definieren wir $a\leq b$ durch $b-a\in\mathbb{N}$. Damit gilt $a\leq a$. Aus $a\leq b$ und $b\leq a$ folgt $a=b$. Aus $a\leq b$ und $b\leq c$ folgt $a\leq c$.

Entsprechend definieren wir die Relation $a<b$ durch $a\leq b$ und $a\neq b$. Symmetrisch hierzu schreiben wir $a\geq b$ für $b\leq a$ und $a>b$ für $b<a$.

Damit ist $(\mathbb{Z},+,\cdot,\leq)$ ein **angeordneter Ring**:
(0) Für je zwei Zahlen $a,b\in\mathbb{Z}$ gilt entweder $a=b$ oder $a<b$ oder $a>b$.
(1) Aus $a\leq b$ folgt $a+c\leq b+c$. (2) Aus $a\leq b$ und $0\leq c$ folgt $ac\leq bc$.

Anordnung der rationalen Zahlen

Aufgabe: Wie erklären Sie die Anordnung $\leq$ der rationalen Zahlen $\mathbb{Q}$? Was sind die grundlegenden Rechenregeln? Wie beweist man sie?

Lösung: Die Menge der nicht-negativen rationalen Zahlen ist

$$P=\mathbb{Q}_{\geq 0}:=\{\,z/n\mid z,n\in\mathbb{N},\ n\neq 0\,\}.$$

Sie erfüllt $P\cap(-P)=\{0\}$ und $P\cup(-P)=\mathbb{Q}$ sowie $P+P\subseteq P$ und $P\cdot P\subseteq P$, das heißt, aus $a,b\in P$ folgt $a+b\in P$ und $a\cdot b\in P$.

Für $a,b\in\mathbb{Q}$ definieren wir die Relation $a\leq b$ durch $b-a\in P$. Damit gilt $a\leq a$. Aus $a\leq b$ und $b\leq a$ folgt $a=b$. Aus $a\leq b$ und $b\leq c$ folgt $a\leq c$.

Entsprechend definieren wir die Relation $a<b$ durch $a\leq b$ und $a\neq b$. Symmetrisch hierzu schreiben wir $a\geq b$ für $b\leq a$ und $a>b$ für $b<a$.

Damit ist $(\mathbb{Q},+,\cdot,\leq)$ ein **angeordneter Körper**:
(0) Für je zwei Zahlen $a,b\in\mathbb{Q}$ gilt entweder $a=b$ oder $a<b$ oder $a>b$.
(1) Aus $a\leq b$ folgt $a+c\leq b+c$. (2) Aus $a\leq b$ und $0\leq c$ folgt $ac\leq bc$.

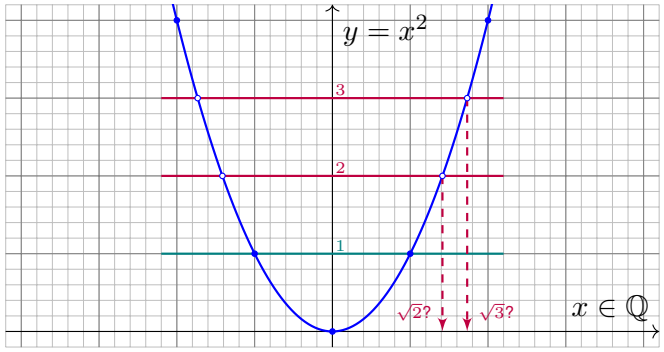
Wir definieren den **Absolutbetrag**

$$|-|:\mathbb{Q}\to\mathbb{Q}_{\geq 0}:x\mapsto|x|=\begin{cases}x & \text{falls } x\geq 0,\\ -x & \text{falls } x\leq 0.\end{cases}$$

Die rationalen Zahlen haben erhebliche Lücken!

A129

In $\mathbb{Q}$ können wir Gleichungen wie $x^2 = 2$ formulieren, aber nicht lösen.



Die Funktion $f : \mathbb{Q} \to \mathbb{Q} : x \mapsto x^2$ trifft die Werte $0 = f(0)$ und $1 = f(\pm 1)$ und $4 = f(\pm 2)$, sogar jeweils zweimal, aber nicht die Werte 2 und 3.

☹ Anschaulich: Der geordnete Körper $(\mathbb{Q}, +, \cdot, \leq)$ hat noch erhebliche Lücken! Diese wollen wir möglichst schließen, je nach Bedarf.

🙂 Ideale Lösung ist der Körper $(\mathbb{R}, +, \cdot, \leq)$ der reellen Zahlen (A3A). Doch wir wollen nicht gleich mit Kanonen auf Spatzen schießen...

Beispiele für irrationale Zahlen

A130

Logik Beweise

In $\mathbb{Q}$ können wir Gleichungen wie $x^2 = 2$ formulieren, aber nicht lösen.

Satz A1F: Irrationalität von $\sqrt{2}$, Euklid ca. 300 v.Chr.

Es gibt keine rationale Zahl $r \in \mathbb{Q}$ mit der Eigenschaft $r^2 = 2$.

Beweis: Angenommen, es gäbe $r \in \mathbb{Q}$ mit $r^2 = 2$.
Rational bedeutet $r = a/b$ mit $a, b \in \mathbb{Z}$ und $b \neq 0$.
Zudem sei der Bruch a/b vollständig gekürzt.

Aus der Gleichung $(a/b)^2 = 2$ folgt $a^2 = 2b^2$.
Daher ist a^2 gerade, also auch a, das heißt $a = 2\overline{a}$ mit $\overline{a} \in \mathbb{Z}$.

Einsetzen in $a^2 = 2b^2$ ergibt $4\overline{a}^2 = 2b^2$, also $2\overline{a}^2 = b^2$.
Daher ist b^2 gerade, also auch b, das heißt $b = 2\overline{b}$ mit $\overline{b} \in \mathbb{Z}$.

Somit ließe sich $a/b = \overline{a}/\overline{b}$ weiter kürzen. Das ist ein Widerspruch!
Also gibt es keine rationale Zahl $r \in \mathbb{Q}$ mit der Eigenschaft $r^2 = 2$. QED

Übung: Ebenso sind $\sqrt[3]{2}, \sqrt[4]{2}, \ldots$ und $\sqrt{3}, \sqrt[3]{3}, \sqrt[4]{3}, \ldots$ irrational.
Denken Sie sich weitere Beispiele aus und beweisen Sie diese!

Rechnen in $\mathbb{Q}[\sqrt{2}]$: Motivation

A131

Wir möchten mit dem Halb/Ring / Körper $\mathbb{K} = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ und $\sqrt{2}$ rechnen.
Wir wünschen uns einen Halb/Ring / Körper $\mathbb{K}[\sqrt{2}] \supset \mathbb{K}$ der Form

$$\mathbb{K}[\sqrt{2}] = \{\, z = x + y\sqrt{2} \mid x, y \in \mathbb{K} \,\}.$$

Wie sehen die Operationen aus? Falls $\mathbb{K}[\sqrt{2}]$ existiert, so erwarten wir:

Vergleich: $x + y\sqrt{2} = u + v\sqrt{2}$ in $\mathbb{K}[\sqrt{2}] \;\Leftrightarrow\; x = u$ und $y = v$ in $\mathbb{K}$

Addition: $(x + y\sqrt{2}) + (u + v\sqrt{2}) = (x + u) + (y + v)\sqrt{2}$

Multiplikation: $(x + y\sqrt{2}) \cdot (u + v\sqrt{2}) = (xu + 2yv) + (xv + yu)\sqrt{2}$

Über $\mathbb{K} = \mathbb{Z}, \mathbb{Q}$ haben wir zu jedem Element $z = x + y\sqrt{2}$ in $\mathbb{K}[\sqrt{2}]$ das Negative $-z = (-x) + (-y)\sqrt{2}$ und das Konjugierte $\overline{z} = x - y\sqrt{2}$.

Ist jedes Element $z \neq 0$ invertierbar? Über $\mathbb{K} = \mathbb{Q}$ gelingt dies:

$$\frac{1}{x + y\sqrt{2}} = \frac{1}{x + y\sqrt{2}} \cdot \frac{x - y\sqrt{2}}{x - y\sqrt{2}} = \frac{x}{x^2 - 2y^2} - \frac{y}{x^2 - 2y^2}\sqrt{2}$$

Wann gilt $x^2 - 2y^2 = 0$? Aus $y \neq 0$ folgt $(x/y)^2 = 2$; das ist für $x, y \in \mathbb{Q}$ unmöglich (A1F). Also gilt $y = 0$ und somit $x = 0$, das heißt $x + y\sqrt{2} = 0$.

Rechnen in $\mathbb{Q}[\sqrt{2}]$: Konstruktion

A132

kartesisches Produkt

Ist das erlaubt? Wie können wir die Menge $\mathbb{Q}[\sqrt{2}]$ und ihre Operationen einwandfrei erklären? Wir nutzen die Menge $\mathbb{Q}^2 = \{\, (x, y) \mid x, y \in \mathbb{Q} \,\}$ aller Paare (x, y) mit $x, y \in \mathbb{Q}$ und $\mathbb{Q}^2 \to \mathbb{Q}[\sqrt{2}] : (x, y) \mapsto x + y\sqrt{2}$.

Satz A1G: Konstruktion des Körpers $\mathbb{Q}[\sqrt{2}]$, siehe B137

Auf der Menge $E = \mathbb{Q}^2$ definieren wir Addition und Multiplikation durch

$$+ : E \times E \to E : (x, y) + (u, v) := (x + u, y + v),$$
$$\cdot : E \times E \to E : (x, y) \cdot (u, v) := (xu + 2yv, xv + yu).$$

Damit ist $(E, +, \cdot)$ ein Körper. Hierin ist $(\mathbb{Q}, +, \cdot)$ ein Teilkörper dank der Einbettung $\mathbb{Q} \hookrightarrow E : x \mapsto (x, 0)$. Wir schreiben kurz $\mathbb{Q} \subset E$.

Im Körper E erfüllt das Element $\xi = (0, 1)$ die Eigenschaft $\xi^2 = 2$.
Jedes Element $z \in E$ schreibt sich eindeutig $z = x + y\xi$ mit $x, y \in \mathbb{Q}$.

Die Konjugation $\overline{} : E \to E : (x, y) \mapsto (x, -y)$ erfüllt $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$. Für $z \in E$ gilt $\overline{z} = z$ genau dann, wenn $z \in \mathbb{Q}$.

Diese Konstruktion des Körpers E rechtfertigt die Schreibweise $\mathbb{Q}[\sqrt{2}]$.

Rechnen in $\mathbb{Q}[\mathrm{i}]$: Motivation

A133

Für jede rationale Zahl $x \in \mathbb{Q}$ gilt $x^2 \geq 0$, also $x^2 + 1 > 0$. Daher können wir Gleichungen wie $x^2 + 1 = 0$ in $\mathbb{Q}$ zwar formulieren, aber nicht lösen.

Können wir eine Lösung $\mathrm{i} = \sqrt{-1}$ erfinden und damit sinnvoll rechnen? Versuchen wir es! Dazu betrachten wir den Ring / Körper $\mathbb{K} = \mathbb{Z}, \mathbb{Q}$, später $\mathbb{K} = \mathbb{R}$. Wir wünschen uns einen Ring / Körper $\mathbb{K}[\mathrm{i}]$ der Form

$$\mathbb{K}[\mathrm{i}] = \{\, z = x + y\mathrm{i} \mid x, y \in \mathbb{K} \,\}.$$

Wie sehen die Operationen aus? Falls $\mathbb{K}[\mathrm{i}]$ existiert, so erwarten wir:

Vergleich:	$x + y\mathrm{i} = u + v\mathrm{i}$ in $\mathbb{K}[\mathrm{i}]$	$\Leftrightarrow$	$x = u$ und $y = v$ in $\mathbb{K}$
Addition:	$(x + y\mathrm{i}) + (u + v\mathrm{i})$	$=$	$(x + u) + (y + v)\mathrm{i}$
Multiplikation:	$(x + y\mathrm{i}) \cdot (u + v\mathrm{i})$	$=$	$(xu - yv) + (xv + yu)\mathrm{i}$

Über $\mathbb{K} = \mathbb{Z}, \mathbb{Q}$ haben wir zu $z = x + y\mathrm{i}$ das Negative $-z = (-x) + (-y)\mathrm{i}$ und das Konjugierte $\overline{z} = x - y\mathrm{i}$. Dabei gilt $z\overline{z} = x^2 + y^2$, über $\mathbb{Q}$ also

$$\frac{1}{x + y\mathrm{i}} = \frac{1}{x + y\mathrm{i}} \cdot \frac{x - y\mathrm{i}}{x - y\mathrm{i}} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}\mathrm{i}$$

Für jedes Element $x + y\mathrm{i} \neq 0$ gilt $x \neq 0$ oder $y \neq 0$, also $x^2 + y^2 > 0$.

Rechnen in $\mathbb{Q}[\mathrm{i}]$: Konstruktion

A134

kartesisches Produkt

Ist das erlaubt? Wie können wir die Menge $\mathbb{Q}[\mathrm{i}]$ und ihre Operationen einwandfrei erklären? Wir nutzen $\mathbb{Q}^2 \to \mathbb{Q}[\mathrm{i}] : (x, y) \mapsto x + y\mathrm{i}$.

Satz A1H: Konstruktion des Körpers $\mathbb{Q}[\mathrm{i}]$, siehe B137

Auf der Menge $E = \mathbb{Q}^2$ definieren wir Addition und Multiplikation durch

$$+ : E \times E \to E : (x, y) + (u, v) := (x + u, y + v),$$
$$\cdot : E \times E \to E : (x, y) \cdot (u, v) := (xu - yv, xv + yu).$$

Damit ist $(E, +, \cdot)$ ein Körper. Hierin ist $(\mathbb{Q}, +, \cdot)$ ein Teilkörper dank der Einbettung $\mathbb{Q} \hookrightarrow E : x \mapsto (x, 0)$. Wir schreiben kurz $\mathbb{Q} \subset E$.

Im Körper E erfüllt das Element $\mathrm{i} = (0, 1)$ die Eigenschaft $\mathrm{i}^2 = -1$. Jedes Element $z \in E$ schreibt sich eindeutig $z = x + y\mathrm{i}$ mit $x, y \in \mathbb{Q}$.

Die Konjugation $\overline{} : E \to E : (x, y) \mapsto (x, -y)$ erfüllt $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$. Für $z \in E$ gilt $\overline{z} = z$ genau dann, wenn $z \in \mathbb{Q}$.

⚠ Es gibt keine Anordnung auf $\mathbb{Q}[\mathrm{i}]$ zu einem geordneten Körper $(\mathbb{Q}[\mathrm{i}], +, \cdot, \leq)$, denn in jedem geordneten Körper gilt $x^2 \geq 0$ für alle x.

Kurzschreibweise für Produkte und Summen

A135

Monoide Gruppen

Im Folgenden seien a_i Elemente in einem kommutativen Monoid, additiv geschrieben wie $(\mathbb{Q}, +, 0)$ oder multiplikativ wie $(\mathbb{Q}, \cdot, 1)$. Mehrfache Summen und Produkte kürzen wir wie folgt ab:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n := (\ldots(a_1 + a_2) + \ldots) + a_n$$
$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \cdots \cdot a_n := (\ldots(a_1 \cdot a_2) \cdot \ldots) \cdot a_n$$

🙂 Dank Assoziativität können wir beliebig umklammern, dank Kommutativität zudem beliebig umordnen.

Allgemein für die Grenzen $k, \ell \in \mathbb{Z}$ vereinbaren wir:

$$\sum_{i=k}^{\ell} a_i := \begin{cases} a_k + a_{k+1} + \cdots + a_\ell & \text{falls } k \leq \ell, \\ 0 \quad \text{(leere Summe)} & \text{falls } k > \ell. \end{cases}$$
$$\prod_{i=k}^{\ell} a_i := \begin{cases} a_k \cdot a_{k+1} \cdot \cdots \cdot a_\ell & \text{falls } k \leq \ell, \\ 1 \quad \text{(leeres Produkt)} & \text{falls } k > \ell. \end{cases}$$

Kurzschreibweise für Produkte und Summen

A136

Monoide Gruppen

Sei $n \in \mathbb{N}$. Im Sonderfall $a_1 = a_2 = a_3 = \cdots = a_n =: a$ erhalten wir

$$a \cdot n := \sum_{i=1}^{n} a = \begin{cases} 0 \quad \text{(leere Summe)} & \text{falls } n = 0, \\ a + a + \cdots + a \quad \text{(mit } n \text{ Summanden)} & \text{falls } n \geq 1. \end{cases}$$
$$a^n := \prod_{i=1}^{n} a = \begin{cases} 1 \quad \text{(leeres Produkt)} & \text{falls } n = 0, \\ a \cdot a \cdot \cdots \cdot a \quad \text{(mit } n \text{ Faktoren)} & \text{falls } n \geq 1. \end{cases}$$

🙂 Das stimmt mit unserer bisherigen Definition A1A überein.
Ist $-a$ das Negative zu a, so setzen wir $a \cdot (-n) := (-a) \cdot n$.
Ist a^{-1} das Inverse zu a, so setzen wir $a^{-n} := (a^{-1})^n$.

Ist $I = \{i_1, i_2, \ldots, i_n\}$ eine n–elementige Menge, so schreiben wir

$$\sum_{i \in I} a_i := \sum_{k=1}^{n} a_{i_k} \quad \text{und} \quad \prod_{i \in I} a_i := \prod_{k=1}^{n} a_{i_k}.$$

Eine Umnummerierung der Elemente ändert das Ergebnis nicht.

Sei J eine Menge und $I \subseteq J$ endlich, sodass $a_i = 0$ für alle $i \in J \setminus I$. Dann definieren wir $\sum_{i \in J} a_i := \sum_{i \in I} a_i$ als endliche Summe wie oben.

Polynome

Sei K ein Körper, wie $\mathbb{Q}$, oder allgemein ein kommutativer Ring, wie $\mathbb{Z}$. Wir betrachten Polynome in der Unbestimmten X mit Koeffizienten in K:

$$K[X] = \left\{ P = p_0 + p_1 X + \cdots + p_n X^n \;\middle|\; n \in \mathbb{N},\ p_0, p_1, \ldots, p_n \in K \right\}.$$

Wir schreiben kurz $P = \sum_{i=0}^{n} p_i X^i$. Im Falle $p_n \neq 0$ ist $\deg(P) := n$ der Grad von P und $\operatorname{lc}(P) := p_n$ der Leitkoeffizient. Wir schreiben noch kürzer $P = \sum_i p_i X^i$ und vereinbaren $p_i = 0$ für alle $i < 0$ und alle $i > n$.

Im Sonderfall $P = 0$ setzen wir $\deg(0) := -\infty$ und $\operatorname{lc}(0) := 0$.
Wir schreiben $K[X]_n$ und $K[X]_{\leq n}$ und $K[X]_{<n}$ für die Menge der Polynome $P \in K[X]$ vom Grad genau / höchstens / kleiner n

Wir übertragen die Operationen von K auf $K[X]$:

Vergleich: $\sum_i p_i X^i = \sum_i q_i X^i$ in $K[X] \;\Leftrightarrow\; p_i = q_i$ in K für alle i
Addition: $\left[\sum_i p_i X^i\right] + \left[\sum_i q_i X^i\right] = \sum_i (p_i + q_i) X^i$
Multiplikation: $\left[\sum_i p_i X^i\right] \cdot \left[\sum_j q_j X^j\right] = \sum_k r_k X^k,\ r_k = \sum_{i+j=k} p_i q_j$

Die letzte Summe durchläuft alle Paare $(i, j) \in \mathbb{N}^2$ mit $i + j = k$.

Polynome

Ein **Integritätsring**, kurz IRing, ist ein kommutativer Ring $(K, +, 0, \cdot, 1)$ mit $0 \neq 1$ sodass für alle $a, b \in K$ gilt: Aus $a \neq 0$ und $b \neq 0$ folgt $a \cdot b \neq 0$.
Das heißt: Ein Produkt ab ist genau dann null, wenn ein Faktor null ist.
Multiplikation mit $a \neq 0$ ist kürzbar: $ab = ac \;\Leftrightarrow\; a(b - c) = 0 \;\Leftrightarrow\; b = c$

Satz A1I: der Polynomring $K[X]$

Ist $(K, +, 0, \cdot, 1)$ ein kommutativer Ring, so auch $(K[X], +, 0, \cdot, 1)$.
Ist zudem K ein Integritätsring, so auch $K[X]$; genauer gilt nämlich

$$\begin{aligned} \deg(P \cdot Q) &= \deg(P) + \deg(Q) && \text{in } \mathbb{N} \cup \{-\infty\}, \\ \operatorname{lc}(P \cdot Q) &= \operatorname{lc}(P) \cdot \operatorname{lc}(Q) && \text{in } K. \end{aligned}$$

Jedes Polynom $P(X) = \sum_{i=0}^{n} p_i X^i$ in $K[X]$ definiert seine zugehörige Polynomfunktion $f_P : K \to K : x \mapsto P(x) = \sum_{i=0}^{n} p_i x^i$ durch Einsetzen.
Wir unterscheiden also sorgsam den formalen Ausdruck $P(X) \in K[X]$ und seine Anwendung $f_P : x \mapsto P(x)$ auf Elemente $x \in K$. Über einem unendlichen Körper wie $\mathbb{Q}$ besteht kein großer Unterschied, über einem endlichen Körper hingegen ist die Unterscheidung ganz wesentlich!

Bruchkörper und gebrochen-rationale Funktionen

Sei R ein Integritätsring, etwa $\mathbb{Z}$ oder $\mathbb{Q}[X]$. Wie / Können wir mit Brüchen sinnvoll rechnen? Versuchen wir es! Dazu betrachten wir

$$K = \operatorname{Frac}(R) := \left\{ q = [a/b] \;\middle|\; a, b \in R,\ b \neq 0 \right\}.$$

Auf dieser Menge K vereinbaren wir die folgenden Operationen:

$$\begin{aligned} \text{Vergleich:} \quad [a/b] = [c/d] \text{ in } K &\;\Leftrightarrow\; ad = cb \text{ in } R \\ \text{Addition:} \quad [a/b] + [c/d] &= [(ad + cb)/(bd)] \\ \text{Negation:} \quad -[a/b] &= [-a/b] \\ \text{Multiplikation:} \quad [a/b] \cdot [c/d] &= [(ac)/(bd)] \\ \text{Inversion:} \quad [a/b]^{-1} &= [b/a] \quad \text{falls } a \neq 0 \end{aligned}$$

Wir haben die Einbettung $R \hookrightarrow K : a \mapsto [a/1]$ und schreiben kurz $R \subseteq K$.

Satz A1J: Bruchkörper zu einem Integritätsring

Ist $(R, +, 0, \cdot, 1)$ ein Integritätsring, so ist $(K, +, 0, \cdot, 1)$ ein Körper.

🙂 So erhalten wir insbesondere die rationalen Zahlen $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z})$ und die gebrochen-rationalen Funktionen $\mathbb{Q}(X) = \operatorname{Frac}(\mathbb{Q}[X])$.

Bruchkörper und gebrochen-rationale Funktionen

Die Erweiterung $\mathbb{Q} \supset \mathbb{Z}$ erhalten wir durch die Bildung von Brüchen:

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

Auch $\mathbb{Q}(X) \supset \mathbb{Q}[X]$ erhalten wir durch die Bildung von Brüchen:

$$\mathbb{Q}(X) = \left\{ \frac{A}{B} = \frac{a_m X^m + \cdots + a_1 X + a_0}{b_n X^n + \cdots + b_1 X + b_0} \;\middle|\; A, B \in \mathbb{Q}[X],\ B \neq 0 \right\}$$

Genau so kennen Sie diese Brüche aus der Schule, dort allerdings eher pragmatisch-experimentell durch *learning by doing*. Hier schauen wir die Voraussetzungen genauer an und entdecken ein allgemeines Prinzip:

Ist R ein Integritätsring, also ein kommutativer Ring ohne Nullteiler, so können wir den Bruchkörper $K = \operatorname{Frac}(R)$ wie oben konstruieren. Das ist eine vollkommen natürliche und allgemeine Konstruktion.

Alles liegt explizit vor, Sie können es nachrechnen! Dahinter stecken jedoch einige scharfsinnige Fragen: Ist der Vergleich „=“ wirklich eine Äquivalenzrelation, also reflexiv, symmetrisch und vor allem: transitiv? Sind die Operationen $+$ und $\cdot$ wohldefiniert, also unabhängig von den Repräsentanten? Wir kommen darauf später noch genauer zurück.

Arithmetik ganzer Zahlen: Division mit Rest

A201

In den ganzen Zahlen $\mathbb{Z}$ haben wir neben den drei Grundrechenarten $+, -, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ auch die **Division mit Rest**. Einfaches Beispiel:

„Teile 372 ganzzahlig durch 25“: $\quad 372 = 25 \cdot q + r = 25 \cdot 14 + 22$

Gelingt das immer? Ist das Ergebnis eindeutig? Glücklicherweise ja!

Satz A2A: euklidische / ganzzahlige Division mit Rest

Sei $b \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ und $\mathbb{Z}_b = \{\, r \in \mathbb{Z} \mid 0 \leq r < |b| \,\} = \{0, 1, \dots, |b|-1\}$.
Jede ganze Zahl $a \in \mathbb{Z}$ schreibt sich eindeutig als **Division mit Rest**

$$a = bq + r \quad \text{mit } q \in \mathbb{Z} \text{ und } r \in \mathbb{Z}_b.$$

Wir nennen diese Zerlegung die **euklidische Division** von a durch b mit **Quotient** q und **Rest** r. Dies definiert die beiden Operationen

$$(\mathrm{quo}, \mathrm{rem}) \,:\, \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{N} \,:\, (a, b) \mapsto (q, r).$$

Wir schreiben kurz $q = a \operatorname{quo} b$ und $r = a \operatorname{rem} b$.

Übung: M Wie beweisen Sie dies? I Wie berechnen Sie es effizient?

Arithmetik ganzer Zahlen: Division mit Rest

A202
Erläuterung

Wenn Sie bereits Erfahrung oder gar Routine haben, dann werden Sie ausrufen „Das ist klar per Induktion!“. Wenn Sie Sorgfalt und Technik anfangs noch üben wollen, so ist dies eine wunderbare Gelegenheit.

Aufgabe: Beweisen Sie Existenz und Eindeutigkeit der Lösung (q, r).

Lösung: Wir fixieren den Divisor $b \in \mathbb{Z} \setminus \{0\}$. Zur Vereinfachung dürfen wir $b > 0$ annehmen, denn $a = bq + r = (-b)(-q) + r$.

Existenz: Für $a = 0$ genügt $(q, r) = (0, 0)$. Ist $a = bq + r$ mit $q \in \mathbb{N}$ und $r \in \mathbb{Z}_b$ gegeben, dann folgt $a + 1 = bq + (r + 1) = bq' + r'$: Für $r + 1 < b$ wähle $(q', r') = (q, r + 1)$. Für $r + 1 = b$ wähle $(q', r') = (q + 1, 0)$. Voilà.

Für negatives $a \in \mathbb{Z}_{<0}$ haben wir $-a = bq + r$ mit $q \in \mathbb{N}$ und $r \in \mathbb{Z}_b$, also $a = b(-q) + (-r)$. Im Falle $r \neq 0$ also $a = b(-q - 1) + (b - r)$.

Eindeutigkeit: Sei $a = bq + r = bq' + r'$ mit $q, q' \in \mathbb{Z}$ und $r, r' \in \mathbb{Z}_b$.
Subtraktion ergibt $0 = (bq' + r') - (bq + r') = b(q' - q) + (r' - r)$.
Also teilt b die Differenz $r' - r \in \{1 - b, \dots, -1, 0, 1, \dots, b - 1\}$.
Daraus folgt $r' - r = 0$, also $r' = r$ und schließlich $q' = q$. QED

Arithmetik ganzer Zahlen: Zifferndarstellung in Basis B

A203

Satz A2B: Zifferndarstellung in Basis B

Wir fixieren $B \in \mathbb{N}_{\geq 2}$, etwa $B = 2$ (binär) oder $B = 10$ (dezimal).
Als Ziffernmenge nutzen wir entsprechend $\mathbb{Z}_B = \{0, 1, \dots, B - 1\}$.
Jede natürliche Zahl $n \in \mathbb{N}$ schreibt sich eindeutig in Basis B gemäß

$$n = n_{\ell-1} B^{\ell-1} + n_{\ell-2} B^{\ell-2} + \cdots + n_2 B^2 + n_1 B + n_0$$

mit Länge $\ell \in \mathbb{N}$ und Ziffern $n_0, n_1, n_2, \dots, n_{\ell-2}, n_{\ell-1} \in \mathbb{Z}_B$, $n_{\ell-1} \neq 0$.

$$\text{natürliche Zahlen} \quad \mathbb{N} \underset{\sigma_B}{\overset{\rho_B}{\underset{\cong}{\rightleftarrows}}} \mathbb{Z}_B^{(\mathbb{N})} \quad \text{Zifferndarstellung}$$

$$n_{\ell-1} B^{\ell-1} + \cdots + n_1 B + n_0 \;\longmapsto\; (n_0, n_1, \dots, n_{\ell-1}, 0, 0, 0, \dots)$$

Diese Bijektion nennen wir die **Zifferndarstellung in Basis** B.

Übung: M Wie erklären Sie die schriftliche Addition und Multiplikation?
I Wie implementieren Sie diese Operationen möglichst effizient?
Überraschung: Die Schulmethode ist nicht die schnellste!

Arithmetik ganzer Zahlen: Zifferndarstellung in Basis B

A204
Erläuterung

Hier ist $\mathbb{Z}_B^{(\mathbb{N})} = \{\, f : \mathbb{N} \to \mathbb{Z}_B \mid \mathrm{supp}(f) \text{ endlich} \,\}$ die Menge aller Folgen f mit endlichem Träger, also $f_k = 0$ für alle $k \geq \ell$ ab einem gewissen Index $\ell \in \mathbb{N}$; dies entspricht der endlichen Folge $(f_0, f_1, \dots, f_{\ell-1})$ in $\mathbb{Z}_B^\ell$.

Zur Basis $B = 10$ ist dies die allgegenwärtige Dezimaldarstellung, die sie seit der Grundschule kennen und täglich überall verwenden. Sie benötigen dazu nur zehn Ziffern: $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Das ist wunderbar handlich und bequem. Im Gegensatz dazu ist die römische Zahlschreibweise hoffnungslos unhandlich und verwirrend.

Binäre Computer nutzen die Basis $B = 2$ und kommen daher bereits mit zwei Ziffern aus: $\mathbb{Z}_2 = \{0, 1\}$. Das ist minimalistisch und effizient. Für größere Speichereinheiten fasst man je 8 (oder 16, 32) Bits zu einem Wort zusammen und rechnet dann zur Basis $B = 2^8$ (oder 2^{16}, 2^{32}). Auch das Hexadezimalsystem zur Basis $B = 16$ ist gebräuchlich.

Die Reihenfolge der Ziffern rechts-nach-links oder links-nach-rechts aufsteigend ist eine Konvention, wie so oft: wichtig aber willkürlich. Im Computer-Jargon sagt man *big-endian* und *little-endian*.

Arithmetik ganzer Zahlen: schriftliche Addition

Übung: Wie funktioniert die schriftliche Addition $\oplus : \mathbb{Z}_B^{(\mathbb{N})} \times \mathbb{Z}_B^{(\mathbb{N})} \to \mathbb{Z}_B^{(\mathbb{N})}$? Wie viele Rechenschritte sind nötig? Schreiben Sie es explizit aus!

Lösung: Als **elementaren Rechenschritt** nutzen wir die Addition $a + b$ von zwei Ziffern $a, b \in \mathbb{Z}_B$ und einem **Übertrag** $c \in \{0, 1\}$, engl. *carry*:

$$\begin{aligned} \mathrm{Add} : \mathbb{Z}_B \times \mathbb{Z}_B \times \{0,1\} &\to \{0,1\} \times \mathbb{Z}_B \\ (a, b, c) &\mapsto (d, e) \quad \text{mit } a + b + c = dB + e \end{aligned}$$

Algo A2C: schriftliche Addition in Basis B

Eingabe: zwei Zifferndarstellungen $x, y \in \mathbb{Z}_B^\ell$
Ausgabe: die Darstellung $z = x \oplus y \in \mathbb{Z}_B^{\ell+1}$ der Summe

1: $c \leftarrow 0$
2: for k from 0 to $\ell - 1$ do $(c, z_k) \leftarrow \mathrm{Add}(x_k, y_k, c)$
3: return $z = (z_0, z_1, \ldots, z_{\ell-1}, c)$

🙂 Dieser Algorithmus verwendet genau ℓ Ziffernoperationen (hier Add). Besser geht es nicht: Mindestens ℓ Schritte sind nötig allein zum Lesen.

Arithmetik ganzer Zahlen: schriftliche Multiplikation

Wie funktioniert die schriftliche Multiplikation $\odot : \mathbb{Z}_B^{(\mathbb{N})} \times \mathbb{Z}_B^{(\mathbb{N})} \to \mathbb{Z}_B^{(\mathbb{N})}$? Wie viele Rechenschritte sind nötig? Schreiben Sie es explizit aus!

(1) Als **elementaren Rechenschritt** nutzen wir die Multiplikation $a \cdot b$ von zwei Ziffern $a, b \in \mathbb{Z}_B$ und zudem einem **Übertrag** $c \in \mathbb{Z}_B$:

$$\begin{aligned} \mathrm{Mul} : \mathbb{Z}_B \times \mathbb{Z}_B \times \mathbb{Z}_B &\to \mathbb{Z}_B \times \mathbb{Z}_B \\ (a, b, c) &\mapsto (d, e) \quad \text{mit } a \cdot b + c = dB + e \end{aligned}$$

Algo A2D: kleine Multiplikation in Basis B

Eingabe: eine Zifferndarstellung $x \in \mathbb{Z}_B^\ell$ und $y \in \mathbb{Z}_B$
Ausgabe: die Darstellung $z = x \odot y \in \mathbb{Z}_B^{\ell+1}$ des Produkts

1: $c \leftarrow 0$
2: for k from 0 to $\ell - 1$ do $(c, z_k) \leftarrow \mathrm{Mul}(x_k, y, c)$
3: return $z = (z_0, z_1, \ldots, z_{\ell-1}, c)$

🙂 Dieser Algorithmus verwendet genau ℓ Ziffernoperationen (hier Mul). Besser geht es nicht: Mindestens ℓ Schritte sind nötig allein zum Lesen.

Arithmetik ganzer Zahlen: schriftliche Multiplikation

(2) Die Multiplikation $x \odot y$ setzen wir aus $x \odot y_k$ zusammen mit der Verschiebung $\mathrm{Shift} : \mathbb{Z}_B^{(\mathbb{N})} \to \mathbb{Z}_B^{(\mathbb{N})} : (f_0, f_1, f_2, \ldots) \mapsto (0, f_0, f_1, f_2, \ldots)$.

Algo A2E: schriftliche Multiplikation in Basis B

Eingabe: zwei Zifferndarstellungen $x \in \mathbb{Z}_B^p$ und $y \in \mathbb{Z}_B^q$
Ausgabe: die Darstellung $z = x \odot y \in \mathbb{Z}_B^{p+q+1}$ des Produkts

1: $z \leftarrow 0$
2: for k from 0 to $q - 1$ do $z \leftarrow z \oplus \mathrm{Shift}^k(x \odot y_k)$
3: return z

🙂 ☹ Dieser Algorithmus verwendet pq mal Add und pq mal Mul. Speziell für $B = 2$ ist $x \odot y_k$ trivial, es bleiben nur die pq Additionen. Das ist für kleine Eingabelängen p und q noch ausreichend effizient, aber für große Eingaben wird diese Methode spürbar zeitaufwändig.

⚠ Die schriftliche Addition hat nur **linearen** Zeitaufwand (optimal), die schriftliche Multiplikation hingegen hat **quadratischen** Aufwand. Können wir das Produkt $x \odot y$ raffinierter und schneller berechnen?

Arithmetik ganzer Zahlen: schriftliche Multiplikation

Übung: Weisen Sie nach, dass die obigen Algorithmen korrekt sind, also tatsächlich Summe und Produkt in $\mathbb{N}$ richtig abbilden. Ausführlich:

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{+} & \mathbb{N} \\ {\scriptstyle \rho \cong \sigma} \downarrow\uparrow & & \downarrow\uparrow {\scriptstyle \rho \cong \sigma} \\ \mathbb{Z}_B^{(\mathbb{N})} \times \mathbb{Z}_B^{(\mathbb{N})} & \xrightarrow[(x,y)\mapsto x \oplus y]{\oplus} & \mathbb{Z}_B^{(\mathbb{N})} \end{array} \qquad \begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{\cdot} & \mathbb{N} \\ {\scriptstyle \rho \cong \sigma} \downarrow\uparrow & & \downarrow\uparrow {\scriptstyle \rho \cong \sigma} \\ \mathbb{Z}_B^{(\mathbb{N})} \times \mathbb{Z}_B^{(\mathbb{N})} & \xrightarrow[(x,y)\mapsto x \odot y]{\odot} & \mathbb{Z}_B^{(\mathbb{N})} \end{array}$$

Übung: Implementieren Sie dies in Ihrer Lieblingsprogrammiersprache. Testen Sie es ausführlich auf zahlreichen, immer größeren Beispielen. Wie macht sich die lineare vs quadratische Laufzeit bemerkbar?

Übung: Formulieren und implementieren Sie die euklidische Division ebenso als Algorithmus $(x, y) \mapsto (q, r)$. Wer's kann, verdient Respekt!

🙂 Bibliotheken wie GMP (*GNU Multiple Precision Arithmetic Library*, `gmplib.org`) implementieren diese Arithmetik – hochgradig optimiert!

Schnelle Multiplikation nach Karatsuba

Even fairly good students, when they have obtained the solution of the problem and written down neatly the argument, shut their books and look for something else. Doing so, they miss an important and instructive phase of the work. [...]
A good teacher should understand and impress on his students the view that no problem whatever is completely exhausted.
George Pólya (1887–1985), *How to Solve It* (1945)

Um 1956 formulierte Andrey Kolmogorov seine Vermutung, dass die Multiplikation ganzer Zahlen nicht schneller als quadratisch gelingen kann. Im Herbst 1960 organisierte er an der Lomonossov–Universität in Moskau ein Seminar zur Kybernetik und Fragen der Komplexität.

Der 23-jährige Anatoly Karatsuba widerlegte Kolmogorovs Vermutung innerhalb einer Woche: Er fand die weltweit erste schnelle Multiplikation!

Damit begann eine neue Forschungsrichtung *Fast Arithmetic*, die seither sehr aktiv ist und sensationelle Erfolge erreicht hat. Diese Grundlagenforschung steckt in allen modernen Computern.

📖 Gathen, Gerhard: *Modern Computer Algebra.* Cambridge CUP 2013

Schnelle Multiplikation nach Karatsuba

Wieviel Zeit kostet die Verknüpfung von Zahlen $a, b \in \mathbb{N}$ mit $\leq \ell$ Ziffern?

- Addition? Der Aufwand ist $\leq \text{const} \cdot \ell$, und linear ist optimal.
- Multiplikation? Aufwand $\leq \text{const} \cdot \ell^2$. Geht es schneller? Ja!

Zur Multiplikation vorgelegt seien $a, b \in \mathbb{N}$ mit $\leq 2n$ Ziffern in Basis B:

$$a = a_0 + a_1 B^n \quad \text{und} \quad b = b_0 + b_1 B^n \quad \text{mit} \quad a_0, a_1, b_0, b_1 < B^n$$
$$a \cdot b = (a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0) B^n + (a_1 \cdot b_1) B^{2n}$$

Wir wollen hierzu das Produkt berechnen: Dies gelingt wie gezeigt mit vier Multiplikationen der Länge n. So weit, so klar, so langweilig. Karatsubas genialer Trick benötigt statt vier nur drei Multiplikationen:

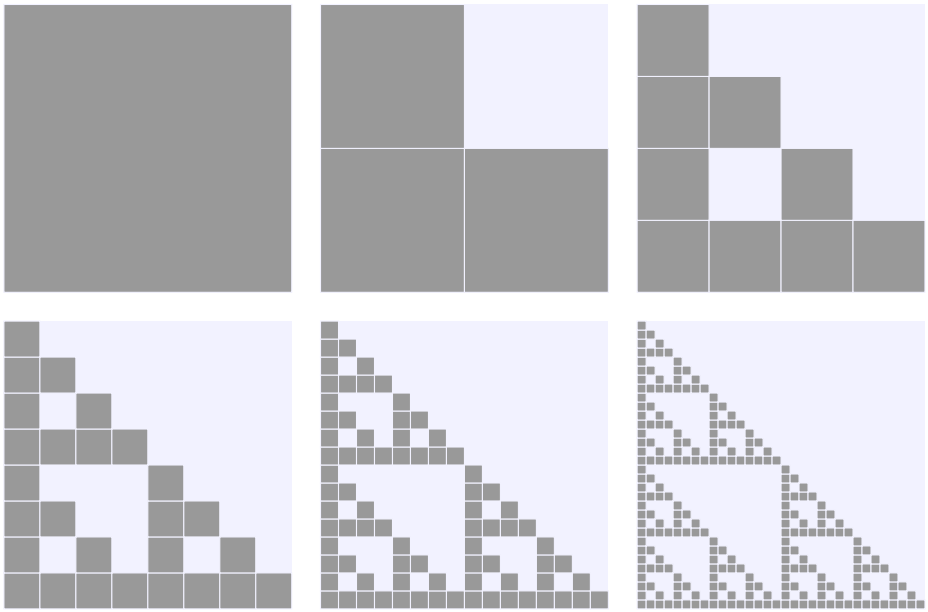
$$s := a_0 \cdot b_0, \quad t := a_1 \cdot b_1, \quad u := (a_0 + a_1) \cdot (b_0 + b_1) - s - t$$

Es gilt $u = a_0 \cdot b_1 + a_1 \cdot b_0$, somit erhalten wir $a \cdot b = s + uB^n + tB^{2n}$. Somit genügen drei Multiplikationen und zwei (billige!) Subtraktionen. Das macht sich bezahlt: Wir können diesen Trick rekursiv anwenden!

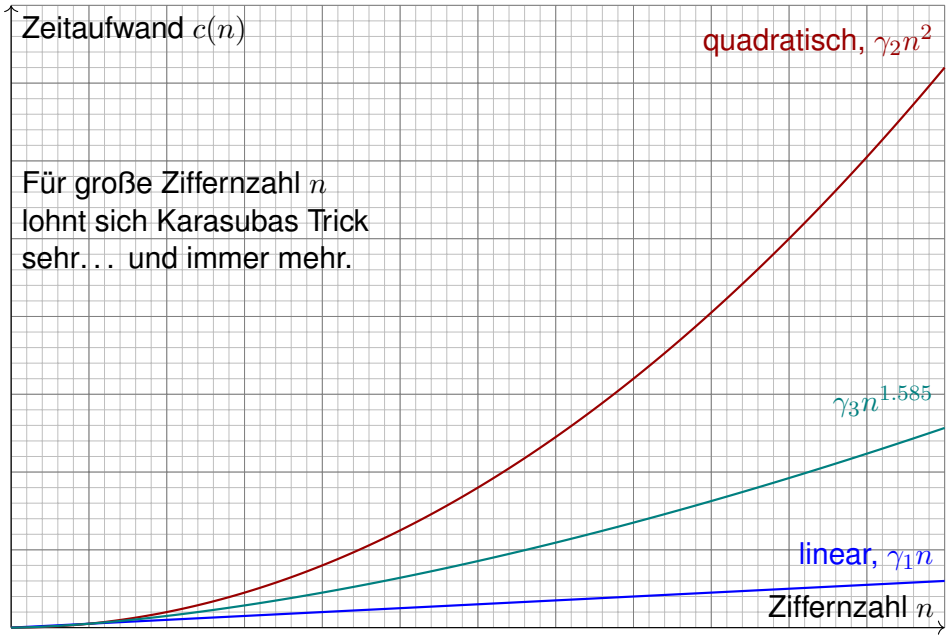
🙂 Der Aufwand beträgt nur $c(2n) \leq 3c(n) + \alpha n$.

Karatsubas Multiplikation ist subquadratisch.

Visualisierung der Rekursion: Kosten (grau) und Ersparnis (blau).



Karatsubas Multiplikation ist subquadratisch.



Schnelle Multiplikation nach Karatsuba

Karatsubas Idee ist ein Musterbeispiel des Prinzips **Teile und herrsche**. Wir zerlegen ein großes Problem in kleinere, leichtere Teilprobleme.

Seine Methode ist ebenso einfach wie genial: Zu multiplizieren seien $a, b \in \mathbb{N}$ mit $a, b < B^{2n}$. Diese sind gegeben als Zifferndarstellungen in Basis B. Wir zerlegen $a = a_0 + a_1 B^n$ und $b = b_0 + b_1 B^n$ in die n niedrigen Ziffern a_0, b_0 und die n hohen Ziffern a_1, b_1. Das Produkt

$$a \cdot b = (a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0) B^n + (a_1 \cdot b_1) B^{2n}$$

benötigt augenscheinlich vier Multiplikationen. Es geht aber besser: Karatsubas genialer Trick benötigt statt vier nur drei Multiplikationen!

$$s \leftarrow a_0 \cdot b_0, \quad t \leftarrow a_1 \cdot b_1, \quad u \leftarrow (a_0 + a_1) \cdot (b_0 + b_1) - s - t$$

Es gilt $u = a_0 \cdot b_1 + a_1 \cdot b_0$, somit erhalten wir $ab = s + uB^n + tB^{2n}$.

🙂 Auf den ersten Blick scheint das keine große Ersparnis zu sein. Im Gegenteil können die ungewohnten Formeln den Anschein erwecken, Karatsubas Methode wäre sogar komplizierter als die Schulmethode. Wir rechnen den Zeitaufwand und die Ersparnis daher sorgfältig nach.

Schnelle Multiplikation nach Karatsuba

Sei $c(n)$ die maximale Laufzeit für Karatsubas Multiplikation bei n Ziffern. Wir messen sie zum Beispiel in Sekunden auf einem Referenzcomputer, noch besser hardwareunabhängig als Anzahl der Ziffernoperationen. Die Umrechnung ist dann nur ein Faktor: die Hardwarekonstante.

Wir wenden Karatsubas Multiplikation rekursiv an, daher finden wir:

$$c(2n) \leq 3c(n) + \alpha n$$

Für eine Multiplikation der Länge $2n$ benötigen wir drei Multiplikationen der Länge n, jeweils mit Aufwand $c(n)$, sowie vier Additionen und zwei zusätzliche Subtraktionen, alle mit linearem Aufwand $\leq \alpha n$, $\alpha \in \mathbb{R}_{\geq 0}$.

Alle Ziffern liegen bereits im Speicher vor, die Aufteilung in niedrige und hohe Ziffern kostet nahezu nichts. Multiplikation mit B^n und B^{2n} ist nur eine Verschiebung der Ziffern, also ebenso vernachlässigbar billig.

🙂 Diese rekursive, implizite Ungleichung können wir explizit auflösen! Der folgende Satz zeigt, dass Karatsubas Algorithmus tatsächlich eine wesentliche Verbesserung ist. Der Satz ist ein einfacher Spezialfall des **Master Theorems**, das rekursive Laufzeitanalysen zusammenfasst.

Karatsubas Multiplikation ist subquadratisch.

Satz A2F: Zeitaufwand von Karatsubas Multiplikation

Vorgelegt sei $c : \mathbb{N} \to \mathbb{R}$ monoton wachsend. Zudem gelte

(1) $\quad c(2n) \leq 3c(n) + \alpha n \quad$ und $\quad c(1) \leq \beta$

für alle $n \in \mathbb{N}$. Hierbei sind $\alpha, \beta \in \mathbb{R}_{\geq 0}$ Konstanten. Dann folgt:

(2) $\quad c(2^k) \leq 3^k(\alpha + \beta) - 2^k \alpha \quad$ für alle $k \in \mathbb{N}$

(3) $\quad c(n) < 3(\alpha + \beta)\, n^{\log_2(3)} \quad$ für alle $n \in \mathbb{N}$

Dank $\log_2(3) \approx 1.585 < 2$ ist dies wesentlich besser als $\text{const} \cdot n^2$.

Beweis: Ungleichung (2) folgt per Induktion über k. Die Abschätzung (3) folgt aus der Monotonie von c dank $n \leq 2^k$ für $k = \lceil \log_2 n \rceil < 1 + \log_2 n$.

🙂 Stehen die Formeln schon da, so ist ihr formaler Beweis relativ leicht: Es gelingt mit vollständiger Induktion und sorgfältigem Nachrechnen.

🙂 Geeignete Ungleichungen zu finden, ist schwieriger; es gelingt gut durch Ausprobieren kleiner Fälle bis zum Auffinden eines Musters.

Karatsubas Multiplikation ist subquadratisch.

Aufgabe: Führen Sie den skizzierten Beweis des Satzes aus.

Lösung: Ungleichung (2) gilt für $k = 0$, denn $c(0) = \beta = 3(\alpha + \beta) - 2\alpha$. Wir nehmen an, die Ungleichung (2) gilt für k, und zeigen sie für $k + 1$:

$$\begin{aligned} c(2^{k+1}) &\overset{(1)}{\leq} 3c(2^k) + \alpha 2^k \\ &\overset{(2)}{\leq} 3^{k+1}(\alpha + \beta) - 3 \cdot 2^k \alpha + 2^k \alpha \\ &= 3^{k+1}(\alpha + \beta) - 2^{k+1} \alpha \end{aligned}$$

Die vereinfachende Abschätzung (3) für alle $n \in \mathbb{N}$ folgt aus $n \leq 2^k$ für $k = \lceil \log_2 n \rceil < 1 + \log_2 n$. Dank der Monotonie von c gilt:

$$\begin{aligned} c(n) \;\leq\; c(2^k) &\overset{(2)}{\leq} 3^k(\alpha + \beta) - 2^k \alpha \;<\; 3^k(\alpha + \beta) \\ &< 3 \cdot 3^{\log_2(n)}(\alpha + \beta) \;=\; 3(\alpha + \beta)\, n^{\log_2(3)} \end{aligned}$$

Damit sind beide Ungleichungen des Satzes bewiesen. QED

🙂 Allein die Konstanten α und β hängen von der Implementierung ab, von der Geschwindigkeit der Hardware, von lokalen Optimierungen, etc. Der entscheidende Exponent $\log_2(3) \approx 1.585$ hingegen ist immer gleich.

Teilbarkeit in ganzen Zahlen

A217

Wir wollen in den ganzen Zahlen $\mathbb{Z}$ effizient rechnen. Ein typisches Problem ist, den größten gemeinsamen Teiler ggT zu bestimmen.

$$\mathrm{GT}(18,24) = \{\pm1,\pm2,\pm3,\pm6\},\ \mathrm{GGT}(18,24) = \{\pm6\},\ \mathrm{ggT}(18,24) = 6$$

Wir benötigen eine präzise Definition und effiziente Algorithmen.

Definition A2G: größter gemeinsamer Teiler in $\mathbb{Z}$

Seien $a, b \in \mathbb{Z}$. Wir sagen a **teilt** b **in** $\mathbb{Z}$, oder b ist ein Vielfaches von a, falls es $a' \in \mathbb{Z}$ gibt mit $aa' = b$. Dies schreiben wir $a \mid_{\mathbb{Z}} b$ oder kurz $a \mid b$. Andernfalls sagen wir a teilt nicht b, geschrieben $a \nmid_{\mathbb{Z}} b$ oder kurz $a \nmid b$.

Die Menge der **gemeinsamen Teiler** von $a_1, \ldots, a_n \in \mathbb{Z}$ ist

$$\mathrm{GT} = \mathrm{GT}_{\mathbb{Z}}(a_1, \ldots, a_n) := \{\, t \in \mathbb{Z} \mid t \mid_{\mathbb{Z}} a_1, \ldots, t \mid_{\mathbb{Z}} a_n \,\}.$$

Die Menge der **größten gemeinsamen Teiler** definieren wir durch

$$\mathrm{GGT} = \mathrm{GGT}_{\mathbb{Z}}(a_1, \ldots, a_n) := \{\, t \in \mathrm{GT} \mid \forall s \in \mathrm{GT} : s \mid_{\mathbb{Z}} t \,\}.$$

Ist GGT nicht leer, so gilt $\mathrm{GGT} = \{\pm g\}$, und wir setzen $\mathrm{ggT} := |g|$.

Teilbarkeit in ganzen Zahlen

A218
Erläuterung

⚠ Beachten Sie, dass „größer“ im Sinne der Teilbarkeit definiert ist: Ein ggT von $a_1, \ldots, a_n$ ist ein Teiler, der von allen Teilern geteilt wird.

Im geordneten Ring $(\mathbb{Z}, +, \cdot, \leq)$ ist der positive ggT das größte Element bezüglich $\leq$, das ist jedoch eine Folgerung und nicht Teil der Definition.

(0) Teilbarkeit ist eine (Prä)Ordnung. Das heißt, für alle $a, b, c \in \mathbb{Z}$ gilt:

Reflexivität,	**Refl**$(\mathbb{Z}, \mid)$:	Es gilt $a \mid a$.
Antisymmetrie,	**Asym**$(\mathbb{Z}, \mid)$:	Aus $a \mid b$ und $b \mid a$ folgt $a = \pm b$.
Transitivität,	**Tran**$(\mathbb{Z}, \mid)$:	Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.

(1) Die Ordnung $\mid$ ist partiell, nicht total, zum Beispiel $2 \nmid 3$ und $3 \nmid 2$. Es gilt $1 \mid a$ und $a \mid 0$, das heißt 1 ist kleinstes Element und 0 ist größtes. Es gilt $0 \mid a$ genau dann wenn $a = 0$, und $a \mid 1$ genau dann wenn $a = \pm 1$.

(2) Teilbarkeit ist verträglich mit Addition und Multiplikation:
Aus $a \mid b$ und $a \mid c$ folgt $a \mid b + c$, allgemein $a \mid bu + cv$ für alle $u, v \in \mathbb{Z}$.
Aus $a \mid b$ und $c \mid d$ folgt $ac \mid bd$, insbesondere dank $c \mid c$ auch $ac \mid bc$.
Kürzungsregel: Für $c \neq 0$ sind $ac \mid bc$ und $a \mid b$ äquivalent.

Übung: Beweisen Sie die Aussagen (0–2).

Der euklidische Algorithmus

A219

Für alle $a, b, c \in \mathbb{Z}$ gilt $\mathrm{GT}(a, b) = \mathrm{GT}(b, a - bc)$ und $\mathrm{GGT}(a, 0) = \{\pm a\}$.

$$\mathrm{GT}\begin{bmatrix}138\\24\end{bmatrix} = \mathrm{GT}\begin{bmatrix}24\\18\end{bmatrix} = \mathrm{GT}\begin{bmatrix}18\\6\end{bmatrix} = \mathrm{GT}\begin{bmatrix}6\\0\end{bmatrix} \quad\Longrightarrow\quad \mathrm{ggT}\begin{bmatrix}138\\24\end{bmatrix} = 6$$

Das beschert uns folgenden Satz mit Algorithmus:

Satz A2H: Euklid in $\mathbb{Z}$

(1) Zu je zwei ganzen Zahlen $a, b \in \mathbb{Z}$ existiert ein ggT in $\mathbb{Z}$.
(2) Der folgende Algorithmus berechnet den positiven ggT.

Algo A2H: Berechnung des ggT in $\mathbb{Z}$

Eingabe: zwei ganze Zahlen $a_0, b_0 \in \mathbb{Z}$
Ausgabe: der größte gemeinsame Teiler $a = \mathrm{ggT}(a_0, b_0)$

1: $\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix}a_0\\b_0\end{smallmatrix}\right]$ // $\mathrm{GT}(a, b) = \mathrm{GT}(a_0, b_0)$
2: while $b \neq 0$ do $\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix}b\\a \operatorname{rem} b\end{smallmatrix}\right]$ // $\mathrm{GT}(a, b) = \mathrm{GT}(b, a - qb)$
3: return $|a|$ // $\mathrm{GGT}(a, 0) = \{\pm a\}$

Der euklidische Algorithmus

A220
Erläuterung

Wir müssen zeigen, dass der angegebene Algorithmus korrekt ist, also dass die Methode tatsächlich liefert, was die Spezifikation verspricht.

Die Methode terminiert: Der Wert $|b|$ nimmt in jedem Schritt ab, bis schließlich $b = 0$ erreicht ist und der Algorithmus endet.

Das gelieferte Ergebnis erfüllt die geforderten Bedingungen:
Die Initialisierung $(a, b) \leftarrow (a_0, b_0)$ garantiert $\mathrm{GT}(a, b) = \mathrm{GT}(a_0, b_0)$.
Jede Iteration erhält $\mathrm{GT}(a, b) = \mathrm{GT}(b, a - qb)$. Zum Schluss gilt also $\mathrm{GT}(a_0, b_0) = \mathrm{GT}(a, 0)$ und somit $\mathrm{GGT}(a_0, b_0) = \mathrm{GGT}(a, 0) = \{\pm a\}$.
Demnach ist $|a|$ der positive ggT von a_0, b_0. QED

🙂 Das ist genial-einfach und einfach-genial. Zudem ist die Methode sehr effizient, das heißt, auch für große Eingaben (a_0, b_0) geeignet.

⚠ Vielleicht kennen Sie ein weiteres Verfahren: Wenn Sie zu a, b die Primfaktorzerlegungen $a = \pm p_1^{a_1} \ldots p_n^{a_n}$ und $b_0 = \pm p_1^{b_1} \ldots p_n^{b_n}$ kennen, so gilt $\mathrm{ggT}(a, b) = p_1^{t_1} \ldots p_n^{t_n}$ mit $t_i = \min\{a_i, b_i\}$ und $\mathrm{kgV}(a, b) = p_1^{v_1} \ldots p_n^{v_n}$ mit $v_i = \max\{a_i, b_i\}$. Für große Eingaben a, b ist die Primfaktorzerlegung jedoch hoffnungslos aufwändig. Euklid ist dagegen blitzschnell.

Der erweiterte euklidische Algorithmus nach Bézout

Satz A2I: Bézout in $\mathbb{Z}$

(1) Zu je zwei Zahlen $a, b \in \mathbb{Z}$ existieren $u, v \in \mathbb{Z}$ mit $au + bv = \mathrm{ggT}(a, b)$.
(2) Das ist ein Zertifikat: Aus $d = au + bv \in \mathrm{GT}(a, b)$ folgt $d \in \mathrm{GGT}(a, b)$.
(3) Der folgende Algorithmus berechnet solche **Bézout–Koeffizienten**.

Algo A2I: Berechnung des ggT mit Bézout–Koeffizienten

Eingabe: zwei ganze Zahlen $a_0, b_0 \in \mathbb{Z}$
Ausgabe: drei Zahlen $a, u, v \in \mathbb{Z}$ mit $a = a_0u + b_0v = \mathrm{ggT}(a_0, b_0)$

1: $\left[\begin{smallmatrix} a & u & v \\ b & s & t \end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \end{smallmatrix}\right]$ // Invariante $\begin{cases} a=a_0u+b_0v \\ b=a_0s+b_0t \end{cases}$
2: while $b \neq 0$ do $q \leftarrow a \operatorname{quo} b$ // euklidische Division
3: $\left[\begin{smallmatrix} a & u & v \\ b & s & t \end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix} b & s & t \\ a-qb & u-qs & v-qt \end{smallmatrix}\right]$ // Invariante $\begin{cases} a=a_0u+b_0v \\ b=a_0s+b_0t \end{cases}$
4: if $a < 0$ then $(a, u, v) \leftarrow -(a, u, v)$ // normiere das Vorzeichen
5: return (a, u, v) // $\mathrm{ggT}(a_0, b_0) = a = a_0u + b_0v$

Beweis: In der ersten Spalte wird der euklidische Algorithmus A2H ausgeführt. Die Invarianten garantieren $a = a_0u + b_0v$. QED

Der erweiterte euklidische Algorithmus nach Bézout

Bemerkung: Die Operationen $q \leftarrow a \operatorname{quo} b$ und

$$\begin{bmatrix} a & u & v \\ b & s & t \end{bmatrix} \leftarrow \begin{bmatrix} b & s & t \\ a-qb & u-qs & v-qt \end{bmatrix}$$

sind Zeilenoperationen, hier für die Invarianten $a = a_0u + b_0v$ und $b = a_0s + b_0t$. Ausführlich: $R_1 \leftrightarrow R_2$, wir tauschen die beiden Zeilen; $R_2 \leftarrow R_2 - qR_1$, von der zweiten Zeile ziehen wir q mal die erste ab.

Numerisches Beispiel: Für $a_0 = 138$ und $b_0 = 24$ erhalten wir:

init		138	1	0	Invariante:	$138 = 1\,a_0 + 0\,b_0$
init		24	0	1	Invariante:	$24 = 0\,a_0 + 1\,b_0$
$q = 5$	$\Rightarrow$	18	1	-5	Invariante:	$18 = 1\,a_0 - 5\,b_0$
$q = 1$	$\Rightarrow$	6	-1	6	Invariante:	$6 = -1\,a_0 + 6\,b_0$
$q = 3$	$\Rightarrow$	0	4	-23	Invariante:	$0 = 4\,a_0 - 23\,b_0$

Somit gilt $\mathrm{ggT}(a_0, b_0) = 6 = ua_0 + vb_0$ mit $u = -1$ und $v = 6$.

Übung: Erfinden und erproben Sie selbst weitere Beispiele!

Algorithmus = Spezifikation + Methode

Unsere ersten Beispiele geben uns wichtiges Anschauungsmaterial.
Ein Algorithmus besteht, wie oben gesehen, immer aus zwei Teilen:

- eine Spezifikation: Was soll er erreichen?
- eine Methode: Wie führt er es aus?

Die Spezifikation erklärt, welche Eingaben erlaubt sind und welche Ausgabe garantiert wird. Am besten verstehen Sie dies als Vertrag: Zum Aufruf des Algorithmus müssen die Vorbedingungen erfüllt sein, bei der Rückgabe sichert der Algorithmus die Nachbedingungen zu.

Jeder Algorithmus, der etwas auf sich hält, muss bewiesen werden!
Zur Korrektheit sind die Angaben der Spezifikation wesentlich:

- Terminiert die angegebene Methode für jede erlaubte Eingabe?
- Liefert die Methode als Ausgabe, was die Spezifikation verspricht?

Nach der Korrektheit können und sollten wir nach den Kosten fragen: Welche Ressourcen (Laufzeit, Speicher, etc.) benötigt der Algorithmus?

Algorithmen und Komplexität sind faszinierende Gebiete der Informatik, und sowohl theoretisch als auch praktisch von überragender Bedeutung.

Satz = Aussage + Beweis

Spezifikation und Methode verhalten sich wie Aussage und Beweis:
Die Methode führt schrittweise von der Eingabe zur Ausgabe.
Der Beweis führt von der Voraussetzung zur Schlussfolgerung.

Die Trennung in Spezifikation und Methode dient der Arbeitsteilung:

- Für die aufrufende Instanz ist allein die Spezifikation maßgeblich, die Methode hingegen ist Privatsache der ausführenden Instanz.
- Ebenso bei einem Satz: Die Nutzerin verlässt sich auf die Aussage, die Mathematikerin garantiert seine Richtigkeit durch einen Beweis.

In sehr vielen Fällen werden Sie Sätze / Algorithmen dankbar nutzen und sich auf deren sorgsame Beweise / Implementierungen verlassen. Ihr Studium gibt Ihnen glücklicherweise die Werkzeuge für beide Seiten, als Nutzer und Hersteller mathematischer Ergebnisse und Methoden.

☺ In der Mathematik lernen sie viele schöne Ideen und Techniken, nicht zuletzt auch algorithmisches Denken und sorgfältiges Beweisen. Damit erkennen Sie Zusammenhänge und Lösungen, wo andernfalls nur heillose Verwirrung und planloses Herumprobieren möglich wären.

Der Fundamentalsatz der Arithmetik

Gilt $a = b \cdot c$ in $\mathbb{Z}$, so sagen wir a ist **zerlegbar** in die Faktoren b und c.
Die **trivialen Zerlegungen** sind $a = (\pm 1) \cdot (\pm a) = (\pm a) \cdot (\pm 1)$; sind dies die einzigen, so nennen wir a **unzerlegbar** (vorsichtig… später „prim“).

Jede natürliche Zahl $a \geq 1$ können wir zerlegen, bis es nicht weiter geht, zum Beispiel $60 = 6 \cdot 10 = (2 \cdot 3) \cdot (2 \cdot 5)$ oder $60 = 4 \cdot 15 = (2 \cdot 2) \cdot (3 \cdot 5)$. Die Wege sind verschieden, aber das Ergebnis ist umgeordnet dasselbe!

Satz A2J: Fundamentalsatz der Arithmetik

(1) Jede natürliche Zahl $a \in \mathbb{N}_{\geq 1}$ können wir zerlegen in ein Produkt

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_\ell$$

der Länge $\ell \in \mathbb{N}$ mit unzerlegbaren Faktoren $p_1, p_2, \ldots, p_\ell \in \mathbb{N}_{\geq 2}$.

(2) Diese Zerlegung ist eindeutig bis auf Umordnung: Gilt

$$p_1 \cdot p_2 \cdot \ldots \cdot p_\ell = q_1 \cdot q_2 \cdot \ldots \cdot q_k$$

mit unzerlegbaren Faktoren $p_1 \leq p_2 \leq \cdots \leq p_\ell$ und $q_1 \leq q_2 \leq \cdots \leq q_k$ in $\mathbb{N}$, so folgt $\ell = k$ und $p_i = q_i$ für alle $i = 1, 2, \ldots, \ell$.

Der Fundamentalsatz: Existenz einer Zerlegung

Für „Produkt unzerlegbarer Faktoren in $\mathbb{N}$“ sage ich kurz UProdukt.
(1) Existenz: Jede natürliche Zahl $a \in \mathbb{N}_{\geq 1}$ ist ein UProdukt
(2) Eindeutigkeit: … auf genau eine Weise (bis auf Umordnung).

Beweis der Existenz (1): Wir führen Induktion und betrachten

$$E = \left\{ n \in \mathbb{N}_{\geq 1} \;\middle|\; \begin{array}{l} \text{Jede natürliche Zahl } a \text{ mit} \\ 1 \leq a \leq n \text{ ist ein UProdukt} \end{array} \right\}$$

Es gilt $1 \in E$: Die Zahl $a = 1$ ist das leere UProdukt der Länge $\ell = 0$.
Sei $n \in E$ und $a = n + 1$. Entweder a ist unzerlegbar: Dann ist a ein UProdukt der Länge 1. Oder a ist zerlegbar gemäß $a = bc$ mit $b, c \geq 2$: Dann gilt $b, c \leq n$, also sind b und c UProdukte der Längen k und ℓ und somit $a = b \cdot c$ ein UProdukt der Länge $k + \ell$. Wir schließen $n + 1 \in E$.
Somit gilt $E = \mathbb{N}_{\geq 1}$: Jede natürliche Zahl $a \geq 1$ ist ein UProdukt. QED

⚠ Die Eindeutigkeit (2) ist schwieriger, interessanter und nützlicher!
Die möglichen Rechenwege bis zu einem UProdukt sind verschieden. Wir müssen zeigen, dass im Endergebnis die unzerlegbaren Faktoren immer dieselben sind bis auf Umordnung. Das ist tatsächlich knifflig.

Fundamentalsatz: unzerlegbar vs prim

Zur weiteren Untersuchung benötigen wir zwei grundlegende Begriffe:

Definition A2K: unzerlegbar / irreduzibel vs prim

Eine ganze Zahl $a \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ heißt **unzerlegbar** in $\mathbb{Z}$, falls gilt:
Für alle $b, c \in \mathbb{Z}$ folgt aus $a = b \cdot c$ entweder $b = \pm 1$ oder $c = \pm 1$.

Hingegen nennen wir $a \in \mathbb{Z} \smallsetminus \{\pm 1\}$ **prim** in $\mathbb{Z}$, falls gilt:
Für alle $b, c \in \mathbb{Z}$ folgt aus $a \mid b \cdot c$ stets $a \mid b$ oder $a \mid c$.

⚠ Oft wird beides „prim“ genannt. Es sind jedoch zwei verschiedene Eigenschaften, sie verdienen daher auch zwei verschiedene Namen.

Beispiele: Die Elemente $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ sind unzerlegbar.
Die Elemente $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, \ldots$ sind echt zerlegbar.
Die Elemente 0 und ± 1 sind speziell, weder zerlegbar noch unzerlegbar.

Die Zahl 0 ist prim: $0 \mid ab$ bedeutet $ab = 0$, also $a = 0$ oder $b = 0$.
Die Zahl 2 ist prim: Ist ab gerade, so muss a oder b gerade sein.
Es gilt $10 \mid 4 \cdot 25$, aber $10 \nmid 4$ und $10 \nmid 25$. Somit ist 10 nicht prim.

Fundamentalsatz: unzerlegbar vs prim

🙂 Wir möchten hoffen, dass unzerlegbar und prim in $\mathbb{Z}$ dasselbe sind.
Ist das klar oder müssen wir es beweisen? Wir müssen es beweisen!
Warum müssen wir es beweisen? Schon nebenan in $1 + 4\mathbb{N}$ gilt es nicht:

Beispiel A2L: Hilbert–Monoid

Wir betrachten $(H, \cdot)$ mit $H = 1 + 4\mathbb{N} = \{1, 5, 9, 13, 17, 21, \ldots\}$.
In $(H, \cdot)$ ist 9 unzerlegbar, aber nicht prim: $9 \mid_H 21 \cdot 21$, aber $9 \nmid_H 21$.

Es kommt sogar noch schlimmer: In $(H, \cdot)$ sind $441 = 21 \cdot 21 = 9 \cdot 49$ zwei verschiedene Zerlegungen der Zahl 441 in unzerlegbare Faktoren.

Übung: In Lufthansa-Flugzeugen fehlen die Reihen 13 und 17.
Finden Sie im Monoid $(M, \cdot)$ mit $M = \mathbb{N}_{\geq 1} \smallsetminus \{13, 17\}$ die kleinste Zahl, die mehr als eine Zerlegung in unzerlegbare Faktoren erlaubt.

Übung: In $\mathbb{N}[X]$ gilt $(1 + X + X^2)(1 + X^3) = (1 + X)(1 + X^2 + X^4)$.
Die Faktoren sind unzerlegbar in $\mathbb{N}[X]$, doch zerlegbar in $\mathbb{Z}[X]$.

Für $(\mathbb{Z}, \cdot)$ wollen wir zeigen, dass solche Pathologien nicht auftreten!
Obige Gegenbeispiele zeigen, dass hier ernsthaft etwas zu tun ist.

Fundamentalsatz: die Lemmata von Gauß und Euklid

Lemma A2M: Lemma von Euklid für $\mathbb{Z}$

(0) Jedes Primelement $p \in \mathbb{Z}^*$ ist unzerlegbar in $\mathbb{Z}$.
(1) Jedes unzerlegbare Element p in $\mathbb{Z}$ ist prim in $\mathbb{Z}$.

Beweis: (0) Sei $p \neq 0$ prim und $p = ab$ in $\mathbb{Z}$. Daraus folgt $p \mid a$ oder $p \mid b$. Nehmen wir $p \mid a$ an, also $a = pp'$ für ein $p' \in \mathbb{Z}$. Damit gilt $p = ab = pp'b$, nach Kürzung $1 = p'b$, also $b = \pm 1$. Analog folgt aus $p \mid b$, dass $a = \pm 1$.

(1) Sei $p > 0$ unzerlegbar und $p \mid ab$. Wir müssen $p \mid a$ oder $p \mid b$ zeigen. Hierzu sei $d = \operatorname{ggT}(p, a)$. Es gilt $d \mid p$; da p unzerlegbar ist, gilt entweder $d = 1$ oder $d = p$. (1a) Im Falle $d = p$ gilt dank $d \mid a$ sofort $p \mid a$.
(1b) Im Falle $d = 1$ folgt $p \mid b$ mit dem Lemma von Gauß. QED

Lemma A2N: Lemma von Gauß für $\mathbb{Z}$

Seien $p, a, b \in \mathbb{Z}$ mit $\operatorname{ggT}(p, a) = 1$. Dann folgt aus $p \mid ab$ bereits $p \mid b$.

Beweis: Dank Bézout A2I existieren $u, v \in \mathbb{Z}$, sodass $pu + av = 1$. Die Teilbarkeit $p \mid ab$ bedeutet $ab = pq$ für ein $q \in \mathbb{Z}$. Daraus folgt $b = (pu + av)b = pub + abv = p(ub + qv)$, also $p \mid b$. QED

Fundamentalsatz: die Lemmata von Gauß und Euklid

Diese beiden Lemmata sind der harte Kern des Fundamentalsatzes: Sie besagen, dass unzerlegbar und prim ($\neq 0$) in $\mathbb{Z}$ dasselbe sind! Daraus folgt, wie wir anschließend sehen, die ersehnte Eindeutigkeit der Primfaktorzerlegung im Ring $\mathbb{Z}$ der ganzen Zahlen.

Ich betone nochmals, dass dies keineswegs selbstverständlich ist. Schon in benachbarten, sehr einfachen Beispielen wie $\mathbb{N}[X]$ oder $1 + 4\mathbb{N}$ (A2L) sind manche Elemente unzerlegbar, aber nicht prim, und die Zerlegung in unzerlegbare Faktoren ist nicht eindeutig.

Dass dies dennoch in $\mathbb{Z}$ gelingt, liegt an zwei wesentlichen Zutaten:

- Wir haben die euklidische Division mit Rest A2A.
- Der euklidische Algorithmus A2H berechnet den ggT.
- Der erweiterte Algorithmus A2I berechnet Bézout–Koeffizienten.

Ich habe den Beweis so organisiert, dass diese zentralen Eigenschaften möglichst klar hervortreten und sich später verallgemeinern lassen. Alle Argumente gelten wörtlich genauso für jeden Polynomring $K[X]$ über einem Körper K, und allgemein für sogenannte euklidische Ringe.

Fundamentalsatz: Eindeutigkeit der Zerlegung

Beweis der Eindeutigkeit (2): In $\mathbb{N}$ betrachten wir zwei UProdukte

$$a \;=\; p_1 p_2 \cdots p_n \;=\; q_1 q_2 \cdots q_m.$$

Wir zeigen, dass $n = m$ gilt und nach Umordnung $p_i = q_i$ für alle i. Sei

$$E = \left\{ n \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{Jedes UProdukt der Länge } n \\ \text{ist im obigen Sinne eindeutig.} \end{array} \right\}$$

Es gilt $0 \in E$: Für $n = 0$ haben wir $a = 1$, somit auch $m = 0$.

Aus $n - 1 \in E$ folgt $n \in E$: Wir betrachten zwei UProdukte wie oben. Der Faktor p_n ist unzerlegbar, somit auch prim dank Euklid A2M. Also gilt $p_n \mid q_i$ für ein $i \in \{1, \ldots, m\}$. Nach Umordnung gilt $i = m$. Da auch q_m unzerlegbar ist, folgt $p_n = q_m$. Kürzen ergibt

$$a/p_n \;=\; p_1 p_2 \cdots p_{n-1} p_n \;=\; q_1 q_2 \cdots q_{m-1} q_m.$$

Nach Voraussetzung $n - 1 \in E$ gilt für diese gekürzten Produkte $n - 1 = m - 1$ und nach Umordnung $p_i = q_i$ für alle $i = 1, \ldots, n - 1$. QED

Fundamentalsatz: Eindeutigkeit der Zerlegung

Bitte schauen Sie sich diesen schönen raffinierten Beweis genau an. Er ist lehrreiches Anschauungsmaterial für mathematische Arbeit. Diese Argumentationskette selbst zu finden, ist sicherlich schwierig, aber sie schrittweise nachzuvollziehen erfordert nur Beharrlichkeit.

Den Fundamentalsatz der Arithmetik kennen Sie vermutlich bereits aus der Schule, wenn auch vielleicht nicht unter diesem Namen, sondern vermutlich nur als „Erfahrungstatsache“ oder als ständig wiederholte, niemals hinterfragte und nie bewiesene Behauptung.

Es ist ein Unterschied, ob Sie Mathematik nur nutzen und anwenden, oder ob Sie Mathematik selbst machen, verstehen und vertiefen wollen. Als Anwender/in genügt es, fertige Ergebnisse dankend zu übernehmen. Als Mathematiker/in wollen Sie die Zusammenhänge genau verstehen.

Unsere obigen Gegenbeispiele belegen eindringlich, dass wir hier tatsächlich etwas beweisen und akribisch argumentieren müssen. Dank präziser Vorbereitung ist der Beweis am Ende nicht schwer. Sorgfältige Arbeit kostet Zeit, doch unsere Mühe lohnt sich!

Rechnen mit Resten modulo 10

A233

Aufgabe: Ich behaupte leichtfertig $13^{14} = 3\,937\,376\,385\,699\,291$.
Weisen Sie ohne Computer nach, dass dieses Behauptung falsch ist.

Lösung: Die Größenordnung 10^{15} stimmt ungefähr, das scheint ok.
Betrachten wir also die letzte Ziffer: Diese ist offensichtlich falsch!

$$1 \xmapsto{\cdot 13} 13 \xmapsto{\cdot 13} 169 \xmapsto{\cdot 13} 2197 \xmapsto{\cdot 13}$$
$$28561 \xmapsto{\cdot 13} 371293 \xmapsto{\cdot 13} 4826809 \xmapsto{\cdot 13} 62748517 \xmapsto{\cdot 13}$$
$$815730721 \xmapsto{\cdot 13} \ldots 3 \xmapsto{\cdot 13} \ldots 9 \xmapsto{\cdot 13} \ldots 7 \xmapsto{\cdot 13} \ldots$$

Die letzte Ziffer von 13^{14} ist demnach 9 und nicht 1.

☺ Die Berechnung der letzten Ziffer lässt sich einfach durchführen.
Wenn Sie den Trick erst einmal kennen, gelingt dies durch Kopfrechnen.
Da uns hier nur die letzte Ziffer interessiert, brauchen wir die vorderen Ziffern gar nicht zu berechnen. Warum ist das so? Gilt das immer?

☺ Dieser genial-einfache Trick heißt „Rechnen modulo 10“.
Diesen wollen wir nun zu einer allgemeinen Methode ausbauen!

Rechnen mit Resten modulo n

A234

Sei $n \in \mathbb{N}_{\geq 2}$. Auf der Restemenge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ definieren wir die Verknüpfungen $a +_n b := (a + b) \operatorname{rem} n$ und $a \cdot_n b := (a \cdot b) \operatorname{rem} n$.

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

Körper!

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Körper!

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

CRing!

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Körper!

Anwendungen modularer Arithmetik

A235
Erläuterung

☺ In der Linearen Algebra sind dies unsere ersten und wichtigsten Beispiele für endliche Körper. Die Klassifikation aller endlichen Körper ist ein schönes Kapitel der Algebra (ab dem dritten Semester).

☺ Auch überall sonst in der Mathematik und Informatik sind die Ringe $\mathbb{Z}_n$ nützlich und allgegenwärtig. Es lohnt sich, sie genau zu verstehen.

☺ Im Ring $(\mathbb{Z}_n, +_n, \cdot_n)$ können wir rechnen wir in $(\mathbb{Z}, +, \cdot)$,
in vielfacher Hinsicht sogar noch besser und effizienter.

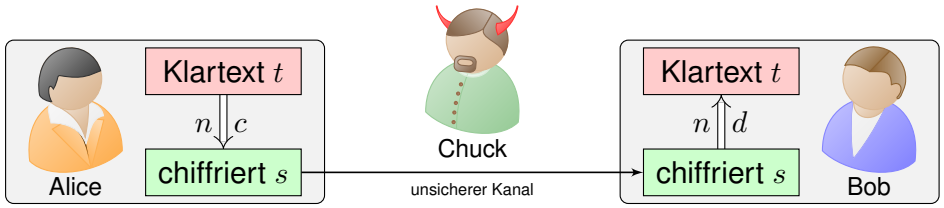
Ein Computer mit b Bit rechnet in $\mathbb{Z}_B$ wobei $B = 2^b$.
Wir haben oben schon die Zifferndarstellung diskutiert.

☺ Ich nenne eine spektakuläre Anwendung unter vielen:
Der **RSA–Cryptosystem** ist das erste *asymmetrische* Verschlüsselungsverfahren und bis heute weit verbreitet,
siehe `en.wikipedia.org/wiki/RSA_(cryptosystem)`.

Ich werde das RSA–Verfahren hier nur ganz grob skizzieren und mich zusammenreißen, nicht zu viel zu verraten. Ausführen will ich aber die universelle arithmetische Grundlage: den Restklassenring $(\mathbb{Z}_n, +_n, \cdot_n)$.

Anwendung: das RSA–Cryptosystem

A236



Das RSA–Verfahren wurde 1977 entwickelt von R. Rivest, A. Shamir und L. Adleman. Nachrichten werden dabei in $\mathbb{Z}_n$ codiert, mit sehr großem n.
Ein vollständiger Schlüssel (n, c, d) besteht aus drei Zahlen $n, c, d \in \mathbb{N}$.

$$\text{public key } (n, c) \quad - \quad \text{encrypt} \quad \mathbb{Z}_n \to \mathbb{Z}_n \;:\; t \mapsto s = t^c$$
$$\text{private key } (n, d) \quad - \quad \text{decrypt} \quad \mathbb{Z}_n \to \mathbb{Z}_n \;:\; s \mapsto t = s^d$$

Jeder Schlüssel (n, c, d) wird dabei so konstruiert, dass folgendes gilt:

Korrektheit dank Bijektivität: Es gilt $(t^c)^d = t^{cd} = t$ für alle $t \in \mathbb{Z}_n$.
Ver- und Entschlüsselung sind somit zueinander inverse Bijektionen.

Sicherheit dank Komplexität: Allein mit Kenntnis von n, c, s lässt sich der Klartext $t = s^d$ nur mit „unwirtschaftlich hohem Aufwand“ berechnen.

Der Restklassenring $\mathbb{Z}_n$

A237

Sei $n \in \mathbb{N}_{\geq 2}$. Wir betrachten die Restemenge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ mit der Projektion $p = p_n : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n : a \mapsto a \operatorname{rem} n$ und folgende Diagramme:

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow[(a,b)\mapsto a+b]{+} & \mathbb{Z} \\ {\scriptstyle p}\downarrow \quad \downarrow{\scriptstyle p} & (=) & \downarrow{\scriptstyle p} \\ \mathbb{Z}_n \times \mathbb{Z}_n & \xrightarrow[(r,s)\mapsto (r+s) \operatorname{rem} n]{+_n} & \mathbb{Z}_n \end{array} \qquad \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow[(a,b)\mapsto a\cdot b]{\cdot} & \mathbb{Z} \\ {\scriptstyle p}\downarrow \quad \downarrow{\scriptstyle p} & (=) & \downarrow{\scriptstyle p} \\ \mathbb{Z}_n \times \mathbb{Z}_n & \xrightarrow[(r,s)\mapsto (r\cdot s) \operatorname{rem} n]{\cdot_n} & \mathbb{Z}_n \end{array}$$

Satz A2O: Konstruktion des Rings $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$

(0) Für alle $a, b \in \mathbb{Z}$ gilt $p(a+b) = p(a) +_n p(b)$ und $p(a \cdot b) = p(a) \cdot_n p(b)$. Das bedeutet p ist ein Homomorphismus für Addition und Multiplikation.

(1) Somit ist $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$ ein kommutativer Ring (CRing), und die Abbildung $p : \mathbb{Z} \to \mathbb{Z}_n$ ist ein Ringhomomorphismus.

(2) Invertierbare Elemente sind $\mathbb{Z}_n^\times = \{\, a \in \mathbb{Z}_n \mid \operatorname{ggT}(a, n) = 1 \,\}$. Explizite Inversion: Dank Bézout $au + nv = 1$ gilt $au \operatorname{rem} n = 1$.

(3) Genau dann ist $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$ ein Körper, wenn $n \in \mathbb{N}_{\geq 2}$ prim ist. In diesem Falle schreiben wir zur Betonung auch $\mathbb{F}_n = \mathbb{Z}_n$ (engl. *field*).

Der Restklassenring $\mathbb{Z}_n$

A238
Erläuterung

Auf der Menge $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ der ganzen Zahlen haben wir die übliche Addition $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ und Multiplikation $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. Damit ist $(\mathbb{Z}, +, 0, \cdot, 1)$ ein kommutativer Ring (CRing). Auf der Menge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ definieren wir nun zwei neue Verknüpfungen:

$$\begin{aligned} +_n &: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n : (a, b) \mapsto a +_n b = (a + b) \operatorname{rem} n \\ \cdot_n &: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n : (a, b) \mapsto a \cdot_n b \ = (a \cdot b) \operatorname{rem} n \end{aligned}$$

Diese sind verschieden von $+$ und $\cdot$, daher betonen wir sorgsam n. Die obigen Diagramme stellen die gesamte Situation übersichtlich dar. Dies führt uns zu einer ganz einfachen aber grundlegenden Frage:

Ist es egal, ob wir erst verknüpfen und dann den Rest mod n bilden oder umgekehrt erst Reste mod n bilden und diese dann verknüpfen?

🙂 Alle Daten liegen explizit vor, jedes konkrete Beispiel können Sie damit ganz direkt nachrechnen: Führen Sie einige zur Übung aus!

🙂 Das allgemeine Ergebnis ist überaus bemerkenswert: Es ist egal, jedes dieser Diagramme kommutiert! Das ist der Inhalt des Satzes.

Der Restklassenring $\mathbb{Z}_n$

A239

Beweis: (0) Vorgelegt seien zwei beliebige ganze Zahlen $a, b \in \mathbb{Z}$. Wir zerlegen $a = nq_a + r_a$ mit $r_a = p(a)$ und $b = nq_b + r_b$ mit $r_b = p(b)$. Somit gilt $a + b = n(q_a + q_b) + r_a + r_b$, also $a + b \operatorname{rem} n = r_a + r_b \operatorname{rem} n$, und $a \cdot b = n^2 q_a q_b + n(q_a r_b + r_a q_b) + r_a r_b$, also $a \cdot b \operatorname{rem} n = r_a \cdot r_b \operatorname{rem} n$.

(1) Wir müssen alle Axiome eines kommutativen Rings nachrechnen.

Wir zeigen zunächst **Ass**$(\mathbb{Z}_n, +_n)$. Vorgelegt seien hierzu $r_1, r_2, r_3 \in \mathbb{Z}_n$. Hierzu existieren Urbilder $a_1, a_2, a_3 \in \mathbb{Z}$ mit $p(a_i) = r_i$. Damit finden wir:

$$\begin{aligned} (r_1 +_n r_2) +_n r_3 &= \big[p(a_1) +_n p(a_2)\big] +_n p(a_3) = p\big[(a_1 + a_2) + a_3\big] \\ r_1 +_n (r_2 +_n r_3) &= p(a_1) +_n \big[p(a_2) +_n p(a_3)\big] = p\big[a_1 + (a_2 + a_3)\big] \end{aligned}$$

Aus **Ass**$(\mathbb{Z}, +)$ folgt **Ass**$(\mathbb{Z}_n, +_n)$. Ebenso alle anderen Ringaxiome!

🙂 Jede Allaussage in $(\mathbb{Z}, +, 0, \cdot, 1)$ vererbt sich auf $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$ dank des Homomorphismus $p : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n$: **Ntr**$(\mathbb{Z}_n, +_n, 0)$, **Com**$(\mathbb{Z}_n, +_n)$, **DL**$(\mathbb{Z}_n, +_n, \cdot_n)$, **DR**$(\mathbb{Z}_n, +_n, \cdot_n)$, **Ass**$(\mathbb{Z}_n, \cdot_n)$, **Ntr**$(\mathbb{Z}_n, \cdot_n, 1)$, **Com**$(\mathbb{Z}_n, \cdot_n)$.

Was fehlt noch? Die Negation $-_n : \mathbb{Z}_n \to \mathbb{Z}_n$ ist gegeben durch $-_n 0 = 0$ und $-_n a = n - a$ für $a \in \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$. Damit gilt **Inv**$(\mathbb{Z}_n, +_n, 0, -_n)$.

Der Restklassenring $\mathbb{Z}_n$

A240
Logik Mengen

Im Ring $(\mathbb{Z}, +, \cdot)$ sind nur die Elemente ± 1 invertierbar:

$$\mathbb{Z}^\times = \{\, \pm 1 \,\}$$

Im Ring $(\mathbb{Z}_n, +_n, \cdot_n)$ ist die Situation viel interessanter:

$$\mathbb{Z}_n^\times = \{\, a \in \mathbb{Z}_n \mid \operatorname{ggT}(a, n) = 1 \,\}$$

(2a) Es gilt „$\supseteq$“: Zu $a \in \mathbb{Z}_n$ mit $\operatorname{ggT}(a, n) = 1$ existieren $u, v \in \mathbb{Z}$ mit $au + nv = 1$ dank Bézout A2I. Also gilt $a \cdot_n u = 1$, somit $a \in \mathbb{Z}_n^\times$.

(2b) Es gilt „$\subseteq$“: Ist $a \in \mathbb{Z}_n$ invertierbar, so existiert $u \in \mathbb{Z}_n$ mit $a \cdot_n u = 1$. Das bedeutet $a \cdot u + n \cdot v = 1$ für ein $v \in \mathbb{Z}$, also $\operatorname{ggT}(a, n) = 1$. (A2I)

(3a) Ist $n \in \mathbb{N}_{\geq 2}$ prim, also unzerlegbar (A2M), so gilt $\operatorname{ggT}(a, n) = 1$ für alle $a \in \{1, \ldots, n-1\} = \mathbb{Z}_n \setminus \{0\}$. Dank (2a) ist a in $\mathbb{Z}_n$ invertierbar. Also gilt $\mathbb{Z}^\times = \mathbb{Z}^*$, und $(\mathbb{Z}_n, +_n, \cdot_n)$ ist ein Körper.

(3b) Ist $n = a \cdot b$ zerlegbar in $a, b \in \mathbb{N}_{\geq 2}$, so gilt $a, b \in \mathbb{Z}_n \setminus \{0\}$, aber $a \cdot_n b = 0$ in $\mathbb{Z}_n$. Somit sind a, b Nullteiler in $\mathbb{Z}_n$ und nicht invertierbar. Also gilt $\mathbb{Z}^\times \subsetneq \mathbb{Z}^*$, und $(\mathbb{Z}_n, +_n, \cdot_n)$ ist kein Körper. QED

Die reellen Zahlen

A301

Wir verfolgen den Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$:

natürliche Zahlen	$\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \}$
ganze Zahlen	$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$
rationale Zahlen	$\mathbb{Q} = \{ z/n \mid z, n \in \mathbb{Z},\ n \neq 0 \}$
reelle Zahlen	$\mathbb{R} =$ „$\mathbb{Q}$ und alle Grenzwerte“

Die **reellen Zahlen** $(\mathbb{R}, +, \cdot, \leq)$ sind ein vollständig geordneter Körper.

Vollständigkeit bedeutet: Zu jeder Teilmenge $M \subseteq \mathbb{R}$, die nicht-leer und nach oben beschränkt ist, existiert in $\mathbb{R}$ eine kleinste obere Schranke.

🙂 Das ist die Grundlage der gesamten Analysis. Daraus erhalten wir Grenzwerte von Folgen und Reihen, Ableitungen und Integrale, usw.

Satz A3A: der Körper $\mathbb{R}$ der reellen Zahlen

Solche Körper $(\mathbb{R}, +, \cdot, \leq)$ existieren: Wir können Modelle konstruieren mit Cauchy–Folgen, Dedekind–Schnitten oder Intervallschachtelungen.

Je zwei sind isomorph bis auf einen eindeutigen Isomorphismus.

Die reellen Zahlen

A302
Erläuterung

In $\mathbb{Q}$ haben manche Intervallschachtelungen leeren Durchschnitt, etwa die Approximationen von $\sqrt{2} = 1.4142\dots$ oder $\mathrm{e} = 2.7182\dots$ oder $\pi = 3.1415\dots$. Dies sind keine Elemente von $\mathbb{Q}$, wir können sie bestenfalls annähern. Dieses grundlegende Ärgernis lösen wir durch die Erweiterung von den rationalen Zahlen $\mathbb{Q}$ zu den reellen Zahlen $\mathbb{R}$.

🙂 Der Körper $(\mathbb{R}, +, \cdot, \leq)$ ist **topologisch vollständig**.

Erst mit $\mathbb{R}$ lassen sich viele fundamentale und praktische Probleme elegant und befriedigend lösen und eine tragfähige Grundlage finden: Zu $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto x^n$ konstruieren wir die Umkehrfunktion $y \mapsto \sqrt[n]{y}$. In der Analysis entwickeln wir die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ und ihre Umkehrfunktion $\ln : \mathbb{R}_{>0} \to \mathbb{R}$, trigonometrische Funktionen $\sin, \cos : \mathbb{R} \to \mathbb{R}$ und viele weitere, und beweisen ihre Eigenschaften.

Die Konstruktion der reellen Zahlen $\mathbb{R}$ und der Aufbau der Theorie ist viel reichhaltiger, als ich es hier zusammenfassend skizzieren könnte. Diese wunderbaren Errungenschaften werden wir im Folgenden dankbar aus der Analysis importieren, wo immer sie nötig oder hilfreich sind.

Die komplexen Zahlen: Motivation

A303

Für jede reelle Zahl $x \in \mathbb{R}$ gilt $x^2 \geq 0$, also $x^2 + 1 > 0$. Daher können wir Gleichungen wie $x^2 + 1 = 0$ in $\mathbb{R}$ zwar formulieren, aber nicht lösen.

Können wir eine Lösung $\mathrm{i} = \sqrt{-1}$ erfinden und damit sinnvoll rechnen? Versuchen wir es! Wir wünschen uns einen Körper $\mathbb{C} \supset \mathbb{R}$ der Form

$$\mathbb{C} = \left\{ z = x + y\mathrm{i} \;\middle|\; x, y \in \mathbb{R} \right\}.$$

Wie sehen die Operationen aus? Falls $\mathbb{C}$ existiert, so erwarten wir:

Vergleich:	$x + y\mathrm{i} = u + v\mathrm{i}$ in $\mathbb{C}$	$\Leftrightarrow$	$x = u$ und $y = v$ in $\mathbb{R}$
Addition:	$(x + y\mathrm{i}) + (u + v\mathrm{i})$	$=$	$(x + u) + (y + v)\mathrm{i}$
Multiplikation:	$(x + y\mathrm{i}) \cdot (u + v\mathrm{i})$	$=$	$(xu - yv) + (xv + yu)\mathrm{i}$

Zu jedem Element $z = x + y\mathrm{i}$ haben wir das Negative $-z = (-x) + (-y)\mathrm{i}$ und das Konjugierte $\overline{z} = x - y\mathrm{i}$. Dabei gilt $z\overline{z} = x^2 + y^2$, also

$$\frac{1}{z} = \frac{1}{x + y\mathrm{i}} = \frac{1}{x + y\mathrm{i}} \cdot \frac{x - y\mathrm{i}}{x - y\mathrm{i}} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}\mathrm{i} = \frac{\overline{z}}{z\overline{z}}$$

Für jedes Element $x + y\mathrm{i} \neq 0$ gilt $x \neq 0$ oder $y \neq 0$, also $x^2 + y^2 > 0$.

Die komplexen Zahlen: Konstruktion

A304
kartesisches Produkt

Ist das erlaubt? Wie können wir die Menge $\mathbb{C}$ und ihre Operationen einwandfrei erklären? Wir nutzen das Modell $\mathbb{R}^2 \xrightarrow{\sim} \mathbb{C} : (x, y) \mapsto x + y\mathrm{i}$.

Satz A3B: Konstruktion des Körpers $\mathbb{C}$ der komplexen Zahlen

Auf der Menge $\mathbb{C} = \mathbb{R}^2$ definieren wir Addition und Multiplikation durch

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : (x, y) + (u, v) := (x + u, y + v),$$
$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : (x, y) \cdot (u, v) := (xu - yv, xv + yu).$$

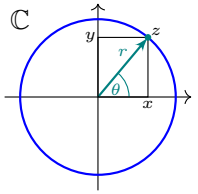
Damit ist $(\mathbb{C}, +, \cdot)$ ein Körper. Hierin ist $(\mathbb{R}, +, \cdot)$ ein Teilkörper dank der Einbettung $\mathbb{R} \hookrightarrow \mathbb{C} : x \mapsto (x, 0)$. Wir schreiben kurz $\mathbb{R} \subset \mathbb{C}$.

Im Körper $\mathbb{C}$ erfüllt das Element $\mathrm{i} = (0, 1)$ die Eigenschaft $\mathrm{i}^2 = -1$. Jedes Element $z \in \mathbb{C}$ schreibt sich eindeutig $z = x + y\mathrm{i}$ mit $x, y \in \mathbb{R}$.

Die Konjugation $\overline{} : \mathbb{C} \to \mathbb{C} : (x, y) \mapsto (x, -y)$ erfüllt $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$. Für $z \in \mathbb{C}$ gilt $\overline{z} = z$ genau dann, wenn $z \in \mathbb{R}$.

⚠ Auf $\mathbb{C}$ existiert keine Anordnung zu einem geordneten Körper $(\mathbb{C}, +, \cdot, \leq)$, denn in jedem geordneten Körper gilt $x^2 \geq 0$ für alle x.

Komplexe Zahlen: Polarkoordinaten



Auf $\mathbb{C}$ haben wir die **komplexe Exponentialfunktion**

$$\exp : \mathbb{C} \twoheadrightarrow \mathbb{C}^* : z = x + y\mathrm{i} \mapsto \mathrm{e}^z = \mathrm{e}^x (\cos y + \mathrm{i} \sin y)$$

Jede komplexe Zahl $z = x + y\mathrm{i} \in \mathbb{C}$ lässt sich damit in **Polarkoordinaten** darstellen vermöge

$$z = r\,\mathrm{e}^{\mathrm{i}\theta} = r\,(\cos\theta + \mathrm{i}\sin\theta)$$

mit dem **Betrag** $r = |z| = \sqrt{z\overline{z}} = \sqrt{x^2+y^2}$ und einem **Argument** $\theta \in \mathbb{R}$. Dabei gilt $\mathrm{e}^{\mathrm{i}\theta} = \mathrm{e}^{\mathrm{i}\varphi}$ genau dann, wenn $\varphi = \theta + 2\pi k$ für ein $k \in \mathbb{Z}$.

Für die Funktionen $\exp$, $\cos$ und $\sin$ gelten **Additionstheoreme**. Die Multiplikation mit $z \in \mathbb{C}$ erweist sich damit als **Drehstreckung**:

$$z = |z|\,\mathrm{e}^{\mathrm{i}\theta},\ w = |w|\,\mathrm{e}^{\mathrm{i}\varphi} \quad \Longrightarrow \quad z \cdot w = |z| \cdot |w| \cdot \mathrm{e}^{\mathrm{i}(\theta+\varphi)}$$

Aufgabe: In $\mathbb{C}$ hat jede Zahl $z \neq 0$ genau n verschiedene $n$te Wurzeln.

Lösung: Wir lösen die Gleichung $w^n = z$ für $z = r\,\mathrm{e}^{\mathrm{i}\theta}$ und $n \in \mathbb{N}_{\geq 2}$ elegant-explizit durch $w_k = \sqrt[n]{r} \cdot \mathrm{e}^{\mathrm{i}(\theta+2\pi k)/n}$ mit $k = 0, 1, \ldots, n-1$.

Komplexe Zahlen: Polarkoordinaten

Viele wichtige Funktionen lassen sich als **Potenzreihen** darstellen; die nötigen Begriffe und Techniken hierzu lernen Sie in der Analysis.

Dies gilt insbesondere für die Exponentialfunktion, Cosinus und Sinus:

$$\exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!} = 1 + z + \frac{z^2}{2} + \frac{z^3}{3!} + \ldots$$

$$\cos(z) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} z^{2k} = 1 - \frac{z^2}{2} + \frac{z^4}{4!} - \frac{z^6}{6!} + \ldots$$

$$\sin(z) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} z^{2k+1} = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \ldots$$

Jede dieser drei Reihen konvergiert für jeden Parameter $z \in \mathbb{C}$. Wir erhalten so die zugehörigen Funktionen $\exp, \cos, \sin : \mathbb{C} \to \mathbb{C}$.

Mit konvergenten Potenzreihen können wir rechnen wie mit Polynomen: addieren und multiplizieren, differenzieren und integrieren, usw.

Komplexe Zahlen: Polarkoordinaten

Aus diesen Potenzreihen lesen wir die **Euler–Formel** ab:

$$\exp(\mathrm{i}z) = \cos z + \mathrm{i}\sin z, \quad \cos(z) = \frac{\mathrm{e}^{\mathrm{i}z} + \mathrm{e}^{-\mathrm{i}z}}{2}, \quad \sin(z) = \frac{\mathrm{e}^{\mathrm{i}z} - \mathrm{e}^{-\mathrm{i}z}}{2\mathrm{i}}$$

Hieraus folgt sofort die geometrisch nützliche Gleichung

$$\cos(z)^2 + \sin(z)^2 = 1.$$

Auch die Ableitungen lesen wir direkt aus den Potenzreihen ab, denn Potenzreihen dürfen wir termweise ableiten und erhalten so:

$$\exp' = \exp, \quad \sin' = \cos, \quad \cos' = -\sin$$

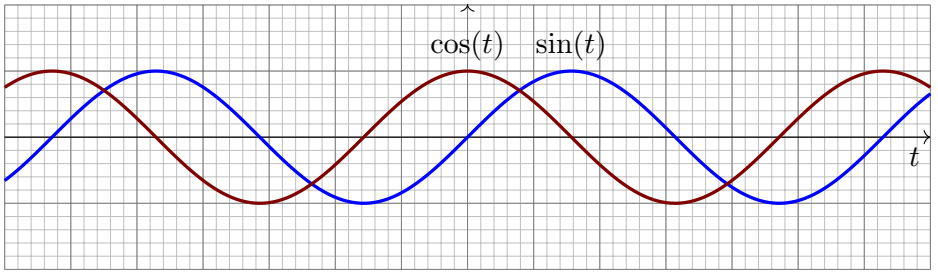
Diese Funktionen sind daher sehr oft nützlich, etwa bei der Integration als Stammfunktionen, als Lösungen von Differentialgleichungen, usw.

Aus der Reihe $\exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!}$ folgt das **Additionstheorem**

$$\exp(z+w) = \exp(z) \cdot \exp(w) \quad \text{für alle } z, w \in \mathbb{C}.$$

Abkürzend schreiben wir $\mathrm{e}^z := \exp(z)$ mit $\mathrm{e} := \exp(1) = 2.71828182\ldots$.

Komplexe Zahlen: Polarkoordinaten



Die trigonometrischen Funktionen $\sin, \cos$ heißen **Kreisfunktionen**, denn $t \mapsto (\cos t, \sin t)$ parametrisiert die Kreislinie $x^2 + y^2 = 1$.

Sie sind periodisch, mit Periode 2π, wobei $\pi = 3.14159265\ldots$. Somit ist auch $\exp : \mathbb{C} \to \mathbb{C}$ periodisch, mit Periode $2\pi\mathrm{i}$.

Für $\sigma, \theta \in \mathbb{R}$ gilt $\exp(\sigma + \mathrm{i}\theta) = \mathrm{e}^{\sigma}(\cos\theta + \mathrm{i}\sin\theta)$. Jede komplexe Zahl $z \in \mathbb{C}$ lässt sich damit in **Polarkoordinaten** darstellen vermöge

$$z = r\,\mathrm{e}^{\mathrm{i}\theta} = r\,(\cos\theta + \mathrm{i}\sin\theta)$$

mit $r = |z| \in \mathbb{R}_{\geq 0}$ und $\theta \in \mathbb{R}$. Im Falle $z = 0$ ist θ beliebig. Im Falle $z \neq 0$ ist θ eindeutig bis Addition eines ganzzahligen Vielfachen von 2π.

Komplexe Zahlen: Fundamentalsatz

Die Erweiterung $\mathbb{C} \supset \mathbb{R}$ beschert dem Polynom X^2+1 die Nullstellen $\pm\mathrm{i}$; damit zerfällt $X^2+1 = (X-\mathrm{i})(X+\mathrm{i})$ in Linearfaktoren über $\mathbb{C}$.

Erfreulicherweise gilt dies sogleich für *jedes* Polynom über $\mathbb{C}$:

Satz A3C: Fundamentalsatz der Algebra (der komplexen Zahlen)

Zu jedem Polynom $P(X) = X^n + c_1X^{n-1} + \cdots + c_n$ mit $c_1, \ldots, c_n \in \mathbb{C}$ existieren Nullstellen $z_1, \ldots, z_n \in \mathbb{C}$ sodass $P(X) = (X-z_1)\cdots(X-z_n)$.

Für $n = 1$ ist das trivial, für $n = 2$ leicht dank Mitternachtsformel:

$$\begin{aligned} z^2 + 2pz + q = 0 \quad &\iff \quad z^2 + 2pz + p^2 = p^2 - q \\ &\iff \quad (z+p)^2 = p^2 - q \\ &\iff \quad z \in \{\, -p \pm \sqrt{p^2 - q}\,\} \end{aligned}$$

Wur nutzen hier: In $\mathbb{C}$ hat jede Zahl $\neq 0$ genau zwei Quadratwurzeln!
Für $n \geq 3$ ist der Beweis raffinierter, siehe Umlaufzahl in der Topologie.

Komplexe Zahlen: Fundamentalsatz

Nicht jedes Polynom $P \in \mathbb{R}[X]$ hat Nullstellen in $\mathbb{R}$, etwa $P = X^2+1$.
Über $\mathbb{C}$ hingegen zerfällt jedes Polynom $P \in \mathbb{C}[X]$ in Linearfaktoren.

🙂 Damit ist der Körper $\mathbb{C}$ **algebraisch abgeschlossen**. Dieser Satz vollendet den langen Marsch der Vervollständigung des Zahlensystems: faszinierend als Theorie und grundlegend für praktische Anwendungen.

Aufgabe: Zerlegen Sie das Polynom $X^2 - \mathrm{i}$ in Linearfaktoren über $\mathbb{C}$.

Lösung: Die Gleichung $z^2 = \mathrm{i}$ hat in $\mathbb{C}$ die Lösungen $\pm(1+\mathrm{i})/\sqrt{2}$.
In $\mathbb{C}[X]$ gilt demnach $X^2 - \mathrm{i} = (X - (1+\mathrm{i})/\sqrt{2})(X + (1+\mathrm{i})/\sqrt{2})$.

Aufgabe: Zerlegen Sie das Polynom $X^n - 1$ in Linearfaktoren über $\mathbb{C}$.

Lösung: Die Gleichung $z^n = 1$ hat in $\mathbb{C}$ die Lösungen $z_k = \mathrm{e}^{2\pi\mathrm{i}k/n}$, also

$$X^n - 1 = \textstyle\prod_{k=0}^{n-1}(X - \mathrm{e}^{2\pi\mathrm{i}k/n}).$$

Die komplexen Zahlen $z_0, z_1, \ldots, z_{n-1}$ sind die **$n$ten Einheitswurzeln**.
Sie bilden die Ecken eines regemäßigen n–Ecks auf dem Einheitskreis.
Polynome und ihre Nullstellen untersuchen wir genauer in Kapitel G.

Hamiltons Quaternionen

Definition A3D: Quaternionen erweitern die komplexen Zahlen.

Die **Quaternionen** $(\mathbb{H}, +, 0, \cdot, 1)$ sind ein Schiefkörper mit $\mathbb{H} \supset \mathbb{C} \supset \mathbb{R}$; dabei gilt $\mathbb{H} = \{\, q = \alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k} \mid \alpha, \beta, \gamma, \delta \in \mathbb{R} \,\}$ mit

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-$j
j	j	$-$k	-1	i
k	k	j	$-$i	-1

kurz $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$,
$\mathrm{ijk} = -1$ und $\mathrm{ij} = -\mathrm{ji}$.

Jede reelle Zahl $\alpha \in \mathbb{R}$ kommutiert dabei mit $\mathrm{i}, \mathrm{j}, \mathrm{k}$, also mit jeder Quaternion.

Die Konjugation ist $\mathbb{H} \to \mathbb{H} : q = \alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k} \mapsto \overline{q} = \alpha - \beta\mathrm{i} - \gamma\mathrm{j} - \delta\mathrm{k}$.

Übung: Prüfen Sie die Ringaxiome nach (direkt oder später in B1G).
Die Inversion in $\mathbb{H}$ ist erfreulich leicht. Ausmultiplizieren ergibt

$$q \cdot \overline{q} = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 =: |q|^2 \quad \in \quad \mathbb{R}_{\geq 0}.$$

Somit ist jede Quaternion $q \neq 0$ invertierbar und $q^{-1} = \overline{q}/|q|^2$.

Hamiltons Quaternionen

Die Körper $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ der rationalen, reellen und komplexen Zahlen werden Ihnen nahezu überall in der Mathematik begegnen, gar noch häufiger in ihren naturwissenschaftlich-technischen Anwendungen.

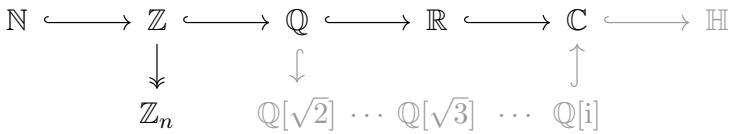
Der Schiefkörper $\mathbb{H}$ der Quaternionen ist weniger prominent und dient uns vor allem zur Illustration, als lockendes oder mahnendes Beispiel. Er zeigt eindrücklich, dass es auch „nicht-kommutative Körper“ gibt.

Ohne konkrete Beispiele und Gegenbeispiele könnten Sie allzu leicht dem Irrglauben verfallen, dass die hier vorgestellten Begriffe gar nicht realisierbar sind. Dagegen helfen am besten explizite Konstruktionen.

Ausgehend von $\mathbb{R}$ können Sie für $\mathbb{C}$ und $\mathbb{H}$ direkt die Körperaxiome nachrechnen; das ist eine gute Übung, aber leider auch etwas länglich. Später gelingt es mühelos mit dem allgemeinen Matrixkalkül (B1F, B1G).

Ein Repertoire an Gegen/Beispielen aufzubauen kostet Zeit und Mühe, doch es lohnt sich. Wie folgen unserer mathematischen Neugier, daran schulen Sie Ihre Anschauung und üben Ihre technische Ausführung.

Zusammenfassung: Aufbau des Zahlensystems



Die **natürlichen Zahlen** $(\mathbb{N}, +, 0, \cdot, 1)$ sind ein kommutativer Halbring; dabei erfüllt $(\mathbb{N}, 0, s)$ mit $s : n \mapsto n + 1$ die Dedekind–Peano–Axiome.

Die **ganzen Zahlen** $(\mathbb{Z}, +, 0, \cdot, 1)$ sind ein kommutativer Ring mit $\mathbb{N} \subset \mathbb{Z}$ als Teilhalbring und $\mathbb{Z} = \{\, z = a - b \mid a, b \in \mathbb{N} \,\}$.

Die **rationalen Zahlen** $(\mathbb{Q}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Z} \subset \mathbb{Q}$ als Teilring und $\mathbb{Q} = \{\, q = z/n \mid z, n \in \mathbb{Z},\ n \neq 0 \,\}$.

Die **reellen Zahlen** $(\mathbb{R}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Q} \subset \mathbb{R}$ und vollständig geordnet durch $x \leq y \ \Leftrightarrow\ \exists a \in \mathbb{R} : x + a^2 = y$.

Die **komplexen Zahlen** $(\mathbb{C}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{R} \subset \mathbb{C}$ dabei gilt $\mathbb{C} = \mathbb{R}[\mathrm{i}] = \{\, z = x + \mathrm{i}y \mid x, y \in \mathbb{R} \,\}$ mit $\mathrm{i}^2 = -1$.

Zusammenfassung: Aufbau des Zahlensystems

Dieses erste Kapitel ist eine Einführung und stellt Ihnen Themen vor, die in den folgenden Kapiteln genauer ausgeführt und vertieft werden. Dazu werden die Begriffe und Techniken hier zunächst motiviert und zugleich soweit erklärt, dass Sie damit sofort arbeiten können.

Wichtige Ergebnisse, Begriffe und Techniken dieses Kapitels:

- Sie sollten sicher in den folgenden Zahlbereichen rechnen können: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, K[X], \mathbb{Z}_n$. Einige sind Ihnen bekannt, andere noch neu.
- Irrationalität von $\sqrt{2}$ (A1F) und die Körpererweiterung $\mathbb{Q}[\sqrt{2}]$ (A1G)
- Kurzschreibweise für Summen $\sum_{i \in I} a_i$ und Produkte $\prod_{i \in I} a_i$ (A135)
- euklidische Division mit Rest in den ganzen Zahlen $\mathbb{Z}$ (A2A)
- Teilbarkeit, ggT und kgV, euklidischer Algorithmus (A2H)
- erweiterter euklidischer Algorithmus nach Bézout (A2I)
- Fundamentalsatz der Arithmetik (A2J) mit Beweis
- Fundamentalsatz der Algebra (A3C) ohne Beweis

Ausblick auf das erste Semester

Diese Einführung vermittelt einen ersten Überblick und erste Methoden, sodass Sie sofort einsteigen, damit üben und bereits arbeiten können:

- ehrliches Beispielmaterial zu den Grundlagen der Mathematik,
- präzise Definitionen und Konstruktionen, soweit bereits möglich,
- wichtige Sätze und instruktive Beweise in unmittelbarer Reichweite.

Das ist ein Sprung ins kalte Wasser, dafür anregend statt langatmig. Die benötigten Begriffe und Techniken werden wir in den nächsten Kapiteln gründlich aufarbeiten. Ich möchte Ihren Appetit und Ihre Neugier wecken, die Mathematik genauer verstehen zu wollen:

- Aussagenlogik und vollständige Induktion
- Mengen, Relationen und Abbildungen
- Monoide und Gruppen, Ringe und Körper

Die entsprechenden Stellen sind durch gelbe Merkzettel markiert, die auf die Ausführungen der folgenden Kapitel verweisen.

Ausblick auf das erste Semester

Mathematische Grundlagen	**Algebraische Grundlagen**	**Lineare Strukturen**
Mathematische Logik und Beweistechniken	Monoide und Gruppen	Lineare Räume und lineare Abbildungen
Mengen und Abbildungen	Ringe und Körper	Basis und Dimension
Kombinatorik und Quotienten	Polynomringe	Darstellung linearer Abbildungen durch Matrizen
Ordnungsrelationen und Kardinalität	Matrixringe	Signatur und Determinante

Kapitel B

Lineare Gleichungssysteme, Matrixkalkül und Gauß–Algorithmus

Give someone a fish and they can eat for a day.
Teach them to fish and they can eat for life.

(anonyme Weisheit)

Inhalt dieses Kapitels B

Motivation und Vorgehensweise

Wie soll man Probleme angehen, insbesondere in der Mathematik? Konkret oder abstrakt? Am besten, Sie beherrschen beides!

- Viele Aufgaben sind ohne passende Theorie schwer bis unlösbar, zur systematischen Lösung entwickeln wir die nötigen Werkzeuge.
- Wenn Sie die allgemein-abstrakten Zusammenhänge gut verstehen, dann können Sie auch speziell-konkrete Probleme effizienter lösen.

🙂 Wir erleben dies hier eindrücklich an einem zentralen Thema: **Lineare Gleichungssysteme, Matrixkalkül und Gauß–Algorithmus**.

Mathematik ist immer beides: sowohl abstrakte Theorie als auch konkrete Anwendung; sie sind keine Gegensätze, sie ergänzen sich, die eine kann nur mit der anderen dauerhaft erfolgreich sein.

Unser treues Arbeitspferd ist der extrem nützliche Gauß–Algorithmus. Mathematik findet nicht nur, aber eben auch auf dem Computer statt. Ich präzisiere dazu Datenstrukturen und Algorithmen soweit möglich.

⚠ Nehmen Sie sich Stift und Papier und arbeiten Sie aktiv mit. An vielen Stellen wollen Sie vermutlich Nebenrechnungen machen.

Motivation und Vorgehensweise

Der Matrixkalkül ist unglaublich vielseitig und flexibel: Matrizen helfen nahezu überall, wo Daten systematisch strukturiert und genutzt werden, in Physik (von Drehmatrizen bis Quantenmechanik) und Informatik (von Computergraphik bis Computeralgebra), allgemein in den Natur- und Ingenieurwissenschaften, ebenso in Ökonometrie und Statistik.

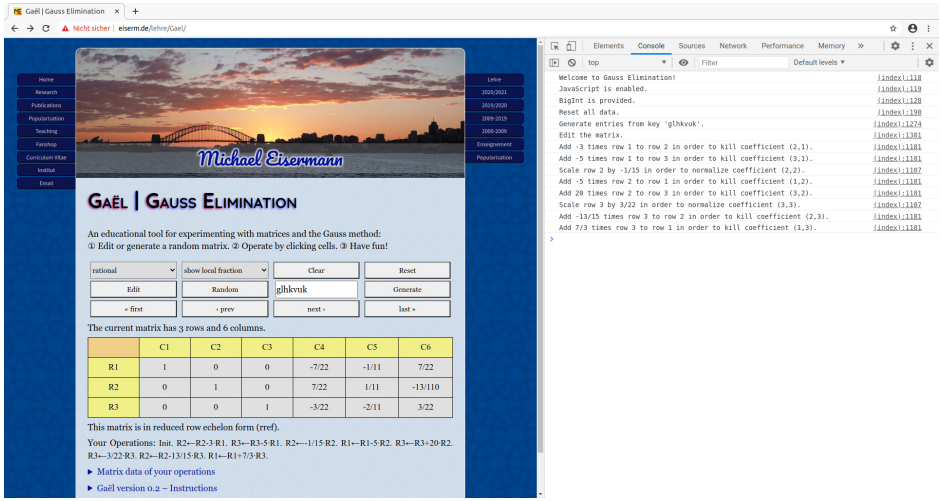
In der Mathematik beginnen Sie im ersten Semester mit der Linearen Algebra (Matrizen für Gleichungssysteme, lineare Abbildungen und quadratische Formen). Dies nutzen Sie im zweiten Semester in der Analysis (als Jacobi–Matrix, Hesse–Matrix, usw.). Ab dem dritten Semester führt die Numerik viele Probleme auf numerische lineare Algebra zurück, dazu entwickelt und untersucht sie Algorithmen zur Matrizenrechnung auf dem Computer. Ebenso werden Matrizen genutzt in der Stochastik (etwa stochastische Matrizen für Markov–Ketten). Nicht zuletzt spielen Matrizen eine wichtige Rolle in der Algebra, etwa Darstellungstheorie, homologische Algebra, algebraische Topologie,. . .

⚠ Der Plural von „die Matrix“ lautet „die Matrizen“, nicht „Matrixen“. Umgekehrt lautet der Singular „die Matrix“ und nicht „die Matrize“.

Gaël: Experimentieren Sie mit dem Gauß–Verfahren

B005
Erläuterung

Das Online-Tool **Gaël** ist intuitiv klickbar, damit können Sie spielen!



Damit lösen Sie lineare Gleichungssysteme, invertieren Matrizen und experimentieren mit Umformungen. Gaël übernimmt die Buchführung.

Panorama: Einige der wichtigsten Algorithmen

B006
Ausblick

Welche Algorithmen scheinen die wichtigsten? Hier meine Vorschläge:
(Diese Liste können Sie durch viele würdige Kandidaten fortsetzen.)

Euklidischer Algorithmus zur Berechnung des ggT

Gröbner–Basen zur Lösung polynomieller Gleichungssysteme

Schnelle Primzahltests und Public Key Cryptography (PKC)

Newtons Methode zur iterativen Nullstellennäherung

Matrixzerlegung, Gauß (LU), Householder-Givens (QR), Cholesky

Lineare Optimierung, Simplexverfahren, Innere-Punkt-Methode

Schnelles Suchen und Sortieren, Quick-/Merge-/Heap-sort

Schnelle Fourier–Transformation (FFT) zur Signalverarbeitung

Datenkompression mittels JPEG, MPEG, MP3, Wavelets, etc.

Monte-Carlo-Methode zur Erwartungsschätzung durch Sampling

Kalman–Filter zur Zeitreihenanalyse und Zustandsschätzung

Googles PageRank zur Popularitätswertung von Internetseiten

Panorama: Einige der wichtigsten Algorithmen

B007
Ausblick

Ich würde mir für Sie wünschen, dass Sie möglichst viele dieser Techniken in Ihrem Studium kennen, nutzen und schätzen lernen.

Meine Liste ist nicht ganz willkürlich, aber naturgemäß subjektiv. Inspiriert wurde sie von einer ähnlichen Top-10-Liste in *Computing in Science and Engineering* (2000), dem *Princeton Companion to Applied Mathematics* (2016) und dem Buch *Modern Computer Algebra* (2013).

Euklid (um 300 v.Chr.) nutzte seinen Algorithmus für natürliche Zahlen, er gilt ebenso für Polynome und allgemein in jedem euklidischen Ring. Die Methode von Newton (1643–1727) zur Nullstellennäherung nutzte bereits Heron von Alexandria (10–70 n.Chr.) in einfachen Spezialfällen.

Alle weiteren Algorithmen sind Entdeckungen des 20. Jahrhunderts und boomen seit Entwicklung und durch Einsatz elektronischer Computer.

Kryptographie, Datenkompression, PageRank und Data Mining erblühen insbesondere durch die rasante Popularisierung des Internets seit 1990. In diesen Bereichen ist die Mathematik auch im Alltag direkt spürbar und deutlich sichtbar für alle, die unter die Oberfläche schauen.

Panorama: Einige der wichtigsten Algorithmen

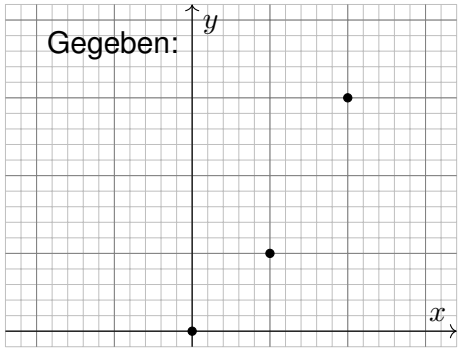
B008
Ausblick

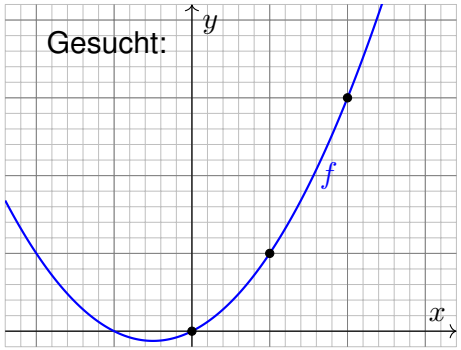
Jede große Entwicklung des 20. Jahrhunderts, etwa die Raumfahrt, benötigte diese algorithmischen Grundlagen – und noch viele weitere. Zu Beginn des 21. Jahrhunderts ist absehbar, dass auch die nächsten großen Entwicklungen darauf aufbauen und die Werkzeuge erweitern. Durch Data Science und Machine Learning werden die algorithmischen Grundlagen nicht ersetzt oder überflüssig, sondern weiter ausgebaut.

Schon heute ist es kaum möglich, sich auf eine „Top-Ten“ zu einigen. In Zukunft wird dies noch schwieriger, da die diversen Teilgebiete der Computational Mathematics weiter gedeihen und expandieren werden. Vielleicht sollte ich daher besser von der „Top-one-hundred“ sprechen, noch fairer von Top-Algorithmen je nach Gebiet und Problemstellung. Differenzierung und Spezialisierung werden weiter fortschreiten.

In diesem Kapitel geht es um einen ersten dieser Top-Algorithmen: Das Gauß–Verfahren zur Lösung linearer Gleichungssysteme. Dies gehört zweifellos zu den Top-Ten der wichtigsten Algorithmen. Zur würdigen Einordnung habe ich das Gesamtpanorama skizziert.

Beispiel: Kurve durch Datenpunkte





Aufgabe: Finden Sie alle Parabeln, also Polynomfunktionen

$$f : \mathbb{R} \to \mathbb{R} : f(x) = ax^2 + bx + c,$$

die durch die Punkte $f(0) = 0$ und $f(1) = 1$ und $f(2) = 3$ laufen.

Wir wollen mindestens eine Lösung finden, am besten alle Lösungen!
Gibt es überhaupt mindestens eine Lösung? Ist sie zudem eindeutig?

Beispiel: Kurve durch Datenpunkte

Diese Aufgabe ist sehr einfach, doch in vielerlei Hinsicht typisch.
In der **Geometrie** betrachten wir Geraden, Kreise, Ellipsen, Parabeln, Hyperbeln, etc. Klassisch konstruieren wir diese mit Lineal, Zirkel und weiteren Werkzeugen. Die geniale Idee der **Analytischen Geometrie** ist es, Punkte durch **Koordinaten** zu beschreiben. Das gibt uns ein Universalwerkzeug an die Hand: Mit Koordinaten können wir rechnen!

Die **Polynominterpolation** durch vorgegebene Datenpunkte ist ein grundlegendes Hilfsmittel in der **Numerik**. In vielen Anwendungen sind diese Datenpunkte gemessene Werte und daher mit Fehlern behaftet. In diesem Falle wollen wir nicht exakt durch alle Punkte gehen, sondern suchen eine gute Näherung. Das ist ein Grundwerkzeug der **Statistik**: Ausgleichsgerade, Fehler minimieren, Methode der kleinsten Quadrate. Allgemein im **Maschinellen Lernen** will man Datenpunkte möglichst effizient und sinnvoll beschreiben, auswerten, bündeln, interpretieren.

Zur Vereinfachung betrachten wir hier ein Minimalbeispiel mit drei exakten Datenpunkten, durch die wir eine Parabel legen wollen.

Erste Lösung durch Lagrange–Interpolation

Erste Lösung: Sei $\mathbb{K}$ ein Körper, etwa $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ oder $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\mathrm{i}], \ldots$.
Vorgegeben seien $n+1$ verschiedene Stützstellen $x_0, x_1, \ldots, x_n \in \mathbb{K}$.
Zu jedem $j = 0, 1, \ldots, n$ definieren wir das **Lagrange–Polynom**

$$L_j(X) := \prod_{i \neq j} \frac{X - x_i}{x_j - x_i} \quad \in \mathbb{K}[X]_n$$

Dieses Polynom erfüllt $L_j(x_j) = 1$ und $L_j(x_i) = 0$ für alle $i \neq j$.
Zu den Werten $y_0, y_1, \ldots, y_n \in \mathbb{K}$ betrachten wir die Linearkombination

$$L(X) := \sum_{j=0}^{n} y_j L_j(X) \quad \in \mathbb{K}[X]_{\leq n}.$$

Diese erfüllt $L(x_j) = y_j$ für alle $j = 0, 1, \ldots, n$, wie gewünscht.

🙂 Dies konstruiert *eine* Lösung. Es könnte noch *weitere* geben!

Übung: Rechnen Sie dies konkret aus für $x = (0, 1, 2)$ und $y = (0, 1, 3)$.
Vergleichen Sie Ihr Ergebnis mit der folgenden zweiten Lösung.

Erste Lösung durch Lagrange–Interpolation

🙂 Diese Lösung können wir direkt hinschreiben, als explizite Formel, ohne weitere Rechnung. Bitte führen Sie dies hier konkret aus!

☹ Dies klärt noch nicht, ob es vielleicht noch weitere Lösungen gibt: Wir haben die Existenz einer Lösung, aber noch nicht ihre Eindeutigkeit.

🙂 Zur Eindeutigkeit benötigen wir ein weiteres Werkzeug:

♦ Satz B3A: Polynom vom Grad $\leq n$ auf $n+1$ Punkten festlegen

Sei $\mathbb{K}$ ein Körper oder allgemein ein kommutativer Ring ohne Nullteiler. Jedes Polynom $P \in \mathbb{K}[X]$ vom Grad $\deg P \leq n$ wird bereits durch seine Werte an $n+1$ Stellen $x_0, x_1, \ldots, x_n \in \mathbb{K}$ eindeutig festgelegt.

Ausführlich: Erfüllen die Polynome $P, Q \in \mathbb{K}[X]_{\leq n}$ die Bedingungen $P(x_i) = Q(x_i)$ für alle $i = 0, 1, \ldots, n$, so folgt $P = Q$.

Diesen schönen und grundlegenden Satz behandeln wir ausführlich im Kapitel über Polynome durch die Abspaltung von Nullstellen durch euklidische Division. Wir erhalten die Eindeutigkeit auch bereits am Ende dieses Kapitels als Folgerung aus dem Gauß–Algorithmus.

Zweite Lösung durch lineares Gleichungssystem

Ausprobieren mit Gaël!

Zweite Lösung: Wir haben den Ansatz $f(x) = ax^2 + bx + c$.
Gesucht sind die Koeffizienten $a, b, c \in \mathbb{R}$, sodass gilt:

$$\begin{aligned} f(0) = 0 \quad &\Leftrightarrow \quad R_1: \quad 0 \cdot a + 0 \cdot b + 1 \cdot c = 0 \\ f(1) = 1 \quad &\Leftrightarrow \quad R_2: \quad 1 \cdot a + 1 \cdot b + 1 \cdot c = 1 \\ f(2) = 3 \quad &\Leftrightarrow \quad R_3: \quad 4 \cdot a + 2 \cdot b + 1 \cdot c = 3 \end{aligned}$$

Wir formen solche Systeme um durch **elementare Zeilenoperationen**:

Permutation	P_{ij}:	$R_i \leftrightarrow R_j$,	vertausche die Zeilen i und j.
Skalierung	$S_i(\mu)$:	$R_i \leftarrow \mu R_i$,	multipliziere Zeile i mit $\mu \neq 0$.
Transvektion	$T_{ij}(\lambda)$:	$R_j \leftarrow R_j + \lambda R_i$,	addiere λ mal Zeile i zur Zeile j.

- Jede dieser Zeilenoperationen können wir verlustfrei umkehren, jeweils durch die inverse Operation P_{ij} und $S_i(\mu^{-1})$ und $T_{ij}(-\lambda)$.
- Jede Lösung vor der Operation ist auch Lösung nach der Operation. Inversion zeigt umgekehrt: Jede Lösung danach ist auch eine davor.

☺ Alle Lösungen bleiben erhalten, und es kommen keine dazu.

Zweite Lösung durch lineares Gleichungssystem

Wir wollen folgendes Gleichungssystem lösen:

$$\left\{\begin{array}{rcrcrcl} 0a & + & 0b & + & 1c & = & 0 \\ 1a & + & 1b & + & 1c & = & 1 \\ 4a & + & 2b & + & 1c & = & 3 \end{array}\right.$$

Zeilenoperation P_{12}: Wir vertauschen die Zeilen 1 und 2.

$$\left\{\begin{array}{rcrcrcl} 1a & + & 1b & + & 1c & = & 1 \\ 0a & + & 0b & + & 1c & = & 0 \\ 4a & + & 2b & + & 1c & = & 3 \end{array}\right.$$

Zeilenoperation $T_{13}(-4)$: Wir addieren (-4) mal Zeile 1 zu Zeile 3.

$$\left\{\begin{array}{rcrcrcl} 1a & + & 1b & + & 1c & = & 1 \\ 0a & + & 0b & + & 1c & = & 0 \\ 0a & - & 2b & - & 3c & = & -1 \end{array}\right.$$

Zeilenoperation P_{23}: Wir vertauschen die Zeilen 2 und 3.

$$\left\{\begin{array}{rcrcrcl} 1a & + & 1b & + & 1c & = & 1 \\ 0a & - & 2b & - & 3c & = & -1 \\ 0a & + & 0b & + & 1c & = & 0 \end{array}\right.$$

Zweite Lösung durch lineares Gleichungssystem

Unser Gleichungssystem lautet nun:

$$\left\{\begin{array}{rcrcrcl} 1a & + & 1b & + & 1c & = & 1 \\ 0a & - & 2b & - & 3c & = & -1 \\ 0a & + & 0b & + & 1c & = & 0 \end{array}\right.$$

Zeilenoperation $S_2(-1/2)$: Wir skalieren die Zeile 2.

$$\left\{\begin{array}{rcrcrcl} 1a & + & 1b & + & 1c & = & 1 \\ 0a & + & 1b & + & 3/2c & = & 1/2 \\ 0a & + & 0b & + & 1c & = & 0 \end{array}\right.$$

Zeilenoperation $T_{21}(-1)$: Wir addieren (-1) mal Zeile 2 zu Zeile 1.

$$\left\{\begin{array}{rcrcrcl} 1a & + & 0b & - & 1/2c & = & 1/2 \\ 0a & + & 1b & + & 3/2c & = & 1/2 \\ 0a & + & 0b & + & 1c & = & 0 \end{array}\right.$$

Zeilenoperation $T_{31}(1/2)$ und $T_{32}(-3/2)$ zum guten Schluss:

$$\left\{\begin{array}{rcrcrcl} 1a & + & 0b & + & 0c & = & 1/2 \\ 0a & + & 1b & + & 0c & = & 1/2 \\ 0a & + & 0b & + & 1c & = & 0 \end{array}\right.$$

Von linearen Gleichungssystemen zu Matrizen

☺ Unser Gleichungssystem hat die Lösung $(a, b, c) = (1/2, 1/2, 0)$.
Unser ursprüngliches Interpolationsproblem wird also gelöst durch

$$f : \mathbb{R} \to \mathbb{R} : f(x) = \frac{1}{2}x^2 + \frac{1}{2}x + 0 = \frac{x(x+1)}{2}.$$

Probe: Es gilt $f(0) = 0$ und $f(1) = 1$ und $f(2) = 3$, wie gefordert.

☺ Unsere Rechnung zeigt zudem, dass dies die einzige Lösung ist.
Diese Gewissheit ist ebenfalls wichtig, und hier Teil der Frage!

Was lernen wir an dieser vorbildlichen Notation und Rechnung?

- In der $j$ten Spalte steht immer die $j$te Variable. Dabei ist es egal, wie die Variablen heißen, etwa a, b, c oder x, y, z oder x_1, x_2, x_3.
- Wir wollen die Variablen nicht immer mitschleppen und wiederholen. Es genügt, die Koeffizienten zu notieren, um mit diesen zu arbeiten.

☺ Wir trennen daher im Folgenden Koeffizienten und Variablen.
Wir rechnen allein mit der Koeffizientenmatrix, das ist effizienter!
Wir nutzen die vier Grundrechenarten, nicht mehr und nicht weniger.

Matrixkalkül: Schreibweise

B109

Produktmenge Abbildungen

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, oder allgemein ein Ring, wie $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{H}$.
Für Addition und Multiplikation allein genügt sogar ein Halbring, wie $\mathbb{N}$.
Wir erklären, was **Matrizen über** $\mathbb{K}$ sind und wie man damit rechnet.

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \quad \text{oder} \quad A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Gegeben sei die Zeilenzahl $m \in \mathbb{N}$ und die Spaltenzahl $n \in \mathbb{N}$.
Als Indexmengen nutzen wir $I = \{1, 2, \ldots, m\}$ und $J = \{1, 2, \ldots, n\}$.
Jedem Indexpaar $(i, j) \in I \times J$ wird ein Koeffizient $a_{i,j} \in \mathbb{K}$ zugeordnet.

Eine **Matrix** A der Größe $m \times n$ über $\mathbb{K}$ ist demnach eine Abbildung

$$A : I \times J \to \mathbb{K} : (i, j) \mapsto A(i, j) = A_{i,j} = A_{ij} = a_{i,j} = a_{ij}.$$

Die Matrix A schreiben wir bequem als rechteckiges Schema, wie oben, mit m Zeilen und n Spalten, kurz $A = (a_{ij})_{i=1,\ldots,m}^{j=1,\ldots,n}$, oder $A = (a_{ij})_{ij}$ oder $A = (a_{ij})$, wenn die Dimensionen m und n aus dem Kontext klar sind.

Matrixkalkül: Schreibweise

B110
Erläuterung

Wir schreiben kurz a_{ij}, wenn keine Verwechslung zu befürchten ist.
Indizes werden nur selten multipliziert; falls nötig schreiben wir $a_{i \cdot j}$.

In vielen Anwendungen, insbesondere auf dem Computer, werden auch andere Indexmengen verwendet, elegant ist $m = \{0, 1, \ldots, m-1\}$ und $n = \{0, 1, \ldots, n-1\}$, aber das bringe ich hier noch nicht übers Herz.

Zur Indizierung genügen beliebige Mengen $I' = \{i_1 < i_2 < \cdots < i_m\}$ und $J' = \{j_1 < j_2 < \cdots < j_n\}$. Zur bequemen Darstellung als Rechteck benötigen wir die vorgegebene Anordnung. Damit können wir eindeutig zu unserm Standard $I = \{1 < 2 < \cdots < m\}$ und $J = \{1 < 2 < \cdots < n\}$ umnummerieren. Somit ist immer klar, was die $i$te Zeile und die $j$te Spalte ist. Genau darauf bauen nahezu alle folgenden Algorithmen.

Das nutzen wir, wenn wir zur Matrix $A : I \times J \to \mathbb{K}$ eine Untermatrix $A|_{I' \times J'} : I' \times J' \to \mathbb{K}$ betrachten mit Teilmengen $I' \subseteq J$ und $J' \subseteq J$.

Zwei Matrizen $A : I \times J \to \mathbb{K}$ und $A' : I' \times J' \to \mathbb{K}'$ sind gleich, wenn sie als Abbildungen gleich sind, also $I = I'$ und $J = J'$ und $\mathbb{K} = \mathbb{K}'$ sowie $a_{ij} = a'_{ij}$ für alle $(i, j) \in I \times J$ gilt. Laxer erlauben wir meist monotone Umnummerierung $I \cong I'$ und $J \cong J'$ mit $a_{ij} = a'_{i'j'}$ für $(i, j) \leftrightarrow (i', j')$.

Matrixkalkül: Transposition

B111

Zu $A = (a_{ij})_{ij}$ definieren wir die **transponierte Matrix** $A^\mathsf{T} = (a_{ij})_{ji}$:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \iff A^\mathsf{T} = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$$

$$A : I \times J \to \mathbb{K} : (i, j) \mapsto a_{ij} \iff A^\mathsf{T} : J \times I \to \mathbb{K} : (j, i) \mapsto a^\mathsf{T}_{ji} = a_{ij}$$

Dies definiert die **Transposition** $\mathbb{K}^{m \times n} \to \mathbb{K}^{n \times m} : A \mapsto A^\mathsf{T}$
für alle $m, n \in \mathbb{N}_{\geq 1}$. Offensichtlich gilt dabei $(A^\mathsf{T})^\mathsf{T} = A$.

Genau dann gilt $A^\mathsf{T} = A$, wenn die Matrix A **symmetrisch** ist, also quadratisch ist (mit $m = n$) und $a_{ij} = a_{ji}$ für alle $i, j = 1, \ldots, n$ erfüllt.

$$S = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}, \qquad Q = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

Beispiel: Die hier gezeigte Matrix $S \in \mathbb{Z}^{3 \times 3}$ ist symmetrisch,
die Matrix $Q \in \mathbb{Z}^{3 \times 3}$ ist zwar quadratisch, aber nicht symmetrisch.
Eine Matrix A mit $A^\mathsf{T} = -A$ heißt **antisymmetrisch**.

Matrixkalkül: Einheitsmatrix

B112

In dieser Schreibweise ist $u \in \mathbb{K}^{1 \times n}$ ein **Zeilenvektor** mit n Spalten.
Entsprechend ist $v \in \mathbb{K}^{m \times 1}$ ein **Spaltenvektor** mit m Zeilen.

$$A = \begin{bmatrix} — & u_1 & — \\ & \vdots & \\ — & u_m & — \end{bmatrix} = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix}, \quad A^\mathsf{T} = \begin{bmatrix} | & & | \\ u_1^\mathsf{T} & \cdots & u_m^\mathsf{T} \\ | & & | \end{bmatrix} = \begin{bmatrix} — & v_1^\mathsf{T} & — \\ & \vdots & \\ — & v_n^\mathsf{T} & — \end{bmatrix}$$

Die Transposition macht Zeilen zu Spalten und umgekehrt.

Die **Einheitsmatrix** der Größe $n \times n$ ist

$$E = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \quad \text{mit} \quad e_{ij} = \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Beliebte Schreibweisen sind $E = E_n = I = I_n = 1 = 1_n = 1_{n \times n}$.

Sie hat als Spalten die **Spalten-Einheitsvektoren** $e_1, \ldots, e_n \in \mathbb{K}^{n \times 1}$,
und als Zeilen die **Zeilen-Einheitsvektoren** $e_1^\mathsf{T}, \ldots, e_n^\mathsf{T} \in \mathbb{K}^{1 \times n}$.

Matrixkalkül: Addition von Matrizen

B113
Gruppen

Matrizen gleicher Größe können wir addieren:

$$\begin{bmatrix}1&2&3\\4&5&6\end{bmatrix} \mathbf{+} \begin{bmatrix}0&2&0\\2&0&3\end{bmatrix} = \begin{bmatrix}1+0&2+2&3+0\\4+2&5+0&6+0\end{bmatrix} = \begin{bmatrix}1&4&3\\6&5&9\end{bmatrix}$$

Wir definieren dazu die **Matrixaddition**:

$$\mathbf{+} : \mathbb{K}^{m\times n} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n} : (A,B) \mapsto C = A \mathbf{+} B, \;\; c_{ij} = a_{ij} + b_{ij}$$

Das ist die koeffizientenweise Addition $+$ im Ring $\mathbb{K}$.
Da $(\mathbb{K}, +, 0, -)$ eine Gruppe ist, haben wir zudem

$$\mathbf{0} = \begin{bmatrix}0&0&0\\0&0&0\end{bmatrix}, \qquad \mathbf{-}\begin{bmatrix}0&1&-2\\3&-5&0\end{bmatrix} = \begin{bmatrix}0&-1&2\\-3&5&0\end{bmatrix}.$$

Wir nennen $\mathbf{0} = 0_{m\times n} = (0)_{i=1,\dots,m}^{j=1,\dots,n}$ die **Nullmatrix** der Größe $m \times n$.
Zur Matrix $A = (a_{ij})$ nennen wir $\mathbf{-}A = (-a_{ij})_{ij}$ die **negative Matrix**.

🙂 Die Skalare $(\mathbb{K}, +, 0, -)$ bilden eine **kommutative Gruppe**,
daher auch die Matrizen $(\mathbb{K}^{m\times n}, \mathbf{+}, \mathbf{0}, \mathbf{-})$ der Größe $m \times n$ über $\mathbb{K}$.

Matrixkalkül: Addition von Matrizen

B114
Gruppen

Übung: Die Matrizen $(\mathbb{K}^{m\times n}, \mathbf{+}, \mathbf{0}, \mathbf{-})$ bilden eine kommutative Gruppe.
(0) Was muss geprüft werden? (1) Rechnen Sie es allgemein nach!

Lösung: (0) Für alle Matrizen $A, B, C \in \mathbb{K}^{m\times n}$ ist zu zeigen:

$$A \mathbf{+} (B \mathbf{+} C) = (A \mathbf{+} B) \mathbf{+} C, \qquad \mathbf{0} \mathbf{+} A = A \mathbf{+} \mathbf{0} = A,$$
$$A \mathbf{+} B = B \mathbf{+} A, \qquad A \mathbf{+} (\mathbf{-}A) = (\mathbf{-}A) \mathbf{+} A = \mathbf{0}$$

(1) Wir rechnen die Assoziativität koordinatenweise nach:

$$\begin{aligned}[A \mathbf{+} (B \mathbf{+} C)]_{ij} &\overset{\text{Def}}{=} a_{ij} + (B \mathbf{+} C)_{ij} \\ &\overset{\text{Def}}{=} a_{ij} + (b_{ij} + c_{ij}) \\ &\overset{\text{Ass}}{=} (a_{ij} + b_{ij}) + c_{ij} \\ &\overset{\text{Def}}{=} (A \mathbf{+} B)_{ij} + c_{ij} \overset{\text{Def}}{=} [(A \mathbf{+} B) \mathbf{+} C]_{ij}\end{aligned}$$

Ebenso folgt Kommutativität, Neutrales und Negatives. QED

🙂 Die guten Eigenschaften von $(\mathbb{K}, +, 0, -)$ übertragen sich
koordinatenweise zu guten Eigenschaften von $(\mathbb{K}^{m\times n}, \mathbf{+}, \mathbf{0}, \mathbf{-})$.

Matrixkalkül: Multiplikation mit Skalaren

B115
Lineare Räume
Vektorräume

Matrizen können wir von links mit Skalaren aus $\mathbb{K}$ multiplizieren:

$$2 \mathbf{\cdot} \begin{bmatrix}1&3&4\\3&4&0\end{bmatrix} = \begin{bmatrix}2\cdot1&2\cdot3&2\cdot4\\2\cdot3&2\cdot4&2\cdot0\end{bmatrix} = \begin{bmatrix}2&6&8\\6&8&0\end{bmatrix}$$

Wir definieren dazu die **Skalarmultiplikation**:

$$\mathbf{\cdot} : \mathbb{K} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n} : (\lambda, A) \mapsto B = \lambda \mathbf{\cdot} A, \;\; b_{ij} = \lambda \cdot a_{ij}$$

Übung: Für alle Skalare $\lambda, \mu \in \mathbb{K}$ und Matrizen $A, B \in \mathbb{K}^{m\times n}$ gilt:

$$\lambda \mathbf{\cdot} (A \mathbf{+} B) = \lambda \mathbf{\cdot} A \mathbf{+} \lambda \mathbf{\cdot} B, \qquad 1 \mathbf{\cdot} A = A,$$
$$(\lambda + \mu) \mathbf{\cdot} A = \lambda \mathbf{\cdot} A \mathbf{+} \mu \mathbf{\cdot} A, \qquad \lambda \mathbf{\cdot} (\mu \mathbf{\cdot} A) = (\lambda \cdot \mu) \mathbf{\cdot} A$$

Zusammenfassend: $(\mathbb{K}^{m\times n}, \mathbf{+}, \mathbf{\cdot})$ ist ein **linearer Raum** über $(\mathbb{K}, +, \cdot)$.
Ebenso können wir von rechts mit Skalaren multiplizieren:

$$\mathbf{\cdot} : \mathbb{K}^{m\times n} \times \mathbb{K} \to \mathbb{K}^{m\times n} : (A, \lambda) \mapsto C = A \mathbf{\cdot} \lambda, \;\; c_{ij} = a_{ij} \cdot \lambda$$

Die obigen Regeln gelten dann von rechts. Ist $(\mathbb{K}, \cdot)$ kommutativ, so gilt
$\lambda \mathbf{\cdot} A = A \mathbf{\cdot} \lambda$, andernfalls sind Links- und Rechtsoperation verschieden.

Matrixkalkül: Addition und Skalarmultiplikation

B116
Erläuterung

Zur Betonung habe ich hier die Addition $\mathbf{+}$ und die Skalarmultiplikation $\mathbf{\cdot}$ für Matrizen fett hervorgehoben. So unterscheiden wir sie graphisch von der zugrundeliegenden Addition $+$ und Multiplikation $\cdot$ der Skalare im Koeffizientenring $(\mathbb{K}, +, \cdot)$. Das ist insbesondere für die ersten Rechnungen didaktisch sinnvoll, wie hier ausgeführt.

Diese pedantische Unterscheidung ist mathematisch gerechtfertigt: Streng genommen sind $\mathbf{+}$ und $+$ bzw. $\mathbf{\cdot}$ und $\cdot$ verschiedene Operationen, daher verdienen sie zur Klarheit auch verschiedene Bezeichnungen.

Auf Dauer wird diese Schreibweise jedoch lästig. Aus dem Kontext ist ohnehin jeweils klar, was gemeint ist, daher schreiben wir später beide Additionen kurz $+$ und beide Multiplikationen kurz $\cdot$. Das ist bequemer.

Für die grundlegenden Rechnungen dieses Abschnitts betone ich weiterhin den Unterschied. Ich hoffe, diese Genauigkeit hilft Ihnen. Die (fahr)lässige Ungenauigkeit kommt früh genug von ganz allein.

Matrixkalkül: Multiplikation von Matrizen

Zwei Matrizen passender Größe können wir **multiplizieren** vermöge

$$\bullet : \mathbb{K}^{p\times q} \times \mathbb{K}^{q\times r} \to \mathbb{K}^{p\times r} : (A,B) \mapsto C = A \bullet B,\ \ c_{ik} = \sum_{j=1}^{q} a_{ij} \cdot b_{jk}.$$

⚠ Voraussetzung: Die Spaltenzahl von A ist die Zeilenzahl von B.
Wir nutzen die Multiplikation $\cdot$ *und* die Addition $+$ der Koeffizienten.
Diese Summenformel bedeutet anschaulich **Zeile mal Spalte**:

$$\begin{bmatrix} u_1 & u_2 & \dots & u_n \end{bmatrix} \bullet \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = u_1 \cdot v_1 + u_2 \cdot v_2 + \dots + u_n \cdot v_n$$

Ein einfaches Beispiel:

$$\begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \bullet \begin{bmatrix} 1 \\ -4 \\ 2 \end{bmatrix} = 1 \cdot 1 + 2 \cdot (-4) + 3 \cdot 2 = -1$$

⚠ Hierzu müssen beide Vektoren dieselbe Länge n haben!

Matrixkalkül: Multiplikation von Matrizen

Zwei Matrizen passender Größe können wir **multiplizieren** vermöge

$$\bullet : \mathbb{K}^{p\times q} \times \mathbb{K}^{q\times r} \to \mathbb{K}^{p\times r} : (A,B) \mapsto C = A \bullet B,\ \ c_{ik} = \sum_{j=1}^{q} a_{ij} \cdot b_{jk}.$$

Im Matrixprodukt $A \bullet B$ multiplizieren wir demnach jede Zeile von A mit jeder Spalte von B. Das lässt sich graphisch geschickt darstellen:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 2 & 4 & 3 \\ -4 & 2 & 3 & -4 \\ 2 & -2 & -5 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} -1 & 0 & -5 & -2 \\ -4 & 6 & 1 & -2 \end{bmatrix} = A \bullet B$$

Übung: Rechnen Sie dieses Beispiel vollständig nach.

⚠ Beim Produkt $A \bullet B$ müssen die Zeilen von A und die Spalten von B dieselbe Länge haben. Andernfalls ist das Matrixprodukt nicht definiert. Wer trotzdem gedankenlos weiterrechnet produziert Unsinn.

Matrixkalkül: Reihenfolge der Multiplikation

Die Matrixmultiplikation ist nicht kommutativ: Für $p \neq q$ und $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times p}$ sind $A \bullet B \in \mathbb{K}^{p\times p}$ und $B \bullet A \in \mathbb{K}^{q\times q}$ verschieden groß.

Selbst für quadratische Matrizen, mit $p = q \geq 2$, gilt meist $A \bullet B \neq B \bullet A$:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{vs} \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Übung: Wählen und prüfen Sie zufällige Beispiele, etwa:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \bullet \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 3 & 7 \end{bmatrix} \quad \text{vs} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \bullet \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 3 & 4 \end{bmatrix}$$

Die Transposition kehrt die Reihenfolge um, $(A \bullet B)^\intercal = B^\intercal \bullet A^\intercal$.

$$\begin{aligned} (A \bullet B)^\intercal_{ki} &= (A \bullet B)_{ik} &&= \textstyle\sum_{j=1}^{q} a_{ij} \cdot b_{jk} \\ (B^\intercal \bullet A^\intercal)_{ki} &= \textstyle\sum_{j=1}^{q} b^\intercal_{kj} \cdot a^\intercal_{ji} &&= \textstyle\sum_{j=1}^{q} b_{jk} \cdot a_{ij} \end{aligned}$$

Hierzu benötigen wir allerdings, dass der Ring $(\mathbb{K}, +, \cdot)$ kommutativ ist! Andernfalls müssten wir in $\mathbb{K}$ die Multiplikationsreihenfolge umkehren.

Matrixkalkül: Distributivität der Multiplikation

Aufgabe: Die Matrixmultiplikation ist distributiv über die Addition.
(0) Was bedeutet das genau? (1) Rechnen Sie es allgemein nach!

Lösung: (0) Für alle Matrizen $A, A' \in \mathbb{K}^{p\times q}$ und $B, B' \in \mathbb{K}^{q\times r}$ gilt:

$$\begin{aligned} &\text{DL:} && A \bullet (B + B') = A \bullet B + A \bullet B' \\ &\text{DR:} && (A + A') \bullet B = A \bullet B + A' \bullet B \end{aligned}$$

(1) Wir rechnen die Linksdistributivität koordinatenweise geduldig nach:

$$\begin{aligned} [A \bullet (B + B')]_{ik} &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot (B + B')_{jk} \\ &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot (b_{jk} + b'_{jk}) \\ &\overset{\text{DL}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot b_{jk} + a_{ij} \cdot b'_{jk} \\ &\overset{\text{Add}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot b_{jk} + \sum_{j=1}^{q} a_{ij} \cdot b'_{jk} \\ &\overset{\text{Def}}{=} (A \bullet B)_{ik} + (A \bullet B')_{ik} \\ &\overset{\text{Def}}{=} [A \bullet B + A \bullet B']_{ik} \end{aligned}$$

Genauso rechnet man auch die Rechtsdistributivität nach.

Matrixkalkül: Assoziativität der Multiplikation

B121

Zu jeder Matrix $A \in \mathbb{K}^{m\times n}$ ist die Einheitsmatrix $1_{m\times m}$ linksneutral, also $1_{m\times m} \cdot A = A$, und $1_{n\times n}$ ist rechtsneutral, also $A \cdot 1_{n\times n} = A$:

$$(1_{m\times m} \cdot A)_{ik} = \sum_{j=1}^{m} e_{ij} \cdot a_{jk} = a_{ik}$$
$$(A \cdot 1_{n\times n})_{ik} = \sum_{j=1}^{n} a_{ij} \cdot e_{jk} = a_{ik}$$

Aufgabe: Die Matrixmultiplikation ist assoziativ, für alle Matrizen $A \in \mathbb{K}^{p\times q}$, $B \in \mathbb{K}^{q\times r}$, $C \in \mathbb{K}^{r\times s}$ gilt $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ in $\mathbb{K}^{p\times s}$.

Lösung: Wir rechnen die Assoziativität koordinatenweise nach:

$$\begin{aligned}
[A \cdot (B \cdot C)]_{i\ell} &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot (B \cdot C)_{j\ell} \\
&\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot \left[\sum_{k=1}^{r} b_{jk} \cdot c_{k\ell}\right] \\
&\overset{\text{DL}}{=} \textstyle\sum_{j=1}^{q} \sum_{k=1}^{r} a_{ij} \cdot (b_{jk} \cdot c_{k\ell}) \\
&\overset{\text{Ass}}{=} \textstyle\sum_{j=1}^{q} \sum_{k=1}^{r} (a_{ij} \cdot b_{jk}) \cdot c_{k\ell} \\
&\overset{\text{Add}}{=} \textstyle\sum_{k=1}^{r} \sum_{j=1}^{q} (a_{ij} \cdot b_{jk}) \cdot c_{k\ell} \\
&\overset{\text{DR}}{=} \textstyle\sum_{k=1}^{r} \left[\sum_{j=1}^{q} a_{ij} \cdot b_{jk}\right] \cdot c_{k\ell} \\
&\overset{\text{Def}}{=} \textstyle\sum_{k=1}^{r} (A \cdot B)_{ik} \cdot c_{k\ell} \qquad \overset{\text{Def}}{=} [(A \cdot B) \cdot C]_{i\ell}
\end{aligned}$$

Matrixkalkül: Assoziativität und Kommutativität

B122
Erläuterung

Zu Koeffizienten $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{K}$ definieren wir die **Diagonalmatrix**

$$D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{bmatrix}, \quad d_{ij} = \begin{cases} \lambda_i & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Das Produkt $D \cdot A$ multipliziert die $i$te Zeile von A mit λ_i von links.
Das Produkt $A \cdot D$ multipliziert die $i$te Spalte von A mit λ_i von rechts.

Speziell für $\Lambda = \operatorname{diag}(\lambda, \ldots, \lambda) = \lambda \cdot 1_{n\times n} = 1_{n\times n} \cdot \lambda$ multipliziert $\Lambda \cdot A = \lambda \cdot A$ bzw. $A \cdot \Lambda = A \cdot \lambda$ jeden Eintrag von A mit λ. Somit gilt:

$$\begin{aligned}
\lambda \cdot (A \cdot B) &\overset{\text{Ass}}{=} (\lambda \cdot A) \cdot B &&\overset{\text{Com}}{=} A \cdot (\lambda \cdot B) \\
(A \cdot B) \cdot \lambda &\overset{\text{Ass}}{=} A \cdot (B \cdot \lambda) &&\overset{\text{Com}}{=} (A \cdot \lambda) \cdot B
\end{aligned}$$

Assoziativität gilt immer, direkt für λ oder dank B121 für $\Lambda = \lambda \cdot 1_{n\times n}$, die rechte Gleichung gilt nur im kommutativen Fall, dank $\lambda \cdot A = A \cdot \lambda$.

Auf diese Weise können wir den Grundring $\mathbb{K}$ in jeden Matrixring $\mathbb{K}^{n\times n}$ diagonal einbetten dank der Abbildung $\iota : \mathbb{K} \hookrightarrow \mathbb{K}^{n\times n} : \lambda \mapsto \lambda \cdot 1_{n\times n}$.

Matrixkalkül: Zusammenfassung

B123
Erläuterung

Unsere Rechnungen sind handwerklich einfach und eine gute Übung: Sie lernen hier präzise Notation und sorgfältige Argumentation.

Ich sage bewusst „einfach“, denn Sie müssen hier nichts selbst erfinden, keinen genialen Trick und keine neue Methode, nur geduldig rechnen.

Dennoch mag Ihnen unser Vorgehen am Anfang schwierig erscheinen. Ich sehe hierfür vor allem zwei mögliche Gründe:

1. Die Schreib- und Denkweise ist für Sie noch neu und ungewohnt.

   Ja, das ist richtig. Genau deshalb erkläre ich Ihnen hier alles detailliert und gehe alle Schritte mit Ihnen ausführlich durch. Mit etwas Gewöhnung und vor allem viel eigener Übung gelingen Ihnen solche Rechnungen dann bald selbst, leicht und routiniert.

2. Die Mühe mag Ihnen übertrieben pedantisch vorkommen.

   Das ist ein allgemeiner Vorwurf an die Mathematik von Menschen, die auf Genauigkeit wenig Wert legen, sondern auf Intuition hoffen. Wir befinden uns jedoch häufig in Situationen, wo die Intuition uns verlässt oder gar täuscht. Hier helfen nur Präzision und Sorgfalt.

Matrixkalkül: Zusammenfassung

B124
algebraische Strukturen

☺ Diese universelle Konstruktion gibt uns eine wunderschöne Struktur:

Satz B1A: Grundrechenarten für Matrizen

Wir betrachten Matrizen $\mathbb{K}^{m\times n}$ über einem Ring $(\mathbb{K}, +, 0, \cdot, 1)$.
Matrizen passender Größe können wir addieren und multiplizieren:

$$\begin{aligned}
+ &: \mathbb{K}^{m\times n} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n} : (A, B) \mapsto C = A + B, \quad c_{ij} = a_{ij} + b_{ij} \\
\cdot &: \mathbb{K}^{p\times q} \times \mathbb{K}^{q\times r} \to \mathbb{K}^{p\times r} : (A, B) \mapsto C = A \cdot B, \quad c_{ik} = \textstyle\sum_{j=1}^{q} a_{ij} \cdot b_{jk}.
\end{aligned}$$

Die Matrixaddition bildet eine kommutative Gruppe $(\mathbb{K}^{m\times n}, +, 0)$ und zusammen mit der Skalarmultiplikation einen linearen Raum über $\mathbb{K}$.

Die Matrixmultiplikation $\cdot$ ist distributiv über $+$. Sie ist nicht kommutativ, aber assoziativ. Die passende Einheitsmatrix ist links-/rechtsneutral.

Die quadratischen Matrizen bilden den Ring $(\mathbb{K}^{n\times n}, +, 0_{n\times n}, \cdot, 1_{n\times n})$.
Für $n \geq 2$ ist dieser Matrixring nicht kommutativ und hat Nullteiler:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{vs} \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Matrixkalkül: Inverse

Vorgelegt seien Matrizen $A \in \mathbb{K}^{m\times n}$ und $B, C \in \mathbb{K}^{n\times m}$.

$$\begin{bmatrix} 1 & 0 & * \\ -2 & 1 & * \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 1 \\ * & * \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Wir nennen B **linksinvers** zu A, falls $B \cdot A = 1_{n\times n}$ gilt.
Wir nennen C **rechtsinvers** zu A, falls $A \cdot C = 1_{m\times m}$ gilt.

Ist B linksinvers zu A und C rechtsinvers zu A, so folgt $B = C$, denn

$$B \overset{\text{rNtr}}{=} B \cdot 1_{m\times m} \overset{\text{rInv}}{=} B \cdot (A \cdot C) \overset{\text{Ass}}{=} (B \cdot A) \cdot C \overset{\text{lInv}}{=} 1_{n\times n} \cdot C \overset{\text{lNtr}}{=} C.$$

Wir nennen B **invers** zu A, falls $B \cdot A = 1_{n\times n}$ und $A \cdot B = 1_{m\times m}$ gilt.
Damit ist B eindeutig durch A bestimmt, und wir schreiben $A^{-1} := B$.

$$\begin{bmatrix} -4 & 9 \\ -3 & 7 \end{bmatrix} \cdot \begin{bmatrix} -7 & 9 \\ -3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} -7 & 9 \\ -3 & 4 \end{bmatrix} \cdot \begin{bmatrix} -4 & 9 \\ -3 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Die Matrix A heißt **invertierbar**, falls zu A eine inverse Matrix existiert.

Matrixkalkül: Inverse

Eines der Ziele in diesem Semester ist es, Invertierbarkeit zu verstehen.
Wann ist eine Matrix invertierbar? Gibt es hierzu hilfreiche Kriterien?
Wenn A invertierbar ist, wie berechnen wir die inverse Matrix A^{-1}?
Wie gelingt das möglichst effizient? Gibt es spezielle Werkzeuge?

Aufgabe: Sind die beiden folgenden Matrizen über $\mathbb{Q}$ invertierbar?
Was würden Sie vermuten? Können Sie es beweisen?

$$A = \begin{bmatrix} 1 & 0 \\ 2 & 1 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \end{bmatrix}$$

Lösung: Nein, weder A noch B ist invertierbar, wie oben gesehen:
Die Matrix A hat mehrere Linksinverse und daher kein Rechtsinverses.
Die Matrix B hat mehrere Rechtsinverse und daher kein Linksinverses.

☺ Über jedem vernünftigen Ring (etwa einem Körper, CRing B1K oder DRing B2D) ist jede invertierbare Matrix auch quadratisch:
Invertierbarkeit ist bestenfalls für quadratische Matrizen möglich.
Das ist keineswegs offensichtlich und ein fundamental wichtiger Satz.

Invertierbarkeit und Inverses in einem Monoid

Abstraktion Monoide

Wir wollen die invertierbaren Matrizen im Ring $(\mathbb{K}^{n\times n}, +, \cdot)$ verstehen.
Als erster Schritt hilft die Klärung allgemeiner Begriffe und Techniken:

Definition B1B: Invertierbarkeit und Inverses

Sei $(M, \cdot, 1)$ ein Monoid, also eine Menge M mit assoziativer Verknüpfung $\cdot : M \times M \to M$ und neutralem Element $1 \in M$.

Vorgelegt sei Elemente $a, b, c \in M$.
Wir nennen b **linksinvers** zu a, falls $b \cdot a = 1$ gilt.
Wir nennen c **rechtsinvers** zu a, falls $a \cdot c = 1$ gilt.

Ist b linksinvers zu a und c rechtsinvers zu a, so folgt $b = c$, denn

$$b \overset{\text{rNtr}}{=} b \cdot 1 \overset{\text{rInv}}{=} b \cdot (a \cdot c) \overset{\text{Ass}}{=} (b \cdot a) \cdot c \overset{\text{lInv}}{=} 1 \cdot c \overset{\text{lNtr}}{=} c.$$

Wir nennen b **invers** zu a, falls sowohl $b \cdot a = 1$ als auch $a \cdot b = 1$ gilt.
Damit ist b eindeutig durch a bestimmt, und wir schreiben $a^{-1} := b$.

Die Menge aller invertierbaren Elemente in $(M, \cdot, 1)$ bezeichnen wir mit

$$M^\times = (M, \cdot)^\times = (M, \cdot, 1)^\times := \{\, a \in M \mid \exists b \in M : a \cdot b = b \cdot a = 1 \,\}.$$

Die invertierbaren Elemente bilden eine Gruppe.

Abstraktion Gruppen

Beispiele: Im Halbring $\mathbb{N}$ gilt $(\mathbb{N}, +, 0)^\times = \{0\}$ und $(\mathbb{N}, \cdot, 1)^\times = \{1\}$.
Im Ring $\mathbb{Z}$ hingegen gilt $(\mathbb{Z}, +, 0)^\times = \mathbb{Z}$ und $(\mathbb{Z}, \cdot, 1)^\times = \{-1, 1\}$.
Im Körper $\mathbb{Q}$ gilt $(\mathbb{Q}, +, 0)^\times = \mathbb{Q}$ und $(\mathbb{Q}, \cdot, 1)^\times = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.
Im Ring $\mathbb{Z}_n$ gilt $\mathbb{Z}_n^\times = (\mathbb{Z}_n, \cdot, 1)^\times = \{\, a \in \mathbb{Z}_n \mid \operatorname{ggT}(a, n) = 1 \,\}$.

Satz B1C: Die invertierbaren Elemente bilden eine Gruppe.

Sei $(M, \cdot, 1)$ ein Monoid. Dann ist $(M^\times, \cdot, 1, {}^{-1})$ ist eine Untergruppe.

Beweis: Zunächst gilt $1 \cdot 1 = 1$, also $1 \in M^\times$ mit $1^{-1} = 1$.
Für $a \in M^\times$ gilt $a \cdot a^{-1} = a^{-1} \cdot a = 1$, also $a^{-1} \in M^\times$ mit $(a^{-1})^{-1} = a$.
Für je zwei Elemente $a, b \in M^\times$ gilt $a \cdot b \in M^\times$, denn wir haben:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) \overset{\text{Ass}}{=} (a \cdot (b \cdot b^{-1})) \cdot a^{-1} \overset{\text{Inv}}{=} (a \cdot 1) \cdot a^{-1} \overset{\text{Ntr}}{=} a \cdot a^{-1} \overset{\text{Inv}}{=} 1$$
$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) \overset{\text{Ass}}{=} (b^{-1} \cdot (a^{-1} \cdot a)) \cdot b \overset{\text{Inv}}{=} (b^{-1} \cdot 1) \cdot b \overset{\text{Ntr}}{=} b^{-1} \cdot b \overset{\text{Inv}}{=} 1$$

Also ist $a \cdot b$ invertierbar mit dem Inversen $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Das heißt, $M^\times$ ist abgeschlossen unter Multiplikation und Inversion.
Wir können diese auf $M^\times$ einschränken und erben Assoziativität. QED

Matrixkalkül: Der Ring der 2×2–Matrizen

Wir wollen den kleinsten Matrixring $(\mathbb{K}^{2\times 2}, \mathbf{+}, \bullet)$ genau untersuchen. Matrixaddition und -multiplikation sind hier besonders übersichtlich:

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \mathbf{+} \begin{bmatrix} a' & c' \\ b' & d' \end{bmatrix} = \begin{bmatrix} a+a' & c+c' \\ b+b' & d+d' \end{bmatrix}$$

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \bullet \begin{bmatrix} a' & c' \\ b' & d' \end{bmatrix} = \begin{bmatrix} aa'+cb' & ac'+cd' \\ ba'+db' & bc'+dd' \end{bmatrix}$$

Wenn Sie es konkret mögen, rechnen Sie die Ringaxiome erneut nach. Vergleichen Sie dies mit der oben ausgeführten allgemeinen Rechnung. Welche ist kürzer? eleganter? lehrreicher? Das ist eine gute Übung!

Wir sparen Klammern durch die übliche Konvention Punkt vor Strich. Wo möglich sparen wir auch Produktzeichen und schreiben $ab = a \bullet b$. Später schreiben wir $+$ und $\cdot$ auch für Matrizen, das ist bequemer.

Es ist nützlich, zunächst den kleinsten interessanten Fall zu verstehen! Der Gauß–Algorithmus beruht im Wesentlichen auf 2×2–Matrizen, deren Operation wir geschickt auf den allgemeinen Fall übertragen.

Matrixkalkül: Der Ring der 2×2–Matrizen

Determinanten

Sei $(\mathbb{K}, +, \cdot)$ ein kommutativer Ring. Wir beobachten folgendes Beispiel:

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \bullet \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} = (ad-bc) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \bullet \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

Ist also $ad - bc$ in $\mathbb{K}$ invertierbar, so auch unsere Matrix in $\mathbb{K}^{2\times 2}$ vermöge

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = (ad-bc)^{-1} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$

Für 2×2–Matrizen definieren wir daher die **Determinante** durch

$$\det : \mathbb{K}^{2\times 2} \to \mathbb{K} : \begin{bmatrix} a & c \\ b & d \end{bmatrix} \mapsto \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = ad - bc.$$

Dies ist ein Polynom in den Matrixkoeffizienten und leicht zu berechnen. Wir entwickeln später eine ähnliche Formel für quadratische Matrizen beliebiger Größe. Das wird sich als sehr nützliches Werkzeug erweisen. Die Determinante bietet uns ein einfaches Kriterium um zu bestimmen, ob unsere Matrix invertierbar ist oder nicht, daher der gewichtige Name.

Matrixkalkül: Der Ring der 2×2–Matrizen

Beispiel: Wir wollen folgendes Gleichungssystem über $\mathbb{Z}$ lösen:

$$\left.\begin{aligned} -4x_1 + 9x_2 &= 3 \\ -3x_1 + 7x_2 &= 2 \end{aligned}\right\} \iff Ax = b \text{ mit } A = \begin{bmatrix} -4 & 9 \\ -3 & 7 \end{bmatrix},\ x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix},\ b = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$$

Hier gilt $\det A = -1 \in \mathbb{Z}^\times$, also ist A in $\mathbb{Z}^{2\times 2}$ invertierbar vermöge

$$A^{-1} = (-1)^{-1} \begin{bmatrix} 7 & -9 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} -7 & 9 \\ -3 & 4 \end{bmatrix}.$$

Probe: Multiplizieren Sie $A \bullet A^{-1} = 1_{2\times 2}$ und $A^{-1} \bullet A = 1_{2\times 2}$ direkt aus! Somit hat $Ax = b$ für jede rechte Seite b genau eine Lösung:

$$\begin{aligned} Ax = b \quad &\implies \quad A^{-1}b = A^{-1}(Ax) = (A^{-1}A)x = 1x = x \\ x = A^{-1}b \quad &\implies \quad Ax = A(A^{-1}b) = (AA^{-1})b = 1b = b \end{aligned}$$

In unserem konkreten Beispiel finden wir so die eindeutige Lösung

$$x = A^{-1}b = \begin{bmatrix} -7 & 9 \\ -3 & 4 \end{bmatrix} \bullet \begin{bmatrix} 3 \\ 2 \end{bmatrix} = \begin{bmatrix} -3 \\ -1 \end{bmatrix}.$$

Probe: Rechnen Sie $Ax = b$ durch Einsetzen direkt nach!
Alternative: Lösen Sie $Ax = b$ mit dem Gauß–Verfahren über $\mathbb{Q}$.

Matrixkalkül: Der Ring der 2×2–Matrizen

Definition B1D: allgemeine lineare Gruppe

Sei $(\mathbb{K}, +, 0, \cdot, 1)$ ein Ring und $(\mathbb{K}^{n\times n}, \mathbf{+}, 0_{n\times n}, \bullet, 1_{n\times n})$ der Matrixring. Die invertierbaren Elemente bilden die **allgemeine lineare Gruppe**

$$\begin{aligned} \mathrm{GL}_n(\mathbb{K}) &:= (\mathbb{K}^{n\times n}, \bullet, 1_{n\times n})^\times \\ &= \left\{ A \in \mathbb{K}^{n\times n} \;\middle|\; \exists B \in \mathbb{K}^{n\times n} : A \bullet B = B \bullet A = 1_{n\times n} \right\}. \end{aligned}$$

Satz B1E: Inversion von 2×2–Matrizen

Sei $(\mathbb{K}, +, 0, \cdot, 1)$ ein kommutativer Ring. Dann ist die Determinante $\det : \mathbb{K}^{2\times 2} \to \mathbb{K}$ multiplikativ, das heißt, sie erfüllt $\det(1_{2\times 2}) = 1$ und

$$\det(A \bullet B) = \det(A) \cdot \det(B).$$

Genau dann ist A in $\mathbb{K}^{2\times 2}$ invertierbar, wenn $\det(A)$ in $\mathbb{K}$ invertierbar ist. In diesem Falle gelingt die Inversion mit der einfachen rationalen Formel

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = (ad-bc)^{-1} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$

Matrixkalkül: komplexe Zahlen als 2×2–Matrizen

B133 Teilring Isomorphie

Beispiel B1F: die komplexen Zahlen $\mathbb{C}$ als Matrizen über $\mathbb{R}$

Im Matrixring $(\mathbb{R}^{2\times2}, +, 0_{2\times2}, \cdot, 1_{2\times2})$ betrachten wir die Teilmenge

$$C := \left\{ z = \left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right] \mid x, y \in \mathbb{R} \right\}.$$

Sie bildet einen Ring, denn sie enthält $0_{2\times2}$ und $1_{2\times2}$ und ist zudem abgeschlossen unter Matrixaddition, Negation und Multiplikation:

$$\left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} u & -v \\ v & u \end{smallmatrix}\right] = \left[\begin{smallmatrix} xu-yv & -(yu+xv) \\ yu+xv & xu-yv \end{smallmatrix}\right]$$

Jedes Element $z \neq 0$ in $(C, \cdot)$ ist invertierbar, denn $\det(z) = x^2 + y^2 > 0$:

$$\left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right]^{-1} = \tfrac{1}{x^2+y^2} \left[\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right]$$

Somit ist $(C, +, \cdot)$ ein Divisionsring. Er ist zudem sogar kommutativ:

$$\left[\begin{smallmatrix} u & -v \\ v & u \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right] = \left[\begin{smallmatrix} ux-vy & -(uy+vx) \\ uy+vx & ux-vy \end{smallmatrix}\right]$$

Somit ist $(C, +, \cdot)$ ein Körper. Er entspricht den komplexen Zahlen A3B:

$$(\mathbb{C}, +, \cdot) \cong (C, +, \cdot) \,:\, x + \mathrm{i}y \leftrightarrows \left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right]$$

Matrixkalkül: komplexe Zahlen als 2×2–Matrizen

B134 Ring und Teilring

Wir betrachten hier nicht die gesamte Menge $\mathbb{R}^{2\times2}$ aller reellen 2×2–Matrizen, sondern nur eine spezielle Teilmenge $C \subset \mathbb{R}^{2\times2}$.

Diese ist abgeschlossen unter Addition, Negation und Multiplikation: Für je zwei Matrizen $z, w \in C$ gilt $z + w \in C$, $-w \in C$ und $z \cdot w \in C$. Zudem gilt $0_{2\times2} \in C$ und $1_{2\times2} \in C$. Wir nennen dies einen **Teilring**.

☺ Allein daraus folgt bereits, dass $(C, +, 0_{2\times2}, \cdot, 1_{2\times2})$ ein Ring ist.

Übung: Wiederholen Sie die acht Ringaxiome und prüfen Sie jedes einzelne hier nach. Sie werden sehen, dass es *trivialerweise* erfüllt ist.

Struktur $(C, +, \cdot)$	$(C, +)$				$(C, +, \cdot)$		$(C, \cdot)$			
Eigenschaft	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	Inv*	Com
erben als Teilring	✓	✓	✓	✓	✓	✓	✓	✓	–	–
extra nachrechnen									✓	✓

Trivial bedeutet, es folgt ohne weiteres Zutun sofort aus der Definition. Erst nachdem Sie sich selbst diese notwendige und lehrreiche Mühe einmal gemacht haben, sind Sie berechtigt auszurufen: „Das ist trivial!“

Matrixkalkül: Quaternionen als 2×2–Matrizen

B135 Teilring Isomorphie

Beispiel B1G: die Quaternionen $\mathbb{H}$ als Matrizen über $\mathbb{C}$

Im Matrixring $(\mathbb{C}^{2\times2}, +, 0_{2\times2}, \cdot, 1_{2\times2})$ betrachten wir die Teilmenge

$$H := \left\{ q = \left[\begin{smallmatrix} z & -w \\ \overline{w} & \overline{z} \end{smallmatrix}\right] \mid z, w \in \mathbb{C} \right\}.$$

Sie bildet einen Ring, denn sie enthält $0_{2\times2}$ und $1_{2\times2}$ und ist zudem abgeschlossen unter Matrixaddition, Negation und Multiplikation:

$$\left[\begin{smallmatrix} z_1 & -w_1 \\ \overline{w_1} & \overline{z_1} \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} z_2 & -w_2 \\ \overline{w_2} & \overline{z_2} \end{smallmatrix}\right] = \left[\begin{smallmatrix} z_1z_2-w_1\overline{w_2} & -z_1w_2-w_1\overline{z_2} \\ \overline{w_1}z_2+\overline{z_1}w_2 & -\overline{w_1}w_2+\overline{z_1}z_2 \end{smallmatrix}\right]$$

Jedes Element $q \neq 0$ in $(H, \cdot)$ ist invertierbar, $\det(q) = |z|^2 + |w|^2 > 0$:

$$\left[\begin{smallmatrix} z & -w \\ \overline{w} & \overline{z} \end{smallmatrix}\right]^{-1} = \tfrac{1}{z\overline{z}+w\overline{w}} \left[\begin{smallmatrix} \overline{z} & w \\ -\overline{w} & z \end{smallmatrix}\right]$$

Somit ist $(H, +, \cdot)$ ein Divisionsring. Er ist jedoch nicht kommutativ:

$$E = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right],\ I = \left[\begin{smallmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{smallmatrix}\right],\ J = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right],\ K = \left[\begin{smallmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{smallmatrix}\right] \quad \Rightarrow$$

$\cdot$	I	J	K
I	$-E$	K	$-J$
J	$-K$	$-E$	I
K	J	$-I$	$-E$

Dieser Divisionsring entspricht Hamiltons Quaternionen A3D gemäß

$$(\mathbb{H}, +, \cdot) \cong (H, +, \cdot) \,:\, \alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k} \leftrightarrows \alpha E + \beta I + \gamma J + \delta K.$$

Matrixkalkül: Quaternionen als 2×2–Matrizen

B136 Ring und Teilring

Die Teilmenge $H \subset \mathbb{C}^{2\times2}$ ist ein Teilring: Es gilt $0_{2\times2} \in H$ und $1_{2\times2} \in H$. Für je zwei Matrizen $z, w \in H$ gilt $z + w \in H$, $-w \in H$ und $z \cdot w \in H$.

☺ Allein daraus folgt bereits, dass $(H, +, 0_{2\times2}, \cdot, 1_{2\times2})$ ein Ring ist.

Struktur $(H, +, \cdot)$	$(H, +)$				$(H, +, \cdot)$		$(H, \cdot)$			
Eigenschaft	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	Inv*	Com
erben als Teilring	✓	✓	✓	✓	✓	✓	✓	✓	–	–
extra nachrechnen									✓	–

☺ Unsere sorgsame Vorbereitung zum Matrixkalkül zahlt sich hier aus! Die Ringaxiome haben wir für $(\mathbb{K}^{n\times n}, +, \cdot)$ allgemein nachgewiesen. Das können wir immer wieder wunderbar nutzen, so auch hier.

☺ Ohne weitere Mühe sehen wir sofort, dass H ein Schiefkörper ist. Das ist eine explizite doch sparsame Konstruktion der Quaternionen. Die naive, direkte Konstruktion A3D ist möglich, aber eher mühsamer.

Ich finde den Weg über Matrizen recht elegant und besonders effizient: Der allgemeine Matrixkalkül beschert uns alle relevanten Eigenschaften!

Matrixkalkül: Darstellung durch Matrizen

In Kapitel A haben wir den Körper $\mathbb{C} = \mathbb{R}[\mathrm{i}]$ der komplexen Zahlen und den Schiefkörper $\mathbb{H} = \mathbb{R}[\mathrm{i}, \mathrm{j}, \mathrm{k}]$ der Quaternionen definiert, aber nicht sofort die Körperaxiome nachgerechnet. Ohne weitere Hilfsmittel ist die Rechnung leider länglich. Dies gelingt in B1F und B1G nun mühelos!

Warum ist das auf einmal so leicht? Weil wir für Matrizen alles Nötige allgemein vorbereitet und dazu die Ringaxiome nachgerechnet haben. Zudem sind Matrizen sehr handlich, effizient und übersichtlich und bieten uns eine erfreuliche Vielfalt an Struktur und Rechentechnik.

Abstraktion strukturiert und vereinfacht: Eine allgemeine Tatsache ist oft leichter zu verstehen und zu erklären als ihre zahlreichen Spezialfälle.

Dieser Trick für $\mathbb{C}$ und $\mathbb{H}$ ist tatsächlich eine allgemeine Methode:
Die **Darstellungstheorie** untersucht Ringe, genauer: Algebren über einem Körper $\mathbb{K}$, durch geeignete Darstellungen als Matrizen über $\mathbb{K}$.
Das ist sehr flexibel und überaus nützlich, zum Beispiel in der Physik.

Wir können zunächst *abstrakt* scheinende Objekte (Gruppen, Algebren) ganz *konkret* durch Matrizen darstellen und so effizient untersuchen.

Matrixkalkül: Darstellung durch Matrizen

Wir wollen diese schöne Technik weiter illustrieren.

Aufgabe: Stellen Sie die Körper $\mathbb{Q}[\mathrm{i}]$ aus A1H und $\mathbb{Q}[\sqrt{2}]$ aus A1G sowie $\mathbb{Q}[\sqrt{3}]$ durch 2×2–Matrizen über $\mathbb{Q}$ dar, nach obigem Vorbild.

Allgemein: Sei $\mathbb{K}$ ein Körper. Untersuchen Sie Matrizen der Form

$$E = E_\alpha = \left\{ z = \begin{bmatrix} x & \alpha y \\ y & x \end{bmatrix} \;\middle|\; x, y \in \mathbb{K} \right\}$$

wobei $\alpha \in \mathbb{K}$ eine Konstante ist und $x, y \in \mathbb{K}$ beliebig sind.
Ist die Teilmenge $E_\alpha \subset \mathbb{K}^{2\times 2}$ ein Teilring im Matrixring $\mathbb{K}^{2\times 2}$?

(1) Welche Eigenschaften müssen Sie für $E_\alpha \subset \mathbb{K}^{2\times 2}$ hier nachprüfen?
(2) Welche Ringaxiome bekommen Sie für E_α dadurch geschenkt?
(3) Für welche Konstanten $\alpha \in \mathbb{K}$ ist E_α ein Körper?

🙂 Damit beweisen Sie die Körperaxiome für $\mathbb{Q}[\mathrm{i}]$ und $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{Q}[\sqrt{3}]$, ganz nebenbei ohne weitere Mühe. Zudem erhalten Sie eine Familie E_α interessanter Beispiele über $\mathbb{K}$, eines für jede Konstante $\alpha \in \mathbb{K}$.

Matrixkalkül: Darstellung durch Matrizen

Lösung: (1) Die Teilmenge $E \subset \mathbb{K}^{2\times 2}$ ist abgeschlossen unter Addition und Multiplikation: Für alle $z, w \in E$ gilt $z + w \in E$ und $z \cdot w \in E$, denn

$$\begin{bmatrix} x & \alpha y \\ y & x \end{bmatrix} + \begin{bmatrix} u & \alpha v \\ v & u \end{bmatrix} = \begin{bmatrix} x+u & \alpha(y+v) \\ y+v & x+u \end{bmatrix},$$

$$\begin{bmatrix} x & \alpha y \\ y & x \end{bmatrix} \cdot \begin{bmatrix} u & \alpha v \\ v & u \end{bmatrix} = \begin{bmatrix} xu+\alpha yv & \alpha(yu+xv) \\ yu+xv & xu+\alpha yv \end{bmatrix}.$$

Ebenso gilt $-E \subseteq E$ sowie $0_{2\times 2} \in E$ und $1_{2\times 2} \in E$.

(2) Somit ist E ein Ring, genauer gesagt ein Teilring von $\mathbb{K}^{2\times 2}$:
Alle Ringaxiome vererben sich vom Matrixring $\mathbb{K}^{2\times 2}$ auf E.

(3) Invertierbarkeit von z in E ist äquivalent zur Invertierbarkeit von $\det(z) = x^2 - \alpha y^2$ in $\mathbb{K}$, siehe Satz B1E. Dies gilt für alle $z \neq 0$ genau dann, wenn die Konstante $\alpha \in \mathbb{K}$ keine Quadratwurzel in $\mathbb{K}$ hat.
In diesem Falle ist E ein Körper, geschrieben $E = \mathbb{K}[\sqrt{\alpha}]$.

Für $\mathbb{K} = \mathbb{Q}$ und $\alpha = -1, 2, 3$ erhalten wir unsere obigen drei Körper.
Für $\mathbb{K} = \mathbb{R}$ und $\alpha = -1$ erhalten wir die komplexen Zahlen $\mathbb{C} = \mathbb{R}[\mathrm{i}]$.

Matrixkalkül: Darstellung durch Matrizen

Übung: Wir betrachten die Menge der oberen Dreiecksmatrizen

$$U = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{bmatrix} := \left\{ \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \;\middle|\; x, y, z \in \mathbb{R} \right\}$$

Ist diese abgeschlossen unter Matrixaddition und Matrixmultiplikation?
In diesem Falle erhalten wir eine Addition bzw. Multiplikation auf U.
Welche der Ringaxiome sind für U erfüllt? Ist U ein Körper?

Beantworten Sie dieselben Fragen für folgende Beispiele:

$$\begin{bmatrix} \mathbb{R} & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{bmatrix}, \quad \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & \mathbb{R} \\ \mathbb{R} & 0 \end{bmatrix}$$

Für 2×2–Matrizen gibt es insgesamt $2^4 = 16$ Beispiele dieser Art.
Wenn Sie möchten, können Sie systematisch alle untersuchen.

Für 3×3–Matrizen mit $2^9 = 512$ Beispielen wird das schwieriger.
Sie können sich aber einige der schönsten Beispiele aussuchen.

Konstruktion eines Körpers mit vier Elementen

Zu jeder Zahl $n \in \mathbb{N}_{\geq 1}$ kennen wir den Ring $\mathbb{Z}_n$ mit n Elementen (A2O). Die invertierbaren Elemente hierin sind $\mathbb{Z}_n^\times = \{\, a \in \mathbb{Z}_n \mid \operatorname{ggT}(a,n) = 1 \,\}$.

Wir interessieren uns für den schönsten Fall: Ist $p \in \mathbb{N}_{\geq 2}$ eine Primzahl, so erhalten wir auf diese Weise den Körper $\mathbb{F}_p = \mathbb{Z}_p$ mit p Elementen

Gibt es weitere endliche Körper? In Satz J2G werden wir zeigen: Ist K ein endlicher Körper, so gilt $\sharp K = p^d$ mit $p \in \mathbb{N}_{\geq 2}$ prim und $d \in \mathbb{N}_{\geq 1}$.

Es gibt insbesondere keinen Körper mit 6 oder 10 Elementen.

Wir kennen bereits Körper mit $2, 3, 5, 7, \ldots$ Elementen, und es wäre interessant, auch Körper mit $4, 8, 9, \ldots$ Elementen zu konstruieren.

Der Ring $\mathbb{Z}_4$ hat vier Elemente, ist aber kein Körper. Was tun?

Das folgende Beispiel zeigt explizit einen Körper F_4 mit vier Elementen. Im Prinzip genügt es dazu, die Addition und die Multiplikation als Tabelle auszuführen, doch dann ist der Nachweis der Körperaxiome leider recht mühselig. Es ist effizienter, F_4 durch geeignete Matrizen darzustellen!

Konstruktion eines Körpers mit vier Elementen

Beispiel B1H: ein Körper mit vier Elementen

Im Matrixring $(\mathbb{F}_2^{2\times 2}, +, 0_{2\times 2}, \cdot, 1_{2\times 2})$ betrachten wir die Teilmengen

$$F_2 := \left\{\, O = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right],\ I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \,\right\}, \quad F_4 := F_2 \cup \left\{\, X = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right],\ Y = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] \,\right\}$$

Diese bilden jeweils Teilringe $F_2 \subset F_4 \subset \mathbb{F}_2^{2\times 2}$ und sind sogar Körper.

Aufgabe: (0) Wie können Sie dies möglichst effizient beweisen?
(1) Schreiben Sie Addition und Multiplikation als Tabellen aus.
(2) Weisen Sie dann für $(F_4, +, \cdot)$ alle zehn Körperaxiome nach.
(3) Wie berechnen Sie die Inversion mit Hilfe der Determinante?

Lösung: (0) Die Körperaxiome zu *nutzen* ist hilfreich und effizient, sie *nachzuweisen* ist meist aufwändig, doch eine gute Investition.

Wir können uns Arbeit ersparen, indem wir den Matrixring nutzen, hier $\mathbb{F}_2^{2\times 2}$, denn für diesen Ring haben wir alle erforderlichen Axiome bereits allgemein nachgewiesen (Satz B1A). Dazu folgen wir der raffinierten Argumentation der vorigen Beispiele B1F und B1G.

Konstruktion eines Körpers mit vier Elementen

(1) Addition und Multiplikation auf F_2 bzw. F_4 ergeben folgende Tabellen:

$+$	O	I	X	Y
O	O	I	X	Y
I	I	O	Y	X
X	X	Y	O	I
Y	Y	X	I	O

$\cdot$	O	I	X	Y
O	O	O	O	O
I	O	I	X	Y
X	O	X	Y	I
Y	O	Y	I	X

Zum Beispiel gilt $X \cdot Y = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] = I$. Rechnen Sie es nach! Somit sind F_2 und F_4 abgeschlossen unter Addition und Multiplikation, zudem unter Negation, und es gilt $0_{2\times 2} = O \in F_4$ und $1_{2\times 2} = I \in F_4$.

(2) Die Körperaxiome folgern wir direkt aus den Tabellen oder erben sie als Teilring von $\mathbb{F}_2^{2\times 2}$: Wir nutzen jeweils geschickt, was leichter ist!

Struktur $(F_4, +, \cdot)$	$(F_4, +)$				$(F_4, +, \cdot)$		$(F_4, \cdot)$			
Eigenschaft	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	Inv*	Com
direkt aus Tabelle		✓	✓	✓				✓	✓	✓
erben als Teilring	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Konstruktion eines Körpers mit vier Elementen

(3) Multiplikative Inverse können wir direkt aus der Tabelle ablesen oder mit der Determinante und der Inversionsformel B1E berechnen.

Speziell über $\mathbb{F}_2$ ist $A = \left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right] \in \mathbb{F}_2^{2\times 2}$ genau dann invertierbar, wenn $\det A = ac - bd = 1$ gilt, und das Inverse ist dann $\left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} d & c \\ b & a \end{smallmatrix}\right]$.

Damit finden wir $X^{-1} = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] = Y$ und ebenso $Y^{-1} = X$. Genau so lesen wir es auch aus der Multiplikationstabelle ab. Insbesondere ist $F_4 \smallsetminus \{O\}$ abgeschlossen unter Inversion.

🙂 Unsere sorgsame Vorbereitung zum Matrixkalkül zahlt sich hier aus! Die Matrizenrechnung ist ein Universalwerkzeug und ungemein nützlich für konkrete Rechnungen, insbesondere für lineare Gleichungssysteme. Dazu führen wir im Folgenden den Gauß–Algorithmus detailliert aus.

🙂 Die vorigen Beispiele illustrieren sehr eindrücklich und elegant, dass Matrixringe ebenso praktisch wie theoretisch interessant sind. So können wir die Teilringe $C \subset \mathbb{R}^{2\times 2}$ und $H \subset \mathbb{C}^{2\times 2}$ und $F_4 \subset \mathbb{F}_2^{2\times 2}$ effizient konstruieren und anschließend als Schief/Körper nachweisen.

Die Spur einer quadratischen Matrix

Definition B1I: die Spur einer quadratischen Matrix

Die **Spur**, engl. *trace*, einer quadratischen Matrix $A \in \mathbb{K}^{n\times n}$ ist die Summe ihrer Diagonaleinträge. Als Formel ausgeschrieben:

$$\operatorname{tr} = \operatorname{tr}_n : \mathbb{K}^{n\times n} \to \mathbb{K} : A \mapsto \textstyle\sum_{k=1}^{n} a_{kk} = a_{11} + a_{22} + \cdots + a_{nn}$$

Aufgabe: Gilt $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ für alle $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times p}$?

Lösung: Wir haben die Produkte $AB \in \mathbb{K}^{p\times p}$ und $BA \in \mathbb{K}^{q\times q}$.
Wir setzen die Definition der Spur ein und vergleichen die Summen:

$$\operatorname{tr}_p(AB) = \textstyle\sum_{i=1}^{p}(AB)_{ii} = \sum_{i=1}^{p}\sum_{j=1}^{q} a_{ij}b_{ji} = \sum_{(i,j)} a_{ij}b_{ji}$$
$$\operatorname{tr}_q(BA) = \textstyle\sum_{j=1}^{q}(AB)_{jj} = \sum_{j=1}^{q}\sum_{i=1}^{p} b_{ji}a_{ij} = \sum_{(i,j)} b_{ji}a_{ij}$$

Summiert wird hierbei jeweils über alle Indexpaare $(i,j) \in I \times J$.
Ist der Ring $\mathbb{K}$ kommutativ, so sind die Summanden jeweils gleich.

🙂 Daraus erhalten wir unmittelbar den folgenden nützlichen Satz, in dem wir erste Eigenschaften der Spur zusammenstellen.

Erste Eigenschaften der Spur

Satz B1J: erste Eigenschaften der Spur

(1) Die Spur erfüllt $\operatorname{tr}(1_{n\times n}) = n$ und ist invariant unter Transposition:

$$\operatorname{tr}(A) = \operatorname{tr}(A^\intercal)$$

(2) Die Spur ist eine (beidseitig) lineare Abbildung über $\mathbb{K}$:
Für alle Matrizen $A, B \in \mathbb{K}^{n\times n}$ und alle Skalare $\lambda \in \mathbb{K}$ gilt

$$\operatorname{tr}(A+B) = \operatorname{tr}(A) + \operatorname{tr}(B), \qquad \operatorname{tr}(\lambda A) = \lambda \operatorname{tr}(A), \qquad \operatorname{tr}(A\lambda) = \operatorname{tr}(A)\lambda.$$

(3) Ist der Ring $\mathbb{K}$ zudem kommutativ, so ist die Spur invariant unter zyklischer Vertauschung: Für alle Matrizen $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times p}$ gilt

$$\operatorname{tr}(AB) = \operatorname{tr}(BA).$$

(4) Speziell für alle $A, B \in \mathbb{K}^{n\times n}$ mit B invertierbar folgt daraus

$$\operatorname{tr}(B^{-1}AB) = \operatorname{tr}(A).$$

Ist jede invertierbare Matrix quadratisch?

Sie kennen bereits rechteckige Matrizen, die einseitig invertierbar sind.
All unsere Beispiele invertierbarer Matrizen waren bislang quadratisch.
Muss das so sein? Nein, nicht immer (siehe J1O), aber doch recht oft:

Satz B1K: invertierbare Matrizen über $\mathbb{Z}$ sind quadratisch.

Sei $\mathbb{K} = \mathbb{Z}$ oder allgemein $\mathbb{K} \supseteq \mathbb{Z}$ ein kommutativer Ring, der $\mathbb{Z}$ enthält.
Dann ist über dem Ring $\mathbb{K}$ jede invertierbare Matrix quadratisch.

Ausführlich: Gegeben seien zwei Matrizen $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times p}$.
Gilt sowohl $AB = 1_{p\times p}$ als auch $BA = 1_{q\times q}$, so folgt daraus $p = q$.

🙂 Dies gilt demnach insbesondere für die Körper $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Aufgabe: Beweisen Sie dies! Genialer Trick: Nutzen Sie die Spur!

Lösung: Mit der Spur $\operatorname{tr} : \mathbb{K}^{n\times n} \to \mathbb{K}$ und Satz B1J gelingt dies leicht:
Aus $AB = 1_{p\times p}$ berechnen wir die Spur $\operatorname{tr}(AB) = p \in \mathbb{Z} \subseteq \mathbb{K}$.
Aus $BA = 1_{q\times q}$ berechnen wir die Spur $\operatorname{tr}(BA) = q \in \mathbb{Z} \subseteq \mathbb{K}$.
Da $\mathbb{K}$ kommutativ ist, gilt $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, also $p = q$. QED

Ist jede invertierbare Matrix quadratisch?

Satz B1K ist beruhigend und unser Beweis sehr elegant.
Unsere Voraussetzung $\mathbb{Z} \subseteq \mathbb{K}$ ist leider technisch notwendig, nicht für die Gültigkeit des Satzes, sondern für unseren Beweis:

Beispiel: Wenn wir über dem kommutativen Ring $\mathbb{K} = \mathbb{Z}_n$ rechnen, so erhalten wir hier nur $p \operatorname{rem} n = q \operatorname{rem} n$ in $\mathbb{Z}_n$. Daraus folgt $p = q$ immerhin für alle kleinen Dimensionen $p, q < n$, aber nicht allgemein.

🙂 Wir werden die Aussage im nächsten Abschnitt für jeden Körper $\mathbb{K}$ und ganz allgemein für jeden Divisionsring beweisen, siehe Satz B2D. Somit gilt sie insbesondere für $\mathbb{Z}_p = \mathbb{F}_p$ und jede Primzahl $p \in \mathbb{N}_{\geq 2}$.

🙂 Die Aussage gilt zudem über jedem kommutativen Ring $\mathbb{K} \neq \{0\}$, auch ohne die technische Einschränkung $\mathbb{K} \supseteq \mathbb{Z}$. Dies beweisen wir in Kapitel L mit Hilfe der Determinante, siehe Satz L3A.

⚠ Es gibt auch exotische Beispiele von Matrizen, die nicht quadratisch und dennoch invertierbar sind, siehe Beispiel J1O. Die hier diskutierte Eigenschaft ist also keineswegs „trivial“ oder „selbstverständlich“.

Lineare Gleichungssysteme

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$; es genügt ein Divisionsring, wie $\mathbb{H}$.
Zu lösen sei ein **lineares Gleichungssystem** über $\mathbb{K}$, kurz LGS:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \vdots \qquad\quad \vdots \qquad\qquad \vdots \qquad\quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

Dies bündeln wir prägnant und effizient zu einer einzigen Gleichung

$$Ax = b$$

mit der Koeffizientenmatrix $A \in \mathbb{K}^{m\times n}$ und der rechten Seite $b \in \mathbb{K}^m$.
Gesucht ist $x \in \mathbb{K}^n$. Wir schreiben kurz $\mathbb{K}^n$ für $\mathbb{K}^{n\times 1}$ (Spaltenvektoren).

🙂 Bequeme Schreibweise strukturiert Daten und vereinfacht Lösung.
Ein sehr effizientes Lösungsverfahren ist der **Gauß–Algorithmus**.

🙂 Wichtiger Spezialfall: Ist die Matrix A **invertierbar**, so wird unser LGS $Ax = b$ gelöst durch $x = A^{-1}b$, und dies ist die einzige Lösung.

Lineare Gleichungssysteme lösen: Diagonalform

Besonders leicht zu lösen ist $Ax = b$ in **Diagonalform**:

$$\begin{bmatrix} a_{11} & 0 & 0 & 0 & 0 \\ 0 & a_{22} & 0 & 0 & 0 \\ 0 & 0 & a_{33} & 0 & 0 \\ 0 & 0 & 0 & a_{44} & 0 \\ 0 & 0 & 0 & 0 & a_{55} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{bmatrix}$$

Hier sind alle n Gleichungen **entkoppelt**, wir können sie separat lösen.
Wir setzen dazu $a_{ii} \neq 0$ voraus, somit ist a_{ii} invertierbar in $\mathbb{K}$:

$$a_{ii}x_i = b_i \quad\Longleftrightarrow\quad x_i = a_{ii}^{-1}b_i$$

Hier nutzen wir, dass $\mathbb{K}$ ein Divisionsring ist, also $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$.
Über dem Ring $\mathbb{Z}$ zum Beispiel können wir $3x = 5$ nicht lösen.

Das ist der typische Fall, die Sonderfälle sind ebenso leicht:
Im Falle $a_{ii} = b_i = 0$ kann x_i beliebig gewählt werden.
Im Falle $a_{ii} = 0$ und $b_i \neq 0$ gibt es keine Lösung.

Lineare Gleichungssysteme lösen: Dreiecksform

Ebenso leicht zu lösen ist $Ax = b$ in **oberer Dreiecksform**:

$$\begin{bmatrix} \blacksquare & * & * & * & * \\ 0 & \blacksquare & * & * & * \\ 0 & 0 & \blacksquare & * & * \\ 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & \blacksquare \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{bmatrix}$$

Wir setzen voraus, dass $a_{ii} \neq 0$ für $i = 1, 2, \ldots, n$ und $a_{ij} = 0$ für $i > j$.
Notation: $*$ = beliebig; $\blacksquare$ = beliebig, aber ungleich 0, also invertierbar.

Wir erhalten die Lösung $x_n, \ldots, x_2, x_1$ durch **Rückwärtseinsetzen**:

$$a_{ii}x_i + \textstyle\sum_{k=i+1}^{n} a_{ik}x_k = b_i \quad\Longleftrightarrow\quad x_i = a_{ii}^{-1}\big(b_i - \sum_{k=i+1}^{n} a_{ik}x_k\big)$$

Dabei nutzen wir für x_i die bereits berechneten Werte $x_{i+1}, \ldots, x_n$.
Unsere Gleichungen sind zwar gekoppelt, aber zum Glück gestuft.
In diesem günstigen Falle existiert genau eine Lösung.

Zeilenstufenform, allgemein und reduziert

Ebenso lösen wir $Ax = b$ in **Zeilenstufenform**:

$$\begin{bmatrix} \blacksquare & * & * & * & * & * & * & * & * & * \\ 0 & 0 & \blacksquare & * & * & * & * & * & * & * \\ 0 & 0 & 0 & \blacksquare & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 0 & * & 0 & * & * & 0 & * & * \\ 0 & 0 & 1 & * & 0 & * & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 1 & * & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Notation: $*$ = beliebig; $\blacksquare$ = beliebig, aber ungleich 0, also invertierbar.

In jeder Zeile heißt das erste Nicht-Null-Element der **Leitkoeffizient** (engl. *leading coefficient*) oder der **Pivot** (frz. 'Dreh- und Angelpunkt').

Die linke Matrix ist in **Zeilenstufenform** mit Stufen $s = (1, 3, 4, 7, 9, 10)$, die rechte in **reduzierter Zeilenstufenform** mit Stufen $s = (2, 3, 5, 8)$.

🙂 In Zeilenstufenform können wir alle Lösungen direkt ablesen!
Zu jeder **freien Spalte** k können wir die Koordinate $x_k \in \mathbb{K}$ frei wählen.
Zu jeder **Pivotspalte** $j = s_n, \ldots, s_2, s_1$ folgt daraus die Koordinate x_j.

Zeilenstufenform, allgemein und reduziert

Definition B2A: Zeilenstufenform, allgemein und reduziert

Gegeben sei eine Matrix $A \in \mathbb{K}^{m\times n}$ mit Koeffizienten in $(\mathbb{K}, +, 0, \cdot, 1)$.
Im Falle einer Nullzeile $a_i = (0, 0, \ldots, 0)$ setzen wir $s_i := \infty$, andernfalls

$$s_i := \min\{\, j \in \{1, 2, \ldots, n\} \mid a_{ij} \neq 0 \,\}.$$

Die Matrix A hat **Zeilenstufenform** (ZSF, engl. *row echelon form*, REF) falls $s_1 < s_2 < \cdots < s_r \leq n$, und alle Zeilen $i = r+1, \ldots, m$ sind Null.
Wir nennen dies eine ZSF vom **Rang** r mit Stufen $s = (s_1, s_2, \ldots, s_r)$.

Die Matrix A hat **reduzierte Zeilenstufenform** (RZSF, engl. RREF), falls zudem gilt: Jeder Pivot ist Eins, und darüber stehen nur Nullen, d.h. in jeder Pivotspalte $j = s_i$ gilt $a_{ij} = 1$ und $a_{kj} = 0$ für alle $k \neq i$.

Beispiel: Die Diagonalmatrix $\operatorname{diag}(d_1, \ldots, d_r, 0, \ldots, 0)$ mit $d_1, \ldots, d_r \neq 0$ ist in Zeilenstufenform, und zudem reduziert, falls $d_1 = \cdots = d_r = 1$ gilt.

Die Einheitsmatrix $1_{n\times n}$ ist in reduzierter Zeilenstufenform vom Rang n.
Die Nullmatrix $0_{m\times n}$ ist in reduzierter Zeilenstufenform vom Rang $r = 0$.

Lineare Gleichungssysteme: erweiterte Koeffizientenmatrix

Wir betrachten ein lineares Gleichungssystem $Ax = b$, ausgeschrieben

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \vdots \qquad \vdots \qquad\qquad \vdots \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

mit der Koeffizientenmatrix $A \in \mathbb{K}^{m\times n}$ und der rechten Seite $b \in \mathbb{K}^m$.

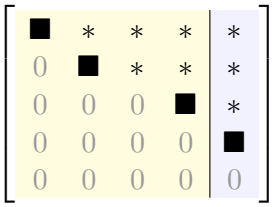
Die **erweiterte Koeffizientenmatrix** ist

$$(A, b) = \left[\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_n \end{array}\right].$$

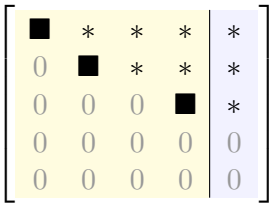
🙂 Das geht auch mit mehreren rechten Seiten $b^{(1)}, \ldots, b^{(\ell)}$ gleichzeitig.
Diese Matrix bringen wir durch Zeilenoperationen in Zeilenstufenform.

Lineare Gleichungssysteme in Zeilenstufenform

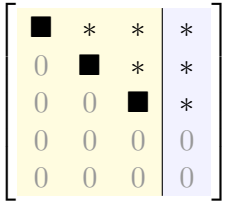
In Zeilenstufenform können wir alle Lösungen leicht ablesen:



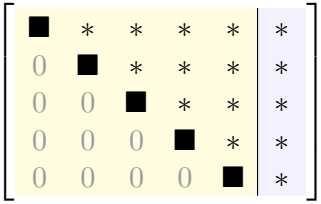
nicht lösbar
für dieses b



lösbar für dieses b
aber nicht eindeutig



lösbar für dieses b
und zudem eindeutig



eindeutig lösbar
für jedes b

Lineare Gleichungssysteme in Zeilenstufenform

Wir werden gleich anschließend mit dem Gauß–Algorithmus erklären, wie wir die (reduzierte) Zeilenstufenform herstellen. Doch zuvor möchte ich zeigen, wie man aus der RZSF alle Lösungen leicht ablesen kann.

Wir wollen zuerst das Ziel fixieren, dann einen möglichen Weg finden. Die (reduzierte) Zeilenstufenform erweist sich als extrem hilfreich, und der Gauß–Algorithmus erreicht sie routiniert und effizient.

Lineare Gleichungssysteme in Zeilenstufenform

B209

Aufgabe: Gegeben ist (A, b) in (reduzierter) Zeilenstufenform.
Explizieren Sie die Lösungsmenge $L(A,b) = \{\, x \in \mathbb{R}^n \mid Ax = b \,\}$.

$$\left[\begin{array}{ccccc|c} 1 & -2 & 1 & -6 & 5 & -6 \\ 0 & 1 & -1 & 2 & -6 & -3 \\ 0 & 0 & 1 & -2 & 3 & 7 \\ 0 & 0 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right] \xrightarrow{\text{reduzieren}} \left[\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 9 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

Lösung: Dieses LGS hat genau eine Lösung:

$$L(A,b) = \left\{ \begin{bmatrix} -1 \\ 4 \\ 9 \\ 1 \\ 0 \end{bmatrix} \right\}$$

☺ In reduzierter Zeilenstufenform ist das Ablesen trivial.
In unreduzierter Form genügt Rückwärtseinsetzen.

Lineare Gleichungssysteme in Zeilenstufenform

B210

Aufgabe: Gegeben ist (A, b) in (reduzierter) Zeilenstufenform.
Explizieren Sie die Lösungsmenge $L(A,b) = \{\, x \in \mathbb{R}^n \mid Ax = b \,\}$.

$$\left[\begin{array}{ccccc|c} 1 & -2 & -1 & -4 & 1 & 4 \\ 0 & 0 & -1 & -7 & 1 & 5 \\ 0 & 0 & 0 & 0 & 1 & 9 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \xrightarrow{\text{reduzieren}} \left[\begin{array}{ccccc|c} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 9 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Lösung: Dieses LGS hat keine Lösung! Also:

$$L(A,b) = \emptyset = \{\,\}$$

☺ In jeder Zeilenstufenform ist das leicht abzulesen!
Der Reduktionsschritt ist in diesem speziellen Falle unnötig.

Reduktion kann aber dennoch sinnvoll sein, zum Beispiel
wenn wir mehrere rechte Seiten gleichzeitig bearbeiten.

Lineare Gleichungssysteme in Zeilenstufenform

B211

Struktur des Lösungsraums

Aufgabe: Gegeben ist (A, b) in reduzierter Zeilenstufenform.
Explizieren Sie die Lösungsmenge $L(A,b) = \{\, x \in \mathbb{R}^n \mid Ax = b \,\}$.

$$\left[\begin{array}{ccccc|c} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \xrightarrow[\text{Merkregel}]{\text{graphische}} \left[\begin{array}{ccccc|c} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 9 \end{array}\right]$$

Lösung: Freie Variablen sind $s = -x_2$, $t = -x_4$. Rückwärtseinsetzen ergibt $x_5 = 9$, $x_4 = -t$, $x_3 = 4 + 7t$, $x_2 = -s$, $x_1 = -1 - 2s + 3t$. Also:

$$L = \left\{ \begin{bmatrix} -1-2s+3t \\ -s \\ 4+7t \\ -t \\ 9 \end{bmatrix} \,\middle|\, s,t \in \mathbb{R} \right\} = \left\{ \begin{bmatrix} -1 \\ 0 \\ 4 \\ 0 \\ 9 \end{bmatrix} + s \begin{bmatrix} -2 \\ -1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + t \begin{bmatrix} 3 \\ 0 \\ 7 \\ -1 \\ 0 \end{bmatrix} \,\middle|\, s,t \in \mathbb{R} \right\}$$

☺ Diese drei Spaltenvektoren können wir leicht aus (A, b) ablesen:
Wir fügen Nullzeilen so ein, dass jeder Pivot auf der Diagonale steht;
jede Null auf der Diagonalen ersetzen wir gedanklich durch -1. Voilà!

Lineare Gleichungssysteme lösen in Zeilenstufenform

B212

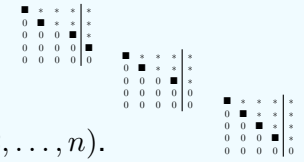
Lösungsraum und Dimension

Satz B2B: Lösung in Zeilenstufenform

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$; es genügt ein Divisionsring, wie $\mathbb{H}$.

Gegeben seien $A \in \mathbb{K}^{m\times n}$ und $b \in \mathbb{K}^m$. Wir setzen voraus, dass (A, b) in einer Zeilenstufenform vorliegt mit Stufen $s = (s_1, s_2, \ldots, s_r)$.

Das Gleichungssystem $Ax = b$ ist



1. unlösbar genau dann, wenn $s_r = n + 1$ gilt,
2. lösbar genau dann, wenn $s_r \leq n$ gilt, sowie
3. eindeutig lösbar genau dann, wenn $s = (1, 2, \ldots, n)$.

Im lösbaren Fall $s_r \leq n$ gibt es genau $d = n - r$ freie Variablen,
der Lösungsraum von $Ax = b$ hat also die affine Dimension d.

Ausführlich: Zu jeder freien Spalte $k \in \{1, 2, \ldots, n\} \smallsetminus \{s_1, s_2, \ldots, s_r\}$ können wir die Koordinate $x_k \in \mathbb{K}$ frei wählen. Zu jeder Pivotspalte $j = s_r, \ldots, s_2, s_1$ folgt die Koordinate $x_j \in \mathbb{K}$ daraus eindeutig.

Beweis: Diese Rechnung haben wir oben bereits ausgeführt. QED

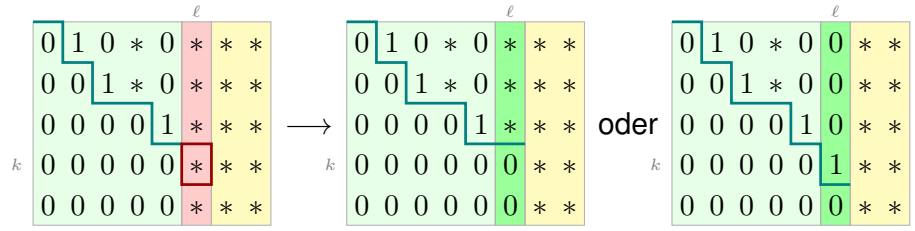
Gauß–Algorithmus zur reduzierten Zeilenstufenform

B213

Ausprobieren mit Gaël!

Eingabe: $A \in \mathbb{K}^{m\times n}$ mit Stufen $s=(s_1,\dots,s_r)$ bis Spalte $\ell \in \{1,2,\dots,n\}$
Voraussetzung: Alle Spalten $< \ell$ liegen in RZSF vor mit Stufen s.

Ausgabe: $A' \in \mathbb{K}^{m\times n}$ zeilenumgeformt aus A mit Stufen $s'=(s'_1,\dots,s'_{r'})$
Zusicherung: Alle Spalten $\leq \ell$ liegen in RZSF vor mit Stufen s'.



Methode: Betrachte die neue Spalte ℓ und die nächste Zeile $k = r+1$.
Gilt $a_{i\ell} = 0$ für alle $i \geq k$, so sind wir fertig. Andernfalls $s \leftarrow (s_1,\dots,s_r,\ell)$.

Tausche Zeile k und die erste Zeile $i \geq k$ mit $a_{i\ell} \neq 0$. Somit gilt $a_{k\ell} \neq 0$.
Multipliziere Zeile k mit dem Inversen $a_{k\ell}^{-1}$. Anschließend gilt $a_{k\ell} = 1$.
Subtrahiere von jeder Zeile $i \neq k$ das $a_{i\ell}$–Fache der Zeile k. Fertig!

🙂 Dies können wir für alle Spalten $\ell = 1,2,\dots,n$ durchführen.

Gauß–Algorithmus zur reduzierten Zeilenstufenform

B214

Satz B2C: Gauß–Algorithmus zur reduzierten Zeilenstufenform

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$; es genügt ein Divisionsring, wie $\mathbb{H}$.

Jede Matrix $A \in \mathbb{K}^{m\times n}$ können wir durch elementare Zeilenoperationen in reduzierte Zeilenstufenform A' überführen. (Diese ist eindeutig: K2K)

Systematisch gelingt dies mit dem Gauß–Algorithmus, indem wir die obige Methode für $\ell = 1,2,\dots,n$ anwenden. Benötigt werden dazu

- höchstens mr Zeilenoperationen, wobei $r \leq \min\{m,n\}$ der Rang ist,
- somit höchstens mnr arithmetische Operationen im Körper $\mathbb{K}$.

Speziell für jede quadratische Matrix, mit $m = n$, genügen demnach $\leq n^2$ Zeilenoperationen, somit $\leq n^3$ arithmetische Operationen in $\mathbb{K}$.

Permutationen sind vernachlässigbar und werden hier nicht mitgezählt.
Zur Vereinfachung zählen wir $a_{ij} \leftarrow a_{ij} - a_{i\ell}a_{kj}$ als eine Operation in $\mathbb{K}$.

Übung: Ist statt der reduzierten nur irgendeine Zeilenstufenform verlangt, so können wir etwa die Hälfte der Operationen sparen. Formulieren Sie sorgsam diesen Algorithmus und zählen Sie seine Zeilenoperationen.

Der Gauß–Algorithmus

B215
Erläuterung

Der **Gauß–Algorithmus** wird auch **Gauß–Verfahren** genannt oder **Gauß–Elimination**, da schrittweise Koeffizienten gelöscht werden.

Die Methode ist sehr einfach: Sie können sie leicht implementieren. Versuchen Sie es! Das ist eine lehrreiche Fingerübung, insbesondere wenn Ihr Programm möglichst schnell und nachweislich korrekt sein soll.

Der Gauß–Algorithmus ist mit $\leq n^3$ Operationen erstaunlich effizient. Für eine Matrix mit ein paar Tausend Zeilen und Spalten benötigt er ein paar Milliarden Operationen in $\mathbb{K}$. Für einen endlichen Körper wie $\mathbb{Z}_p$ dürfen wir hier konstante Kosten annehmen; das ist der Idealfall.

Für nicht-endliche Körper wie $\mathbb{Q}$ müssen wir mit Koeffizientenexplosion rechnen. Fließkommazahlen haben zwar feste Länge und sind schnell, produzieren dafür aber Rundungsfehler. Hierzu lernen Sie Numerik!

Moderne PCs schaffen knapp eine Billion Operationen in einer Sekunde, TerraFlops = 10^{12} *floating point operations per second*. Europas derzeit schnellster Supercomputer (Stand 2020) mit rund 26 PetaFlops, also $26 \cdot 10^{15}$ *floating point operations per second*, ist das System Hawk im Höchstleistungsrechenzentrum Stuttgart (HLRS).

Der Gauß–Algorithmus

B216

Größe n	Operationen in $\mathbb{K}$ (feste Kosten)	Zeit bei 10^9 op/s (Standard PC)	Zeit bei 10^{15} op/s (Supercomputer)
10^1	$< 10^3$	$< 1\mu$s	
10^2	$< 10^6$	< 1ms	
10^3	$< 10^9$	< 1 s	
10^4	$< 10^{12}$	< 30 min	
10^5	$< 10^{15}$	< 12 Tage	< 1 s
10^6	$< 10^{18}$	< 32 Jahre	< 30 min
10^7	$< 10^{21}$	< 32000 Jahre	< 12 Tage
10^8	$< 10^{24}$		< 32 Jahre
10^9	$< 10^{27}$		< 32000 Jahre

In datenintensiven Anwendungen und realen Modellen (wie Googles PageRank oder Wettersimulationen) entstehen noch größere Matrizen. Glücklicherweise sind diese meist dünn besetzt, mit nur sehr wenigen Einträgen ungleich Null. Hierzu gibt es hochspezialisierte Verfahren. Die Numerik erklärt Ihnen, wie Sie Fehler und Laufzeit klein halten.

Zeilenoperation als Matrixmultiplikation von links

B217

Wir betrachten Zeilenoperationen auf einer Matrix $A \in \mathbb{K}^{m\times n}$.
Zunächst illustrieren wir diese für $m = 2$ sowie $i = 1$ und $j = 2$.

Alle **elementaren Zeilenoperationen** sind Linksmultiplikationen:

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \cdot \begin{bmatrix}a_{i1} & \dots & a_{in}\\ a_{j1} & \dots & a_{jn}\end{bmatrix} = \begin{bmatrix}a_{j1} & \dots & a_{jn}\\ a_{i1} & \dots & a_{in}\end{bmatrix}$$

$$\begin{bmatrix}\mu & 0\\ 0 & 1\end{bmatrix} \cdot \begin{bmatrix}a_{i1} & \dots & a_{in}\\ a_{j1} & \dots & a_{jn}\end{bmatrix} = \begin{bmatrix}\mu a_{i1} & \dots & \mu a_{in}\\ a_{j1} & \dots & a_{jn}\end{bmatrix}$$

$$\begin{bmatrix}1 & 0\\ \lambda & 1\end{bmatrix} \cdot \begin{bmatrix}a_{i1} & \dots & a_{in}\\ a_{j1} & \dots & a_{jn}\end{bmatrix} = \begin{bmatrix}a_{i1} & \dots & a_{in}\\ \lambda a_{i1} + a_{j1} & \dots & \lambda a_{in} + a_{jn}\end{bmatrix}$$

Wir schreiben dies zusammenfassend als **Elementarmatrizen**:

$$P_{12} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \quad S_1(\mu) = \begin{bmatrix}\mu & 0\\ 0 & 1\end{bmatrix}, \quad T_{12}(\lambda) = \begin{bmatrix}1 & 0\\ \lambda & 1\end{bmatrix}$$

Ihre inversen Matrizen haben glücklicherweise dieselbe Form:

$$P_{12}^{-1} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \quad S_1(\mu)^{-1} = \begin{bmatrix}\mu^{-1} & 0\\ 0 & 1\end{bmatrix}, \quad T_{12}(\lambda)^{-1} = \begin{bmatrix}1 & 0\\ -\lambda & 1\end{bmatrix}$$

Zeilenoperation als Matrixmultiplikation von links

B218

Wir definieren $S_i : \mathbb{K} \hookrightarrow \mathbb{K}^{m\times m} : a \mapsto B = S_i(a)$.
Die Matrix B ist gleich $1_{m\times m}$ mit der Ausnahme $b_{ii} = a$.
Somit ist $A \mapsto S_i(\mu)A$ die Multiplikation der $i$ten Zeile mit μ.

$$\begin{bmatrix}1 & & & & \\ & 1 & & & \\ & & a & & \\ & & & 1 & \\ & & & & 1\end{bmatrix}$$

Wir definieren die Einbettung $\Psi_{ij} : \mathbb{K}^{2\times 2} \hookrightarrow \mathbb{K}^{m\times m} : A \mapsto B = \Psi_{ij}(A)$.
Die Matrix B ist gleich der Einheitsmatrix $1_{m\times m}$ mit den vier Ausnahmen

$$\begin{bmatrix}b_{ii} & b_{ij}\\ b_{ji} & b_{jj}\end{bmatrix} = \begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}.$$

Damit erhalten wir die Permutation P_{ij} und die Transvektion $T_{ij}(\lambda)$:

$$P_{ij} = \Psi_{ij}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \quad T_{ij}(\lambda) = \Psi_{ij}\begin{bmatrix}1 & 0\\ \lambda & 1\end{bmatrix}$$

Ihre inversen Matrizen haben glücklicherweise dieselbe Form:

$$P_{ij}^{-1} = P_{ij}, \quad S_i(\mu)^{-1} = S_i(\mu^{-1}), \quad T_{ij}(\lambda)^{-1} = T_{ij}(-\lambda)$$

Dies definiert unsere **Elementarmatrizen** $P_{ij}, S_i(\mu), T_{ij}(\lambda) \in \mathrm{GL}_m\,\mathbb{K}$.

Zeilenoperation als Matrixmultiplikation von links

B219

Die Matrix $A \in \mathbb{K}^{m\times n}$ formen wir um zu A' durch die Zeilenoperationen $B_1, B_2, \dots, B_\ell \in \{P_{ij}, S_i(\mu), T_{ij}(\lambda)\} \subset \mathrm{GL}_m\,\mathbb{K}$. Somit erhalten wir

$$A' \;=\; B_\ell(\cdots(B_2(B_1A))\cdots) \;=\; B_\ell \cdots B_2B_1A.$$

Assoziativität sei Dank! Dieses Produkt fassen wir zusammen zu

$$A' = BA \quad \text{mit} \quad B = B_\ell \cdots B_2B_1.$$

Jede der Operationen $B_1, B_2, \dots, B_\ell$ können wir umkehren, also gilt:

$$B_1^{-1}B_2^{-1}\dots B_\ell^{-1}A' = A$$

Auch dieses Produkt können wir zusammenfassen zu

$$B^{-1}A' = A \quad \text{mit} \quad B^{-1} = B_1^{-1}B_2^{-1}\dots B_\ell^{-1}.$$

🙂 Jede Zeilenoperation entspricht einer Elementarmatrix B_i.
Ihre Komposition entspricht der Linksmultiplikation mit $B \in \mathrm{GL}_m\,\mathbb{K}$.

🙂 Im Spezialfall $A' = 1_{m\times m}$ finden wir $A = B^{-1}$, und somit $A^{-1} = B$.
Das ist ein elegant-effizienter Algorithmus zur Inversion von Matrizen.

Zeilenoperation als Matrixmultiplikation von links

B220
Erläuterung

Wir erleben hier ein erstes nützliches Wunder des Matrixkalküls.
Wir können jedes lineare Gleichungssystem bündeln zu $Ax = b$.
Zudem können wir elementare Zeilenoperationen elegant als Linksmultiplikation mit einer Elementarmatrix interpretieren.

🙂 Alles fügt sich wunderbar zusammen, elegant und effizient!

Übung: Wir können lineare Gleichungssysteme auch $xA = b$ schreiben mit der Matrix $A \in \mathbb{K}^{m\times n}$ und Zeilenvektoren $x \in \mathbb{K}^{1\times m}$ und $b \in \mathbb{K}^{1\times n}$.
In diesem Falle nutzen wir Spaltenoperationen, und diese entsprechen der Rechtsmultiplikation mit einer geeigneten Elementarmatrix.

Führen Sie dies zur Übung bzw. Wiederholung sorgfältig aus!

🙂 Die Unbekannte x steht in $Ax = b$ bzw. $xA = b$ auf der einen Seite, wir operieren auf der Matrix A jeweils von der anderen Seite.

In einem Körper oder allgemein CRing ist die Multiplikation kommutativ, daher sind $Ax = b$ und $x^\intercal A^\intercal = b^\intercal$ äquivalent durch Transposition (B119).
In einem Schiefkörper oder allgemein nicht-kommutativem Ring müssen wir im Allgemeinen links und rechts sorgsam auseinanderhalten.

Invertierbarkeitskriterien für Matrizen

surjektiv injektiv bijektiv

Satz B2D: Invertierbarkeitskriterien für Matrizen

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$; es genügt ein Divisionsring, wie $\mathbb{H}$.
Zur Matrix $A \in \mathbb{K}^{m\times n}$ untersuchen wir das Gleichungssystem $Ax = b$.
Dazu bringen wir A auf Zeilenstufenform A', mit Rang $r \leq \min\{m, n\}$.

(1) Surjektivität. Die folgenden drei Aussagen sind äquivalent:
(a) Zu jedem $b \in \mathbb{K}^m$ existiert mindestens ein $x \in \mathbb{K}^n$ mit $Ax = b$.
(b) Die Matrix A ist rechtsinvertierbar, $\exists C \in \mathbb{K}^{n\times m} : AC = 1_{m\times m}$.
(c) Es gilt $r = m \leq n$, also Rang gleich Zeilenzahl.

(2) Injektivität. Die folgenden drei Aussagen sind äquivalent:
(a) Zu jedem $b \in \mathbb{K}^m$ existiert höchstens ein $x \in \mathbb{K}^n$ mit $Ax = b$.
(b) Die Matrix A ist linksinvertierbar, $\exists B \in \mathbb{K}^{n\times m} : BA = 1_{n\times n}$.
(c) Es gilt $r = n \leq m$, also Rang gleich Spaltenzahl.

(3) Bijektivität. Die folgenden drei Aussagen sind äquivalent:
(a) Zu jedem $b \in \mathbb{K}^m$ existiert genau ein $x \in \mathbb{K}^n$ mit $Ax = b$.
(b) Die Matrix A ist invertierbar, $\exists B \in \mathbb{K}^{n\times m} : BA = 1_{n\times n},\ AB = 1_{m\times m}$.
(c) Es gilt $r = m = n$, also A quadratisch mit vollem Rang.

Invertierbarkeitskriterien für Matrizen

Logik Implikation Äquivalenz

Behauptung (1): Die folgenden drei Aussagen sind äquivalent:
(a) Zu jedem $b \in \mathbb{K}^m$ existiert mindestens ein $x \in \mathbb{K}^n$ mit $Ax = b$.
(b) Die Matrix A ist rechtsinvertierbar: $\exists C \in \mathbb{K}^{n\times m} : AC = 1_{m\times m}$.
(c) Es gilt $r = m \leq n$, also Rang gleich Zeilenzahl.

Beweis: „(a) ⇒ (b)“: Zu $e_1, \ldots, e_m \in \mathbb{K}^m$ existieren $c_1, \ldots, c_m \in \mathbb{K}^n$ mit $Ac_i = e_i$. Die Matrix $C = (c_1, \ldots, c_m) \in \mathbb{K}^{n\times m}$ erfüllt also

$$AC = (Ac_1, \ldots Ac_m) = (e_1, \ldots, e_m) = 1_{m\times m}.$$

„(b) ⇒ (a)“: Zu $b \in \mathbb{K}^m$ erfüllt $x = Cb \in \mathbb{K}^n$ die gewünschte Gleichung

$$Ax = A(Cb) = (AC)b = 1_{m\times m}b = b.$$

„(c) ⇔ (a)“: Gilt $r = m$, so ist $Ax = b$ für jedes $b \in \mathbb{K}^m$ lösbar (Satz B2B).
Umgekehrt, gilt $r < m$, so ist $Ax = b$ für manche $b \in \mathbb{K}^m$ unlösbar:
Wir betrachten zu A die Zeilenstufenform $A' = SA$ mit $S \in \mathrm{GL}_m \mathbb{K}$.
Die Gleichungen $Ax = b$ und $A'x = b'$ mit $A' = SA$ und $b' = Sb$ sind äquivalent, haben also dieselbe Lösungsmenge $L(A, b) = L(A', b')$.
Wegen $r < m$ ist $A'x = e_m$ unlösbar, somit auch $Ax = b$ für $b = S^{-1}e_m$.

Invertierbarkeitskriterien für Matrizen

Logik Implikation Äquivalenz

Behauptung (2): Die folgenden drei Aussagen sind äquivalent:
(a) Zu jedem $b \in \mathbb{K}^m$ existiert höchstens ein $x \in \mathbb{K}^n$ mit $Ax = b$.
(b) Die Matrix A ist linksinvertierbar, $\exists B \in \mathbb{K}^{n\times m} : BA = 1_{n\times n}$.
(c) Es gilt $r = n \leq m$, also Rang gleich Spaltenzahl.

Beweis: „(c) ⇔ (a)“: Wir nutzen Satz B2B. Gilt $r = n$, so hat $Ax = b$ für jedes $b \in \mathbb{K}^m$ höchstens eine Lösung $x \in \mathbb{K}^n$. Gilt $r < n$, so haben wir für $Ax = 0$ genau $n - r$ freie Variablen, also mehrere Lösungen $x \in \mathbb{K}^n$.

„(b) ⇒ (a)“: Wir haben $BA = 1_{n\times n}$. Gilt $Ax = Ax' = b$, so folgt

$$x = 1_{n\times n}x = (BA)x = B(Ax) = B(Ax') = (BA)x' = 1_{n\times n}x' = x'.$$

„(a) ⇒ (b)“: Wir haben die reduzierte Zeilenstufenform $A' = SA$ mit $S \in \mathrm{GL}_m \mathbb{K}$. Wegen $r = n$ beginnt A' mit den Zeilen $e_1^\intercal, \ldots, e_n^\intercal$.
Seien $b_1^\intercal, \ldots, b_n^\intercal \in \mathbb{K}^m$ die ersten Zeilen von S, also $b_i^\intercal A = e_i^\intercal$.
Die daraus gebildete Matrix $B \in \mathbb{K}^{n\times m}$ erfüllt $BA = 1_{n\times n}$. QED

Aufgabe: Behauptung (3) folgt aus (1) und (2). Erklären Sie wie!

Invertierbarkeitskriterien für Matrizen

Erläuterung

Lösung: Dies ist eine Übung der Logik und des genauen Lesens:

- Bijektivität (3a) ist nach Definition äquivalent zu Surjektivität (1a) und Injektivität (2a).
- Invertierbarkeit (3b) ist nach Definition äquivalent zu Rechtsinvertierbarkeit (1b) und Linksinvertierbarkeit (2b).

Dazu haben wir oben bereits gezeigt:

- Surjektivität (1a) ist äquivalent zu Rechtsinvertierbarkeit (1b).
- Injektivität (2a) ist äquivalent zu Linksinvertierbarkeit (2b).

Somit ist Aussage (3a) äquivalent zu Aussage (3b).
Genauso folgt: Aussage (3b) ist äquivalent zu (3c).

🙂 Wenn Sie möchten, können Sie zur Übung die Äquivalenzen „(3a) ⇔ (3b)“ und „(3b) ⇔ (3c)“ erneut beweisen, indem Sie alle obigen Argumente wiederholen und hier noch einmal ausführen. Didaktisch gesehen ist Wiederholung meist eine gute Übung.

🙂 Wenn Sie jedoch Zeit sparen wollen, dann können Sie diese Arbeit effizient abkürzen. Die Logik hilft Ihnen. Abstraktion wirkt ganz konkret.

Invertierbarkeitskriterien für Matrizen

☺ Nach getaner Arbeit ist es ratsam und hilfreich zurückzublicken:
Wie sehen konkrete Anwendungen, Beispiele und Gegenbeispiele aus?
Was lässt sich noch vereinfachen? Was lässt sich verallgemeinern?

Zusatz B2D: Invertierbarkeit über einem beliebigen Ring

Wichtige Teile des Satzes B2D gelten über jedem Ring $\mathbb{K}$:

1. Die Äquivalenz „(1a) $\Leftrightarrow$ (1b)“ gilt über jedem Ring $\mathbb{K}$.
2. Die Implikation „(2b) $\Rightarrow$ (2a)“ gilt über jedem Ring $\mathbb{K}$, doch die Umkehrung „(2a) $\Rightarrow$ (2b)“ gilt nicht über dem Ring $\mathbb{Z}$.
3. Die Äquivalenz „(3a) $\Leftrightarrow$ (3b)“ hingegen gilt über jedem Ring $\mathbb{K}$.

Aufgabe: Beweisen Sie dies nach dem Muster des vorigen Satzes.

Lösung: (1) In unserem obigen Beweis der Äquivalenz „(1a) $\Leftrightarrow$ (1b)“ haben wir nur benutzt, dass $\mathbb{K}$ ein Ring ist; damit stehen uns alle hierzu benötigten Rechenregeln für Matrizen über $\mathbb{K}$ weiterhin zur Verfügung.

☺ Den Gauß–Algorithmus haben wir nur für „(1c) $\Leftrightarrow$ (1a)“ eingesetzt.
Die Äquivalenz „(1a) $\Leftrightarrow$ (1b)“ kommt wunderbar ohne aus.

Invertierbarkeitskriterien für Matrizen

(2) In unserem obigen Beweis der Implikation „(2b) $\Rightarrow$ (2a)“ haben wir nur benutzt, dass $\mathbb{K}$ ein Ring ist; damit stehen uns alle hierzu benötigten Rechenregeln für Matrizen über $\mathbb{K}$ weiterhin zur Verfügung.

⚠ Zur Umkehrung „(2a) $\Rightarrow$ (2b)“ nutzen wir den Gauß–Algorithmus, und dieser beruht wesentlich darauf, dass wir in $\mathbb{K}$ invertieren können. Ohne diese Voraussetzung schlägt der Beweis tatsächlich fehl!

Zur Illustration betrachten wir den Ring $\mathbb{Z}$ der ganzen Zahlen.
Wir betrachten 1×1–Matrizen, also Ringelemente $a \in \mathbb{Z}^{1\times 1} = \mathbb{Z}$.
Ein ganz konkretes und sehr einfaches Gegenbeispiel ist $a = 2$:
(a) Zu jedem $b \in \mathbb{Z}$ existiert höchstens ein $x \in \mathbb{Z}$ mit $2x = b$.
(b) Dennoch ist das Element $a = 2$ in $\mathbb{Z}$ nicht (links)invertierbar.

☺ In Satz B2D tritt dieses Problem nicht auf, da wir dort $\mathbb{K}$ als Divisionsring voraussetzen. Wenn wir statt des Rings $\mathbb{Z}$ den Körper $\mathbb{Q}$ betrachten, so ist das Element $a = 2$ in $\mathbb{Q}$ invertierbar, und alles wird gut.

Invertierbarkeitskriterien für Matrizen

(3) Die Äquivalenz „(3a) $\Leftrightarrow$ (3b)“ gilt über jedem Ring $\mathbb{K}$.
Zum Beweis müssen wir jedoch etwas genauer hinsehen!

Die Implikation „(3b) $\Rightarrow$ (3a)“ gilt weiterhin, wie oben gezeigt:
Die Invertierbarkeit (3b) ist nach Definition äquivalent zu Rechtsinvertierbarkeit (1b) und Linksinvertierbarkeit (2b).
Daraus folgt Surjektivität (1a) und Injektivität (2a) wie zuvor, und dies ist nach Definition äquivalent zu Bijektivität (3a).

Die Umkehrung „(3a) $\Rightarrow$ (3b)“ hingegen ist etwas raffinierter, da wir nun nicht mehr „(2a) $\Rightarrow$ (2b)“ nutzen können, wie oben über $\mathbb{Z}$ illustriert.
Dank „(3a) $\Rightarrow$ (1a) $\Rightarrow$ (1b)“ ist A rechtsinvertierbar, zu A existiert demnach eine rechtsinverse Matrix $C \in \mathbb{K}^{n\times m}$ mit $AC = 1_{m\times m}$.
Dank „(3a) $\Rightarrow$ (2a)“ ist die Matrix A zudem linkskürzbar. Wir haben $A1 = A = 1A = (AC)A = A(CA)$, nach Kürzen also $1 = CA$.
Demnach ist die Matrix A invertierbar durch C, denn $AC = 1 = CA$.

Wie lernen Sie Mathematik?

Dieser Satz ist überaus praktisch, aber zugegeben nicht ganz leicht.
Was lernen Sie aus seinem Beweis und den zugehörigen Übungen?

- Theoretische Grundlagen und praktische Algorithmen sind eng verzahnt, sie stützen sich gegenseitig und arbeiten zusammen. Bei der Lösung linearer Gleichungen ist dies besonders eindrücklich.
- Es lohnt sich, die zentralen Probleme allgemein zu lösen und dabei genau zu formulieren: Was sind die Voraussetzungen? Was sind die Folgerungen? Wie verlaufen die Beweise und die Algorithmen?

Zudem sehen Sie die angestrebte Arbeitsteilung zwischen Vorlesung, eigener Nacharbeit und konkreten Anwendungen, etwa in den Übungen:

- Vorlesung / Skript erklären Ihnen die wesentlichen Ideen, Begriffe und Techniken, insb. Definitionen und Sätze, Beweise und Beispiele.
- Ihre eigene Nacharbeit sichert Ihnen das Verständnis in den Details. In den Anwendungen führen Sie dies an konkreten Beispielen aus.

Die Abgrenzung dieser Phasen ist nicht leicht und keinesfalls eindeutig.
In jedem Falle beruht Ihr Lernerfolg auf Ihrer individuellen Investition.

Invertierbarkeit quadratischer Matrizen

Ausprobieren mit Gaël!

Korollar B2E: Invertierbarkeit quadratischer Matrizen

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$; es genügt ein Divisionsring, wie $\mathbb{H}$.

(0) Für jede quadratische Matrix $A \in \mathbb{K}^{n\times n}$ gilt dank Satz B2D:
A ist linksinvertierbar $\Leftrightarrow$ A ist rechtsinvertierbar $\Leftrightarrow$ A ist invertierbar.
Jede Linksinverse zu A ist eine Rechtsinverse zu A und umgekehrt.

🙂 Damit können wir jeweils die Hälfte der Arbeit einsparen!

Wir gewinnen zwei praktische Verfahren zur Inversion von $A \in \mathbb{K}^{n\times n}$:

(1) Bringe A in reduzierte Zeilenstufenform $A' = SA$, mit $S \in \mathrm{GL}_n \mathbb{K}$.
Gilt dabei $A' = 1_{n\times n}$, so ist die Matrix A invertierbar und $A^{-1} = S$.
Andernfalls gilt $r < n$ und A ist nicht invertierbar.

(2) Beginne mit der erweiterten Matrix $X = (A, 1_{n\times n})$. Bringe X in reduzierte Zeilenstufenform X'. Sind die Stufen $(1, 2, \ldots, n)$, so ist A invertierbar und $X' = (1_{n\times n}, A^{-1})$. Andernfalls ist A nicht invertierbar.

(3) Jede invertierbare Matrix $A \in \mathrm{GL}_n \mathbb{K}$ ist demnach ein Produkt von elementaren Matrizen $\{P_{ij}, S_i(\mu), T_{ij}(\lambda)\} \subset \mathrm{GL}_n \mathbb{K}$.

Invertierbarkeit quadratischer Matrizen

Aufgabe: Führen Sie den Beweis dieses Korollars sorgsam aus.
Sie müssen hierzu nichts Neues erfinden, alles liegt vor Ihnen.

Lösung: Die Aussage (0) ist ein einfacher aber wichtiger Spezialfall der Äquivalenz „(b) $\Leftrightarrow$ (c)“ im obigen Invertierbarkeitskriterium (Satz B2D):
Genau dann ist $A \in \mathbb{K}^{n\times n}$ links-/rechts-/invertierbar, wenn $r = n$ gilt.

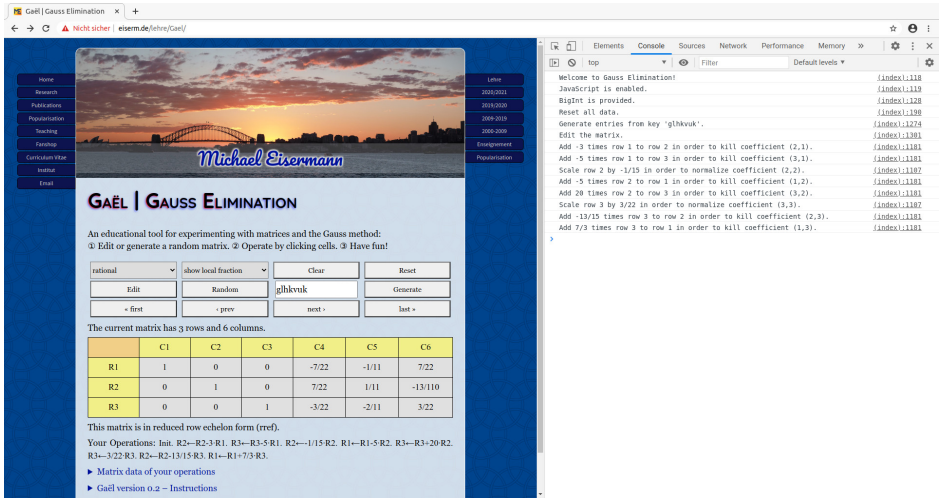
Die Aussagen (1) und (2) sowie (3) fassen unsere vorhergehenden Überlegungen zum Gauß–Algorithmus zusammen. Zur Krönung unserer Mühen habe ich dies als Korollar an den Schluss gestellt.

Bemerkung: Ein **Korollar** ist eine Aussage, die sich aus einem vorigen Satz oder Beweis ohne großen Aufwand folgern lässt (lat. *corollarium* ‘Zugabe’, ‘Geschenk’, von *corona* ‘Kranz’ zu *corolla* ‘Kränzchen’).

Korollare sind demnach einfache Schlussfolgerungen, manchmal auch Umformulierungen oder Spezialisierungen. Die Abgrenzung zwischen Lemma und Satz und Korollar ist weitgehend subjektiv und dient vor allem der Betonung und relativen Gewichtung der Ergebnisse.

Gaël: Experimentieren Sie mit dem Gauß–Verfahren!

Das Online-Tool **Gaël** ist intuitiv klickbar, damit können Sie spielen!



Damit lösen Sie lineare Gleichungssysteme, invertieren Matrizen und experimentieren mit Umformungen. Gaël übernimmt die Buchführung.

Gaël: Experimentieren Sie mit dem Gauß–Verfahren!

Sie kennen nun die theoretischen Grundlagen und erste Methoden zu Matrizen und linearen Gleichungssystemen. Sie lernen Neues und verfestigen Ihr Wissen im Wechselspiel von zwei Aktivitäten:

1. Wiederholen Sie die wesentlichen Ideen, Begriffe und Techniken, also die Definitionen und Sätze sowie Beweise und Beispiele.
2. Wenden Sie diese möglichst vielfältig in neuen Aufgaben an und führen Sie diese an konkreten Beispielen aus.

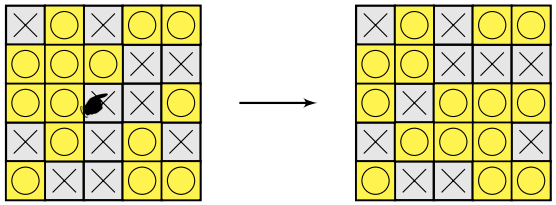
In konkreten Aufgaben (2), etwa in unseren wöchentlichen Quizzen und Übungen, werden Sie immer wieder auf Verständnisfragen (1) stoßen. Das gilt bereits für die folgenden Anwendungen und Illustrationen. Theorie und Anwendung helfen beide Ihrem Verständnis.

🙂 Lernen ist kein strikt linearer Prozess, sondern eher zyklisch.

Es ist gut und richtig, dass Sie auf die Grundlagen später immer wieder zurückkommen und jedesmal etwas besser und umfassender verstehen. Dadurch erkennen Sie auch in konkreten Anwendungen nützliche Zusammenhänge und können diese dann effizient nutzen.

Es werde Licht! . . . mit Linearer Algebra

Sie spielen auf einem rechteckigen Spielbrett der Größe $n = a \times b$.
An jeder Position befindet sich eine Lampe, entweder an oder aus.



Wenn Sie eine Lampe umschalten, dann schalten sich automatisch auch alle Nachbarn um: oben, unten, links, rechts, soweit vorhanden.

☺ Alternativ als Spiel für unterwegs mit Münzen, Kopf 0 oder Zahl 1.
Probieren Sie es selbst aus! Es macht Spaß und ist lehrreich. . .

Aufgabe: (a) Alle Lampen sind aus. Können Sie alle anschalten? Wie?
(b) Können Sie jede beliebige Konfiguration erreichen? Falls ja, wie?

(0) Untersuchen Sie kleine Spielfelder wie 1×3, 1×4, 1×5, 2×2.
(1) Wie lösen Sie dies systematisch? Tipp: als Gleichungssystem!

Es werde Licht! . . . mit Linearer Algebra

1	2	3
4	5	6
7	8	9

Lösung: (1) Die Reihenfolge der Aktionen ist egal. Für jede Lampe $i \in \{1, \ldots, n\}$ zählt allein, ob die Anzahl der Umschaltungen gerade oder ungerade war, also der Rest $x_i \in \mathbb{Z}_2$. Die Umschaltungen codieren wir als Vektor $x = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$.

Welche Lampen brennen am Ende? Dies codieren wir durch $y \in \mathbb{Z}_2^n$.
Den Zusammenhang $y = Ax$ beschreiben wir durch die Matrix

$$A = \left[\begin{array}{ccc|ccc|ccc} 1&1&0&1&0&0&0&0&0\\ 1&1&1&0&1&0&0&0&0\\ 0&1&1&0&0&1&0&0&0\\ \hline 1&0&0&1&1&0&1&0&0\\ 0&1&0&1&1&1&0&1&0\\ 0&0&1&0&1&1&0&0&1\\ \hline 0&0&0&1&0&0&1&1&0\\ 0&0&0&0&1&0&1&1&1\\ 0&0&0&0&0&1&0&1&1 \end{array}\right], \quad x = \begin{bmatrix} x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9 \end{bmatrix}, \quad y = \begin{bmatrix} y_1\\y_2\\y_3\\y_4\\y_5\\y_6\\y_7\\y_8\\y_9 \end{bmatrix}.$$

Ist jede Konfiguration y erreichbar? Ist A invertierbar? Gauß hilft!

Es werde Licht! . . . mit Linearer Algebra

Wir überführen $X = (A, 1_{n\times n})$ in reduzierte Zeilenstufenform X':

$$X = \left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc} 1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\ 1&1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\ 0&1&1&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0\\ \hline 1&0&0&1&1&0&1&0&0&0&0&0&1&0&0&0&0&0\\ 0&1&0&1&1&1&0&1&0&0&0&0&0&1&0&0&0&0\\ 0&0&1&0&1&1&0&0&1&0&0&0&0&0&1&0&0&0\\ \hline 0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&1 \end{array}\right]$$

$$X' = \left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc} 1&0&0&0&0&0&0&0&0&1&0&1&0&0&1&1&1&0\\ 0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1\\ 0&0&1&0&0&0&0&0&0&1&0&1&1&0&0&0&1&1\\ \hline 0&0&0&1&0&0&0&0&0&0&0&1&0&1&1&0&0&1\\ 0&0&0&0&1&0&0&0&0&0&1&0&1&1&1&0&1&0\\ 0&0&0&0&0&1&0&0&0&1&0&0&1&1&0&1&0&0\\ \hline 0&0&0&0&0&0&1&0&0&1&1&0&0&0&1&1&0&1\\ 0&0&0&0&0&0&0&1&0&1&1&1&0&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&0&1 \end{array}\right]$$

Es werde Licht! . . . mit Linearer Algebra

Mit welcher Umschaltung x gelangen wir von „alle aus“ zu „alle an“?
Dies können wir nun leicht ausrechnen gemäß $x = A^{-1}y$ mit

$$A^{-1} = \left[\begin{array}{ccc|ccc|ccc} 1&0&1&0&0&1&1&1&0\\ 0&0&0&0&1&0&1&1&1\\ 1&0&1&1&0&0&0&1&1\\ \hline 0&0&1&0&1&1&0&0&1\\ 0&1&0&1&1&1&0&1&0\\ 1&0&0&1&1&0&1&0&0\\ \hline 1&1&0&0&0&1&1&0&1\\ 1&1&1&0&1&0&0&0&0\\ 0&1&1&1&0&0&1&0&1 \end{array}\right], \quad y = \begin{bmatrix} 1\\1\\1\\1\\1\\1\\1\\1\\1 \end{bmatrix}, \quad x = \begin{bmatrix} 1\\0\\1\\0\\1\\0\\1\\0\\1 \end{bmatrix}.$$

Probieren Sie es aus! Unsere Rechnung findet diese Lösung routiniert und systematisch und zeigt zudem, dass dies die einzige Lösung ist.

☺ Auf dem 3×3–Spielbrett sind alle Konfigurationen erreichbar!

☺ Auf 4×4 und 5×5 lässt sich alles umschalten, aber nicht eindeutig, und manche Konfigurationen sind unerreichbar. Das passt zu Satz B2D!
Mehr Infos unter `mathworld.wolfram.com/LightsOutPuzzle.html`.

Übung: Denken Sie sich eine beliebige Konfiguration $y \in \mathbb{Z}_2^n$ aus. Versuchen Sie, diese vom Ausgangszustand $(0, \ldots, 0)$ zu erreichen: Wie gelingt Ihnen dies? zudem mit möglichst wenig Zügen? Beispiel:

$$A^{-1} = \left[\begin{array}{ccc|ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}\right], \quad y = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad x = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

Versuchen Sie es zunächst selbst, dann mit den obigen Matrizen. Nur durch mutiges Ausprobieren und eigene Erfahrung lernen Sie die Klarheit und Eleganz der algebraischen Methode schätzen.

Ich habe die Schritte des Gauß–Algorithmus hier nicht ausgeführt. Sie wissen im Prinzip, wie es geht, und ich empfehle es als Übung.

Übung: Invertieren Sie die Matrix $A \in \mathbb{Z}_2^{9\times 9}$. Die Matrix ist zwar nicht ganz klein, doch zum Glück sind die Rechnungen in $\mathbb{Z}_2$ extrem einfach. Das Wichtigste sind hierzu eine gute Notation und sorgsame Arbeit. Mit Mut und Sorgfalt ist es möglich. Respekt, wenn es Ihnen gelingt!

Tipp: Versuchen Sie, möglichst wenig Schreibarbeit zu erzeugen. Auf Karopapier genügt es, die Einsen zu markieren, Nullen bleiben leer. Die vollständige Rechnung benötigt dann etwa drei DIN-A4-Seiten: Jeder einzelne Schritt ist leicht, aber viele sind nötig.

Alternative: Vielleicht möchten Sie das Verfahren programmieren? Das liegt in Ihrer Reichweite und Sie können sehr viel dabei lernen. Es ist ideal für einen Computer: einfache Schritte, davon sehr viele. Sie können dies sogar gleich über dem Körper $\mathbb{Z}_p$ implementieren, dazu kennen Sie bereits alle nötigen Methoden. Mathematik wirkt!

Varianten dieses Spiels wurden sehr erfolgreich vermarktet:

- *Merlin* 1978 als 3×3–Version. Dieses frühe *handheld electronic game* wurde mehr als fünf Millionen mal verkauft!
  `en.wikipedia.org/wiki/Merlin_(console)`
- *Lights Out* 1995 als 5×5–Version. Heutzutage würde man eine Web- oder Handy-App schreiben. . . Die gibt es tatsächlich!
  `en.wikipedia.org/wiki/Lights_Out_(game)`

🙂 Bitte beachten Sie: Weder die Spielregeln noch die Strategien sprechen von Linearer Algebra oder überhaupt von Mathematik. Problem und Lösung lassen sich ganz anschaulich formulieren.

Die dahinter liegende Mathematik ist versteckt, doch überaus spannend: Zur systematischen Lösung erweisen sich lineare Gleichungssysteme und der Gauß–Algorithmus als Schlüssel zum Erfolg.

🙂 Mathematische Methoden sind häufig Voraussetzung für den Erfolg, auch wenn sie im Inneren wirken und oberflächlich nicht sichtbar sind.

Auch die nächsten beiden Anwendungsbeispiele sind von dieser Art: Frage und Antwort sprechen vordergründig nicht von Linearer Algebra. Diese erweist sich jedoch als effizientes Werkzeug zur Lösung!

Deshalb studieren Sie Mathematik, deshalb beginnen wir mit Linearer Algebra und Analysis: Es lohnt sich, diese universellen Methoden zu erlernen und in die mathematischen Grundlagen zu investieren:

Damit erkennen Sie Zusammenhänge und Lösungen, wo andernfalls nur heillose Verwirrung und planloses Herumprobieren möglich wären.

Anwendungsbeispiel: Lagrange–Interpolation

Aufgabe: Sei $\mathbb{K}$ ein Körper, etwa $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$. Gegeben seien Punkte $(x_0, y_0), \dots, (x_n, y_n) \in \mathbb{K}^2$ mit $x_i \neq x_j$ für $i \neq j$. Gesucht ist ein Polynom $P(X) = c_0 + c_1 X + \cdots + c_n X^n$ in $\mathbb{K}[X]$ mit $P(x_i) = y_i$ für alle i. (B101)

(1) Schreiben Sie dies als ein lineares Gleichungssystem.
(2) Gibt es immer mindestens eine Lösung $P \in \mathbb{K}[X]_{\leq n}$?
(3) Gibt es immer genau eine Lösung $P \in \mathbb{K}[X]_{\leq n}$?

Lösung: (1) Wir suchen c, sodass $Vc = y$ mit der Vandermonde–Matrix

$$V = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix} \quad \text{sowie} \quad c = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{bmatrix} \quad \text{und} \quad y = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix}.$$

(2) Zu jeder Problemstellung y existiert die Lagrange–Interpolation

$$L(X) := \sum_{j=0}^{n} y_j L_j(X) \in \mathbb{K}[X]_{\leq n} \quad \text{mit} \quad L_j(X) := \prod_{i \neq j} \frac{X - x_i}{x_j - x_i} \in \mathbb{K}[X]_n.$$

(3) Dank B2D ist V invertierbar, also $c = V^{-1} y$ die eindeutige Lösung!

Anwendungsbeispiel: Lagrange–Interpolation

Ausführlich: (1) Wir schreiben das Gleichungssystem aus, hier $Vc = y$. Die Matrix V ist quadratisch, hier von der Größe $(n+1) \times (n+1)$.

🙂 Übrigens ist dies ein schönes Beispiel, wo die Indizierung $0, 1, \dots, n$ natürlicher ist als die Standardindizierung $1, 2, \dots, n+1$ (siehe B110). Es ist daher bequem und nützlich, auch diese Indizes zuzulassen.

(2) Die Lagrange–Interpolation können wir explizit ausschreiben. Zu jeder rechten Seite y existiert demnach mindestens eine Lösung c.

🙂 Dazu mussten wir nicht wirklich rechnen oder Gauß bemühen: Diese Lösung fällt uns anderweitig in den Schoß, dank Polynomring!

(3) Nun der Clou: Dank Satz B2D ist unsere Matrix V invertierbar!

🙂 Zu dieser Erkenntnis mussten wir die inverse Matrix V^{-1} nicht explizit ausrechnen. Im Moment interessiert sie uns auch gar nicht, denn eine Lösung L haben wir ja schon, es geht uns lediglich um die noch fehlende Eindeutigkeit. Abstrakte Theorie wirkt ganz konkret!

🙂 Im nächsten Beispiel „harmonische Gewinnerwartung“ nutzen wir Satz B2D umgekehrt, das heißt, aus Eindeutigkeit folgern wir Existenz.

Anwendungsbeispiel: Vandermonde–Matrix

Satz B3A: Die Vandermonde–Matrix ist invertierbar.

(0) Sei $\mathbb{K}$ ein Körper und $x_0, x_1, \dots, x_n \in \mathbb{K}$.
Wir definieren die **Vandermonde–Matrix**

$$\mathrm{VDM}(x_0, x_1, \dots, x_n) := (x_i^j)_{i,j=0,1,\dots,n} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix}$$

Diese ist genau dann invertierbar, wenn $x_i \neq x_j$ für alle $i \neq j$ gilt.

(1) Durch beliebige Datenpunkte $(x_0, y_0), \dots, (x_n, y_n) \in \mathbb{K}^2$ mit $x_i \neq x_j$ für alle $i \neq j$ verläuft demnach genau ein Polynom $P \in \mathbb{K}[X]_{\leq n}$.

(2) Je zwei Polynome $P, Q \in \mathbb{K}[X]_{\leq n}$ sind bereits dann gleich, wenn sie an $n+1$ Stellen $x_0, x_1, \dots, x_n \in \mathbb{K}$ übereinstimmen.

(3) Über jedem unendlichen Körper $\mathbb{K}$ ist die Abbildung $\delta_0 : \mathbb{K} \to \mathbb{K}$ mit $\delta_0(0) = 1$ und $\delta_0(x) = 0$ für $x \neq 0$ keine Polynomfunktion.

(4) Über jedem endlichen Körper $\mathbb{K}$ ist jede Abbildung $f : \mathbb{K} \to \mathbb{K}$ eine Polynomfunktion; es gilt $f = f_P$ für genau ein $P \in \mathbb{K}[X]_{<\sharp\mathbb{K}}$.

Anwendungsbeispiel: Polynomvergleich

Übung: Beweisen Sie diesen Satz nach Vorbild der vorigen Aufgabe. Hinweis: Die Inverse von V ist hier nicht gefragt. Wenn Sie möchten, können Sie kleine Beispiele per Hand oder mit Gaël ausrechnen.

⚠ Das praktische Vergleichskriterium (2) gilt für alle Polynome über einem Körper, aber nicht über jedem kommutativen Ring!

Beispiel: Im Ring $\mathbb{Z}_8$ hat das Polynom $P = X^2 - 1 \in \mathbb{Z}_8[X]$ genau vier Nullstellen: $1, 3, 5, 7$. Es stimmt dort mit dem Nullpolynom 0 überein. Wir würden daher $P = 0$ erwarten, es gilt aber $P \neq 0$.

🙂 Dieses praktische Vergleichskriterium (2) lässt sich retten über Integritätsringen, also kommutativen Ringen ohne Nullteiler, wie $\mathbb{Z}$.

Leider können wir in $\mathbb{Z}$ nicht invertieren, und daher für Matrizen über $\mathbb{Z}$ nicht den Gauß–Algorithmus anwenden. Aber über $\mathbb{Q} \supset \mathbb{Z}$ gelingt dies!

Übung: (a) Für je zwei Polynome $P, Q \in \mathbb{Q}[X]_{\leq n}$ gilt das Kriterium (2). Also gilt es auch für je zwei Polynome $P, Q \in \mathbb{Z}[X]_{\leq n}$ über $\mathbb{Z} \subset \mathbb{R}$.
(b) Allgemein: Ist R ein Integritätsring, so können wir im Bruchkörper $K \supseteq R$ rechnen (A1J). Das Argument (a) gilt dann wörtlich genauso.

Zufällige Irrfahrt und harmonische Gewinnerwartung

B313

0	1	2	3	4	5	6	7	8
7€								23€

Aufgabe: Ihre Spielfigur startet auf einem gelben Spielfeld im Inneren. In jedem Zug rückt sie auf ein Nachbarfeld, zufällig und gleichverteilt. Das Spiel endet am Rand $\partial X = \{0, 8\}$ mit dem gezeigten Gewinn.

(a) Welche Gewinnerwartung $u(x)$ hat jedes Feld $x \in X = \{0, \dots, 8\}$?
(b) Variante: Jeder Zug kostet, sagen wir $c(1) = \cdots = c(7) = -1$€.
Das Spiel startet in der Mitte, $x = 4$. Würden Sie dies spielen?

(0) Schätzen Sie zunächst! Wie treffsicher ist Ihre intuitive Erwartung?
(1) Formulieren Sie allgemeine Gleichungen und Lösungsmethoden!

Lösung: (1) Für jedes innere Feld $x \in X^\circ = \{1, \dots, 7\}$ gilt

$$u(x) = \tfrac{1}{2}u(x-1) + \tfrac{1}{2}u(x+1) \quad + c(x).$$

Damit finden wir folgende Lösungen (alle Angaben in €):

7	9	11	13	15	17	19	21	23
7	2	−1	−2	−1	2	7	14	23

Zufällige Irrfahrt und harmonische Gewinnerwartung

B314
Erläuterung

Hier ist (a) ein extrem einfaches Spiel, schon (b) dürfte Sie überraschen: Ungeschult haben wir herzlich wenig Erfahrung mit zufälligen Irrfahrten. Erfahrungsgemäß fällt Menschen rekursives Denken recht schwer, doch gerade dies ist für rationale Entscheidungen wesentlich!

Bevor wir die Lösung diskutieren, schätzen Sie bitte die Erwartung. Ist Ihre Intuition präzise und treffsicher, oder allzu vage und irrig?

Diese quantitativen Schätzfragen sind ein aufschlussreicher Test der vielzitierten Schwarmintelligenz und mahnen eindringlich zur Vorsicht: Betrügerische Geschäftspraktiken beruhen darauf, dass das Gegenüber die Situation schlecht einschätzen kann und Fehlentscheidungen trifft.

Es ist schön und gut, die eigene Intuition zu nutzen und zu entwickeln. Leider hilft es wenig, eine Antwort ohne Begründung anzugeben. Wir wollen begründete, nachvollziehbar, tragfähige Argumente! Auch das ist ein Qualitätsmerkmal rationalen Handelns.

Bilden die oben angegebenen Zahlen eine Lösung? sogar die einzige? Mehrdeutigkeiten müssen wir erkennen und nötigenfalls auch beheben.

Zufällige Irrfahrt und harmonische Gewinnerwartung

B315
Ausprobieren mit Gaël!

0	1	2	3	4	5	6	7	8
7	9	11	13	15	17	19	21	23

Aufgabe: (1a) Wie berechnen Sie die Gewinnerwartung?

Lösung: Für $x \in X = \{0, 1, \dots, 8\}$ suchen wir $u_x = u(x)$. Wir haben:

$$\begin{aligned}
u_0 &= 7 \\
-\tfrac{1}{2}u_0 + u_1 - \tfrac{1}{2}u_2 &= 0 \\
-\tfrac{1}{2}u_1 + u_2 - \tfrac{1}{2}u_3 &= 0 \\
-\tfrac{1}{2}u_2 + u_3 - \tfrac{1}{2}u_4 &= 0 \\
-\tfrac{1}{2}u_3 + u_4 - \tfrac{1}{2}u_5 &= 0 \\
-\tfrac{1}{2}u_4 + u_5 - \tfrac{1}{2}u_6 &= 0 \\
-\tfrac{1}{2}u_5 + u_6 - \tfrac{1}{2}u_7 &= 0 \\
-\tfrac{1}{2}u_6 + u_7 - \tfrac{1}{2}u_8 &= 0 \\
u_8 &= 23
\end{aligned}$$

Die Koeffizienten bilden eine Bandmatrix: tridiagonal, dünn besetzt

☺ Lineare Gleichungssysteme können Sie lösen: Gauß geht immer.
Vereinfachung: Für $d_x = u_x - u_{x-1}$ erhalten wir $d_1 = d_2 = \cdots = d_8 = d$ und $8d = 23 - 7 = 16$, also $d = 2$ und $u_x = 7 + d \cdot x$ für alle $x \in X$.

Zufällige Irrfahrt und harmonische Gewinnerwartung

B316
Ausprobieren mit Gaël!

0	1	2	3	4	5	6	7	8
7	2	−1	−2	−1	2	7	14	23

Aufgabe: (1b) Wie berechnen Sie die Gewinnerwartung bei Zugkosten?

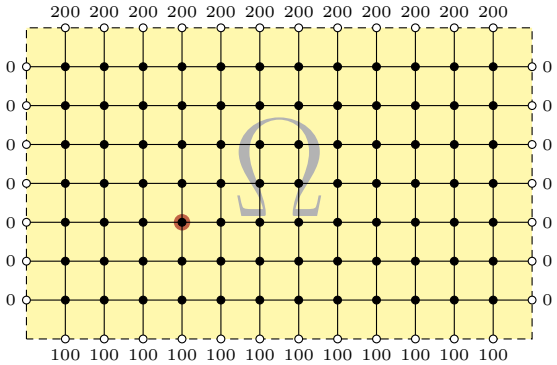
Lösung: Für $x \in X = \{0, 1, \dots, 8\}$ suchen wir $u_x = u(x)$. Wir haben:

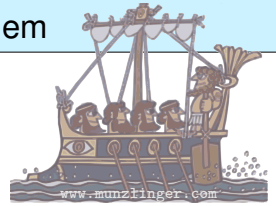
$$\begin{aligned}
u_0 &= 7 \\
-\tfrac{1}{2}u_0 + u_1 - \tfrac{1}{2}u_2 &= c_1 \\
-\tfrac{1}{2}u_1 + u_2 - \tfrac{1}{2}u_3 &= c_2 \\
-\tfrac{1}{2}u_2 + u_3 - \tfrac{1}{2}u_4 &= c_3 \\
-\tfrac{1}{2}u_3 + u_4 - \tfrac{1}{2}u_5 &= c_4 \\
-\tfrac{1}{2}u_4 + u_5 - \tfrac{1}{2}u_6 &= c_5 \\
-\tfrac{1}{2}u_5 + u_6 - \tfrac{1}{2}u_7 &= c_6 \\
-\tfrac{1}{2}u_6 + u_7 - \tfrac{1}{2}u_8 &= c_7 \\
u_8 &= 23
\end{aligned}$$

Die Koeffizienten bilden eine Bandmatrix: tridiagonal, dünn besetzt

☺ Allgemeine Faustregel: Ausrechnen ist mühsam. Prüfen ist leicht!
Wir vermuten anschaulich, dass die Lösung eindeutig ist... Beweis?
Negative Gewinnerwartung bedeutet: Ab hier besser nicht spielen!

Irrfahrten und Potentiale: das Dirichlet–Problem





Auf einem Spielfeld $\Omega \subset \mathbb{Z}^2$ ziehen Sie mit Wkt $1/4$ nach links / rechts / oben / unten.

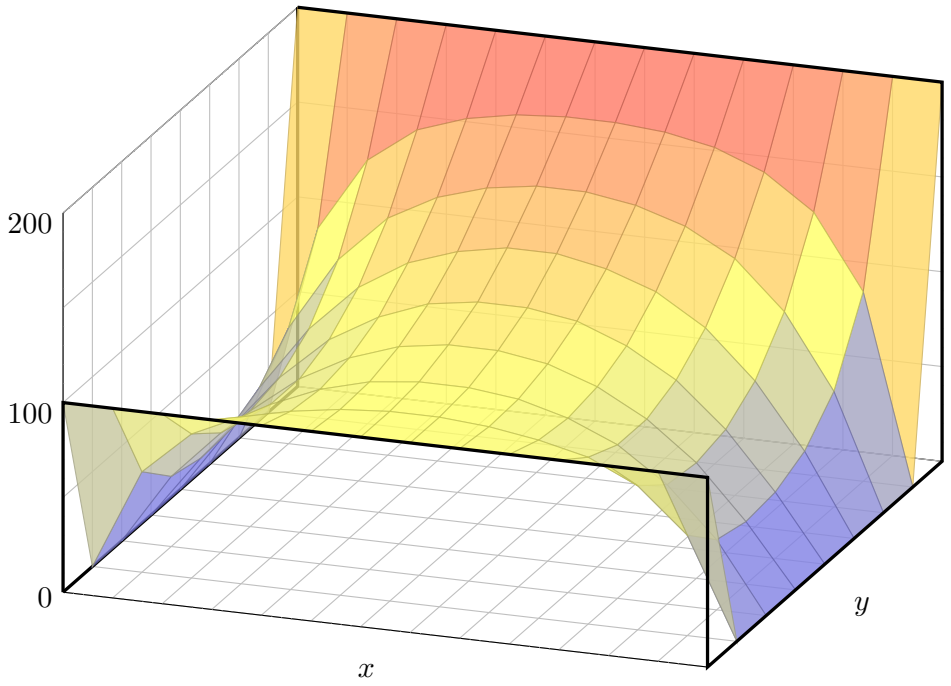
Das Spiel endet am Rand mit dem gezeigten Gewinn.

Wie viel würden Sie setzen beim Start im roten Punkt?

Aufgabe: (1) Wie groß ist die Gewinnerwartung $u(x,y)$ auf jedem Feld? Wo ist sie maximal? Ist die gesuchte Lösung $u : \Omega \to \mathbb{R}$ eindeutig? Wie berechnet man sie? möglichst effizient? näherungsweise?

Kontext und Anwendung ändern sich, die Rechnung bleibt dieselbe!
(2) Hooke: Netz aus Massen und Federn. (3) Kirchhoff: Spannung einer elektrischen Schaltung. (4) Fourier: diskrete Wärmeleitung / Diffusion.

Irrfahrten und Potentiale: das Dirichlet–Problem



Irrfahrten und Potentiale: das Dirichlet–Problem

Lösung: (1) Sei $u(x,y)$ die Gewinnerwartung auf dem Feld $(x,y) \in \Omega$.
In jedem Randpunkt $(x,y) \in \partial\Omega$ ist der Gewinn $u(x,y)$ fest vorgegeben.
In jedem inneren Punkt $(x,y) \in \Omega^\circ$ gilt die **Mittelwerteigenschaft**:

$$u(x,y) = \tfrac{1}{4}u(x{-}1,y) + \tfrac{1}{4}u(x{+}1,y) + \tfrac{1}{4}u(x,y{-}1) + \tfrac{1}{4}u(x,y{+}1)$$

Eine solche diskrete Funktion $u : \mathbb{Z}^2 \supset \Omega \to \mathbb{R}$ nennen wir **harmonisch**.

	200	200	200	200	200	200	200	200	200	200	200	200	
000	100	139	158	167	172	174	174	172	167	157	139	100	000
000	061	100	125	139	147	151	151	147	139	125	100	061	000
000	043	077	102	118	127	132	132	127	118	102	077	043	000
000	035	065	088	103	113	117	117	113	103	088	065	035	000
000	033	061	081	095	104	108	108	104	095	081	061	033	000
000	037	063	081	092	099	102	102	099	092	081	063	037	000
000	053	076	088	094	098	100	100	098	094	088	076	053	000
	100	100	100	100	100	100	100	100	100	100	100	100	

Harmonische Funktionen sind ein wunderschönes Thema in Analysis, Numerik, WTheorie, ...

Irrfahrten und Potentiale: das Dirichlet–Problem

Wir betrachten eine endliche Teilmenge $\Omega \subset \mathbb{Z}^2$. Innere Punkte $z \in \Omega^\circ$ sind solche, deren vier Nachbarn ebenfalls in Ω liegen. Bei einem Randpunkt $z \in \partial\Omega$ liegt mindestens ein Nachbar außerhalb von Ω.

Dirichlet–Problem: In jedem Randpunkt $z \in \partial\Omega$ ist der Wert $u(z)$ festgelegt durch die vorgegebene Randfunktion $v = u|_{\partial\Omega} : \partial\Omega \to \mathbb{R}$. Gesucht sind alle harmonischen Funktion $u : \Omega \to \mathbb{R}$ mit $u|_{\partial\Omega} = v$. Existiert eine Lösung? Ist sie eindeutig? Wie können wir sie berechnen bzw. annähern? Kurzum: Ist das Dirichlet–Problem **gut gestellt**?

Die Aufgabe führt uns zu einem **linearen Gleichungssystem** mit $7 \times 12 = 84$ Unbekannten. Für diese haben wir genau 84 Gleichungen. Das sieht vernünftig aus, bedeutet aber noch nicht, dass es genau eine Lösung gibt. Hierzu müssen wir genauer hinschauen und begründen!

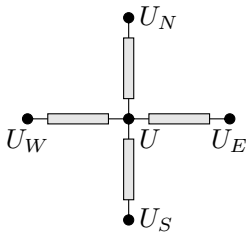
Diese Anwendung ist faszinierend, sie fördert sowohl die physikalische Anschauung als auch die mathematisch-methodische Vorgehensweise. Hier gilt das Minimum-Maximum-Prinzip (Satz B3B). Daraus können wir die Eindeutigkeit und sodann die Existenz einer Lösung ableiten!

Harmonische Funktionen: Gleichgewicht!

☺ Kontext und Anwendung ändern sich, die Rechnung bleibt dieselbe!

(2) Wir betrachten Massenpunkte in $(x, y, u(x, y)) \in \mathbb{R}^3$ in Ruhelage. Jeder ist durch gleich starke Federn mit seinen Nachbarn verbunden. Es gilt: Ruhelage $=$ Kräftegleichgewicht $\approx$ Mittelwerteigenschaft!

Sie können es nachrechnen! Genauer gesagt ist dies die Näherung bei geringer Krümmung.



(3) Wir betrachten die gezeigte Schaltung mit vier gleichen Widerstände. An den Nachbarpunkten liegen die Potentiale U_E, U_N, U_W, U_S an.

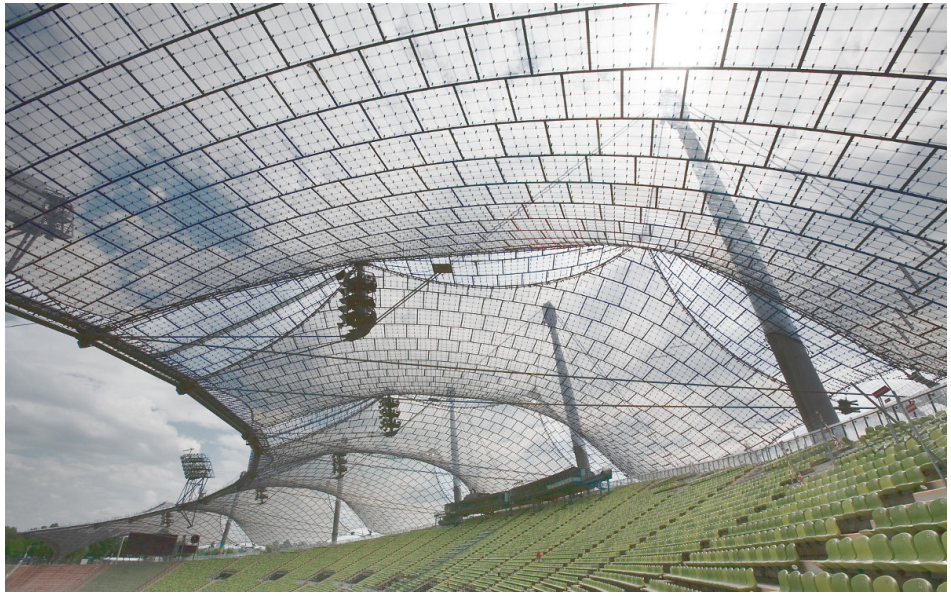
Ohmsches Gesetz und Kirchhoffsche Regel:

$$U = \frac{U_E + U_N + U_W + U_S}{4}$$

Ausführlich: Es gilt das Ohmsche Gesetz $I_E = (U_E - U)/R$. Die Kirchhoffsche Regel besagt hier $I_E + I_N + I_W + I_S = 0$. Einsetzen und Auflösen nach U ergibt die Mittelwerteigenschaft!

☺ Wir können Ω als Schaltung realisieren und am Rand die genannten Spannungen anlegen. Mit einem Voltmeter messen wir das Potential $u(x, y)$ im Inneren und finden obige Lösung. Physikalische Intuition suggeriert Existenz und Eindeutigkeit der Lösung, siehe Satz B3B.

Minimalflächen in der Architektur



Das Zeltdach des Olympiastadions in München ist eine Minimalfläche. Es beruht auf Ideen von Frei Paul Otto (1925–2015) vom Institut für Leichte Flächentragwerke der Universität Stuttgart.

Harmonische Funktionen: Minimum-Maximum-Prinzip

geordnete Körper

Satz B3B: Minimum-Maximum-Prinzip, Eindeutigkeit, Existenz

(1) Jede harmonische Funktion $u : \Omega \to \mathbb{R}$ nimmt ihr Minimum und ihr Maximum am Rand $\partial\Omega$ an: $\min_\Omega u = \min_{\partial\Omega} u$ und $\max_\Omega u = \max_{\partial\Omega} u$.

Für je zwei harmonische Funktionen $u, \tilde{u} : \Omega \to \mathbb{R}$ gilt demnach:
(2) Eindeutigkeit: Aus $u = \tilde{u}$ auf dem Rand $\partial\Omega$ folgt $u = \tilde{u}$ auf ganz Ω.

Aus der Eindeutigkeit gewinnen wir die Existenz dank Satz B2D:
(3) Existenz: Zu jeder vorgegebenen Randfunktion $v : \partial\Omega \to \mathbb{R}$ existiert genau eine harmonische Funktion $u : \Omega \to \mathbb{R}$ mit $u|_{\partial\Omega} = v$.

Beweis: (1) Sei $z \in \Omega$ eine Minimalstelle. Für $z \in \partial\Omega$ sind wir fertig. Für $z \in \Omega^\circ$ gilt die Mittelwerteigenschaft, also sind alle Nachbarn von z ebenfalls Minimalstellen. Es gibt einen Weg von z zu einem Randpunkt $z' \in \partial\Omega$, also ist auch z' eine Minimalstelle. (Ebenso für das Maximum.)

(2) Auch die Differenz $v = \tilde{u} - u$ ist harmonisch. Sie erfüllt $v = 0$ auf $\partial\Omega$. Dank (1) folgt $v = 0$ auf ganz Ω. (3) Unsere Matrix ist quadratisch, und für jede rechte Seite existiert höchstens eine Lösung. QED

Harmonische Funktionen: Eindeutigkeit und Existenz

Das ist ein trickreich-eleganter Beweis! Wir zeigen, dass es für jede rechte Seite *höchstens* eine Lösung gibt. Daraus folgern wir dank Satz B2D, dass für jede rechte Seite (genau) eine Lösung existiert.

Harmonische Funktionen sind wichtig in der Mathematik, der Physik und den Ingenieurwissenschaften. Die Analysis erklärt Ihnen hierzu das kontinuierliche Modell und zugehörige partielle Differentialgleichungen.

Wir betrachten hier ein endliches Modell und erhalten ein tendenziell großes, aber einfaches lineares Gleichungssystem. Wir haben bereits geeignete Werkzeuge! Dies schult, wie gesagt, wunderbar unsere physikalische Anschauung und unsere mathematische Methodik.

Wir sehen zudem, dass unsere Koeffizientenmatrix hier dünn besetzt ist; das ist typisch für Anwendungen, in denen jeder Punkt nur mit wenigen Nachbarn interagiert. Für so strukturierte Probleme bietet die Numerik spezialisierte und besonders effiziente (Näherungs-)Verfahren.

Wenn Ihnen partout nichts Besseres einfällt: Gauß geht immer… und für kleine Matrizen auch ausreichend schnell, siehe B216.

Zusammenfassung: Zielsetzung und Lernstrategie

Das wichtigste Ziel für dieses Kapitel ist, dass Sie sicher mit Matrizen rechnen können, insbesondere den Gauß–Algorithmus beherrschen und in all seinen Aspekten anwenden können, korrekt und routiniert. Sobald es etwas zu rechnen gibt, wird dies nahezu überall benötigt.

Es lohnt sich daher, die Techniken, Beispiele und Anwendungen dieses Kapitels gründlich zu verstehen. Dazu sollten Sie diese Ergebnisse nicht (nur) auswendiglernen, sondern sie vielmehr nachvollziehen, aktiv erarbeiten und beständig in Ihrem Repertoire einüben.

Zum aktiven Erinnern helfen Ihnen insbesondere die Übungen! Ein Instrument lernt man nicht durch den Besuch von Konzerten.

Versuchen Sie nach einem ersten Durchgang, sich den Inhalt dieses Kapitels selbst zu erklären, noch besser: sich gegenseitig zu erklären, genaue zu formulieren, kritisch zu hinterfragen, um so die neue Materie zu durchdringen und wirklich zu verstehen. Was wollen wir erreichen? Wie definieren wir die nötigen Begriffe? Was besagen die Sätze? Wie beweisen wir sie? Wie wenden wir dies auf Beispiele an?

Zusammenfassung: Matrixkalkül und Gauß–Algorithmus

- Grundrechenarten für Matrizen (B1A) und Matrixkalkül: transponierte Matrix, symmetrisch und antisymmetrisch, Zeilen- und Spaltenvektoren als wichtiger Spezialfall, Einheitsmatrix und Einheitsvektoren, Addition von Matrizen, skalare Multiplikation, Multiplikation von Matrizen
- inverse Matrizen, linksinvers und rechtsinvers, Invertierbarkeit (B1B)
- die allgemeine lineare Gruppe $\mathrm{GL}_n \mathbb{K}$ (B1C, B1D)
- 2×2-Matrizen: Determinante, Multiplikativität und Inversion (B1E)
- Zeilenstufenform, allgemein und reduziert, Rang (B2A)
- Lösung eines linearen Gleichungssystems (B2B)
- Gauß–Algorithmus zur Zeilenstufenform (B2C)
- Zeilen-/Spaltenoperationen durch Matrizenmultiplikation (B219)
- Invertierbarkeitskriterien für Matrizen (B2D)
- Algorithmus zur Inversion (B2E)

Rückblick: einige Fragen zum Verständnis

Um Ihr Verständnis zu fördern und selbst Sicherheit zu gewinnen, sollten Sie sich immer wieder Fragen und eigene Aufgaben stellen! Selbst scheinbar banale Fragen helfen ungemein, insbesondere wenn Sie von Ihnen kommen. Ich gebe ein paar Beispiele zur Inspiration:

Lassen sich je zwei beliebige Matrizen addieren? und multiplizieren? Welche Größen passen zusammen? Dürfen dabei die Matrixeinträge / Koeffizienten beliebig sein? sogar auch in verschiedenen Ringen?

🙂 Solche Fragen müssen Sie insbesondere dann dringend klären, sobald Sie diese mathematische Techniken auf einem Computer nutzen oder implementieren möchten. Das zwingt zu Klarheit und Präzision!

Kommutieren je zwei Matrizen? Können sich Matrizen $A \neq 0$ und $B \neq 0$ zu $AB = 0$ multiplizieren? Wie prüft / berechnet man Inverse? Welcher Zusammenhang besteht zwischen Nullteilern und Invertierbarkeit?

🙂 Solche und viele ähnliche Fragen müssen Sie grundlegend klären, wenn Sie selbst effizient rechnen und sicher schließen wollen. Fassen Sie Mut, stellen Sie sich (gegenseitig) Fragen!

Rückblick: einige Fragen zum Verständnis

Wie hängen lineare Gleichungssysteme und Matrixkalkül zusammen? Zeilenumformungen und Matrixmultiplikationen? Welche Operationen im Koeffizientenbereich $\mathbb{K}$ benötigen Sie für den Gauß–Algorithmus?

Wie implementieren Sie dieses Verfahren auf einem Computer? Denken Sie dabei insbesondere an konkrete Beispiele wie $\mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}$. Welche Schwierigkeiten können auftreten? Wie lösen Sie diese?

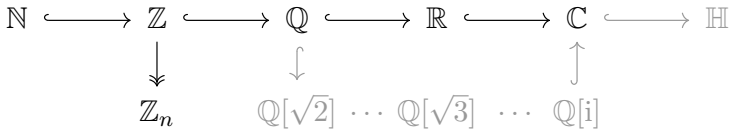
Wie können Sie garantieren, dass das Gauß–Verfahren (gerade auf einem Computer) immer zum Ziel führt? Was ist überhaupt das Ziel? Welche Rechenregeln benötigen Sie zum Nachweis der Korrektheit?

🙂 So entdecken Sie erneut den Begriff des Körpers / Divisionsrings!

Diese einfachen Grundlagenfragen mögen Ihnen allzu naiv vorkommen, doch nur genau so verstehen Sie, wie Mathematik funktioniert, warum die Definitionen und Sätze so sind, wie Sie sie vorgefunden haben. Nur durch aktives Erinnern, Nachvollziehen, Hinterfragen verstehen Sie im Nachgang, wie alles zusammenhängt. Ich kann es für Sie erklären, aber ich kann es nicht für Sie verstehen; das können nur Sie selbst.

Rückblick auf Kapitel A & B und Ausblick

Die Grundlage aller Mathematik ist das Zahlensystem:



Zum korrekten Rechnen benötigen wir die Grundbegriffe zu Ringen.
Unsere ersten Beobachtungen werden in der Algebra fortgeführt, doch die Grundlagen benötigen wir bereits jetzt in der Linearen Algebra.

- Der Ring $\mathbb{Z}$ ist kommutativ und hat keine Nullteiler (A1C).
  Dies nennen wir einen **Integritätsring**, kurz IRing.
- Im Ring $\mathbb{Z}$ haben wir eine euklidische Division mit Rest (A2A).
  Dies nennen wir einen **euklidischen Ring**, kurz ERing.
- Im Ring $\mathbb{Z}$ gilt „unzerlegbar impliziert prim“, und jedes Element lässt sich eindeutig zerlegen in ein Produkt unzerlegbarer Elemente (A2J).
  Dies nennen wir einen **faktoriellen Ring**, kurz FRing.

Rückblick auf Kapitel A & B und Ausblick

In Kapitel A zum Aufbau des Zahlensystems treffen Sie mit $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ gute, alte Bekannte aus der Schule. Neu ist, dass wir uns diese Objekte wesentlich genauer anschauen: Dazu definieren wir präzise Begriffe, formulieren grundlegende Sätze und führen erste schöne Beweise.

Darüber hinaus lernen Sie einige neue nützliche Zahlbereiche kennen, insbesondere den Restklassenring $\mathbb{Z}_n$ und die komplexen Zahlen $\mathbb{C}$.
Es gibt auch „nicht-kommutative Körper“, kurz Schiefkörper genannt, das erste und wichtigste Beispiel sind Hamiltons Quaternionen $\mathbb{H}$.

Mit Kapitel B zur Matrizenrechnung erweitern wir unser mathematisches Repertoire durch zahlreiche schöne Objekte und effiziente Methoden.
Matrizen sind ein Universalwerkzeug und werden uns überall nützen.
Unser treues Arbeitspferd ist der extrem nützliche Gauß–Algorithmus.

Zu diesem frühen Zeitpunkt fehlen uns noch die nötigen Grundlagen: Logik und Beweistechniken, Mengen und Abbildungen, sowie Monoide und Gruppen, dann Ringe und Körper. Dies führen wir nachfolgend aus.
Die Mathematik ist reich und großzügig, darüber dürfen Sie sich freuen.

Rückblick auf Kapitel A & B und Ausblick

Die stärksten Strukturen sind Körper, doch Ringe sind unvermeidbar.
Dies gilt bereits, wenn wir über Polynomringen (A1I) arbeiten wollen:

$$\begin{array}{ccc} \mathbb{K} & \hookrightarrow & \mathbb{K}[X] \\ \text{CRing} & \Longrightarrow & \text{CRing} \\ \text{IRing} & \Longrightarrow & \text{IRing} \\ \text{FRing} & \Longrightarrow & \text{FRing} \\ \text{Körper} & \Longrightarrow & \text{ERing} \end{array}$$

☺ Je mehr wir hineinstecken, desto mehr bekommen wir heraus.
Jeder IRing lässt sich in seinen Bruchkörper einbetten (A1J):

$$\begin{array}{ccc} R & \hookrightarrow & \operatorname{Frac}(R) \\ \text{IRing} & \Longrightarrow & \text{Körper} \end{array}$$

So erhalten wir insbesondere $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z})$ und $\mathbb{Q}(X) = \operatorname{Frac}(\mathbb{Q}[X])$.

☺ Es lohnt sich, Gemeinsamkeiten zu erkennen und zu nutzen.
Konkret oder abstrakt? Am besten, Sie beherrschen beides!

Rückblick auf Kapitel A & B und Ausblick

Die stärksten Strukturen sind Körper, doch Ringe sind unvermeidbar.
Selbst wenn wir möglichst lange nur mit Körpern $\mathbb{K}$ arbeiten wollten, so begegnen uns doch sofort Polynomringe $\mathbb{K}[X]$ und Matrixringe $\mathbb{K}^{n\times n}$.

$$\begin{array}{ccc} \mathbb{K} & \hookrightarrow & \mathbb{K}^{n\times n} \\ \text{Ring} & \Longrightarrow & \text{Ring} \\ \text{CRing} & \Longrightarrow & \text{Ring + Determinante} \\ \text{DRing} & \Longrightarrow & \text{Ring + Gauß–Algorithmus} \\ \text{Körper} & \Longrightarrow & \text{Ring + Det und Gauß!} \end{array}$$

☺ Je mehr wir hineinstecken, desto mehr bekommen wir heraus.
Die invertierbaren Matrizen bilden die allgemeine lineare Gruppe

$$\mathrm{GL}_n(\mathbb{K}) = \left\{ A \in \mathbb{K}^{n\times n} \;\middle|\; \exists B \in \mathbb{K}^{n\times n} : AB = BA = 1_{n\times n} \right\}.$$

Diese beschreibt insbesondere die Zeilenumformungen à la Gauß.
Gruppen erweisen sich für die Mathematik als fundamentaler Begriff.

Kapitel C

Mathematische Logik und Beweistechniken

Mathematics, rightly viewed, possesses not only truth,
but supreme beauty […] The true spirit of delight, […]
is to be found in mathematics as surely as poetry.

Bertrand Russel (1872–1970), Nobelpreis 1950

Inhalt dieses Kapitels C

Zielsetzung

In der Mathematik wollen wir **wahre Aussagen** effizient auffinden, präzise formulieren und streng beweisen. Ebenso müssen wir **falsche Aussagen** als unwahr erkennen und ebenso begründet zurückweisen. Algorithmisch führt das direkt zu einem der Millenium-Probleme C1K!

Solide und bescheiden benötigen wir mathematisches Handwerkszeug. Grundlegend und allgegenwärtig sind die Regeln der **Aussagenlogik**; sie strukturieren unser Vorgehen und vereinfachen die Kommunikation. Dazu präsentiere ich Ihnen in diesem Kapitel die nötigen Grundlagen.

Unser akribisches logisches Vorgehen hat viele gute Gründe:
(1) Sie sollen verstehen, was ich tue und auch warum ich es tue.
(2) Sie sollen selbstständig nachprüfen, dass ich es richtig mache.
(3) Sie sollen selbst wahre Aussagen finden und beweisen lernen.
(4) Sie sollen selbst nachprüfen können, dass Sie es richtig machen.
(5) Wir wollen uns darüber verständigen, was wahr und was falsch ist.
(6) Sie sollen Ihre Erkenntnisse richtig anwenden und weitergeben.

Kurzum: Die Logik benötigen und nutzen Sie überall.

Zielsetzung

Tradition ist nicht die Bewahrung der Asche,
sondern die Weitergabe des Feuers.

nach Jean Jaurès (1859–1914)

Als Anfänger macht man zunächst viele Fehler, das ist völlig normal. Aber dabei soll es nicht bleiben. Wachsen Sie über sich hinaus! Sie sollen in Ihrem Studium möglichst rasch und gründlich lernen, diese Fehler zu *erkennen* und dann auch zu *vermeiden*.

Auch ich mache gelegentlich Fehler, das ist leider unvermeidlich, aber Sie können die Fehler *erkennen* und sollen sie *korrigieren*. Das ist ein Grundprinzip der Mathematik: Es geht nicht um Autorität, Überredung oder Einschüchterung, sondern um schlüssige Argumente.

Unser gemeinsames Ziel ist die nachvollziehbare Verständigung über und die nachhaltige Erarbeitung von mathematischen Sachverhalten. Lernen wir also die mathematische Sprache! Lernen wir Logik!

Habe Mut, dich deines eigenen Verstandes zu bedienen!

Immanuel Kant (1724–1804)

Zweck und Nutzen der Logik: Korrektheit

Sie sollen mit Aussagen und ihren Wahrheitswerten sicher rechnen: **korrekt und kritisch, kreativ und effizient.** Das ist nicht leicht! Dazu gehört insbesondere auch das Beweisen: Ein Beweis ist nichts anderes als die Berechnung des Wahrheitswerts der Behauptung.

Sie sollen mathematische Beweise und Beweisversuche prüfen, und dabei gültige von ungültigen Argumenten unterscheiden lernen. Dazu müssen Sie wie oben genannt *korrekt und kritisch* arbeiten. Das ist solides Handwerk, Sie lernen es am besten durch Übung.

Auch kleine Fehler können entscheidend sein, scheinbar zwingende Schlüsse können zu absurden Ergebnissen führen! Das hat auch sportlich-spielerische Aspekte: Immer wieder wurden und werden Paradoxien formuliert und als logische Herausforderung behandelt.

Seit man begonnen hat, die einfachsten Behauptungen zu beweisen, erwiesen sich viele von ihnen als falsch.
Bertrand Russell (1872–1970)

Zweck und Nutzen der Logik: Erkenntnis

Mit zunehmender Übung und mathematischer Erfahrung sollen Sie auch selbst Beweise finden, erarbeiten und ausformulieren lernen. Dazu müssen Sie wie oben genannt *kreativ und effizient* arbeiten. Hierbei hilft es, sich an bewährten Vorbildern zu orientieren.

Oft wird der Mathematik vorgeworfen, dass sie nur „richtig“ oder „falsch“ kenne, und dies wird als übertrieben streng, ja grausam empfunden. Sehen wir das Positive: Die Mathematik kennt richtig und falsch! Dies können Sie nutzen und damit Klarheit schaffen.

Müssen wir alles so genau nehmen? Präzision ist Fluch und Segen: Als Anwender mathematischer Ergebnisse schätzen Sie die Garantie. Als Hersteller mathematischer Ergebnisse spüren Sie die Pflicht. Ihre Vorbereitung von heute ist Ihr Nutzen von morgen!

Die mit Tränen säen, werden mit Freuden ernten.
Die Bibel, Psalm 126:5

Zweck und Nutzen der Logik: Sprache

Sprache ist ungeheuer wichtig! Sie soll möglichst praktisch und präzise sein, doch nicht unnötig pedantisch und prätentiös. Das fordert Disziplin.

Jura: Verträge, Gesetze, Regeln müssen klar und eindeutig sein, soweit möglich vollständig und möglichst nicht mehrdeutig.

Physik: qualitative und quantitative Vorhersagen zu Experimenten. Nur diese sind prüfbar, wichtiger noch: Sie müssen widerlegbar sein.

Informatik: Spezifikationen für Software, Pflichtenheft bei Arbeitsteilung. Unklare Vereinbarungen führen zu unnötigem Kummer und Leid.

Mathematik: Logik und Mengenlehre dienen als gemeinsame Sprache für die gesamte Mathematik, in diversen Dialekten je nach Teilgebiet. Exploration: erste Formulierung von Ideen, Hypothesen, Versuchen. Konsolidierung: Präzisierung, Beweis, Archivierung, Weitergabe.

Die Grenzen meiner Sprache bedeuten die Grenzen meiner Welt.
Ludwig Wittgenstein (1889-1951), *Tractatus logico-philosophicus*

Zweck und Nutzen der Logik: Kalkül

Eines der Ziele und Werkzeuge der Mathematik ist gute Notation.

By relieving the brain of all unnecessary work, a good notation sets it free to concentrate on more advanced problems.
Alfred North Whitehead (1861–1947), *An Introduction to Mathematics* (1911)

Idealerweise lassen sich dadurch komplexe Aufgaben routiniert lösen. Es kann sogar dazu verleiten, sich blind auf den Kalkül zu verlassen:

Die Mathematik ist eine gar herrliche Wissenschaft, aber die Mathematiker taugen oft den Henker nicht. Es ist fast mit der Mathematik, wie mit der Theologie. […] so verlangt sehr oft der so genannte Mathematiker für einen tiefen Denker gehalten zu werden, ob es gleich darunter die größten Plunderköpfe gibt, die man nur finden kann, untauglich zu irgend einem Geschäft, das Nachdenken erfordert, wenn es nicht unmittelbar durch jene leichte Verbindung von Zeichen geschehen kann, die mehr das Werk der Routine, als des Denkens sind.
Georg Christoph Lichtenberg (1742–1799), *Sudelbuch K.185*

Klarheit der Sprache und des Denkens

C101

Wir wollen **wahre und falsche Aussagen** als solche erkennen.

Wissenschaft sucht Erkenntnis, nachvollziehbar und begründet.
Oberstes Ziel wissenschaftlicher Kommunikation ist daher Klarheit!
Idealerweise ist sie redlich und transparent, eindeutig und klar, objektiv / intersubjektiv, überprüfbar / widerlegbar. Grundlage dafür ist die Logik!

Dramatische Beispiele: Welche der folgenden Aussagen sind wahr?

🙂 Sorgfalt bei Primzahlen:
A: „Wenn $1, 2, 3$ prim sind, dann heiße ich Rumpelstilzchen.“

🙂 Mathematische Urlaubsgrüße:
B: „Immer wenn es geregnet hat, haben Aliens unser Zelt geklaut.“

🙂 Doch keine Verschwörung:
C: „Ist die Erde eine Scheibe, dann war die Mondlandung inszeniert.“

Full disclosure: Ich heiße Michael Eisermann, kenne bislang keine Belege für Aliens, und die Erde ist eine Kugel (mit Unebenheiten).
Was soll ich von den obigen Aussagen halten: wahr oder falsch?

Klarheit der Sprache und des Denkens

C102
Erläuterung

Ich halte alle drei Aussagen für wahr und kann dies gut begründen.
Auch Sie können diese schockierenden Behauptungen überprüfen:

A: Wir haben eine präzise Definition: 1 ist keine Primzahl!
Alles weitere ist dann irrelevant, die Aussage A ist wahr.

B: Wir dürfen weiterhin davon ausgehen, dass keine Aliens die Erde besuchen. Es hat während des Urlaubs einfach nicht geregnet!

C: Die Erde ist keine Scheibe, sondern eine Kugel (mit Unebenheiten).
Alles weitere ist dann irrelevant, die Aussage C ist wahr.

In diesen anschaulichen Beispielen ist Ihnen die Logik vermutlich klar.
Das ändert sich, sobald Sie über neue, unbekannte Dinge nachdenken.

Wir werden bald komplexe, mathematische Sachverhalte bearbeiten, zu denen Sie (noch) keine Anschauung haben. Sie können dann nicht auf vage Intuition bauen, Sie müssen die Logik sicher beherrschen!

🙂 Die Logik ist zum Glück nicht schwer, sondern solides Handwerk.
Dazu gehen wir die grundlegenden Regeln der Logik schrittweise durch.

Klarheit der Sprache und des Denkens

C103

Vielleicht finden Sie die obigen Beispiele allzu konstruiert und denken „In der Natur kommen logische Probleme nicht vor". Oh, weit gefehlt!
Beispiele von unklaren oder unlogischen Formulierung gibt es zuhauf.

Beispiel: Ein Fall für das Gesetz…
von Augustus De Morgan (1806–1871).
Was genau ist hier verboten und strafbar?

„Euer Ehren, ich habe nur gepflückt, aber nicht auch noch ausgegraben, denn beides zugleich ist verboten.“

— „Angeklagter, beides ist verboten! Sie machen sich also bereits strafbar, wenn Sie pflücken *oder* ausgraben.“

— „Euer Ehren, hier muss ein bedauerlicher Irrtum vorliegen, auf dem Schild steht *und*. Ich habe nicht gepflückt *und* ausgegraben.“

Klarheit der Sprache und des Denkens

C104
Erläuterung

Das Verbot habe ich tatsächlich beim Spaziergang im Wald *gefunden*.
Die Feld-Wald-und-Wiesen-Seifenoper dazu ist natürlich frei *erfunden*.

Kommunikation kann auf viele Weisen scheitern. Zwei typische Quellen logischer Fehlschlüsse sind Inkompetenz und Bösartigkeit, sowohl auf Seite des Senders als auch auf Seite des Empfängers.

Sophistik ist nach Aristoteles die Philosophie des Scheins,
das heißt die Kunst, durch falsche Dialektik
das Wahre mit dem Falschen zu verwirren
und durch Disputieren, Widerspruch und Schönschwatzen
Beifall und Reichtum zu erwerben; sophistisch heißt demnach
trügerisch, Sophisterei ein verfängliches Räsonnement.
Kirchner, Michaëlis: *Wörterbuch der Philosophischen Grundbegriffe* (1907)

Wir bauen auf Logik, wir vermeiden Polemik. Daher müssen wir zuerst erklären, was wir unter Logik verstehen und wie sie zu benutzen ist!
Idealerweise löst das Verständnisprobleme schon bevor sie entstehen und macht Sie wehrhaft gegen (Selbst)Betrug und Schönschwatzen.

Klarheit der Sprache und des Denkens

Das vorige Beispiel scheint Ihnen allzu fiktiv? Wie ist es mit folgendem?

The fee for new UK and EU students starting in 2020 is £9,250. [...]
The fee for new overseas (non-UK or EU) undergraduates is £21,570.
London School of Economics am 05.01.2020.

Benötigt man für die erste Klausel die doppelte Staatsangehörigkeit? Gilt die zweite Klausel für deutsche Studierende? Sind Sie „*overseas*“? Wie programmieren Sie die Buchhaltung für die Gebührenerhebung?

Nach Rückfrage und Klärung ist vermutlich folgendes gemeint:

```
1 if isUKCitizen or isEUCitizen:
2     print("Your fee is 9250 pounds stirling.")
3 if (not isUKCitizen) and (not isEUCitizen):
4     print("Your fee is 21570 pounds stirling.")
```

☺ Präzise Formulierung und korrekte Logik sind unabdingbar, wenn Sie genaue Regeln formulieren oder programmieren wollen. Genau diese Klarheit und Präzision schulden wir uns auch gegenseitig.

Klarheit der Sprache und des Denkens

Hätten Sie sich dieses Jahr neben Stuttgart auch an der London School of Economics (LSE) beworben, dann stünden Sie vor der dringenden und kniffligen Frage: Wie viel Studiengebühren müssen Sie zahlen? Wie sollten „*and*“, „*or*“, „*non*“ hier verwendet und verstanden werden?

Zugegeben, im Alltag sind viele Aussagen nicht eindeutig wahr oder falsch, meist gibt es vage Graubereiche und mehr oder weniger große Spielräume. Das ist unvermeidlich selbst in einfachsten Beispielen.

Es gibt aber oft genug auch Fragen, die mit einem klaren „ja“ oder „nein“ beantwortet werden können, gar müssen, so wie hier: Zahlen Sie die niedrigen Gebühren? Oder zahlen Sie die hohen Gebühren? Natürlich könnten Sie nachfragen, aber auch dann sollte eine klare Regel zugrundeliegen und keine Willkür.

Für viele Anwendungen ist diese Klarheit wünschenswert, gar essentiell: Gesellschaft: Hat Kandidat X die Wahl gewonnen? Sport: Gilt das Tor? Wirtschaft und Verträge: Wurde fristgerecht geliefert / überwiesen? Naturwissenschaft und Technik: Hat das Instrument angeschlagen?

Klarheit der Sprache und des Denkens

Wie würden Sie die obigen Klauseln als Programm implementieren? Logische Präzision und sprachliche Klarheit sind dazu unerlässlich, etwa für Datenbanken, Expertensysteme, Künstliche Intelligenzen, etc.

☺ Die Formulierung als Computerprogramm zwingt uns zur Präzision. Das ist auch in vielen anderen Situationen ein strenger, aber guter Test. Manche sagen: „Du hast es erst dann verstanden, wenn du es einem Computer beibringen kannst.“ Das ist etwas extrem, aber doch nützlich.

☺ Leichter zu schreiben und zu lesen ist die äquivalente Formulierung, in der wir Zeile 3 `if ...:` durch `else:` ersetzen. Eleganter und klarer!

Beide Formulierungen sind äquivalent dank der Regel von De Morgan: Die Aussage „nicht(p oder q)“ ist äquivalent zu „(nicht p) und (nicht q)“. Die Aussage „nicht(p und q)“ ist äquivalent zu „(nicht p) oder (nicht q)“.

Bitte beachten Sie die Klammern: Diese sind hier ganz wesentlich! Beim Sprechen fallen sie oft weg, das stiftet dann große Verwirrung. Wenn wir Klammern weglassen, müssen wir erklären, was wir meinen.

Klarheit der Sprache und des Denkens

☺ Mit dem Brexit fällt die Ausnahme für Studierende aus der EU weg. Das vereinfacht die Logik, aber verdoppelt ihre Studiengebühren:

The fee for new UK students starting in 2021 is £9,250. [...]
The fee for new overseas (non-UK) undergraduates is £22,430.
London School of Economics am 03.10.2020.

Logische Aussagen begegnen uns überall – auch viel komplexere!

- Zulassung, Prüfungsordnung,
- Verträge, Gesetze, Spielregeln,
- Gebrauchsanweisung, Spezifikation,
- Formulierung / Hypothesen zu Naturgesetzen,
- mathematisch-statistische Analyse von Daten.

Nahezu immer und überall benötigen wir verlässliche präzise Aussagen. Die Logik ist daher keine theoretische Haarspalterei, sondern praktische Notwendigkeit: Davon hängen handfeste Entscheidungen ab!

Aussagen und Wahrheitswerte

Wir wollen wahre und falsche **Aussagen** erkennen und nachweisen. Als Handwerkszeug entwickeln wir hierzu sorgsam die **Aussagenlogik** und ihre **Schlussregeln**, sodass wir mit Aussagen sicher rechnen können.

Die Mathematik nutzt einen strengen und präzisen Wahrheitsbegriff – für manche Anwendungen zu streng, dafür wunderbar einfach und klar.

If people do not believe that mathematics is simple,
it is only because they do not realize how complicated life is.
John von Neumann (1903–1957)

Definition C1A: Aussage und Wahrheitswert

Eine **Aussage** A ist ein sprachlicher Ausdruck, dem ein eindeutiger Wahrheitswert $\langle A \rangle$ zugeordnet ist: entweder $0 =$ falsch oder $1 =$ wahr.

Wir lassen vorerst offen, was genau ein „sprachlicher Ausdruck“ A ist. Wichtig ist nur, ihn zu einem Wahrheitswert $\langle A \rangle$ auswerten zu können.

Zunächst nutzen wir die Umgangssprache (C1B). Später präzisieren wir Sprache (Syntax) und Bedeutung (Semantik) und Wahrheitswerte (C1D).

Aussagen und Wahrheitswerte

Im Alltag sind viele Aussagen nicht eindeutig wahr oder falsch, oft gibt es Graubereiche und Ermessensfragen. Das ist unvermeidlich selbst in einfachsten Beispielen wie „die Nudeln sind al dente“ oder „es regnet“, erst recht bei Urteilen wie „diese Impfung ist sicher und wirksam“.

Die Mathematik bietet dazu sehr erfolgreiche und ausgefeilte Methoden, etwa Wahrscheinlichkeit als Grad der Un/Gewissheit, entweder subjektiv als Mangel an Information oder objektiv als physikalisches Grundprinzip.

Zum Aufbau der Mathematik jedoch beginnen wir mit den Grundlagen, und diese beruhen auf der klassischen, zweiwertigen **Aussagenlogik**. Hier arbeiten wir nur mit genau zwei **Wahrheitswerten**:

$0 =$ falsch, alternative Schreibweise: $\bot =$ falsum $=$ false $=$ faux
$1 =$ wahr, alternative Schreibweise: $\top =$ verum $=$ true $=$ vrai

Für viele Anwendungen ist diese Vereinfachung sinnvoll, gar essentiell: Gesellschaft: Hat Kandidat X die Wahl gewonnen? Sport: Gilt das Tor? Wirtschaft und Verträge: Wurde fristgerecht geliefert / überwiesen?

Aussagen und Wahrheitswerte

Beispiel C1B: Aussage oder nicht? wahr oder falsch?

Wir untersuchen die folgenden umgangssprachlichen Ausdrücke:

$A =$ (Alle Primzahlen sind ungerade.)
$\neg A =$ (Es gibt eine gerade Primzahl.)
$B =$ (Dieses Beispiel C1B ist nicht leicht aber hilfreich.)
$\neg B =$ (Dieses Beispiel C1B ist leicht oder nicht hilfreich.)
$C =$ (Diese Aussage C ist falsch.)
$D =$ (Diese Aussage D ist wahr.)
$E =$ (Ein Quadrat mit Seitenlänge ℓ hat den Flächeninhalt 4ℓ.)
$F =$ (Ist jedes Quadrat ein Rechteck oder umgekehrt?)
$G =$ (Jede gerade Zahl $n \geq 4$ ist Summe zweier Primzahlen.)
$H =$ (Nächste Saison gewinnt der VfB Stuttgart die Meisterschaft.)

Welche dieser Ausdrücke sind Aussagen? wahr? falsch?

Aussagen und Wahrheitswerte

Aufgabe: Welche dieser Ausdrücke sind Aussagen? wahr? falsch?

Lösung: Die Frage ist weit und offen, ich gebe hier nur eine Skizze.

Die Aussage A ist falsch: Nicht alle Primzahlen sind ungerade.
Ihre Negation $\neg A$ ist wahr, denn 2 ist eine gerade Primzahl.

Die Ausdrücke B und $\neg B$ sind subjektive **Meinungsäußerungen** ohne objektiven Wahrheitswert, es gibt dazu verschiedene Meinungen.

⚠ Die umgangssprachliche Konjunktion „aber“ bedeutet logisch „und“. Zusätzlich drückt sie eine Bewertung aus, etwa einen Gegensatz, eine Einschränkung, einen Einwand, eine Entgegnung, eine Überraschung. Für die logische Verknüpfung ist diese Bewertung überflüssig.

⚠ Beachten Sie die korrekt ausformulierte Verneinung von B zu $\neg B$: Aus „und“ wird „oder“ gemäß der Regel von De Morgan! Ausführlich:
Die Aussage „nicht(p und q)“ ist äquivalent zu „(nicht p) oder (nicht q)“.
Die Aussage „nicht(p oder q)“ ist äquivalent zu „(nicht p) und (nicht q)“.

Aussagen und Wahrheitswerte

C113
Erläuterung

Der selbstbezügliche Ausdruck C ist das berüchtigte **Lügner–Paradox**:
Ist C wahr, dann ist C falsch. Ist C falsch, dann ist C wahr.
Der Ausdruck C ist somit in sich widersprüchlich:
Er kann weder wahr noch falsch sein.

⚠ Wir lassen den Ausdruck C nicht als Aussage zu,
da ihm kein Wahrheitswert zugeordnet werden kann.

Ausdruck D kann sowohl wahr als auch falsch sein, das ist vollkommen beliebig. Einen eindeutigen Wahrheitswert hat also auch D nicht.

⚠ Vorsichtshalber lassen wir auch D nicht als Aussage zu.
da ihm kein eindeutiger Wahrheitswert zugeordnet ist.

Sie sehen bereits an diesen einfachen umgangssprachlichen Beispielen, dass die Frage nach dem Wahrheitswert erstaunlich vertrackt sein kann. Das sollte Sie vor naiver Sorglosigkeit warnen und zu mathematischer Sorgfalt motivieren: Selbst für die einfachsten Grundbegriffe müssen wir umsichtig vorgehen, wenn wir Widersprüche vermeiden wollen.

Aussagen und Wahrheitswerte

C114
Erläuterung

Ausdruck E ist missverständlich formuliert! Soll E heißen „Mindestens ein Quadrat…“? Dann ist ein Quadrat mit $\ell = 4$ ein Beleg, also E wahr. Oder soll E heißen „Ein beliebiges Quadrat…“, also eigentlich „Jedes Quadrat…“? Dann ist ein Quadrat mit $\ell = 3$ ein Gegenbeispiel, somit E falsch. Wir müssen präzise und unmissverständlich formulieren!

⚠ Streng genommen müssen wir auch den Ausdruck E als Aussage zurückweisen, da ihm kein eindeutiger Wahrheitswert zugeordnet ist.

Ausdruck F ist keine Aussage sondern eine Frage. Die logisch korrekte Antwort lautet: „Ja, jedes Quadrat ist ein Rechteck oder umgekehrt.“

⚠ Eine Alternativfrage wie diese ist meist eine implizite Aufforderung an den Gefragten, die zutreffende/n Alternative/n explizit zu nennen. Eine freundlichere, hilfreichere Antwort wäre daher: „Ja, jedes Quadrat ist ein Rechteck, aber umgekehrt ist nicht jedes Rechteck ein Quadrat.“

⚠ Auch Aufforderungen („Rechnen wir!“) und Annahmen („Sei $x = 2$.“) sind logisch gesehen keine Aussagen: Sie haben keinen Wahrheitswert.

Aussagen und Wahrheitswerte

C115
Erläuterung

Ausdruck G ist eine **Vermutung von Christian Goldbach** (1690-1764). Ihr Wahrheitswert ist bislang unbekannt (Stand 2020): Trotz großer Anstrengungen (und zwischenzeitlich einem Preisgeld von 1 Million Dollar) wurde weder ein Beweis noch ein Gegenbeispiel gefunden. Die Aussage gilt für $4 \leq n \leq 4 \cdot 10^{18}$ dank maschineller Prüfung.

⚠ Ist G eine Aussage oder nicht? Die **klassische Sichtweise** ist, dass jeder wohlgeformte Ausdruck A einen Wahrheitswert $\langle A \rangle$ hat, egal ob wir ihn kennen oder nicht. Die **konstruktive Sichtweise** ist strenger: Sie verlangt einen Beweis für A oder einen Beweis für die Negation $\neg A$, der Wahrheitswert muss also explizit durch einen Beweis belegt sein.

Diese stärkere Anforderung eines Nachweises ist natürlich und nützlich. Sie bereitet wesentlich mehr Mühe und ist manchmal sogar unmöglich: Es gibt Aussagen, analog zu c, die nachweislich unentscheidbar sind. Dies ist der berühmte **Unvollständigkeitssatz** von Kurt Gödel (1931).

Fun fact: Wäre G unentscheidbar, also weder G noch $\neg G$ beweisbar, dann wäre G wahr, denn jedes Gegenbeispiel lässt sich entscheiden.

Aussagen und Wahrheitswerte

C116
Erläuterung

Auch das Beispiel H ist noch nicht entscheidbar: Wer Meister wird, stellt sich erst gegen Ende der nächsten Saison heraus und ist jetzt, zu Beginn dieser Saison, keineswegs sicher. Jeder Fußballfan kann sich zwar eine gefühlte Wahrscheinlichkeit einbilden und vielleicht sogar begründen, aber das ersetzt keine Auswertung zu wahr oder falsch.

Ebenso ist $K = (\text{Am Ende der nächsten Saison jubeln die VfB-Fans.})$ noch nicht entscheidbar. Hingegen ist $H \Rightarrow K$ eine wahre Aussage. Ähnliche Phänomene begegnen uns tatsächlich auch in der Mathematik.

⚠ Vorsichtigerweise sollten wir G, H, K als Vermutungen betrachten, wie „zukünftige Aussagen“, deren Wahrheitswert noch unbekannt ist. Für die weitere Arbeit ist es bequem, sie wie Aussagen zu behandeln, auch wenn die klassische Sichtweise hier an ihre Grenzen stößt.

🙂 Im Folgenden vermeiden wir Paradoxien und Unentscheidbarkeit. Die Problematik der Beweisbarkeit bzw. Unentscheidbarkeit ist ganz real und konkret, doch wir wollen und können ihr vorerst sorgsam ausweichen und dabei viel gute Mathematik entwickeln.

Verknüpfung von Aussagen

Definition C1c: logische Verknüpfungen

Sind A und B Aussagen, so auch die folgenden Ausdrücke:

Aussage	Bedeutung	Name
$\neg A$	nicht A	Negation
$(A \wedge B)$	A und B	Konjunktion
$(A \vee B)$	A oder B	(inklusive) Disjunktion
$(A \dot{\vee} B)$	entweder A oder B	exklusive Disjunktion
$(A \Leftrightarrow B)$	A gilt genau dann, wenn B gilt	Äquivalenz (Bijunktion)
$(A \Rightarrow B)$	wenn A gilt, dann gilt B	Implikation (Subjunktion)

Die zugehörigen Wahrheitswerte definieren wir wie folgt:

$\langle A \rangle$	$\langle B \rangle$	$\langle \neg A \rangle$	$\langle A \wedge B \rangle$	$\langle A \vee B \rangle$	$\langle A \dot{\vee} B \rangle$	$\langle A \Leftrightarrow B \rangle$	$\langle A \Rightarrow B \rangle$
1	1	0	1	1	0	1	1
1	0	0	0	1	1	0	0
0	1	1	0	1	1	0	1
0	0	1	0	0	0	1	1

Verknüpfung von Aussagen

☺ Die Wahrheitstabelle *definiert* diese logischen Verknüpfungen, klar und unmissverständlich, besser als jede Prosa. Hier die Prosa:

Die Negation $\neg p$ kehrt den Wahrheitswert um, von 0 zu 1 und von 1 zu 0: Die Aussage $\neg p$ ist falsch, wenn p wahr ist, und wahr, wenn p falsch ist. Alternative Schreibweisen für die Negation $\neg p$ sind $\sim p$ oder $\overline{p}$, oder `!p` wie in C/C++ oder `not p` wie in Python.

Die Konjunktion $p \wedge q$ ist das logische Und: Die Aussage $p \wedge q$ ist wahr, wenn p und q wahr sind. Die Aussage $p \wedge q$ ist falsch, wenn p oder q falsch ist. (Letzteres ist die Regel von De Morgan, siehe C135)

Die Disjunktion $p \vee q$ ist das inklusive Oder: Die Aussage $p \vee q$ ist wahr, wenn p oder q wahr ist. Die Aussage $p \vee q$ ist falsch, wenn p und q falsch sind. (Letzteres ist die Regel von De Morgan, siehe C135)

Das exklusive Oder schreiben wir $p \dot{\vee} q$ und sagen ausdrücklich „entweder p oder q“. Die Aussage $p \dot{\vee} q$ ist wahr, wenn entweder p oder q wahr ist, also genau eine, nicht beide. Die Aussage $p \dot{\vee} q$ ist falsch, wenn p und q falsch sind, aber auch, wenn p und q beide zugleich wahr sind.

Beispiel: Wenn Spinat, dann Nachtisch?

(1) Die strengen Eltern mahnen ihre Kinder: „Wenn ihr euren Spinat nicht aufesst, dann bekommt ihr heute keinen Nachtisch.“ Die Kinder essen tapfer ihren Spinat, bekommen aber dennoch keinen Nachtisch.

Können sie ihre Eltern auf Herausgabe des Nachtischs verklagen?
Nein! Für diesen Fall haben die Eltern keine Zusage gemacht.

(2) Die Dozentin mahnt: „Wenn Sie nicht fleißig üben, kommt kein Aha.“ Die Studierenden üben fleißig, aber es kommt (vorerst noch) kein Aha.

Hat die Dozentin nun gelogen oder doch die Wahrheit gesagt?
Über diesen Fall hat die Dozentin keine Aussage gemacht.

(3) Für $n \in \mathbb{N}_{\geq 1}$ sei $A(n)$ die Aussage: „Wenn n Quadrat einer Primzahl ist, dann hat n als Teiler genau drei verschiedene natürliche Zahlen.“

Diese Aussage $A(n)$ ist wahr für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$, unabhängig davon, ob n Quadrat einer Primzahl ist oder nicht.

Um die Aussage $A(n)$ zu beweisen, müssen Sie lediglich zeigen:
Wenn die Voraussetzung wahr ist, dann ist die Folgerung wahr.

Implikationen

☺ Sie sehen an diesen einfachen Beispiele bereits sehr deutlich, wie wichtig unsere klare und unmissverständliche Definition C1c ist.

Wir nennen „$p \Rightarrow q$“ eine **Implikation** oder **Schlussfolgerung**, p heißt die **Voraussetzung** oder **Prämisse** und q die **Folgerung**.

Gilt $p \Rightarrow q$, so ist p eine **hinreichende Bedingung** für q:
Wann immer p wahr ist, dann ist auch q wahr.

Gilt $p \Rightarrow q$, so ist q ist **notwendige Bedingung** für p:
Wenn q nicht gilt, dann kann auch p nicht gelten.

Die Implikation $p \Rightarrow q$, wie oben definiert, mag überraschen:
Wenn die Prämisse nicht gilt, so ist die Implikation dennoch wahr!
Von allen logischen Operationen ist diese anfangs die Schwierigste, am wenigsten intuitiv, und läuft dem Alltagsgebrauch entgegen.

Bitte folgen Sie streng der Definition und machen Sie sich mit möglichst vielfältigen Beispielen vertraut, alltäglichen und mathematischen.
Auch die Logik verlangt und belohnt gewissenhafte Übung.

Verknüpfung von Wahrheitswerten

Wie zuvor nutzen wir die beiden Wahrheitswerte 0 (falsch) und 1 (wahr).
Die Negation ist die Abbildung $\neg : \{0,1\} \to \{0,1\}$ mit $\neg 0 = 1$ und $\neg 1 = 0$.
Wir definieren die Verknüpfungen $\wedge, \vee, \dot\vee, \Rightarrow, \Leftrightarrow : \{0,1\} \times \{0,1\} \to \{0,1\}$:

a	b	$a \wedge b$	$a \vee b$	$a \mathbin{\dot\vee} b$	$a \Rightarrow b$	$a \Leftrightarrow b$
1	1	1	1	0	1	1
1	0	0	1	1	0	0
0	1	0	1	1	1	0
0	0	0	0	0	1	1

Für alle $a, b \in \{0,1\}$ gilt $(a \wedge b) = \min\{a, b\}$ und $(a \vee b) = \max\{a, b\}$.
Damit können wir alle anderen ausdrücken: $(a \Rightarrow b) = (\neg a \vee b)$
sowie $(a \Leftrightarrow b) = ((a \Rightarrow b) \wedge (b \Rightarrow a))$ und $(a \mathbin{\dot\vee} b) = \neg(a \Leftrightarrow b)$.

a	b	$\neg a$	$\neg a \vee b$	$a \Rightarrow b$	$b \Rightarrow a$	$(a \Rightarrow b) \wedge (b \Rightarrow a)$
1	1	0	1	1	1	1
1	0	0	0	0	1	0
0	1	1	1	1	0	0
0	0	1	1	1	1	1

Verknüpfung von Wahrheitswerten

🙂 Genau so rechnen Sie mit Wahrheitswerten, ganz einfach.
Dies sind elementare Rechenoperationen auf den Werten 0 und 1,
inspiriert, extrahiert und abstrahiert von unseren vorigen Beispielen.

Bitte beachten Sie, dass die logischen Verknüpfungssymbole
$\neg, \wedge, \vee, \dot\vee, \Rightarrow, \Leftrightarrow$ hier in zwei verschiedenen Rollen auftreten:

1. Bei der Verknüpfung von Aussagen sind dies verbindende Symbole.
   Sind zum Beispiel a, b aussagenlogische Variablen, so ist „$a \wedge b$“ eine
   Abfolge von drei Symbolen, eine Zeichenkette der Länge 3.
2. Beim Rechnen mit Wahrheitswerten $0, 1$ sind dies Operationen.
   So ergibt die Operation $0 \wedge 1$ den Wert 0, kurz $0 \wedge 1 = 0$.
   Hier geht es um den Wert, nicht den Ausdruck.

Aus dem Kontext der Verknüpfung ist jeweils klar, was gemeint ist.

Die folgende Definition C1D erklärt die Sichtweise (1) noch ausführlicher,
also was genau wir unter einer aussagenlogischen Formel verstehen.
Die Definition C1E leistet die Übersetzung von aussagenlogischen
Formeln zur Auswertung der Wahrheitswerte in $\{0,1\}$ wie in (2).

Verknüpfung von Wahrheitswerten

Alle logischen Operationen lassen sich auf $\neg$, $\wedge$ und $\vee$ zurückführen!

$$(a \Rightarrow b) = (\neg a \vee b)$$

$$\begin{aligned}(a \Leftrightarrow b) &= ((a \Rightarrow b) \wedge (b \Rightarrow a)) \\ &= ((\neg a \vee b) \wedge (a \vee \neg b)) \\ &= ((a \wedge b) \vee (\neg a \wedge \neg b))\end{aligned}$$

$$\begin{aligned}(a \mathbin{\dot\vee} b) &= \neg(a \Leftrightarrow b) \\ &= \neg((\neg a \vee b) \wedge (a \vee \neg b)) \\ &= ((a \wedge \neg b) \vee (\neg a \wedge b))\end{aligned}$$

🙂 Definition C1G erklärt die konjunktive und disjunktive Normalform,
und Satz C1H zeigt, dass wir jeden Junktor so darstellen können.

Insbesondere das Exklusiv-Oder $\dot\vee$ lassen wir daher meistens weg;
bei Bedarf können wir jederzeit $(a \mathbin{\dot\vee} b) = \neg(a \Leftrightarrow b)$ vereinbaren.

Die Implikation $\Rightarrow$ und die Äquivalenz $\Leftrightarrow$ hingegen werden sehr häufig
gebraucht, sodass wir diese bequeme Notation beibehalten wollen.

Verknüpfung von Wahrheitswerten

Wir haben oben die wichtigsten logischen Verknüpfungen erklärt.
Es gibt daneben noch einige weitere, wie zum Beispiel:

NAND $\quad a \mathbin{\overline{\wedge}} b := \neg(a \wedge b)$
NOR $\quad a \mathbin{\overline{\vee}} b := \neg(a \vee b)$

Übung: Wie viele Verknüpfungen $\{0,1\} \times \{0,1\} \to \{0,1\}$ gibt es?
Zählen Sie alle Möglichkeiten explizit auf. (Lösung auf Seite C142)

🙂 Es ist eine gute Übung, neu definierte Objekte aufzuzählen.
Das verschafft Ihnen einen guten Überblick und mehr Sicherheit.

Übung: Jede logische Verknüpfung $\neg, \vee, \wedge, \ldots$ lässt sich aufbauen
(1) alleine aus NAND sowie alternativ (2) alleine aus NOR.

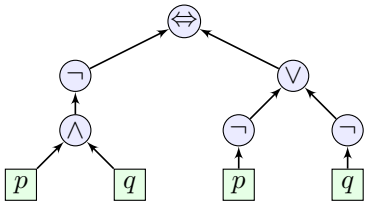
🙂 Das hilft beispielsweise zur Herstellung von Computerchips, um alle
logischen Schaltungen aus einem einzigen Grundbaustein herzustellen.

Übung: Allein aus $\wedge$ und $\vee$ lassen sich nicht alle Verknüpfungen
$\{0,1\} \times \{0,1\} \to \{0,1\}$ aufbauen: Alle daraus gebauten Formeln $f(a,b)$
sind monoton, das heißt, aus $a \le a'$ und $b \le b'$ folgt $f(a,b) \le f(a',b')$.

Aussagenlogische Variablen und Formeln

Wir wollen aussagenlogische Formeln aufbauen, wie zum Beispiel

$$\begin{aligned} \neg(p \wedge q) &\Leftrightarrow (\neg p \vee \neg q) \\ \neg(p \vee q) &\Leftrightarrow (\neg p \wedge \neg q) \\ ((p \Rightarrow q) \wedge (q \Rightarrow p)) &\Leftrightarrow (p \Leftrightarrow q) \\ ((p \Rightarrow q) \wedge (q \Rightarrow r)) &\Rightarrow (p \Rightarrow r) \end{aligned}$$



Als Bausteine haben wir dazu

- die Konstanten $\bot$ (falsum, falsch) und $\top$ (verum, wahr),
- die Verknüpfungen $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ mit Klammern (und),
- die Variablen $p, q, r, \ldots$ als freie Symbole (noch nicht belegt).

Daraus bauen wir alle Formeln rekursiv auf:

Definition C1D: aussagenlogische Formeln

Konstanten und Variablen x sind Formeln der Komplexität $\kappa(x) = 0$.

Sind a, b Formeln, so auch $\neg a$ mit Komplexität $\kappa(\neg a) = 1 + \kappa(a)$
und $c = (a \wedge b), (a \vee b), (a \Rightarrow b), (a \Leftrightarrow b)$, mit $\kappa(c) = 1 + \kappa(a) + \kappa(b)$.

Aussagenlogische Variablen und Formeln

Das erklärt den formalen Aufbau aller aussagenlogischen Formeln.
Wir nutzen folgende Konventionen, um Klammern zu sparen:

- Wir können äußere Klammern weglassen.
  Beispiel: Wir kürzen $(p \Rightarrow q)$ ab zu $p \Rightarrow q$.
- Die Negation $\neg$ bindet stärker als $\wedge$ und $\vee$.
  Beispiel: $(\neg p \wedge q) \neq \neg(p \wedge q)$ und $(\neg p \vee q) \neq \neg(p \vee q)$
- die Verknüpfungen $\wedge$ und $\vee$ binden stärker als $\Leftrightarrow$ und $\Rightarrow$.
  Beispiel: Wir können $(p \wedge q) \Leftrightarrow (q \wedge q)$ abkürzen zu $p \wedge q \Leftrightarrow q \wedge q$.

Prinzip der Klarheit: Eine Bezeichnung / Abkürzung ist nur sinnvoll, wenn der gemeinte Gegenstand daraus unmissverständlich hervorgeht.

Test: Können Sie auf einem Computer die Ersetzung programmieren? Können Sie umgekehrt die Baumstruktur eindeutig rekonstruieren? Spätestens hier bemerken Sie Unklarheiten und Unstimmigkeiten.

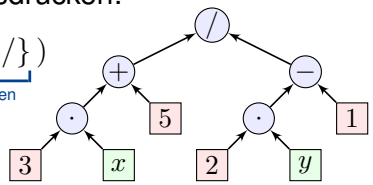
Die obigen Konventionen zum Sparen von Klammern erinnern an die Regel „Punkt-vor-Strich“, die Sie noch gut aus der Schule kennen. Tatsächlich besteht hier eine sehr enge und schöne Analogie.

Aussagenlogische Variablen und Formeln

Sie kennen das Prinzip von rationalen Ausdrücken:

$$\mathrm{RAT} = \mathscr{F}(\underbrace{\mathbb{Z}}_{\text{Konstanten}}, \underbrace{\{x, y, z, \ldots\}}_{\text{Variablen}}, \underbrace{\{+, -, \cdot, /\}}_{\text{Verknüpfungen}})$$

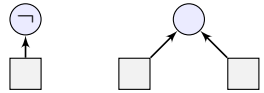
$$\frac{3x+5}{2y-1} = ((3 \cdot x) + 5)/((2 \cdot y) - 1)$$



Ebenso konstruieren wir alle aussagenlogischen Formeln:

$$\mathrm{ALF} = \mathscr{F}(\underbrace{\{\bot, \top\}}_{\text{Konstanten}}, \underbrace{\{p, q, r, \ldots\}}_{\text{Variablen}}, \underbrace{\{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}}_{\text{Verknüpfungen}})$$

Aufgabe: Wir betrachten die Konstanten $\bot, \top$ und drei Variablen p, q, r. Wie viele aussagenlogische Formeln der Komplexität $0, 1, 2$ gibt es?



Lösung: Es gibt genau $5 + 4 \cdot 5^2 = 105$ Formeln der Komplexität 1. Komplexität 2 empfehle ich als Übung. Lesen Sie die Definition!

Aussagenlogische Variablen und Formeln

Definition C1D erklärt den Aufbau aller aussagenlogischen Formeln. Jede Formel entspricht genau einer Baumstruktur wie oben skizziert. Zur Betonung: Nichts anderes ist eine aussagenlogische Formel.

Es ist oft lehrreich, neu definierte Objekte zu zählen. Dies zwingt dazu, die Definition genau zu verstehen und klärt so Missverständnisse auf. *Defendit numerus.* [Die Zahl gibt Schutz.] Juvenal (58–138 n.Chr.), *Satiren*

Jede Variable p ist ein Platzhalter und hat noch keinen Wahrheitswert. Wir können jede beliebige Aussage A für p einsetzen, geschrieben $p \mapsto A$, gelesen „ersetze der Variable p überall durch die Aussage A“.

Beispiel: Durch die beiden Ersetzungen $p \mapsto$ (die Sonne scheint) und $q \mapsto$ (ich gehe ins Freibad) wird aus der allgemeinen Formel $(p \Rightarrow q)$ die spezielle Aussage (die Sonne scheint) $\Rightarrow$ (ich gehe ins Freibad), gesprochen „Wenn die Sonne scheint, dann gehe ich ins Freibad.“

Wir wollen von Sonnenschein und Freizeitaktivitäten abstrahieren, mit allgemeinen aussagenlogischen Formeln arbeiten und rechnen. Besonders nützlich sind Tautologien, also Formeln, die immer gelten.

Auswertungen und Tautologien

Definition C1E: Auswertungen und Tautologien

Eine **Belegung** der Variablen ist eine Abbildung $\beta : \{p, q, r, \ldots\} \to \{0, 1\}$: Sie ordnet jeder Variablen x einen Wahrheitswert $\beta(x) \in \{0, 1\}$ zu.

Diese Abbildung setzen wir fort zu einer Auswertung aller Formeln: Die Konstanten $\bot$ und $\top$ werten wir aus zu $\beta(\bot) = 0$ und $\beta(\top) = 1$. Zusammengesetzte Formeln werten wir daraufhin rekursiv aus:

$$\begin{aligned} \beta(\neg a) &= \neg\beta(a) \\ \beta(a \wedge b) &= \beta(a) \wedge \beta(b) \\ \beta(a \vee b) &= \beta(a) \vee \beta(b) \\ \beta(a \Rightarrow b) &= \beta(a) \Rightarrow \beta(b) \\ \beta(a \Leftrightarrow b) &= \beta(a) \Leftrightarrow \beta(b) \end{aligned}$$

Eine Formel a heißt **erfüllbar**, wenn sie für eine Belegung wahr ist.
Eine Formel a heißt **Tautologie**, wenn sie für jede Belegung wahr ist.
Zwei Formeln a, b heißen **äquivalent**, wenn $a \Leftrightarrow b$ eine Tautologie ist.

Auswertungen und Tautologien

Definition C1D erklärt die **Sprache** (Syntax) aussagenlogischer Formeln und C1E ihre **Interpretation** (Semantik) bezüglich einer Belegung β. Wir betrachten jede Belegung β als ein **Beispiel** oder ein **Modell**, erst dadurch wird eine Formel zur Aussage, also wahr oder falsch.

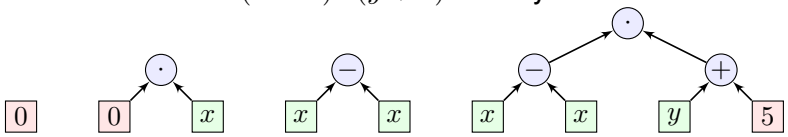
Zwei Formeln a und b sind **gleich**, wenn sie identisch aufgebaut sind, also durch denselben Text dargestellt werden, somit denselben Baum. Zur Betonung sagen wir, a und b sind **syntaktisch gleich**. Das ist leicht zu prüfen: Es genügt a und b Buchstabe für Buchstabe zu vergleichen.

Hingegen sind a und b **logisch äquivalent**, wenn sie immer dasselbe Ergebnis liefern, egal auf welches Beispiel / Modell wir sie anwenden. Das bedeutet $a \Leftrightarrow b$ ist eine Tautologie, also wahr für jede Belegung β. Zur Betonung sagen wir, a und b verhalten sich **semantisch gleich**.

Letzteres ist mühsamer zu prüfen. Für den syntaktischen Vergleich von zwei Formeln a und b der Länge $\leq \ell$ benötigen wir $\leq \ell$ Schritte. Für den semantischen Vergleich bezüglich aller Belegungen der n Variablen benötigen wir 2^n Rechnungen: Das ist exponentiell in n.

Auswertungen und Tautologien

Sie kennen das Prinzip von rationalen Ausdrücken: Die vier Ausdrücke 0 und $0 \cdot x$ und $x - x$ und $(x - x) \cdot (y + 5)$ sind syntaktisch verschieden:



Alle vier sind jedoch semantisch gleich: Sie liefern dasselbe Ergebnis, egal welche (ganzzahligen) Werte wir für die Variablen x, y einsetzen. Alle vier definieren dieselbe Funktion $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z} : (x, y) \mapsto f(x, y)$.

Zum Schluss einer Rechnung versuchen Sie, Ihre Antwort soweit wie möglich zu vereinfachen, also unter den semantisch gleichen Lösungen eine syntaktisch möglichst einfache herzustellen, manchmal sogar *die* Normalform: Zum Beispiel möchten Sie Brüche vollständig kürzen.

Wir werden daher penibel zwischen Formel und Funktion unterscheiden. Mit der Formel können wir explizit arbeiten und das Objekt benennen. Die Funktion hingegen sagt uns, was die Formel bei Auswertung tut. Verschiedene Formeln können dieselbe Funktion definieren!

Auswertungen und Tautologien

Sie haben in der Schule gelernt, wie man solche Formeln, sagen wir in $\mathscr{F}(\mathbb{Q}, \{x\}, \{+, -, \cdot\})$, als Polynome in eine geeignete Normalform bringt und somit schließlich bequem vergleichen kann: Koeffizientenvergleich!

Solche Normalformen sind Fluch und Segen: Sie dürfen sich freuen, sie zu nutzen, doch Sie müssen sich etwas mühen, sie herzustellen. Sie kennen das von Hausaufgaben und vor allem Klausuren.

Auch für aussagenlogische Formeln gibt es solche Normalformen, CNF und DNF, diese werden wir unten definieren und Beispiele erarbeiten. Bemerkenswerterweise ist jedoch der semantische Vergleich von zwei aussagenlogischen Formeln rechnerisch sehr aufwändig. Das führt uns zu einer der größten ungelösten Fragen der Komplexitätstheorie: C1K.

Sie sehen hier ein eindrückliches Beispiel für die sinnvolle Trennung zwischen der *Definition* eines Begriffs (konkret: Erfüllbarkeit, Tautologie, Äquivalenz) und möglichen *Algorithmen* zu seiner expliziten Berechnung (Wahrheitstabelle, Normalform, . . . ?). Die Trennung ist notwendig und schafft Klarheit: (1) Was wollen wir wissen? (2) Wie berechnen wir es?

Doppelte Verneinung und das ausgeschlossene Dritte

Als einfache Illustration untersuchen wir die folgenden Ausdrücke:

p	$\neg p$	$\neg\neg p$	$p \wedge \neg p$	$\neg(p \wedge \neg p)$	$p \vee \neg p$	$p \dot\vee \neg p$
1	0	1	0	1	1	1
0	1	0	0	1	1	1

Mein Hund gehorcht mir aufs Wort. Wenn ich sage „Komm her oder nicht!“, dann kommt er her oder nicht, und zwar sofort! (Otto Waalkes)

Satz C1F: doppelte Verneinung und das ausgeschlossene Dritte

Folgende Ausdrücke sind Tautologien, also allgemeingültig:

$\neg\neg p \Leftrightarrow p$	die doppelte Verneinung
$\neg(p \wedge \neg p)$	der ausgeschlossene Widerspruch
$p \vee \neg p$	das ausgeschlossene Dritte, *Tertium non datur*
$p \dot\vee \neg p$	beides zusammengefasst

Lesen Sie dies laut vor! Das klingt tautologisch? Ja, klar! Jetzt haben wir die Sprache, dies zu formulieren, und auch die Technik, es zu beweisen.

Doppelte Verneinung und das ausgeschlossene Dritte

In der klassischen Aussagenlogik ist die Formel $p \vee \neg p$ eine Tautologie, also immer wahr. So werden wir es im Folgenden bequem verwenden.

Die konstruktive Sichtweise ist hier wesentlich strenger: Zum Beweis der Disjunktion $p \vee q$ fordert die Konstruktivistin einen Nachweis von p oder einen Nachweis von q. Das ist viel informativer, aber auch schwieriger! Insbesondere ist für eine Konstruktivistin die Formel $p \vee \neg p$ noch nicht automatisch bewiesen, sie fordert einen Nachweis von p oder von $\neg p$.

Beispiel: Wir erinnern uns an die Goldbachsche Vermutung:

$$G = (\text{Jede gerade Zahl } n \geq 4 \text{ ist Summe zweier Primzahlen.})$$

Klassisch gilt $G \vee \neg G$. Konstruktiv bleibt die Aussage offen: Wir wissen (noch) nicht, ob die Vermutung G gilt, oder ob ihre Negation $\neg G$ gilt.

Beispiel: „Ich bin verzweifelt: Ich habe meine Schlüssel verbummelt. Das war entweder in der Mensa oder in der Bahn.“ Das ist prinzipiell gut zu wissen, sagt uns aber leider noch lange nicht, wo wir suchen sollen! Für viele praktische Fragen ist die konstruktive Sichtweise hilfreicher.

Nützliche Rechenregeln

Die folgenden einfachen Tautologien sind allgegenwärtig und hilfreich:

(1) Kommutativität	$(p \wedge q)$	$\Leftrightarrow$	$(q \wedge p)$
	$(p \vee q)$	$\Leftrightarrow$	$(q \vee p)$
(2) Assoziativität	$((p \wedge q) \wedge r)$	$\Leftrightarrow$	$(p \wedge (q \wedge r))$
	$((p \vee q) \vee r)$	$\Leftrightarrow$	$(p \vee (q \vee r))$
(3) Distributivität	$(p \vee (q \wedge r))$	$\Leftrightarrow$	$((p \vee q) \wedge (p \vee r))$
	$(p \wedge (q \vee r))$	$\Leftrightarrow$	$((p \wedge q) \vee (p \wedge r))$
(4) Idempotenz	$(p \wedge p)$	$\Leftrightarrow$	p
	$(p \vee p)$	$\Leftrightarrow$	p
(5) Absorption	$(p \vee (p \wedge q))$	$\Leftrightarrow$	p
	$(p \wedge (p \vee q))$	$\Leftrightarrow$	p
(6) De Morgan	$\neg(p \wedge q)$	$\Leftrightarrow$	$(\neg p \vee \neg q)$
	$\neg(p \vee q)$	$\Leftrightarrow$	$(\neg p \wedge \neg q)$

🙂 Damit können Sie rechnen, Formeln umformen und vereinfachen.

Nützliche Rechenregeln

Aufgabe: Beweisen Sie, dass dies Tautologien sind! Was ist zu tun?

Lösung: Wir prüfen dies als Wahrheitstabelle, hier exemplarisch für (6):

p	q	$p \wedge q$	$p \vee q$	$\neg p$	$\neg q$	$(\neg p) \vee (\neg q)$	$(\neg p) \wedge (\neg q)$
1	1	1	1	0	0	0	0
1	0	0	1	0	1	1	0
0	1	0	1	1	0	1	0
0	0	0	0	1	1	1	1

Die Negation der dritten/vierten Spalte ergibt die siebte/achte Spalte. Die verbleibenden Rechnungen (1–5) empfehle ich als Übung.

Aufgabe: Ist $\Rightarrow$ kommutativ / assoziativ? Ist $\Leftrightarrow$ kommutativ / assoziativ?

Lösung: Nein, $\Rightarrow$ ist nicht kommutativ: $(1 \Rightarrow 0) = 0$ und $(0 \Rightarrow 1) = 1$, ebensowenig assoziativ: $((0 \Rightarrow 1) \Rightarrow 0) = 0$ und $(0 \Rightarrow (1 \Rightarrow 0)) = 1$.

⚠ Zum Beweis einer Tautologie müssen wir (laut Definition) die gesamte Wahrheitstabelle prüfen. Zum Widerlegen genügt ein Gegenbeispiel! Die Rechnung für $\Leftrightarrow$ empfehle ich als Übung.

Konventionen für mehrfache Verknüpfungen

Die mehrfache Konjunktion definieren wir als Linksklammerung:

$$\textstyle\bigwedge_{i=1}^{n} p_i \;:=\; p_1 \wedge p_2 \wedge \cdots \wedge p_n \;:=\; (\cdots(p_1 \wedge p_2) \wedge \cdots) \wedge p_n$$

Das ist wahr, wenn p_i für jeden Index $i \in \{1,\ldots,n\}$ wahr ist.
Hierfür schreiben wir abkürzend auch $\forall i \in \{1,\ldots,n\} : p_i$.

Die mehrfache Disjunktion definieren wir als Linksklammerung:

$$\textstyle\bigvee_{i=1}^{n} p_i \;:=\; p_1 \vee p_2 \vee \cdots \vee p_n \;:=\; (\cdots(p_1 \vee p_2) \vee \cdots) \vee p_n$$

Das ist wahr, wenn p_i für (mind.) einen Index $i \in \{1,\ldots,n\}$ wahr ist.
Hierfür schreiben wir abkürzend auch $\exists i \in \{1,\ldots,n\} : p_i$.

🙂 Dank Assoziativität dürfen wir beliebig umklammern
und dank Kommutativität zudem beliebig umordnen.

Die mehrfache Implikation bzw. Äquivalenz definieren wir durch

$$p_1 \Rightarrow p_2 \Rightarrow \ldots \Rightarrow p_n \;:=\; (p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \cdots \wedge (p_{n-1} \Rightarrow p_n),$$
$$p_1 \Leftrightarrow p_2 \Leftrightarrow \ldots \Leftrightarrow p_n \;:=\; (p_1 \Leftrightarrow p_2) \wedge (p_2 \Leftrightarrow p_3) \wedge \cdots \wedge (p_{n-1} \Leftrightarrow p_n).$$

Konjunktive und disjunktive Normalformen

Jede polynomielle Formel $f \in \mathrm{POL} = \mathscr{F}(\mathbb{C}, \{x\}, \{+,-,\cdot\})$ können Sie umformen in eine **Summe von Produkten** $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ und ebenso in ein **Produkt von Summen** $a_n(x-z_1)(x-z_2)\cdots(x-z_n)$.

Ebenso können Sie jede aussagenlogische Formel

$$a \in \mathrm{ALF} = \mathscr{F}(\{\bot,\top\}, \{p,q,r,\ldots\}, \{\neg,\wedge,\vee,\Rightarrow,\Leftrightarrow\})$$

umformen in eine äquivalente **Disjunktion von Konjunktionen** und ebenso in eine **Konjunktion von Disjunktionen**. Zum Beispiel:

$$((p \wedge q) \vee (\neg p \wedge \neg q)) \;\Leftrightarrow\; ((\neg p \vee q) \wedge (p \vee \neg q))$$

Definition C1G: konjunktive und disjunktive Normalform

Wir nennen $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$ eine **konjunktive Normalform** (CNF) und $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} a_{ij}$ eine **disjunktive Normalform** (DNF); hierbei ist a_{ij} ein Literal, also eine Variable x oder ihre Negation $\neg x$, und jede Klausel $\bigvee_{j=1}^{m_i} a_{ij}$ bzw. $\bigwedge_{j=1}^{m_i} a_{ij}$ enthält jede Variable höchstens einmal.

Konjunktive und disjunktive Normalformen

Beispiel: Die Formel $p \wedge (\neg p \vee q) \wedge (q \vee r)$ ist eine CNF, aber keine DNF.
Die Formel $(p \wedge q) \vee (p \wedge q) \vee (\neg p \wedge r) \vee q$ ist eine DNF, aber keine CNF.
Die Formeln $\neg p \vee q$ und $p \wedge q \wedge \neg r$ sind sowohl CNF als auch DNF;
dasselbe gilt für jede Disjunktion und jede Konjunktion von Literalen.

In jedem konkreten Beispiel ist das leicht: Eine CNF ist eine Konjunktion von Disjunktionen, und eine DNF ist eine Disjunktion von Konjunktionen. Zur Ausformulierung dieser Idee benötigen wir eine geeignete Notation, nur so können wir sie präzise definieren und effizient mit ihr arbeiten.

Ausführlich: Ein **Literal** ist eine Variable x oder ihre Negation $\neg x$. Eine **disjunktive Klausel** $d_i = \bigvee_{j=1}^{m_i} a_{ij}$ ist eine Disjunktion von Literalen a_{ij} ohne doppelte Variablen. Eine **konjunktive Normalform** $c = \bigwedge_{i=1}^{\ell} d_i$ ist eine Konjunktion von disjunktiven Klauseln d_i, also $c = \bigwedge_{i=1}^{\ell} (\bigvee_{j=1}^{m_i} a_{ij})$.

Dual ist eine **konjunktive Klausel** $c_i = \bigwedge_{j=1}^{m_i} a_{ij}$ eine Konjunktion von Literalen a_{ij} ohne doppelte Variablen. Eine **disjunktive Normalform** $d = \bigvee_{i=1}^{\ell} c_i$ ist eine Disjunktion von konjunktiven Klauseln c_i, also ausgeschrieben $d = \bigvee_{i=1}^{\ell} (\bigwedge_{j=1}^{m_i} a_{ij})$. Soweit das Vokabular.

Konjunktive und disjunktive Normalformen

🙂 Konjunktive und disjunktive Normalformen sind dual durch Negation:
Für jede CNF $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$ ist die Negation $\neg c$ äquivalent zur DNF $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} b_{ij}$, mit $b_{ij} = \neg x$ falls $a_{ij} = x$ und $b_{ij} = x$ falls $a_{ij} = \neg x$.

🙂 Doppelte Variablen lassen sich leicht und effizient kürzen!

In der Disjunktion $\bigvee_{j=1}^{m_i} a_{ij}$ können wir jede doppelte Variable p kürzen, entweder dank Idempotenz $(p \vee p) \Leftrightarrow p$ und $(\neg p \vee \neg p) \Leftrightarrow \neg p$ oder dank $(p \vee \neg p) \Leftrightarrow \top$ und in $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$ wird diese Disjunktion gelöscht.

In jeder Konjunktion $\bigwedge_{j=1}^{m_i} a_{ij}$ gilt entsprechend dieselbe Kürzungsregel, entweder dank Idempotenz $(p \wedge p) \Leftrightarrow p$ und $(\neg p \wedge \neg p) \Leftrightarrow \neg p$ oder dank $(p \wedge \neg p) \Leftrightarrow \bot$ und in $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} a_{ij}$ wird diese Konjunktion gelöscht.

🙂 Die kleinen Längen $\ell \leq 2$ schreibe ich zur Deutlichkeit explizit aus:

$$\textstyle\bigvee_{i=1}^{2} p_i = p_1 \vee p_2, \qquad \bigvee_{i=1}^{1} p_i = p_1, \qquad \bigvee_{i=1}^{0} p_i = \bot,$$
$$\textstyle\bigwedge_{i=1}^{2} p_i = p_1 \wedge p_2, \qquad \bigwedge_{i=1}^{1} p_i = p_1, \qquad \bigwedge_{i=1}^{0} p_i = \top.$$

Letzteres entspricht unserer Definition für leere Summen $\sum_{i=1}^{0} s_i = 0$ und leere Produkte $\prod_{i=1}^{0} t_i = 1$, jeweils durch das neutrale Element.

Junktoren

C141

Wir kennen die logischen Verknüpfungen $\wedge, \vee, \Rightarrow, \Leftrightarrow : \{0,1\}^2 \to \{0,1\}$.
Ein n–stelliger **Junktor** ordnet jedem n–Tupel $a = (a_1, a_2, \ldots, a_n)$ mit Einträgen $a_1, a_2, \ldots, a_n \in \{0,1\}$ einen Wert $J(a) \in \{0,1\}$ zu, kurz

$$J : \{0,1\}^n \to \{0,1\} : a \mapsto J(a).$$

Aufgabe: Wie viele n–Tupel $a \in \{0,1\}^n$ gibt es? Wie viele n–stellige Junktoren gibt es? Berechnen Sie dies explizit für $n = 0, 1, 2, \ldots, 8$.

Lösung: Für $n \in \mathbb{N}$ gibt es genau 2^n Tupel und 2^{2^n} Junktoren.

n	Anzahl der n–Tupel	Anzahl der n–Junktoren
0	$2^0 = 1$ leeres Tupel	$2^1 = 2$
1	$2^1 = 2$ Elemente	$2^2 = 4$
2	$2^2 = 4$ Paare	$2^4 = 16$
3	$2^3 = 8$ Tripel	$2^8 = 256$
4	$2^4 = 16$ Quadrupel	$2^{16} = 65\,536$
5	$2^5 = 32$ Quintupel	$2^{32} = 4\,294\,967\,296$
6	$2^6 = 64$ Sextupel	$2^{64} \approx 1.84 \cdot 10^{19}$
7	$2^7 = 128$ Septupel	$2^{128} \approx 3.40 \cdot 10^{38}$
8	$2^8 = 256$ Octupel	$2^{256} \approx 1.16 \cdot 10^{77}$

Junktoren

C142

Aufgabe: Nennen Sie alle zweistelligen Junktoren $J : \{0,1\}^2 \to \{0,1\}$.

c_0	0	1
0	0	0
1	0	0

$\overline{\vee}$	0	1
0	1	0
1	0	0

$<$	0	1
0	0	1
1	0	0

$\overline{\mathrm{pr}_1}$	0	1
0	1	1
1	0	0

$>$	0	1
0	0	0
1	1	0

$\overline{\mathrm{pr}_2}$	0	1
0	1	0
1	1	0

$\dot{\vee}$	0	1
0	0	1
1	1	0

$\overline{\wedge}$	0	1
0	1	1
1	1	0

$\wedge$	0	1
0	0	0
1	0	1

$=$	0	1
0	1	0
1	0	1

pr_2	0	1
0	0	1
1	0	1

$\leq$	0	1
0	1	1
1	0	1

pr_1	0	1
0	0	0
1	1	1

$\geq$	0	1
0	1	0
1	1	1

$\vee$	0	1
0	0	1
1	1	1

c_1	0	1
0	1	1
1	1	1

Von Formeln zu Junktoren

C143

Sei $V = \{x_1, x_2, \ldots, x_n\}$ die Menge der betrachteten Variablen und $f \in \mathscr{F}(\{\bot, \top\}, V, \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\})$ eine aussagenlogische Formel.
Der zugehörige Junktor $J_f : \{0,1\}^n \to \{0,1\}$ ist die Wahrheitstabelle:

x_1	x_2	x_3	$f = x_1 \wedge (x_2 \vee x_3)$	$(x_1 \wedge x_2) \vee (x_1 \wedge x_3)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Ausführlich entsteht diese Tabelle wie folgt: Jedes n–Tupel $b \in \{0,1\}^n$ definiert die zugehörige Belegung $\beta : V \to \{0,1\} : x_1 \mapsto b_1, \ldots, x_n \mapsto b_n$.
Wir definieren $J_f(b) := \beta(f)$, also f ausgewertet mit der Belegung β.

Von Formeln zu Junktoren

C144
Erläuterung

Zwei verschiedene Formeln $f \neq g$ können denselben Junktor $J_f = J_g$ definieren; f und g sind dann äquivalent, $f \Leftrightarrow g$ ist eine Tautologie (C1E).
Die Formeln f, g sind syntaktisch verschieden, aber semantisch gleich: Sie liefern dasselbe Ergebnis, egal welche Belegung β wir auswerten.

Wir haben oben die Variablen $x_1, x_2, \ldots, x_n$ nummeriert, um es konkret und einfach zu machen; Belegungen β entsprechen dann n–Tupeln $(a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ von Wahrheitswerten $a_1, a_2, \ldots, a_n \in \{0,1\}$.
Die folgende Sichtweise ist eleganter und allgemeiner und abstrakter:

Sei $V = \{x_1, x_2, \ldots, x_n\}$ die Menge der hier betrachteten Variablen.
Mit $\{0,1\}^V$ bezeichnen wir die Menge aller Belegungen dieser Variablen, also der Abbildungen $\beta : V \to \{0,1\}$. Jeder Variablen $x_i \in V$ wird ein Wert $\beta(x_i) \in \{0,1\}$ zugeordnet. Sortiert wie oben sind dies n–Tupel.

Sei $f \in \mathscr{F}(\{\bot, \top\}, V, \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\})$ eine aussagenlogische Formel.
Diese definiert einen Junktor $J_f : \{0,1\}^V \to \{0,1\}$ gemäß $J_f(\beta) = \beta(f)$, das heißt J_f ausgewertet auf β ist f ausgewertet mit der Belegung β.
Anders gesagt: Der Junktor J_f ist die Wahrheitstabelle der Formel f.

Von Junktoren zu Formeln

Jede aussagenlogische Formel f in den Variablen $x_1, \ldots, x_n$ definiert einen Junktor $J_f : \{0,1\}^n \to \{0,1\}$. Lässt sich umgekehrt jeder Junktor $J : \{0,1\}^n \to \{0,1\}$ durch eine Formel f darstellen? Ja, sogar in DNF!

Aufgabe: Finden Sie Formeln (in DNF) für die folgenden Junktoren:

x_1	x_2	x_3	J_1	J_2	J_3	J_4
0	0	0	0	0	0	1
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	1	1	1
1	0	0	0	0	0	0
1	0	1	0	0	0	1
1	1	0	0	0	0	0
1	1	1	1	0	1	1

Lösung: Es gelingt mit $f_1 = x_1 \wedge x_2 \wedge x_3$ und $f_2 = \neg x_1 \wedge x_2 \wedge x_3$ sowie $f_3 = f_1 \vee f_2 = (x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) = x_2 \wedge x_3$ und schließlich $f_4 = (\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$.

Von Junktoren zu Formeln

Sie sehen hier ein sehr schönes Beispiel für mathematisches Vorgehen. Zunächst einmal sollten Sie lernen, mit offenen Augen durch die Welt zu gehen, naheliegende Fragen zu erkennen und sich explizit zu stellen! Hier geht es um ein **Umkehrproblem**, das tritt sehr häufig auf (B3A).

Bitte nehmen Sie sich die Zeit, versuchen Sie die Frage zunächst selbst, dann schrittweise anhand der vorgeschlagenen Beispiele und Aufgaben. Dann fällt der folgende Satz C1H für Sie nicht unerwartet vom Himmel, sondern Sie können ihn selbst entdecken und auch selbst beweisen!

☹ Die Frage scheint auf den ersten Blick schwierig, gar überwältigend. Vermutlich sehen Sie zunächst keine Lösung, keinen Ansatz, keine Idee.

🙂 In solchen Fällen gibt es verschiedene Strategien. Betrachten Sie Beispiele, zunächst ganz kleine und einfache… dann etwas größere und kompliziertere…. Mit etwas Glück erkennen Sie dann ein Muster.

🙂 Dieses Muster können Sie nun weiter testen. Schließlich können Sie damit eine Vermutung formulieren und idealerweise sogar beweisen. Genau dies geschieht hier. Es gelingt auch sonst erfreulich häufig!

Von Junktoren zu Formeln

Aufgabe: Extrahieren Sie aus den Beispielen eine allgemeine Lösung!

Lösung: Wir beschaffen uns zunächst eine bequeme Schreibweise.

Sei $a = (a_1, \ldots, a_n) \in \{0,1\}^n$. Zu jeder Variablen $x_1, \ldots, x_n$ definieren wir das zugehörige Literal $[a_i]x_i$ durch $[1]x_i = x_1$ und $[0]x_i = \neg x_i$.

Für jede Belegung $\beta : x_i \mapsto b_i \in \{0,1\}$ gilt somit

$$\beta([a_i]x_i) = (a_i \Leftrightarrow b_i) = \begin{cases} 1 & \text{falls } a_i = b_i, \\ 0 & \text{falls } a_i \neq b_i. \end{cases}$$

Die konjunktive Klausel $c = \bigwedge_{i=1}^n [a_i]x_i$ definiert somit den Junktor $J_c : \{0,1\}^n \to \{0,1\}$ mit $J_c(b) = 1$ für $b = a$ und $J_c(b) = 0$ für $b \neq a$.

Allgemeiner sei $A \subseteq \{0,1\}^n$ eine beliebige Teilmenge.
Dann ist $d = \bigvee_{a \in A} \bigwedge_{i=1}^n [a_i]x_i$ eine disjunktive Normalform mit

$$J_d(b) = \begin{cases} 1 & \text{falls } b \in A, \\ 0 & \text{falls } b \notin A. \end{cases}$$

Von Junktoren zu Formeln

Satz C1H: kanonische Darstellung eines Junktors

Sei $n \in \mathbb{N}$. Jeder n–stellige Junktor $J : \{0,1\}^n \to \{0,1\}$ lässt sich durch eine aussagenlogische Formel f darstellen: Es existiert f mit $J_f = J$.

Genauer: Dies gelingt in disjunktiver / konjunktiver Normalform vermöge

$$d_J = \bigvee_{a\,:\,J(a)=1} \bigwedge_{i=1}^n [a_i]x_i,$$
$$c_J = \bigwedge_{a\,:\,J(a)=0} \bigvee_{i=1}^n [\neg a_i]x_i.$$

Wir nennen d_J die **kanonische disjunktive Normalform** (CDNF) und c_J die **kanonische konjunktive Normalform** (CCNF) des Junktors J.

Beweis: Sei $A = \{\, a \in \{0,1\}^n \mid J(a) = 1 \,\}$ die Menge aller $a \in \{0,1\}^n$, für die J den Wert $J(a) = 1$ annimmt. Das nennen wir den Träger von J. Für $d = \bigvee_{a \in A} \bigwedge_{i=1}^n [a_i]x_i$ gilt $J_d = J$, wie in der Aufgabe ausgerechnet.

Der Junktor $\neg J$ wird demnach dargestellt durch $\bigvee_{a\,:\,\neg J(a)=1} \bigwedge_{i=1}^n [a_i]x_i$.
Somit wird $J = \neg\neg J$ dargestellt durch $c = \bigwedge_{a\,:\,J(a)=0} \bigvee_{i=1}^n [\neg a_i]x_i$. QED

Normalform und Entscheidungsproblem

Wir wollen prüfen, ob eine aussagenlogische Formel f eine Tautologie ist, also $\beta(f) = 1$ für *jede* Belegung f, oder wenigstens erfüllbar ist, also $\beta(f) = 1$ für *irgendeine* Belegung β. In Normalform gelingt dies leicht:

Satz C1I: eine Lösung des Entscheidungsproblems

(1) Sei $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$ eine konjunktive Normalform.
Genau dann ist c eine Tautologie, wenn $\ell = 0$ gilt, also $c = \top$.

(2) Sei $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} a_{ij}$ eine disjunktive Normalform.
Genau dann ist d unerfüllbar, wenn $\ell = 0$ gilt, also $d = \bot$.

Beweis: (1) Ist $\ell = 0$, so ist $c = \top$ eine Tautologie. Sei umgekehrt $\ell \geq 1$.
Für jedes Literal a_{1j} gilt $a_{1j} = x$ oder $a_{1j} = \neg x$ mit einer Variablen x.
Im ersten Falle setzen wir $\beta(x) = 0$, im zweiten Falle hingegen $\beta(x) = 1$.
Jede Variable tritt höchstens einmal auf, also entsteht kein Widerspruch.
Für jede nicht-auftretende Variable y setzen wir willkürlich $\beta(y) = 0$.
Für diese Belegung β gilt $\beta(\bigvee_{j=1}^{m_1} a_{1j}) = 0$ und somit $\beta(c) = 0$.

Aussage (2) beweist man analog. Versuchen Sie es als Übung! QED

Normalform und Entscheidungsproblem

Gegeben sei eine aussagenlogische Formel f mit Variablen $x_1, \ldots, x_n$.
Gesucht ist eine zu f äquivalente disjunktive Normalform d.

Hierzu kennen wir nun zwei komplementäre Methoden:

1. Ausmultiplizieren: Wende auf f Distributivität an bis zu einer DNF.
2. Wahrheitstabelle: Bestimme zum Junktor J_f die kanonische DNF.

🙂 Die gute Nachricht: Beide Methoden gelingen immer.
Unser Problem wird dadurch also gelöst... zumindest prinzipiell.

☹ Die schlechte Nachricht: Beide Methoden sind oft kostspielig.
Im schlimmsten Fall verursachen sie **exponentiellen Aufwand**:

1. Die kurze Formel $(x_1^0 \vee x_1^1) \wedge \cdots \wedge (x_n^0 \vee x_n^1)$ mit n Klauseln wird zur langen DNF $\bigvee_{a \in \{0,1\}^n} \bigwedge_{i=1}^{n} x_i^{a_i}$ mit 2^n Klauseln.
2. Bei n Variablen benötigt die Wahrheitstabelle 2^n Einträge.
   Für $n = 500$ Variablen sind das $2^{500} \approx 3.27 \cdot 10^{150}$ Einträge.

Exponentieller Aufwand ist nur für sehr kleine n überhaupt durchführbar.
Wir suchen daher Methoden mit **polynomiellen Aufwand** $\leq \text{const} \cdot n^c$.

Eines der sieben Millennium-Probleme: P vs NP

Wir untersuchen $f \in \text{ALF}_n = \mathscr{F}(\{\bot, \top\}, \{x_1, x_2, \ldots, x_n\}, \{\neg, \wedge, \vee\})$.

Definition C1J: Erfüllbarkeitsproblem (*satisfiability*, SAT)

Tautologieproblem, TAU: Eingabe $f \in \text{ALF}$. Ist f eine Tautologie?
Erfüllbarkeitsproblem, SAT: Eingabe $f \in \text{ALF}$. Ist f erfüllbar?

Beide Fragen sind prinzipiell über die Wahrheitstabelle J_f entscheidbar, dies erfordert jedoch exponentiellen Aufwand, im schlimmsten Fall $\kappa 2^n$.

Beide Probleme sind äquivalent: Genau dann ist f eine Tautologie, wenn die Negation $\neg f$ nicht erfüllbar ist. Meist betrachtet man daher nur SAT.

Problem C1K: Gilt $\text{P} = \text{NP}$?

Erlaubt das Erfüllbarkeitsproblem eine Lösung in polynomieller Zeit?

Das ist eine der größten ungelösten Fragen der Komplexitätstheorie.
Es ist eines der sieben Millennium-Probleme mit einem Preisgeld von 1Mio Dollar, siehe `de.wikipedia.org/wiki/Millennium-Probleme`.

🙂 Zum Kontrast: Gauß B2C hat polynomiellen Aufwand, nur $\sim n^3$.

Eines der sieben Millennium-Probleme: P vs NP

Das Erfüllbarkeitsproblem ist keineswegs isoliert, sondern typisch.

Prüfen vs Finden: Dieses Problem illustriert ein Grundprinzip:

- Es ist oft leicht, für eine vorgelegte Lösung die Probe zu machen.
- Es ist meist viel schwerer, überhaupt eine Lösung zu finden.

Wir sehen dies hier ganz konkret für aussagenlogische Formeln f.

Für jede Belegung $\beta : \{0,1\}^n \to \{0,1\}$ können wir leicht $\beta(f)$ auswerten:
Definition C1E ist ein Algorithmus in $\kappa(f)$ Schritten, linear in der Länge.
Ein **Beleg für die Erfüllbarkeit** ist also in polynomieller Zeit prüfbar.

Einen **Beleg zu finden**, benötigt jedoch exponentielle Zeit $\kappa 2^n$ mit dem simplen Algorithmus, der die gesamte Wahrheitstabelle J_f durchgeht.
Die dringende Frage ist: Gelingt auch das Finden in polynomieller Zeit?

Lösungen des Erfüllbarkeitsproblems werden genutzt zum Design von Schaltkreisen, in automatischen Beweisen und künstlicher Intelligenz.
Heuristische Verfahren lösen (gutartige) Fälle mit tausenden Variablen.
Ein allgemeines, polynomielles Verfahren ist jedoch nicht bekannt.

Schlussregeln: neue wahre Aussagen aus alten!

C201

Eine **Schlussregel** erlaubt uns, aus bereits bewiesenen Aussagen neue Aussagen abzuleiten. Solche Regeln der „Textverarbeitung“ dienen uns zum strukturierten Aufbau mathematischer Beweise.

$p \wedge q$	Wir beweisen $p \wedge q$.
$\hline q$	Wir schließen q.

p	Wir beweisen p.
$\hline p \vee q$	Wir schließen $p \vee q$.

Ein **Beweis** eines Satzes entsteht durch schrittweise Schlussfolgerung, als ein logisch schlüssiger Weg von der Voraussetzung zur Behauptung.

p	Wir beweisen p.
q	Wir beweisen q.
$\hline p \wedge q$	Wir schließen $p \wedge q$.

$p \vee q$	Wir beweisen $p \vee q$.
$\neg p$	Wir beweisen $\neg p$.
$\hline q$	Wir schließen q.

Die ersten beiden oben gezeigten Schlussregeln entsprechen den Tautologien $p \wedge q \Rightarrow q$ und $p \Rightarrow p \vee q$. Die dritte Schlussregel zeigt, wie wir $p \wedge q$ beweisen, also als Folgerung ableiten. Die vierte Schlussregel zeigt, wie wir $p \vee q$ nutzen, also als Voraussetzung einsetzen können.

Schlussregeln und Beweisverfahren

C202
Erläuterung

Schlussregeln entsprechen Tautologien, sie sind aber keine Aussagen, sondern Regeln für Beweise: Sie verarbeiten Aussagen, sie sind Vorlagen für Argumente, sie erklären, wie wir Beweise führen.

Die hier gezeigte Darstellung als Tabelle ist dekorativ und übersichtlich. Links steht die formale Schreibweise, rechts die umgangssprachliche Interpretation. Diese Regeln zeigen, wie wir die Aussagen $p \wedge q$ und $p \vee q$ *nutzen*, d.h. als Voraussetzung einsetzen, und auch, wie wir sie *beweisen*, d.h. als Folgerung ableiten. sie formulieren praktische Handlungsanweisungen, wie wir Beweise führen: Zunächst ich in der Vorlesung, dann Sie in den Übungen. Ich erkläre Ihnen die wichtigsten *Beweismuster*, damit Sie diese kennen, verstehen, anwenden lernen.

Diese Begriffe scheinen zunächst sperrig. Lohnt sich der Aufwand? Ja! Wir unterscheiden zwischen der *Behauptung* einer Aussage und dem *Beweis* einer Aussage. Dazu haben wir zunächst geklärt, wie Aussagen aufgebaut sind; wir können damit bereits Aussagen aussprechen und aufschreiben. Wir wollen nun klären, wie wir Aussagen beweisen.

Die Schnittregel: Modus Ponens

C203

Die folgende Implikation ist eine Tautologie, also allgemeingültig:

$$(p \wedge (p \Rightarrow q)) \Rightarrow q$$

Wir vereinbaren die **Schnittregel**, lat. **Modus Ponens**:

$p \Rightarrow q$	Wir beweisen die Aussage $p \Rightarrow q$.
p	Wir beweisen die Aussage p.
$\hline q$	Wir schließen die Aussage q.

Beispiel: Wenn es regnet, dann ist die Straße nass.
Jetzt regnet es. Daraus folgt: Die Straße ist nass.

☺ Die Schnittregel ist die einfachste und wichtigste Schlussregel, denn alle weiteren ergeben sich hieraus mit Hilfe von Tautologien:

Definition C2A: Schlussregeln der Aussagenlogik

Alle Schlussregeln der Aussagenlogik entstehen
aus den Tautologien mit Hilfe der Schnittregel.

Die Schnittregel: Modus Ponens

C204
Erläuterung

Die zentrale Aufgabe der mathematischen Logik ist es,
die Gesetze des logischen Schließens zu untersuchen.

Die Schnittregel heißt genauer *Modus ponendo ponens* (lat. ‘das zu Setzende setzend’), *Abtrennungsregel* oder *Implikationsbeseitigung*.

Sie ist die einfachste und wichtigste Schlussregel, alle weiteren unserer Schlussregeln ergeben sich hieraus mit Hilfe von Tautologien.

☺ Dieses Vorgehen stellt sicher, dass wir aus gegebenen wahren Aussagen weitere wahre Aussagen ableiten. Bei korrekter Anwendung der Schlussregeln können wir niemals eine falsche Aussage ableiten. Die Schlussregeln sind narrensicher, vornehm sagt man *konsistent*.

☺ Die Schlussregeln sagen uns genau, welche Beweisschritte wir als logische Schlüsse akzeptieren und welche nicht. Hingegen geben sie uns keinerlei Hinweis, welche die erlaubten Schritte wir in einem Beweis gehen sollen. Das ist eine Frage der Kreativität und der Erfahrung!

☺ Ich führe im Folgenden einige der wichtigsten Beweisformen aus. Aus Kapitel A und B kennen Sie schon wichtige, konkrete Beispiele!

Beweis durch Kettenschluss

Die folgende Implikation ist eine Tautologie, genannt **Transitivität**:

$$((p \Rightarrow q) \wedge (q \Rightarrow r)) \quad \Rightarrow \quad (p \Rightarrow r)$$

Dank Schnittregel folgt hieraus der **Kettenschluss:**

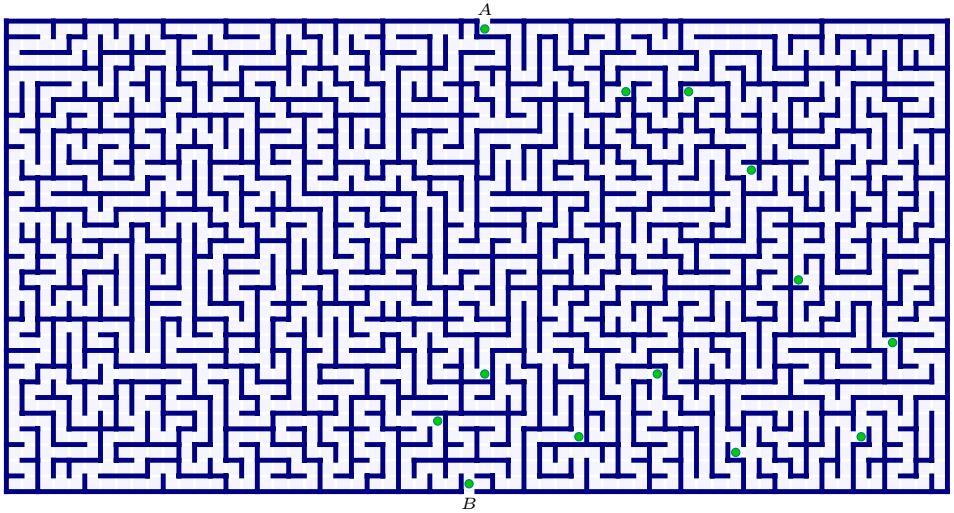
$p \Rightarrow q$	Wir beweisen die Aussage $p \Rightarrow q$.
$q \Rightarrow r$	Wir beweisen die Aussage $q \Rightarrow r$.
$p \Rightarrow r$	Wir schließen die Aussage $p \Rightarrow r$.

Beispiel: Wenn es regnet, dann ist die Straße nass.
Wenn die Straße nass ist, dann besteht Schleudergefahr.
Daraus folgt: Wenn es regnet, dann besteht Schleudergefahr.

🙂 Das ist eine nützliche **Beweisstrategie**: Um $p \Rightarrow r$ zu beweisen, führen wir Zwischenschritte ein und zeigen $p \Rightarrow q_1 \Rightarrow \cdots \Rightarrow q_n \Rightarrow r$.
Das unterteilt einen komplizierten Beweis in leichtere Schritte.

Beweis durch Kettenschluss

Ein Beweis ist eine Kette von logischen Schlüssen: Ausgehend von der Voraussetzung A wird schrittweise die Folgerung B geschlossen. Zwischenschritte helfen bei der Exploration und der Konsolidierung.



Wie detailliert muss ein Beweis sein?

Der Vergleich *Beweis – Methode – Weg* ist anschaulich und treffend!

Beweise in einem Lehrbuch für Studienanfänger sind recht ausführlich, für ein Expertenpublikum werden Beweise deutlich knapper formuliert. Was also ist ein Beweis genau? Wie detailliert ausgeführt muss er sein? Wie groß dürfen die logischen Sprünge maximal sein? Hierzu sind zwei Antworten möglich: formal dogmatisch oder sozial pragmatisch.

Dogmatische Antwort: In einem vollständig formalisierten Beweis ist jeder Schritt die Anwendung einer Schlussregel. Wir beginnen mit einer Liste von wahren Aussagen (Axiome, Voraussetzungen) und erweitern diese schrittweise durch logisches Schließen, jeweils mit Angabe der verwendeten Schlussregel. Am Ende steht die ersehnte Behauptung.

Im obigen Bild ist das der vollständig ausgeführte Lösungsweg, etwa als eine lange Folge von kleinen Beweisschritten, jeder davon ist elementar. Die Richtigkeit kann ein Computer mechanisch prüfen (*proof checker*). Für menschliche Leser ist die mechanische Prüfung sehr mühsam und wenig lehrreich, sie vermittelt meist keine Idee, Vision oder Inspiration.

Wie detailliert muss ein Beweis sein?

Pragmatische Antwort: Traditionell schreiben wir Beweise nicht für Maschinen, sondern für Menschen. Es gibt immer mehr Ausnahmen, etwa in der Programmierung, aber denken wir an diese Vorlesung.

Für ein menschliches Gegenüber ist es üblich, nicht alle elementaren Schritte auszuführen, sondern den Beweisgang allein durch geeignete Zwischenpunkte abzustecken. Das ist effizienter, sowohl für den Sender als auch für den Empfänger. Die Zwischenpunkte sollen eng genug sein, sodass der Empfänger den Weg dazwischen selbst rekonstruieren kann.

Das rechte Maß, ob detailliert ausgeführt oder nur grob skizziert, hängt somit vom Empfänger ab! Beweise in Lehrbüchern sind recht detailliert ausgeführt, Artikel in Fachzeitschriften sind meist knapper formuliert und die Beweise nur grob skizziert. Das verschiebt die Beweislast vom Sender zum Empfänger. Die richtige Balance ist eine Kunst!

Beispiel: In dieser Vorlesung bemühe ich mich, alle entscheidenden Zwischenschritte anzugeben. Routinierte Rechnungen hingegen führe ich meist nicht aus, sondern übertrage sie Ihnen. Das ist effizienter.

Beweis durch Fallunterscheidung

Ein Beweis durch **Fallunterscheidung** verläuft wie folgt:

$p \Rightarrow p_1 \vee \ldots \vee p_n$	Wir zerlegen p in mehrere Fälle
$p_1 \Rightarrow q$	Wir beweisen jeden Fall einzeln.
$\ldots$	Also jeden Fall…
$p_n \Rightarrow q$	… wirklich jeden!
$p \Rightarrow q$	Wir schließen $p \Rightarrow q$.

Beispiel: Wir wollen die folgende Aussage beweisen:
$q =$ (Es gibt irrationale Zahlen $x, y \in \mathbb{R} \setminus \mathbb{Q}$, sodass x^y rational ist.)

Beweis: Wir betrachten die Zahlen $a = \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ und $b = a^a$.
Es gilt $p_1 =$ (b ist rational) oder $p_2 =$ (b ist irrational).

- $p_1 \Rightarrow q$: Ist b rational, so gilt Aussage q dank $(x, y) = (a, a)$.
  Nachrechnen: $a^a = b \in \mathbb{Q}$.
- $p_2 \Rightarrow q$: Ist b irrational, so gilt Aussage q dank $(x, y) = (b, a)$.
  Nachrechnen: $b^a = (a^a)^a = a^{a^2} = a^2 = 2 \in \mathbb{Q}$.

Wir schließen: Die Behauptung q ist wahr. QED

Beweis durch Fallunterscheidung

☺ Beweisstrategie: Wir zeigen zunächst $p \Rightarrow p_1 \vee p_2 \vee \ldots \vee p_n$.
Dies ist eine **vollständige Fallunterscheidung** zur Voraussetzung p.
Die Wahl und geeignete Formulierung dieser Fälle erfordert Kreativität, ihre Vollständigkeit erfordert Sorgfalt. Die Fälle dürfen sich durchaus überlappen, aber sie müssen alles abdecken! Dann zeigen wir einzeln $p_1 \Rightarrow q$, $p_2 \Rightarrow q$, …, $p_n \Rightarrow q$; diese kleineren Beweise gelingen leichter.

Unser Beispiel beweist die Existenzaussage q, aber können Sie explizit eine Lösung nennen? Nein, das können Sie nicht: Sie wissen nicht, welcher Fall wirklich eintritt. Dieser Beweis ist nicht konstruktiv!

Das Problem versteckt sich hier in der harmlosen Oder-Aussage $p_1 \vee p_2$. Klassisch ist diese immer wahr, dank ausgeschlossenem Dritten C1F. Konstruktiv wissen wir aber nicht, welcher der beiden Fälle eintritt, also welches der Paare (a, a) oder (b, a) wirklich eine Lösung ist.

Der Beweis nutzt korrekt unsere Schlussregeln, und er ist vollständig. Konstruktiv zu arbeiten kostet mehr Mühe, bringt aber auch mehr Ertrag.

☺ Der Satz von Gelfond–Schneider zeigt die Transzendenz von $\sqrt{2}^{\sqrt{2}}$.

Äquivalenz als gegenseitige Implikation

Folgende Äquivalenz ist eine Tautologie, also allgemeingültig:

$$(p \Leftrightarrow q) \quad \Leftrightarrow \quad ((p \Rightarrow q) \wedge (q \Rightarrow p))$$

Dank Schnittregel können wir Äquivalenz zur Implikation abschwächen:

$$\frac{p \Leftrightarrow q}{p \Rightarrow q} \qquad \frac{p \Leftrightarrow q}{q \Rightarrow p}$$

Umgekehrt folgt die **Äquivalenz durch gegenseitige Implikation:**

$p \Rightarrow q$	Wir beweisen: p impliziert q.
$q \Rightarrow p$	Wir beweisen: q impliziert p.
$p \Leftrightarrow q$	Wir schließen: p und q sind äquivalent.

Beispiel: Für alle $x \in \mathbb{R}$ gilt die Äquivalenz $(x^2 = x) \Leftrightarrow (x \in \{0, 1\})$.

Beweis: „⇐“: Für $x = 0$ gilt $x^2 = x$, für $x = 1$ ebenso. (Lösungen prüfen)
„⇒“: Aus $x^2 = x$ folgt $x^2 - x = 0$, und daraus $x(x - 1) = 0$. Hieraus folgt $x = 0$ oder $x = 1$, also $x \in \{0, 1\}$ wie behauptet. (Alle Lösungen finden)

Äquivalenz als gegenseitige Implikation

☺ Damit ist die Äquivalenz bewiesen. … In diesem einfachen Beispiel gelingt dies auch ebenso leicht direkt mit einer Folge von Äquivalenzen.

Übung: Die Implikation „⇐“ gilt in jedem Ring $(R, +, 0, \cdot, 1)$.
Die Umkehrung „⇒“ gilt zum Beispiel im Ring $\mathbb{Z}_6$ nicht mehr!

Für alle $x \in \mathbb{Z}_6$ gilt: $(x^2 = x) \Leftrightarrow (x \in \{0, 1, 3, 4\})$

Dies illustriert, dass sich beide Implikationen verschieden verhalten. Auch deshalb lohnt es sich, sie getrennt zu untersuchen.

☺ Die Zerlegung in zwei Implikationen ist vor allem dann wichtig, wenn beide Implikationen verschiedene, unabhängige Wege gehen.

Diese Trennung zerlegt den Beweis in zwei leichtere Hälften.
Diese sind unabhängig, das erleichtert oft unsere Argumentation.

Zum Beweis einer Äquivalenz $p \Leftrightarrow q$ nutzen wir daher fast immer die Zerlegung in die beiden Implikationen $p \Rightarrow q$ und $q \Rightarrow p$.

☺ Für Implikationen haben wir maßgeschneiderte Beweistechniken, etwa die Kontraposition oder den indirekten Beweis durch Widerspruch.

Implikation und Kontraposition

Die Schnittregel **Modus ponens** besagt:

$p \Rightarrow q$	Wir beweisen $p \Rightarrow q$:	„Wenn's regnet, ist die Straße nass."
p	Wir beweisen p:	„Es regnet."
q	Wir schließen q:	„Die Straße ist nass."

Die gültige Umkehrung dieser Regel heißt **Modus tollens**:

$p \Rightarrow q$	Wir beweisen $p \Rightarrow q$:	„Wenn's regnet, ist die Straße nass."
$\neg q$	Wir widerlegen q:	„Die Straße ist nicht nass."
$\neg p$	Wir schließen $\neg p$:	„Es regnet nicht."

Dies entspricht der **Kontraposition**:

$p \Rightarrow q$	$\neg q \Rightarrow \neg p$
$\neg q \Rightarrow \neg p$	$p \Rightarrow q$

Modus ponens, Modus tollens und Kontraposition sind überall nützlich! Sie haben jedoch böse Stiefbrüder und -schwestern: die **Trugschlüsse**. Diese sollen sie weder akzeptieren noch selbst produzieren.

Implikation und Kontraposition

Aufgabe: Sie verfügen über ein aktuelles Stuttgarter Telefonbuch, nicht als elektronische Datenbank, sondern ausgedruckt auf Papier.

Beweisen oder widerlegen Sie folgende Aussage: „Wenn die Nummer mit `456` beginnt, dann beginnt der zugehörige Name nicht mit `Sto`."

Wie würden Sie dies prüfen? naiv-ungeschickt? geschickt-effizient?

Lösung: Eine direkte Prüfung geht *alle* Paare $(\mathrm{Name}, \mathrm{Nummer})$ durch und prüft jeweils die Aussage $(\mathrm{Nummer} = \texttt{456*}) \Rightarrow (\mathrm{Name} \neq \texttt{Sto*})$.

Äquivalent ist die Kontraposition $(\mathrm{Name} = \texttt{Sto*}) \Rightarrow (\mathrm{Nummer} \neq \texttt{456*})$. Es genügt dazu, *nur* die kurze Liste dieser Namen durchzugehen.

Im vorliegenden Szenario ist die zweite Frage leichter zu beantworten als die erste, da das Telefonbuch schon nach Namen sortiert vorliegt!

🙂 Das ist der eigentliche Nutzen der Kontraposition. Beide Aussagen, $p \Rightarrow q$ und $\neg q \Rightarrow \neg q$, sind logisch äquivalent. In der Praxis kommt es jedoch häufig vor, dass eine leichter zugänglich ist als die andere.

🙂 Logik nützt nicht nur in Beweisen, sondern ebenso in vielen Abläufen wie Datenbankanfragen oder allgemein in der Programmierung.

Implikation und Kontraposition

Aufgabe: Für jede ganze Zahl $a \in \mathbb{Z}$ gilt $(2 \mid a) \Leftrightarrow (2 \mid a^2)$.

Lösung: Wir beweisen die Äquivalenz durch die beiden Implikationen.
Wir zeigen $(2 \mid a) \Rightarrow (2 \mid a^2)$ direkt: Ist $a = 2c$ gerade, so auch $a^2 = 4c^2$.
Wir zeigen $(2 \mid a) \Leftarrow (2 \mid a^2)$ durch die Kontraposition $(2 \nmid a) \Rightarrow (2 \nmid a^2)$:
Aus $2 \nmid a$ folgt $a = 2c + 1$ mit $c \in \mathbb{Z}$. Es gilt $a^2 = 4c^2 + 4c + 1$, also $2 \nmid a^2$.

Aufgabe: Für jede ganze Zahl $a \in \mathbb{Z}$ gilt $(3 \mid a) \Leftrightarrow (3 \mid a^2)$.

Lösung: Euklidische Division ergibt $a = 3c + r$ mit $c \in \mathbb{Z}$ und $r \in \mathbb{Z}_3$.

$$\begin{aligned}
a = 3c &\Rightarrow a^2 = 9c^2 &&= 3(3c^2) \\
a = 3c+1 &\Rightarrow a^2 = 9c^2 + 6c + 1 &&= 3(3c^2 + 2c) + 1 \\
a = 3c+2 &\Rightarrow a^2 = 9c^2 + 12c + 4 &&= 3(3c^2 + 4c + 1) + 1
\end{aligned}$$

Das zeigt $(3 \mid a) \Rightarrow (3 \mid a^2)$ direkt und umgekehrt $(3 \mid a) \Leftarrow (3 \mid a^2)$ per Kontraposition. Noch genauer gilt sogar: Aus $3 \nmid a$ folgt $a^2 \operatorname{rem} 3 = 1$.

Implikation und Kontraposition

Aufgabe: Prüfen Sie die Äquivalenz $(p \mid a) \Leftrightarrow (p \mid a^2)$ für p prim.

Lösung: „$\Rightarrow$": Für jede ganze Zahl $p \in \mathbb{Z}$ gilt: Aus $p \mid a$ folgt $p \mid a^2$.
Ausführlich: $p \mid a$ bedeutet $pq = a$ für ein $q \in \mathbb{Z}$, also gilt $p(qa) = a^2$.

„$\Leftarrow$": Ist p prim, so folgt aus $p \mid a \cdot a$ stets $p \mid a$ (siehe Definition A2K).

Alternative: $\mathbb{Z}_p$ ist ein Körper, aus $a \operatorname{rem} p \neq 0$ folgt also $a^2 \operatorname{rem} p \neq 0$.
Diese Rechnung beweist somit die Kontraposition $(p \nmid a) \Rightarrow (p \nmid a^2)$.

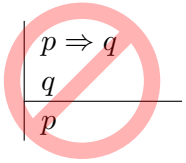
Aufgabe: Prüfen Sie ebenso $(4 \mid a) \overset{?}{\Leftrightarrow} (4 \mid a^2)$ und $(6 \mid a) \overset{?}{\Leftrightarrow} (6 \mid a^2)$.

Lösung: Es gilt „$(4 \mid a) \Rightarrow (4 \mid a^2)$", aber nicht „$(4 \mid a) \Leftarrow (4 \mid a^2)$".
Ein Gegenbeispiel ist $a = 2$: Es gilt $4 \mid 2^2$, aber $4 \nmid 2$.

Es gilt „$(6 \mid a) \Rightarrow (6 \mid a^2)$" und zudem „$(6 \mid a) \Leftarrow (6 \mid a^2)$".
Dies folgt aus dem Fundamentalsatz der Arithmetik (A2J).

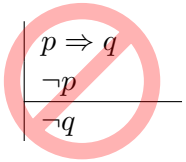
Alternative: Im Ring $\mathbb{Z}_6$ berechnen wir die Quadratabbildung $a \mapsto a^2$ gemäß $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 4$, $3 \mapsto 3$, $4 \mapsto 4$, $5 \mapsto 1$. Diese Rechnung zeigt $(6 \mid a) \Rightarrow (6 \mid a^2)$ und zudem die Umkehrung $(6 \nmid a) \Rightarrow (6 \nmid a^2)$.

Warnung vor Trugschlüssen!



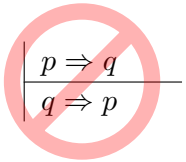
$p \Rightarrow q$
q
p

„Am Ende der Vorlesung trinke ich immer Wasser.“
„Ich trinke jetzt einen Schluck Wasser.“
„Also ist die Vorlesung zu Ende.“



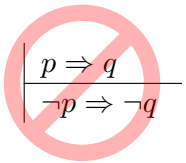
$p \Rightarrow q$
$\neg p$
$\neg q$

„Wenn Sie alles wissen, dann bestehen Sie mit Eins.“
„Sie wissen aber noch nicht alles.“
„Also bestehen Sie nicht mit Eins.“



$p \Rightarrow q$
$q \Rightarrow p$

„Wenn ich Logik verstehe, dann bin ich glücklich.“
„Also, wenn ich glücklich bin, verstehe ich Logik.“



$p \Rightarrow q$
$\neg p \Rightarrow \neg q$

„Wenn Freitag ist, dann tanze ich.“
„Also, wenn nicht Freitag ist, dann tanze ich nicht.“

Warnung vor Trugschlüssen!

Zur Illustration habe ich hier übertrieben einfache Beispiele gewählt, die besonders anschaulich und klar sind: *logisch* und *inhaltlich* falsch.

Das perfide Problem mit Trugschlüssen ist:

- Sie liefern nicht immer *wahre* Aussagen, deshalb sind sie als Schlussregeln ungeeignet.
- Sie liefern aber auch nicht immer *falsche* Aussagen, deshalb sind sie so verlockend und nicht leicht zu entlarven.

Das erklärt und betont noch einmal unsere Definition C2A: Wir wollen Schlussregeln, die aus wahren Aussagen nur wahre Aussagen ableiten. Diese Sicherheit garantieren wir durch die Vorlage von Tautologien!

♦ Definition C2A: Schlussregeln der Aussagenlogik

Alle Schlussregeln der Aussagenlogik entstehen aus den Tautologien mit Hilfe der Schnittregel.

Genau das sind unsere Schlussregeln, nicht mehr und nicht weniger. Alles andere sind Trugschlüsse und potentiell gefährlich.

Warnung vor Trugschlüssen!

Aufgabe: Überprüfen Sie, ob der folgende Schluss logisch gültig ist:

Wenn Herr K. ein Konservativer ist, dann ist er für die Privatisierung.
Herr K. ist für die Privatisierung.

Herr K. ist ein Konservativer.

Lösung: Dies ist eine Instanz des folgenden Musters:

$p \Rightarrow q$
q
---
p

Die Formel $(p \Rightarrow q) \wedge q \Rightarrow p$ ist jedoch keine Tautologie:

p	q	$s = (p \Rightarrow q)$	$t = (s \wedge q)$	$t \Rightarrow p$
1	1	1	1	1
1	0	0	0	1
0	1	1	1	0
0	0	1	0	1

Warnung vor Trugschlüssen!

Der angegebene Schluss ist logisch ungültig, er ist ein Trugschluss! Aus den vorliegenden Prämissen können wir nicht logisch schließen, dass Herr K. ein Konservativer ist. Anschaulich ist das vollkommen klar: Auch manche Nicht-Konservative können für die Privatisierung sein.

So weit so klar. Es gibt allerdings ein mögliches Missverständnis: Der Schluss ist zwar logisch ungültig, die fälschlicherweise abgeleitete Aussage kann aber trotzdem wahr sein. Auch durch falsche Argumente und Schlüsse kann man (zufällig) auf eine wahre Aussage kommen.

Nehmen wir einmal an, auf anderen Wegen erfahren wir, dass Herr K. tatsächlich ein Konservativer ist, etwa durch seine eigene Aussage. „Habe ich doch gleich gewusst, dass Herr K. ein Konservativer ist; er ist ja auch für die Privatisierung, da war mir schon alles klar.“

⚠ Es kommt nicht auf die (hier zufällig richtige) Behauptung an, sondern auf die nachvollziehbare, logisch korrekte Begründung! Das wird außerhalb der Mathematik oft sträflich missachtet. Ehren Sie Ihr logisches Handwerk, schließen Sie richtig!

Beweis durch Widerspruch

C221

Schließlich kommen wir zum berühmt-berüchtigten, aber nützlichen **Beweis durch Widerspruch**, lat. **Reductio ad absurdum**:

$$\frac{(p \wedge \neg q) \Rightarrow \bot}{p \Rightarrow q}$$

Wir führen p und $\neg q$ zum Widerspruch.
Wir schließen $p \Rightarrow q$.

♦ Satz A1F: Irrationalität von $\sqrt{2}$, Euklid ca. 300 v.Chr.

Es gibt keine rationale Zahl $r \in \mathbb{Q}$ mit der Eigenschaft $r^2 = 2$.

Beweis: Angenommen, es gäbe $r \in \mathbb{Q}$ mit $r^2 = 2$.
Rational bedeutet $r = a/b$ mit $a, b \in \mathbb{Z}$ und $b \neq 0$.
Zudem sei der Bruch a/b vollständig gekürzt.
Aus der Gleichung $(a/b)^2 = 2$ folgt $a^2 = 2b^2$.
Daher ist a^2 gerade, also auch a, das heißt $a = 2\bar{a}$ mit $\bar{a} \in \mathbb{Z}$.
Einsetzen in $a^2 = 2b^2$ ergibt $4\bar{a}^2 = 2b^2$, also $2\bar{a}^2 = b^2$.
Daher ist b^2 gerade, also auch b, das heißt $b = 2\bar{b}$ mit $\bar{b} \in \mathbb{Z}$.
Somit ließe sich $a/b = \bar{a}/\bar{b}$ weiter kürzen. Das ist ein Widerspruch!
Also gibt es keine rationale Zahl $r \in \mathbb{Q}$ mit der Eigenschaft $r^2 = 2$. QED

Beweis durch Widerspruch

C222
Erläuterung

Diese trickreich-raffinierte Beweisform heißt auch **indirekter Beweis**. Erfahrungsgemäß bereitet sie anfänglich am meisten Kopfzerbrechen. Formal folgt sie aus Schnittregel und Kontraposition:

$$\begin{aligned} ((p \wedge \neg q) \Rightarrow \bot) &\Leftrightarrow (\top \Rightarrow (\neg p \vee q)) \\ &\Leftrightarrow (\neg p \vee q) \\ &\Leftrightarrow (p \Rightarrow q) \end{aligned}$$

In Worten: Um $p \Rightarrow q$ zu beweisen, nehmen wir $p \wedge \neg q$ an und leiten einen Widerspruch ab. Also können p und $\neg q$ nicht gleichzeitig gelten. Daraus schließen wir: Wenn p gilt, dann muss auch q gelten.

Das klassische Beispiel eines Widerspruchsbeweises ist, wie oben ausgeführt, die Irrationalität von $\sqrt{2}$: Keine rationale Zahl $r \in \mathbb{Q}$ erfüllt die Gleichung $r^2 = 2$. Wir formulieren und beweisen dies indirekt so:

Hier ist p die Voraussetzung $r \in \mathbb{Q}$, und q ist die Folgerung $r^2 \neq 2$.
Zum Beweis nehmen wir p und $\neg q$ an, also $r \in \mathbb{Q}$ und $r^2 = 2$, und führen dies zum Widerspruch. Dies zeigt $(p \wedge \neg q) \Rightarrow \bot$. Wir schließen $p \Rightarrow q$.

Es gibt unendliche viele Primzahlen: durch Widerspruch

C223

Satz C2B: Unendlichkeit der Primzahlmenge

In den natürlichen Zahlen $\mathbb{N}_{\geq 1}$ gibt es unendlich viele Primzahlen.

Manchmal wird dies durch Widerspruch bewiesen, das ist möglich:

Beweis durch Widerspruch „nach Euklid“: Angenommen, es gäbe nur endlich viele Primzahlen $2 = p_1 < p_2 < \cdots < p_n$. Wir untersuchen $q = p_1 \cdot p_2 \cdots p_n + 1$. Keine der Primzahlen p_i teilt q. Also ist q prim.
Wegen $q > p_n$ ist q eine weitere Primzahl. Widerspruch! QED

Fragen: M Ist dieser Beweis gültig? I Können Sie damit arbeiten?
L Was entgegnen Sie dem folgenden, bitter enttäuschten Vorwurf?

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

Ja, der Beweis ist logisch korrekt, doch eher schlechter Stil:

- Historisch falsch: So hat Euklid den Satz nicht bewiesen!
- Didaktisch unklug: Der Beweis provoziert Missverständnisse!
- Algorithmisch nutzlos: Es gelingt besser direkt und konstruktiv!

Es gibt unendliche viele Primzahlen: konstruktiver Beweis

C224

Zu $n \in \mathbb{N}_{\geq 2}$ sei $\operatorname{lpf}(n) := \min\{\, p \in \mathbb{N}_{\geq 2} \mid p \mid n \,\}$ der kleinste Faktor ≥ 2.
Dies ist eine Primzahl, da ≥ 2 und unzerlegbar: $\operatorname{lpf} =$ least prime factor.

Satz C2C: Unendlichkeit der Primzahlmenge, konstruktiv

In den natürlichen Zahlen $\mathbb{N}_{\geq 1}$ gibt es unendlich viele Primzahlen:
Zu Primzahlen $p_1, p_2, \ldots, p_n$ ist $\operatorname{lpf}(p_1 \cdot p_2 \cdots p_n + 1)$ eine weitere.

Beweis: Wir haben $p = p_1 \cdot p_2 \cdots p_n \geq 1$ und $q = p + 1 \geq 2$. Dazu sei $q_1 = \operatorname{lpf}(q)$ der kleinste Primfaktor. Wir zeigen $q_1 \notin \{p_1, p_2, \ldots, p_n\}$:
Es gilt $q \operatorname{rem} q_1 = 0$ und $q \operatorname{rem} p_i = 1$, also $q_1 \neq p_i$. QED

☺ Dieser Beweis gefällt mir wesentlich besser. Er liefert objektiv mehr:

Algorithmus: Zu jeder Menge $M = \{\, p_1, p_2, \ldots, p_n \,\}$ von Primzahlen erhalten wir die echt größere Menge $M' = M \cup \{\, \operatorname{lpf}(p_1 p_2 \cdots p_n + 1) \,\}$.

Beispiel: $\{\} \mapsto \{2\} \mapsto \{2,3\} \mapsto \{2,3,7\} \mapsto \{2,3,7,43\} \mapsto \{2,3,7,13,43\}$ $\mapsto \{2,3,7,13,43,53\} \mapsto \ldots$ Dies können wir beliebig lange fortführen!

M So entsteht die **Euklid–Mullin–Folge**, siehe `oeis.org/A000945`.
I Die effiziente Suche nach großen Primzahlen ist ein eigenes Gebiet.

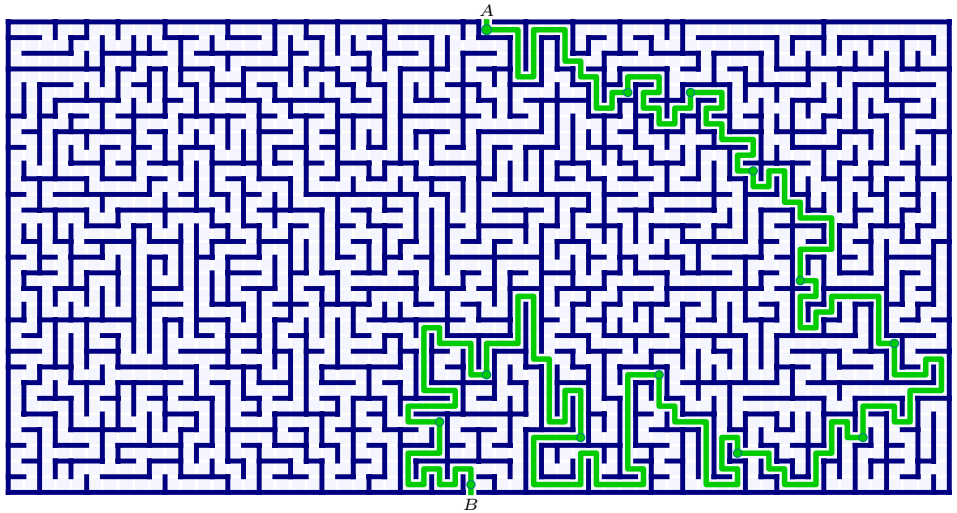
Ein Beweis ist eine Abfolge logischer Schlüsse.

C225

Satz	Beh	Voraussetzung
		Folgerung
	Beweis	

Algo	Spez	Eingabe
		Ausgabe
	Methode	

Lösung	Prob	Start
		Ziel
	Weg	



Ein Beweis ist eine Abfolge logischer Schlüsse.

C226
Erläuterung

Ein Satz besteht immer aus zwei Teilen: Erstens seiner Behauptung „Wenn A, dann B“, also einer Voraussetzung A und einer Folgerung B. Zweitens aus einem Beweis, also einer Kette von logischen Schlüssen: Ausgehend von der Voraussetzung A wird die Folgerung B geschlossen.

Auch ein Algorithmus hat immer zwei Teile: Erstens seine Spezifikation, sie präzisiert die geforderte Eingabe und die zugesicherte Ausgabe. Zweitens eine Methode, also eine Kette von elementaren Operationen: Ausgehend von der Eingabe A wird die Ausgabe B produziert.

Ganz allgemein verläuft so die Lösung jedes Problems, etwa das Finden eines Weges in einem Labyrinth: Das Problem besteht aus der Angabe von Start und Ziel. Der Weg führt schrittweise vom Start zum Ziel. Diese graphische Analogie ist erstaunlich präzise und treffsicher.

Zwecks Aufgabenteilung werden Behauptung und Beweis getrennt, ebenso Spezifikation und Methode, allgemein Problem und Lösung. Insbesondere kann es auch mehrere mögliche Beweise / Methoden / Lösungen geben, oder noch keine/r ist bekannt und wird gesucht.

Beweisen = Berechnen = Lösen

C227
Erläuterung

Wie lösen Sie ein mathematisches Problem? George Pólya erklärt hierzu in seinem Buch *How to solve it* die folgenden vier Phasen:

1. Zuerst müssen Sie das vorliegende Problem verstehen:
   Was ist das Ziel? Wo liegt der Start?
2. Anschließend machen Sie sich einen Plan:
   Was sind mögliche Wege vom Start zum Ziel?
3. Führen Sie Ihren Plan sorgfältig aus:
   Führt Ihr vermuteter Weg vom Start zum Ziel?
4. Schließlich schauen Sie zurück:
   Was lässt sich vereinfachen oder verbessern?

Das Suchen eines Weges ist meist kein geradliniger Prozess, sondern eher ein verzweigtes Erkunden und planvolles Probieren. Dazu benötigen Sie Kreativität und Sorgfalt, Geduld und Erfahrung! Es lässt sich erlernen, und dies erfordert vor allem viel eigene Übung.

Probleme zu lösen lernen Sie nur, indem Sie selbst Probleme lösen.

Intuition oder Präzision? Beides!

C228
Erläuterung

Anschauung und Intuition sind überall nützlich, auch in der Mathematik. Sie bieten Motivation und Orientierung sowie schnelle Kommunikation.

Präzision und Formalisierung sind Markenzeichen mathematischer Sorgfalt; sie bieten Sicherheit, Vollständigkeit und dauerhafte Gültigkeit.

Für mathematische Arbeit benötigen Sie beides, Intuition und Präzision.

Idealerweise erkläre ich Ihnen beides. Das ist allerdings aufwändig.

Manchmal genügt die Anschauung: Ich nenne die Idee, Sie führen sie aus (und nutzen dabei Ihre bisherigen Fähigkeiten zur Formalisierung).

Manchmal genügt die Formalisierung: Ich führe sie aus, Sie fassen sie zusammen (und entwickeln dabei Ihre Anschauung und Intuition).

Auf dem Weg von der Idee / Vermutung zum Satz / Beweis wird die erste Formulierung meist präzisiert, manchmal auch angepasst und korrigiert. In der Ausführung (Rechnung, Beweis) stellt sich nämlich häufig heraus, dass zunächst Sonderfälle oder Einschränkungen vergessen wurden.

Aussageformen aka Prädikate

Beispiel: Über den natürlichen Zahlen $\mathbb{N}$ betrachten wir die Ausdrücke

$$\begin{aligned} p(x) &:\Leftrightarrow (5 \leq x) \wedge (x < 10), \\ q(x,y) &:\Leftrightarrow x^2 = y. \end{aligned}$$

Hier ist p zunächst noch keine Aussage, also weder wahr noch falsch, sondern eine **Aussageform** oder ein **Prädikat** für natürliche Zahlen.

Erst durch Einsetzen einer natürlichen Zahl $n \in \mathbb{N}$ wird die Aussageform p zur Aussage $p(n)$; diese Aussage kann nun wahr oder falsch sein.

Beispiele: Die Aussage $p(9)$ ist wahr, doch $p(10)$ ist falsch.
Die Aussage $q(2,4)$ ist wahr, doch die Aussage $q(4,2)$ ist falsch.
Hingegen ist $q(x,4)$ eine Aussageform in der noch freien Variablen x.

Definition C3A: Aussageform aka Prädikat

Ein **Prädikat** $p(x,y,\dots)$ in den Variablen $x,y,\dots$ ist ein Ausdruck, der zu einer Aussage wird durch Spezialisieren $(x,y,\dots) \mapsto (\alpha,\beta,\dots)$ der Variablen $x,y,\dots$ zu konkreten Objekten $\alpha,\beta,\dots$ im Diskursuniversum.

Aussageformen aka Prädikate

Wir nennen hierbei das Prädikat $p(x)$ **einstellig**, wenn es nur eine freie Variable x enthält. Ebenso definieren wir **zweistellige Prädikate** $q(x,y)$ oder **dreistellige Prädikate** $r(x,y,z)$ etc. Ein **nullstelliges Prädikat** p ist ganz einfach eine Aussage, denn es hängt von keiner Variablen ab.

Wie schon bei Aussagen (C1A) lassen wir bei Prädikaten (C3A) vorerst offen, wie genau diese Ausdrücke aufgebaut sind. Zunächst nutzen wir naiv die Umgangssprache; je nach Anwendung präzisieren wir dann die verwendete Sprache (Syntax), im obigen Beispiel $(\mathbb{N},+,\cdot,\leq)$.

Dabei muss unzweifelhaft klar sein, über welche Objekte wir sprechen! Typische Beispiele sind die natürlichen Zahlen $\mathbb{N}$, die ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$, die komplexen Zahlen $\mathbb{C}$ … oder ganz allgemein über eine beliebige Menge Ω von Objekten.

Dies nennen wir das **Diskursuniversum**, engl. *universe of discourse*. Es umfasst jeweils alle Objekte, über die wir gerade sprechen wollen.

Aussageformen aka Prädikate

⚠ Zu jeder Variablen x müssen wir festlegen, welche Menge Ω_x sie durchläuft, also welche Ersetzungen $x \mapsto \alpha \in \Omega_x$ vorgesehen sind.

Beispiel: Wir betrachten weiterhin die obigen Prädikate.

$$\begin{aligned} p(x) &:\Leftrightarrow (5 \leq x) \wedge (x < 10) \\ q(x,y) &:\Leftrightarrow x^2 = y \end{aligned}$$

Diese können wir als Prädikate für natürliche Zahlen nutzen, das heißt, wir können x,y durch natürliche Zahlen ersetzen.

Alternativ können wir p und q als Prädikate für ganze, rationale oder reelle Zahlen nutzen: Durch Ersetzen von x,y durch reelle Zahlen $\alpha,\beta \in \mathbb{R}$ erhalten wir eine Aussage; diese kann wahr oder falsch sein. Für komplexe Zahlen $x \in \mathbb{C} \smallsetminus \mathbb{R}$ hat p keinen Sinn mehr, q jedoch schon.

Hingegen hat es überhaupt keinen Sinn, für x,y Farben einzusetzen, oder Personennamen oder MP3-Dateien oder Python-Programme; auch für diese Daten sind Prädikate denkbar, aber p,q gehören nicht dazu.

Aussageformen aka Prädikate

Wir arbeiten über dem Ring $(\mathbb{Z},+,0,\cdot,1)$ der ganzen Zahlen; implizit ist dabei auch die Vergleichsoperation $=$ eingeschlossen.

Aufgabe: Formulieren Sie das Prädikat $d(a,c)$ für „a teilt c in $\mathbb{Z}$“ und das Prädikat $u(a)$ für „a ist unzerlegbar in $\mathbb{Z}$“ mit den Daten $(\mathbb{Z},+,0,\cdot,1,=)$.

Lösung: Wir nutzen die Umgangssprache, denn erst die folgende Definition C3B bietet uns eine hilfreiche formale Ausdrucksweise.

$$\begin{aligned} d(a,c) &= (\text{Es existiert } b \in \mathbb{Z}, \text{ sodass } a \cdot b = c \text{ gilt.}) \\ u(a) &= (\text{Für alle } b,c \in \mathbb{Z} \text{ gilt:} \\ &\qquad \text{Aus } a = b \cdot c \text{ folgt entweder } b = \pm 1 \text{ oder } c = \pm 1.) \end{aligned}$$

Die Quantoren „es existiert“ und „für alle“ benötigen wir sehr häufig. Daher lohnt es sich, hierfür eine bequeme und präzise Schreibweise einzuführen und die zugehörigen Rechenregeln genau zu untersuchen. Genau das ist unser Ziel in diesem Abschnitt zu Quantoren.

Existenz- und Allquantor

In der Mathematik nutzen wir häufig **Quantoren**. Diese helfen, komplizierte Sachverhalte präzise und effizient auszudrücken.

Definition C3B: Existenz- und Allquantor

Aus jedem Prädikat $p(x)$ erhalten wir folgende Aussagen:

Aussage	Bedeutung	Name
$(\forall x : p(x))$	Für jedes x gilt die Aussage $p(x)$.	Allquantor
$(\exists x : p(x))$	Für mindestens ein x gilt $p(x)$.	Existenzquantor

In diesen Aussagen ist die Variable x nicht mehr frei sondern gebunden; sie kann nun nicht mehr durch ein konkretes Objekt α ersetzt werden. Sie kann jedoch überall durch eine neue Variable y ersetzt werden: $\forall x : p(x)$ und $\forall y : p(y)$ sind äquivalent, ebenso $\exists x : p(x)$ und $\exists y : p(y)$.

Ist $q(x, y, \dots)$ ein Prädikat in mehreren Variablen $x, y, \dots$, so wird in $\forall x : q(x, y, \dots)$ und $\exists x : q(x, y, \dots)$ nur die Variable x gebunden: Wir erhalten Aussageformen in den verbleibenden Variablen $y, \dots$.

Existenz- und Allquantor

Sprechen wir nur über endlich viele Objekte $\Omega = \{a_1, a_2, \dots, a_n\}$, so gilt:

$$\begin{aligned} \forall x \in \Omega : p(x) &\quad\Leftrightarrow\quad p(a_1) \wedge p(a_2) \wedge \dots \wedge p(a_n) \\ \exists x \in \Omega : p(x) &\quad\Leftrightarrow\quad p(a_1) \vee p(a_2) \vee \dots \vee p(a_n) \end{aligned}$$

In der Literatur finden Sie daher auch folgende Schreibweisen:

$$\bigwedge_{i=1}^{n} p(a_i) \quad \text{oder allgemein} \quad \bigwedge_{x\in\Omega} p(x) \quad \text{für} \quad \forall x \in \Omega : p(x)$$

$$\bigvee_{i=1}^{n} p(a_i) \quad \text{oder allgemein} \quad \bigvee_{x\in\Omega} p(x) \quad \text{für} \quad \exists x \in \Omega : p(x)$$

Wir nutzen die Wahrheitswerte $0 =$ falsch oder $1 =$ wahr, wobei $0 < 1$. Damit erklären wir zu Quantoren die Wahrheitswerte wie folgt:

$$\begin{aligned} \langle\, \forall x : p(x) \,\rangle &:= \min_{x\in\Omega} \langle\, p(x) \,\rangle \quad \in \{0, 1\} \\ \langle\, \exists x : p(x) \,\rangle &:= \max_{x\in\Omega} \langle\, p(x) \,\rangle \quad \in \{0, 1\} \end{aligned}$$

☺ Die explizite Angabe der Menge Ω ist redundant, aber sehr hilfreich.

Existenz- und Allquantor

Beispiel: Wir arbeiten im Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ der ganzen Zahlen. Formulieren Sie teilbar, invertierbar, unzerlegbar und prim im Ring $\mathbb{Z}$ sowie Euklids Lemma (1) umgangssprachlich und (2) mit Quantoren.

$$\begin{aligned} a \mid c \quad &:\Leftrightarrow\ (\exists b\,(a \cdot b = c)) \\ &\Leftrightarrow\ \exists b : a \cdot b = c \\ \text{invertierbar}(a) \quad &:\Leftrightarrow\ \exists b : a \cdot b = 1 \\ &\Leftrightarrow\ a \mid 1 \\ \text{unzerlegbar}(a) \quad &:\Leftrightarrow\ (\forall b\,(\forall c\,((a = b \cdot c) \Rightarrow ((b \mid 1) \,\dot\vee\, (c \mid 1))))) \\ &\Leftrightarrow\ \forall b, c : a = b \cdot c \ \Rightarrow\ b \mid 1 \,\dot\vee\, c \mid 1 \\ \text{prim}(a) \quad &:\Leftrightarrow\ \neg(a \mid 1) \wedge (\forall b\,(\forall c\,((a \mid b \cdot c) \Rightarrow ((a \mid b) \vee (a \mid c))))) \\ &\Leftrightarrow\ a \nmid 1 \ \wedge\ \forall b, c : a \mid b \cdot c \ \Rightarrow\ a \mid b \vee a \mid c \end{aligned}$$

Euklids Lemma über $\mathbb{Z}$ sagt $\forall a : \text{prim}(a) \Leftrightarrow (a = 0 \,\dot\vee\, \text{unzerlegbar}(a))$.

Wir dürfen Klammern weglassen, solange die Bedeutung klar bleibt. Das Trennzeichen ':' dient der besseren Lesbarkeit und darf entfallen. Die Abkürzung $\forall x, y$ steht für $\forall x\,\forall y$. Ebenso steht $\exists x, y$ kurz für $\exists x\,\exists y$.

Existenz- und Allquantor

Um Klammern zu sparen nutzen wir „Potenz vor Punkt vor Strich". Bei logischen Operatoren vereinbaren wir entsprechend die Rangfolge Negation vor Konjunktion vor Disjunktion vor Implikation vor Äquivalenz.

Aufgabe: Prüfen Sie anhand obiger Definitionen sorgfältig nach, ob die Zahl $a = 0, 1, 2$ in $\mathbb{Z}$ unzerlegbar bzw. prim ist. Das hilft!

Lösung: Wir setzen $a = 0, 1, 2$ in diese beiden Prädikate ein:

$$\begin{aligned} &\text{unzerlegbar}(0) \ \Leftrightarrow\ \forall b, c : 0 = b \cdot c \ \Rightarrow\ b \mid 1 \,\dot\vee\, c \mid 1 && \text{falsch (0)} \\ &\text{prim}(0) \ \Leftrightarrow\ 0 \nmid 1 \ \wedge\ \forall b, c : 0 \mid b \cdot c \ \Rightarrow\ 0 \mid b \vee 0 \mid c && \text{wahr} \\ &\text{unzerlegbar}(1) \ \Leftrightarrow\ \forall b, c : 1 = b \cdot c \ \Rightarrow\ b \mid 1 \,\dot\vee\, c \mid 1 && \text{falsch (1)} \\ &\text{prim}(1) \ \Leftrightarrow\ 1 \nmid 1 \ \wedge\ \forall b, c : 1 \mid b \cdot c \ \Rightarrow\ 1 \mid b \vee 1 \mid c && \text{falsch (1')} \\ &\text{unzerlegbar}(2) \ \Leftrightarrow\ \forall b, c : 2 = b \cdot c \ \Rightarrow\ b \mid 1 \,\dot\vee\, c \mid 1 && \text{wahr} \\ &\text{prim}(2) \ \Leftrightarrow\ 2 \nmid 1 \ \wedge\ \forall b, c : 2 \mid b \cdot c \ \Rightarrow\ 2 \mid b \vee 2 \mid c && \text{wahr} \end{aligned}$$

Beweis durch Gegenbeispiel: (0) $(b, c) = (0, 0)$ und (1) $(b, c) = (1, 1)$.
(1') Die Forderung $a \nmid 1$ schließt alle invertierbaren Elemente aus.

Beweisverfahren für Existenz- und Allquantor

Quantoren erhalten ihre Bedeutung durch die folgenden Schlussregeln.
Für den Allquantor $\forall$ nutzen wir **Spezialisieren** und **Verallgemeinern**:

$$\frac{\forall x : p(x)}{p(\alpha) \text{ für jedes } \alpha \text{ (beliebig gewählt)}} \qquad \frac{p(\alpha) \text{ für jedes } \alpha \text{ / für alle } \alpha}{\forall x : p(x)}$$

Für den Existenzquantor $\exists$ nutzen wir **Auswählen** und **Konstruieren**:

$$\frac{\exists x : p(x)}{p(\alpha) \text{ für ein } \alpha \text{ (geeignet gewählt)}} \qquad \frac{p(\alpha) \text{ für (mindestens) ein } \alpha}{\exists x : p(x)}$$

Das präzisiert die Bedeutung von „für alle“ und „es existiert“.

Links steht jeweils, wie wir eine quantifizierte Aussage *nutzen*,
also als Voraussetzung einsetzen und daraus Folgerungen ziehen.

Rechts steht, wie wir die quantifizierte Aussage *beweisen*,
also als eine Folgerung aus gegebenem Wissen ableiten.

Rechenregeln für Existenz- und Allquantor

Die Reihenfolge der Quantoren ist wesentlich! Beispiel $p(a,b) = (a < b)$:

$$\forall a : \exists b : a < b \quad \text{also ausgeschrieben} \quad \forall a \underbrace{(\exists b\,(a < b))}_{q(a)}$$

$$\exists b : \forall a : a < b \quad \text{also ausgeschrieben} \quad \exists b \underbrace{(\forall a\,(a < b))}_{r(b)}$$

In $(\mathbb{Z}, <)$ ist die erste Aussage wahr, die zweite jedoch falsch!
Allquantoren vertauschen untereinander, ebenso Existenzquantoren:

$$\begin{aligned} \forall x : \forall y : p(x,y) &\quad\Leftrightarrow\quad \forall y : \forall x : p(x,y) \\ \exists x : \exists y : p(x,y) &\quad\Leftrightarrow\quad \exists y : \exists x : p(x,y) \end{aligned}$$

Wenn wir einen Allquantor über einen Existenzquantor nach vorne
ziehen, so bleibt die Aussage wahr, wird dabei aber schwächer:

$$\exists x : \forall y : p(x,y) \quad \underset{\not\Leftarrow}{\Rightarrow} \quad \forall y : \exists x : p(x,y)$$

Beispiel $p(x,y) =$ „x ist Mutter von y“: Zu jedem Menschen existiert eine
Mutter, aber es existiert keine Mutter zu allen Menschen gemeinsam.

Rechenregeln für Existenz- und Allquantor

Wir kennen die beiden Regeln von **De Morgan** (C135, endlicher Fall):

$$\begin{aligned} \neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) &\quad\Leftrightarrow\quad (\neg p_1) \vee (\neg p_2) \vee \cdots \vee (\neg p_n) \\ \neg(p_1 \vee p_2 \vee \cdots \vee p_n) &\quad\Leftrightarrow\quad (\neg p_1) \wedge (\neg p_2) \wedge \cdots \wedge (\neg p_n) \end{aligned}$$

Allgemein gelten die Regeln von **De Morgan für Quantoren**:

$$\begin{aligned} \neg(\forall x : p(x)) &\quad\Leftrightarrow\quad \exists x : (\neg p(x)) \\ \neg(\exists x : p(x)) &\quad\Leftrightarrow\quad \forall x : (\neg p(x)) \end{aligned}$$

Um eine Allaussage $\forall x : p(x)$ zu *beweisen*, müssen wir $p(\alpha)$ für jedes α
nachweisen. Um sie zu *widerlegen*, genügt ein einziges Gegenbeispiel;
das ist genau die Aussage der ersten Regel von De Morgan.

Die Existenzaussage $\exists x : p(x)$ beweisen wir, indem wir ein α vorweisen,
das $p(\alpha)$ erfüllt. Die Negation $\neg\exists x : p(x)$ besagt, kein α erfüllt $p(\alpha)$;
das ist äquivalent zu $\forall x : \neg p(x)$, also alle α erfüllen nicht $p(\alpha)$.

Rechenregeln für Existenz- und Allquantor

Ebenso verallgemeinern sich die Distributivgesetze (C135):

$$\begin{aligned} (\forall x : p(x)) \vee q &\quad\Leftrightarrow\quad \forall x : (p(x) \vee q) \\ (\exists x : p(x)) \wedge q &\quad\Leftrightarrow\quad \exists x : (p(x) \wedge q) \end{aligned}$$

Hier helfen die Klammern zur Präzisierung. Weiterhin gilt:

$$\begin{aligned} (\forall x : p(x)) \wedge q &\quad\Leftrightarrow\quad \forall x : (p(x) \wedge q) \\ (\exists x : p(x)) \vee q &\quad\Leftrightarrow\quad \exists x : (p(x) \vee q) \end{aligned}$$

Ebenso verhalten sich Quantoren bezüglich Implikationen:

$$\begin{aligned} (\forall x : (p \Rightarrow q(x))) &\quad\Leftrightarrow\quad (p \Rightarrow (\forall x : q(x))) \\ (\exists x : (p \Rightarrow q(x))) &\quad\Leftrightarrow\quad (p \Rightarrow (\exists x : q(x))) \\ (\forall x : (p(x) \Rightarrow q)) &\quad\Leftrightarrow\quad ((\exists x : p(x)) \Rightarrow q) \\ (\exists x : (p(x) \Rightarrow q)) &\quad\Leftrightarrow\quad ((\forall x : p(x)) \Rightarrow q) \end{aligned}$$

Das folgt aus den obigen Regeln dank $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$. Wir nutzen
diese Regeln insbesondere zum **Beweis durch Fallunterscheidung**.

Existenz und Eindeutigkeit: Definition

C313

Definition C3C: Existenz und Eindeutigkeit als Quantor

Für $\exists x$ sagen wir zur Betonung auch „Es existiert *mindestens* ein x“.

$$\exists^{\geq 1} x : p(x) \quad :\Leftrightarrow \quad \exists x : p(x)$$

Wir definieren den Quantor „Es existiert *höchstens* ein x“ wie folgt:

$$\exists^{\leq 1} x : p(x) \quad :\Leftrightarrow \quad (\forall x, y : (p(x) \wedge p(y)) \Rightarrow (x = y))$$

Wir definieren den Quantor „Es existiert *genau* ein x“ wie folgt:

$$\exists! \, x : p(x) \quad :\Leftrightarrow \quad (\exists x : p(x)) \wedge (\forall x, y : (p(x) \wedge p(y)) \Rightarrow (x = y))$$

Manche Autoren schreiben statt $\exists! \, x$ daher suggestiv $\exists^{=1} x$.

Beispiele:

Aussage	über $\mathbb{Q}$	über $\mathbb{R}_{\geq 0}$	über $\mathbb{R}$
$\exists^{\geq 1} x \,:\, x^2 = 2$	falsch	wahr	wahr
$\exists^{\leq 1} x \,:\, x^2 = 2$	wahr	wahr	falsch
$\exists^{=1} x \,:\, x^2 = 2$	falsch	wahr	falsch

Existenz und Eindeutigkeit: ein Beispiel

C314

Aufgabe: Sei $(M, \cdot, 1)$ ein Monoid. Formulieren Sie mit Quantoren:
(1) $\mathrm{Inv}(a)$: „Das Element $a \in M$ ist im Monoid $(M, \cdot, 1)$ invertierbar.“
(2) $\mathrm{Lös}(a)$: „Für jedes $b \in M$ ist $a \cdot x = b$ in M eindeutig lösbar.“
(3) Beweisen Sie schließlich: $\forall a \in M : (\mathrm{Inv}(a) \Rightarrow \mathrm{Lös}(a))$

Lösung: Diese Prädikate lauten in Quantorenschreibweise:

$$\begin{aligned} &(1) \quad \mathrm{Inv}(a) \quad :\Leftrightarrow \quad \exists a' \in M \,:\, a \cdot a' = 1 \wedge a' \cdot a = 1 \\ &(2) \quad \mathrm{Lös}(a) \quad :\Leftrightarrow \quad \forall b \in M \;\; \exists! x \in M \,:\, a \cdot x = b \end{aligned}$$

(3) Vorgelegt seien $a, a' \in M$ mit $a \cdot a' = 1$ und $a' \cdot a = 1$. Sei $b \in M$.
(3a) Existenz: Das Element $x := a' \cdot b$ erfüllt $a \cdot x = b$, denn

$$a \cdot x \overset{\text{Def}}{=} a \cdot (a' \cdot b) \overset{\text{Ass}}{=} (a \cdot a') \cdot b \overset{\text{rInv}}{=} 1 \cdot b \overset{\text{lNtr}}{=} b.$$

(3b) Eindeutigkeit: Für $x, y \in M$ gelte $a \cdot x = b$ und $a \cdot y = b$. Dann folgt:

$$\begin{aligned} x \overset{\text{lNtr}}{=} 1 \cdot x \overset{\text{lInv}}{=} (a' \cdot a) \cdot x \overset{\text{Ass}}{=} a' \cdot (a \cdot x) \\ \overset{\text{Vor}}{=} a' \cdot (a \cdot y) \overset{\text{Ass}}{=} (a' \cdot a) \cdot y \overset{\text{lInv}}{=} 1 \cdot y \overset{\text{lNtr}}{=} y. \end{aligned}$$

Existenz und Eindeutigkeit: weitere Beispiele

C315

Die Frage der Existenz und Eindeutigkeit begegnet uns sehr häufig in der Mathematik, und eigentlich auch sonst überall bei der Lösung von relevanten Problemen. Sie kennen bereits erste wichtige Beispiele:

Division mit Rest (A2A). Zu je zwei ganzen Zahlen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}^*$ existiert genau ein Paar $q, r \in \mathbb{Z}$ mit $a = bq + r$ und $0 \leq r < |b|$.

Zifferndarstellung (A2B). Zu jeder natürlichen Zahl $n \in \mathbb{N}$ existiert genau eine Zifferndarstellung $x \in \mathbb{Z}_B^{(\mathbb{N})}$ zur Basis $B \in \mathbb{N}_{\geq 2}$.

Fundamentalsatz der Arithmetik (A2J). Zu jeder natürlichen Zahl $a \in \mathbb{N}_{\geq 1}$ existiert genau eine Primfaktorzerlegung, also eine Familie von Primzahlen $p_1 \leq p_2 \leq \cdots \leq p_n$ in $\mathbb{N}$ mit der Eigenschaft $a = p_1 p_2 \cdots p_n$.

Invertierbarkeit von Matrizen (B2D). Sei $A \in \mathbb{K}^{n \times n}$ invertierbar und $b \in \mathbb{K}^n$. Zur Gleichung $Ax = b$ existiert genau eine Lösung $x \in \mathbb{K}^n$.

Lagrange–Interpolation (B3A). Durch beliebige Datenpunkte $(x_0, y_0), \ldots, (x_n, y_n) \in \mathbb{K}^2$ verläuft genau ein Polynom $P \in \mathbb{K}[X]_{\leq n}$.

Minimum-Maximum-Prinzip (B3B). Zu jedem Spielbrett $\Omega \subset \mathbb{Z}^2$ und beliebigen Randdaten existiert genau eine Gewinnerwartung $u : \Omega \to \mathbb{R}$.

Existenz und Eindeutigkeit: typisches Alltagsbeispiel

C316

Beispiel: Ein Beispiel aus dem Alltag, nach einer wahren Begebenheit: „Zum Wandern treffen wir uns früh um 8 Uhr am Parkplatz im Wald.“

Dahinter stecken zwei wichtige Annahmen / Forderungen / Probleme:

1. Es gibt tatsächlich einen Parkplatz im Wald
2. . . . und er ist eindeutig; alle meinen denselben.

Andernfalls ist die Verabredung schlecht formuliert und wird scheitern. Existenz und Eindeutigkeit sind meist die unabdingbare Grundlage!

Praktisch gesehen schließen sich noch zwei weitere Probleme an:

3. Wir finden effektiv einen Weg zu dem (!) Parkplatz im Wald
4. . . . und zwar ausreichend effizient, schnell genug bis 8 Uhr.

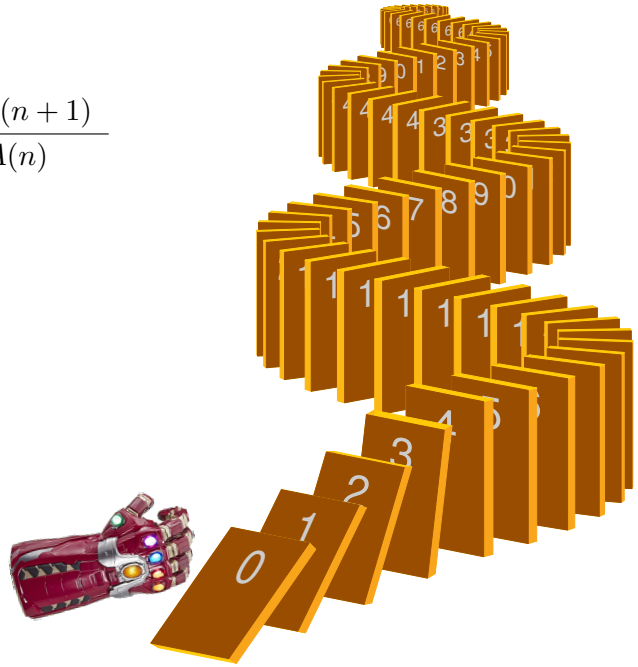
🙂 Genauso verhält es sich nahezu immer beim Lösen von Problemen, insbesondere in der Mathematik, aber erstaunlich oft auch überall sonst:

Das gestellte Problem sollte idealerweise genau eine Lösung haben, wir wollen diese effektiv herstellen und zudem möglichst effizient.

Welche der obigen Probleme können Sie lösen? effektiv oder effizient?

Vollständige Induktion: the road to infinity!

$$\begin{array}{l} A(0) \\ A(n) \Rightarrow A(n+1) \\ \hline \forall n \in \mathbb{N} : A(n) \end{array}$$



Vollständige Induktion: the road to infinity!

Sie wollen für jede natürliche Zahl $n \in \mathbb{N}$ die Aussage $A(n)$ beweisen.
Das ist insgesamt eine unendliche Familie $(A(n))_{n\in\mathbb{N}}$ von Aussagen!
Ist das überhaupt möglich? Wie können Sie das jemals erreichen?

☹ Sie haben, wie jeder Mensch, natürlich nur endlich viel Zeit!
Es gibt demgegenüber aber unendlich viele natürliche Zahlen.

Sie können nicht selbst hingehen und alles einzeln prüfen,
das ist zu weit, zu viel, zu lang, Sie würden damit nie fertig.

Sie benötigen eine Maschine, die das effizient für Sie erledigt.
Die vollständige Induktion leistet genau das, klar und effizient!

☺ Per Induktion beweisen Sie die Aussage $A(n)$ für jedes $n \in \mathbb{N}$:

$A(0)$	Induktionsanfang: Sie beweisen die Aussage $A(0)$.
$A(n) \Rightarrow A(n+1)$	Induktionsschritt: Sie beweisen $A(n) \Rightarrow A(n+1)$.
$\forall n \in \mathbb{N} : A(n)$	Induktionsschluss: die Allaussage $\forall n \in \mathbb{N} : A(n)$.

Der Induktionsschritt ist die Implikation $A(n) \Rightarrow A(n+1)$, dabei ist $A(n)$ die (Induktions)Voraussetzung und $A(n+1)$ die (Induktions)Folgerung.

Vollständige Induktion: the road to infinity!

Satz C4A: Prinzip der vollständigen Induktion, erste Fassung

Sei $(A(n))_{n\in\mathbb{N}}$ eine Familie von Aussagen $A(n)$ indiziert durch $n \in \mathbb{N}$.
Dann sind die folgenden beiden Aussagen zueinander äquivalent:

(1) Für jede natürliche Zahl $n \in \mathbb{N}$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in \mathbb{N} : A(n)$$

(2) Es gilt der Induktionsanfang $A(0)$ und für jedes $n \in \mathbb{N}$
zudem der Induktionsschritt $A(n) \Rightarrow A(n+1)$, kurz:

$$A(0) \ \wedge \ \forall n \in \mathbb{N} : [\, A(n) \Rightarrow A(n+1) \,]$$

Beweis: Die Implikation „(1) ⇒ (2)“ ist klar, genauer sogar trivial.
Die Implikation „(2) ⇒ (1)“ ist Teil der Dedekind–Peano–Axiome (A1B):
Vorgelegt sei $E \subseteq \mathbb{N}$, hier die Erfüllungsmenge $E = \{\, n \in \mathbb{N} \mid A(n) \,\}$
aller natürlichen Zahlen $n \in \mathbb{N}$, für die die Aussage $A(n)$ wahr ist.
Gilt $0 \in E$ und für jedes $n \in E$ auch $(n+1) \in E$, so folgt $E = \mathbb{N}$. QED

Vollständige Induktion: the road to infinity!

Unter **Induktion** verstehen wir fast immer die **vollständige Induktion**.
Andere Gebiete nutzen vor allem die unvollständige Induktion, also den Schluss von speziellen Beispielen auf das (vermutete) Allgemeine; als Gegenstück schließt die Deduktion vom Allgemeinen auf das Spezielle.

Die Physik zum Beispiel nutzt Induktion zur Erstellung von Hypothesen, diese werden experimentell getestet, entweder *erhärtet* oder *widerlegt*, jedoch prinzipiell niemals vollständig *bewiesen*. Die Deduktion leitet umgekehrt Vorhersagen ab, auch diese werden experimentell getestet.

Das Prinzip der vollständigen Induktion ist an sich nichts Schwieriges, es ist als Fundament in die Definition der natürlichen Zahlen eingebaut.

Zur Erinnerung an Satz A1B über $(\mathbb{N}, 0, s)$: Die Nachfolgerabbildung $s : \mathbb{N} \to \mathbb{N} : n \mapsto n+1$ erfüllt die **Dedekind–Peano–Axiome**:

- D0: Null ist kein Nachfolger: $0 \notin s(\mathbb{N})$, also $\forall n \in \mathbb{N} : n+1 \neq 0$.
- D1: Die Abbildung s ist injektiv: $\forall p, q \in \mathbb{N} : p \neq q \Rightarrow p+1 \neq q+1$.
- D2: Prinzip der **vollständigen Induktion**: Vorgelegt sei $E \subseteq \mathbb{N}$ mit $0 \in E$, und für jedes $n \in E$ gilt $n+1 \in E$. Dann gilt bereits $E = \mathbb{N}$.

Ein klassisches Beispiel: der kleine Gauß

Aufgabe: Wir suchen eine geschlossene Formel für die Summe

$$S(n) \;:=\; \sum_{k=1}^{n} k \;=\; 1+2+\cdots+n.$$

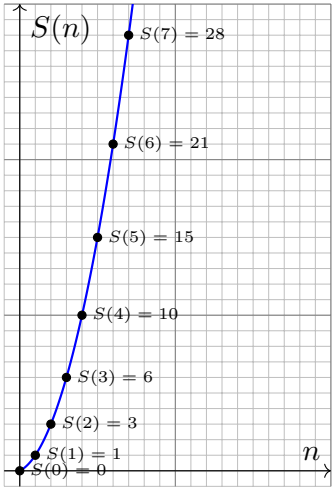
Wie können Sie das Problem angehen?

1. Berechnen Sie kleine Beispiele.
2. Formulieren Sie eine Vermutung.
3. Beweisen Sie Ihre Vermutung!

Lösung: (1) Für kleine Werte $n = 0, 1, 2, \ldots$ finden wir die Werte $S(n)$ in der Graphik.

(2) Das sieht aus wie eine Parabel! Durch diese Datenpunkte verläuft $F(x) = x(x+1)/2$, siehe B101.

(3) Beweis durch Induktion!



Ein klassisches Beispiel: der kleine Gauß

Wir summieren die Terme $f(k) = k$ für $k = 1, 2, 3, \ldots$ und vergleichen

die Summe $S(n) := \sum_{k=1}^{n} f(k)$ mit der Formel $F(n) := \frac{n(n+1)}{2}$.

Behauptung: Für alle $n \in \mathbb{N}$ gilt die Aussage $A(n) : S(n) = F(n)$.

Beweis: Wir beweisen die Behauptung durch vollständige Induktion.

Induktionsanfang: Wir finden $S(0) = 0$ und $F(0) = 0$, also gilt $A(0)$.

Induktionsschritt $A(n) \Rightarrow A(n+1)$: Sei $n \in \mathbb{N}$. Wir setzen $A(n)$ voraus und folgern daraus die Aussage $A(n+1)$, also $S(n+1) = F(n+1)$:

$$\begin{aligned} S(n+1) &\overset{\text{Def}}{=} S(n) + f(n+1) \\ &\overset{\text{IV}}{=} F(n) + (n+1) \\ &\overset{\text{Def}}{=} \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &\overset{\mathbb{Q}}{=} \frac{(n+2)(n+1)}{2} \qquad \overset{\text{Def}}{=} F(n+1) \end{aligned}$$

Ein klassisches Beispiel: der kleine Gauß

Wie *finden* wir die geschlossene Formel für die Summe $S(n) = \sum_{k=1}^{n} k$?

Speziell wenn wir schon wissen oder zumindest vermuten, dass $S(n)$ eine Polynomfunktion vom Grad ≤ 2 ist?

Dann genügt es, drei Punkte auszuwerten, etwa $S(0) = 0$ und $S(1) = 1$ und $S(2) = 3$.

Dies liefert die Polynomfunktion $S(n) = n(n+1)/2$, siehe B101.
Diese Vermutung können wir anschließend per Induktion beweisen!

☺ Die Induktion sagt uns, wie wir eine Vermutung *beweisen* können. Sie sagt uns jedoch nicht, wie wir mögliche Vermutungen *finden* können.

☺ Die Induktion ist ein Standardverfahren und oft einfache Routine. Alternativ gelingen manchmal auch kreativere, noch schönere Beweise.

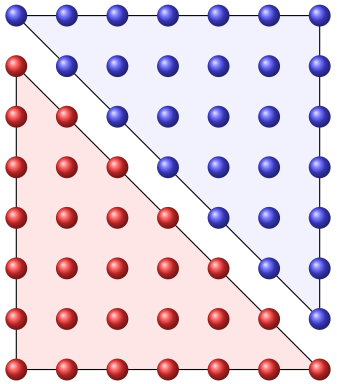
☺ Der folgende Beweis ist geometrisch-anschaulich und genial-einfach. Auch dieses Argument kann und will ich Ihnen nicht vorenthalten.

☺ In diesem Falle muss ich doch zugeben: Unsere erste bescheidene Induktion schießt mit Kanonen auf Spatzen, hier auf den kleinen Gauß.

Ein klassisches Beispiel: der kleine Gauß

Wie *finden* wir die geschlossene Formel für die Summe $S(n) = \sum_{k=1}^{n} k$?
Hier ein geometrischer Beweis, als Bild ganz ohne Worte:

$1 + 2 + 3 + \quad \ldots \quad + n =: S(n)$



$$2S(n) = n(n+1)$$

C'est par la logique que l'on prouve, et par l'intuition que l'on découvre.
[Mit der Logik beweisen wir, mit der Intuition entdecken wir.]
Henri Poincaré (1854–1912)

Induktion: Mehr ist leichter. Weniger ist schwer.

C409

Aufgabe: (1) Finden und beweisen Sie eine geschlossene Formel für

$$s_n := \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)}.$$

(2) Eine genauere Aussage ist hier leichter zu beweisen! Zeigen Sie

$$A(n) \,:\, s_n = 1 - 1/(n+1).$$

Beweis: (2) Induktionsanfang: Wir haben $s_0 = 0$, also gilt $A(0)$.
Induktionsschritt $A(n) \Rightarrow A(n+1)$: Sei $n \in \mathbb{N}$ eine natürliche Zahl.
Wir setzen $A(n)$ voraus und folgern daraus die Aussage $A(n+1)$:

$$\begin{aligned} s_{n+1} &\overset{\text{Def}}{=} s_n + \frac{1}{(n+1)(n+2)} \overset{\text{IV}}{=} 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} \\ &\overset{\mathbb{Q}}{=} 1 - \frac{n+2}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} \overset{\mathbb{Q}}{=} 1 - \frac{1}{n+2} \end{aligned}$$

☺ Der Induktionsbeweis für (2) gelingt erfreulich leicht und routiniert.
Induktion ist ein Standardverfahren, im Idealfall ganz einfach und direkt.

Induktion: Teleskopsummen sind genial-einfach

C410

(1) Eine geschlossene Formel zu *finden* erfordert Kreativität!

☺ Der Term $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$ führt zu folgender **Teleskopsumme**:

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \cdots + \left(\frac{1}{n} - \frac{1}{n+1}\right) = 1 - \frac{1}{n+1}$$

Die Induktion ist eine sehr nützliche und mächtige Beweistechnik:

☺ Vorgegeben sei eine geeignete Aussageform $(A(n))_{n\in\mathbb{N}}$.
In günstigen Fällen erhalten wir per Induktion $\forall n \in \mathbb{N} : A(n)$.

☺ Induktionsbeweise können schwierig sein, doch Induktion hilft:
Wir arbeiten systematisch, strukturiert, routiniert: Standardverfahren!

Die Induktion löst leider nicht alle Probleme! Inventor's paradox:

☹ Die Methode der Induktion sagt uns nicht, wie wir $A(n)_{n\in\mathbb{N}}$ finden.
Das hängt ab von unseren Zielen, Wünschen, Ideen, Ambitionen, ...

☹ Selbst wenn das globale Ziel $\forall n \in \mathbb{N} : A(n)$ klar ist, erfordert es manchmal Geschick, es in geeignete Zwischenschritte zu zerlegen.

Induktion mit Start in $m \in \mathbb{N}$

C411

Satz C4B: Prinzip der vollständigen Induktion, zweite Fassung

Sei $A(n)_{n\geq m}$ eine Familie von Aussagen $A(n)$ indiziert durch $n \in \mathbb{N}_{\geq m}$.
Dann sind die folgenden beiden Aussagen zueinander äquivalent:

(1) Für jede natürliche Zahl $n \in \mathbb{N}_{\geq m}$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in \mathbb{N}_{\geq m} \,:\, A(n)$$

(2) Es gilt $A(m)$, und $A(n)$ impliziert $A(n+1)$ für jedes $n \in \mathbb{N}_{\geq m}$, kurz:

$$A(m) \,\wedge\, \forall n \in \mathbb{N}_{\geq m} \,:\, \big[\, A(n) \Rightarrow A(n+1) \,\big]$$

Indexverschiebung: Die zweite Fassung ist äquivalent zur ersten für

$$B(n) = A(m+n).$$

Für den Startwert $m = 0$ ist die zweite Fassung identisch zur ersten.
Für einen beliebigen Startwert $m \in \mathbb{N}$ ist die zweite meist bequemer.
Beide Sichtweisen sind nützlich, daher führe ich sie hier explizit aus.

Induktion: Mehr ist leichter. Weniger ist schwer.

C412

Aufgabe: (1) Beweisen Sie für alle $n \in \mathbb{N}$ die obere Schranke

$$s_n := \sum_{k=1}^{n} \frac{1}{k^2} = \frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \;<\; 2.$$

☹ Der direkte Versuch per Induktion schlägt hier leider fehl!

(2) Eine stärkere Aussage ist hier leichter zu beweisen! Zeigen Sie

$$A(n) \,:\, s_n \leq 2 - 1/n \quad \text{für alle } n \in \mathbb{N}_{\geq 1}.$$

☺ Bei Induktion gilt oft: Mehr ist leichter. Weniger ist schwer.

Beweis: (2) Induktionsanfang: $s_1 = 1 \leq 2 - 1/1$. Induktionsschritt:

$$s_n = s_{n-1} + \frac{1}{n^2} \leq 2 - \frac{1}{n-1} + \frac{1}{n^2} < 2 - \frac{n}{n(n-1)} + \frac{1}{n(n-1)} = 2 - \frac{1}{n}$$

Alternative: (1) Für alle $k \geq 2$ gilt $1/k^2 < 1/k(k-1) = 1/(k-1) - 1/k$.
(2) Daraus folgt $\sum_{k=2}^{n} 1/k^2 < 1 - 1/n$ dank Teleskopsumme wie oben.

Inventor's paradox nach George Pólya

Wir stehen staunend vor einem einfachen doch trickreichen Beweis:
Die *stärkere* Aussage ist *einfacher* zu beweisen. Wie kann das sein?

Das ist bei vollständiger Induktion ein häufiges, ja typisches Phänomen!
George Pólya nannte es das **inventor's paradox**:

The typical proposition A accessible to proof by mathematical induction has an infinity of cases $A_0, A_1, A_2, \ldots, A_n, \ldots$. The case A_0 is often easy; at any rate, A_0 has to be handled by specific means. Once A_0 is established, we have to prove A_{n+1} assuming A_n.

A proposition A' stronger than A may be easier to prove than A.

In fact, let A' consist of the cases $A'_0, A'_1, A'_2, \ldots, A'_n, \ldots$. In passing from A to A' we make the burden of the proof heavier: we have to prove the stronger A'_{n+1} instead of A_{n+1}. Yet we make also the support of the proof stronger: we may use the more informative A'_n instead of A_n.

🙂 Grundprinzip: Ihre Investition von heute ist Ihr Ertrag von morgen!

Inventor's paradox nach George Pólya

In general, in trying to devise a proof by mathematical induction, you may fail for two opposite reasons. You may fail because you try to prove too much: your A_{n+1} is too heavy a burden. Yet you may also fail because you try to prove too little: your A_n is too weak a support.

You have to balance the statement of your theorem so that the support is just enough for the burden.

George Pólya, 1887–1985, *Mathematics and plausible reasoning, vol. I, Induction and analogy in mathematics*, 1954, p. 119

Wenn Sie eigenständig Induktionsbeweise führen, müssen Sie also

1. die Behauptung $A(n)_{n\geq m}$ geeignet formulieren und ausbalancieren
2. und damit anschließend den Induktionsbeweis sorgfältig ausführen.

Viele Übungsaufgaben verlangen nur (2), das ist leichter, aber künstlich.
Aufgabe (1) erfordert verzweigtes Erkunden und planvolles Probieren.

Induktion: starke Fassung

Satz C4C: Prinzip der vollständigen Induktion, starke Fassung

Sei $A(n)_{n\geq m}$ eine Familie von Aussagen $A(n)$ indiziert durch $n \in \mathbb{N}_{\geq m}$.
Dann sind die folgenden beiden Aussagen zueinander äquivalent:

(1) Für jede natürliche Zahl $n \in \mathbb{N}_{\geq m}$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in \mathbb{N}_{\geq m} \,:\, A(n)$$

(2) Es gilt $A(m)$ und $A(m) \wedge \cdots \wedge A(n) \Rightarrow A(n+1)$ für jedes $n \in \mathbb{N}_{\geq m}$:

$$A(m) \;\wedge\; \forall n \in \mathbb{N}_{\geq m} \,:\, \big[\, A(m) \wedge \cdots \wedge A(n) \Rightarrow A(n+1) \,\big]$$

Das ist äquivalent zur einfachen Induktion C4B für die starke Aussage

$$B(n) = A(m) \wedge \cdots \wedge A(n).$$

Wir haben nämlich den Anfang $B(m) = A(m)$ und den Induktionsschritt
$B(n) \Leftrightarrow A(m) \wedge \cdots \wedge A(n) \Rightarrow A(m) \wedge \cdots \wedge A(n) \wedge A(n+1) \Leftrightarrow B(n+1)$.
Die starke Induktion ist eine bequeme Umformulierung der Induktion.
Beide Sichtweisen sind nützlich, daher führe ich sie hier explizit aus.

Induktion: starke Fassung

Beispiel: Zum Fundamentalsatz der Arithmetik zeigen wir für $n \in \mathbb{N}_{\geq 1}$:

$A(n)$: Die natürliche Zahl n ist ein Produkt unzerlegbarer Faktoren.

Für „Produkt unzerlegbarer Faktoren in $\mathbb{N}$" sage ich kurz UProdukt.

Beweis: Wir führen Induktion über n in der starken Fassung C4C.
Induktionsanfang: Es gilt $A(1)$: Die Zahl 1 ist das leere UProdukt.
Induktionsschritt: Sei $n \in \mathbb{N}_{\geq 1}$. Wir setzen $A(1) \wedge \cdots \wedge A(n)$ voraus.
Wir untersuchen $a = n+1$. Hierzu unterscheiden wir zwei Fälle:

- Entweder a ist unzerlegbar: Dann ist a ein UProdukt der Länge 1.
- Oder a ist zerlegbar gemäß $a = b \cdot c$ mit $b, c \geq 2$. Somit gilt $b, c \leq n$. Nach Voraussetzung sind b und c UProdukte, somit auch $a = b \cdot c$.

Per Induktion schließen wir $A(n)$ für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$. QED

🙂 Bitte wiederholen Sie den Fundamentalsatz der Arithmetik A2J.
Die Eindeutigkeit ist schwieriger, noch interessanter und nützlicher!
Der Fundamentalsatz ist sehr wichtig und hilfreich, zudem bieten Ihnen die dort genutzten Beweistechniken lebendiges Anschauungsmaterial.

Induktion: einheitliche Fassung

🙂 Wir können die Induktion auch ohne Induktionsanfang formulieren!

Satz C4D: vollständige Induktion, einheitliche Fassung

Sei $A(n)_{n\in M}$ eine Familie von Aussagen indiziert durch $n \in M \subseteq \mathbb{N}$.
Dann sind die folgenden beiden Aussagen zueinander äquivalent:

(1) Für jede natürliche Zahl $n \in M$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in M \,:\, A(n)$$

(2) Für jede natürliche Zahl $n \in M$ gilt die Aussage:

$$\big[\, \forall k \in M_{<n} \,:\, A(k) \,\big] \;\Rightarrow\; A(n)$$

Beweis: Das ist äquivalent zur starken Induktion C4C: Die Implikation „(1) ⇒ (2)“ ist ist klar, genauer sogar trivial. Für „(2) ⇒ (1)“ betrachten wir $M = \{\, n_0 < n_1 < n_2 < \dots \,\}$. Dank (2) gilt $\top \Rightarrow A(n_0)$, also $A(n_0)$. Für jedes $i \in \mathbb{N}$ gilt $A(n_0) \wedge \dots \wedge A(n_i) \Rightarrow A(n_{i+1})$. Wir schließen (1).

Induktion: einheitliche Fassung

🙂 Das ist elegant und effizient. Manche Beweise nutzen diese Form: In Bedingung (2) ist der Induktionsanfang schon raffiniert eingebacken.

Das ist insbesondere dann eine willkommene Vereinfachung, wenn der Induktionsanfang genauso verläuft wie der Schritt.

☹ In manchen Induktionsbeweisen ist der Anfang anders strukturiert als der Schritt und erfordert daher sein eigenes, separates Argument.

Dann spaltet (2) wieder auf in Induktionsanfang und Induktionsschritt. Nun gut, die einheitliche Form hat dann weder Vor- noch Nachteile.

🙂 Die einheitliche Form C4D nützt auch für (große) endliche Mengen. Auch hier ist eine Betrachtung aller Einzelfälle meist unwirtschaftlich, der Induktionsbeweis hingegen spart Arbeit und schafft Klarheit.

🙂 Die Formulierung C4D lässt sich noch wesentlich allgemeiner nutzen für die „transfinite“ Induktion, statt über $M \subseteq \mathbb{N}$ über jede beliebige wohlgeordnete Menge $(M, \leq)$, siehe F1T. Mehr hierzu in Kapitel F.

Induktionsbeweise in der Linearen Algebra

Als Ausblick nenne ich exemplarisch einige Sätze, die wir im Verlauf der Linearen Algebra durch Induktion beweisen (in der Fassung rechts).

E1C Die Zykelzerlegung von Permutationen	(C4C)
§E1.2 Der Zählsatz für endliche Mengen	(C4C)
§E1.3 Dirichlets Schubfachprinzip	(C4C)
§E2.1 Grundrechenarten für endliche Mengen	(C4C)
E2I Teilmengen und Binomialkoeffizient	(C4A)
E2K Zerlegungen und Stirling–Zahlen	(C4A)
F1S Die natürlichen Zahlen sind wohlgeordnet.	(C4A)
F2B Rekursionssatz von Dedekind	(C4C)
F2M Aus der Bijektion $\mathbb{N}^2 \cong \mathbb{N}$ folgt $\mathbb{N}^n \cong \mathbb{N}$	(C4B)
F2P Aus der Bijektion $\mathbb{Q}^2 \cong \mathbb{Q}$ folgt $\mathbb{Q}^n \cong \mathbb{Q}$	(C4B)

Als Alternative entrolle ich manchmal den Induktionsbeweis zu einem expliziten Algorithmus, um die konkrete Konstruktion hervorzuheben. Das sind zwei Seiten einer Medaille: Die Korrektheit des angegebenen Algorithmus zeigen wir, indem wir dann den Induktionsbeweis führen.

Induktionsbeweise in der Mathematik

Mit zunehmender Erfahrung verschmelzen die vier Formulierungen zu einem universellen „Prinzip der Induktion“; alle vier sind ja äquivalent.

Meist genügt dann eine Skizze, die Idee, der entscheidende Schritt, die detaillierte Ausformulierung ist anschließend eine routinierte Übung.

Je fortgeschrittener das Thema, desto kürzer sind die Routinebeweise, schließlich fallen sie weg zu Gunsten der wesentlichen neuen Ideen.

Ausführliche Beweise, insbesondere per Induktion, kosten viel Platz, den sparen wir später zu Gunsten der Lesbarkeit und der Übersicht.

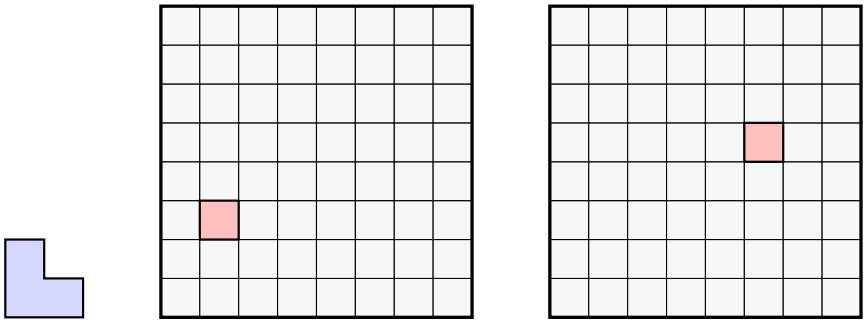
Gelegentlich schreibe ich kurz „Dies folgt per Induktion über n“, und dies soll genügen, um daraus das vollständige Argument herzuleiten.

Daher müssen Sie alle Beweistechniken, insbesondere die Induktion, verinnerlichen, um damit Beweise prüfen und produzieren zu können.

⚠ Bei aller Abkürzung: Den ausführlichen und genauen Beweis sollte man immer in der Hinterhand halten, um etwaige Zweifel zu klären. Das folgende schöne Beispiel illustriert dies eindrücklich.

Induktion: Mehr ist leichter. Weniger ist schwer.

C421



Aufgabe: (1) Wir betrachten ein Schachbrett, mit 8×8 Quadraten. Ein beliebiges dieser 64 Quadrate wird rot markiert. Lassen sich die verbleibenden 63 Quadrate mit L-Steinen zu je 3 Quadraten abdecken?

☹ In dieser allzu speziellen Form ist die Aufgabe recht schwierig. Mangels Struktur erkennen wir zunächst keinen Lösungsansatz.

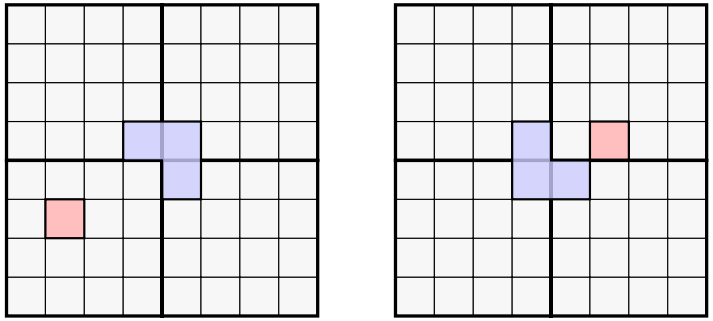
🙂 Eine allgemeinere Frage ist hier viel leichter zu beantworten… Durch eine geschickte Induktion wird das Problem kinderleicht!

Induktion: Mehr ist leichter. Weniger ist schwer.

C422
Erläuterung

(2) Lösen Sie das Problem für alle Spielbretter mit $2^n \times 2^n$ Quadraten. Das klingt zunächst noch schwieriger, ist aber tatsächlich einfacher!

Lösung: Die geniale Idee als Bild ohne Worte:



Übung: Formulieren Sie dies sorgfältig als Induktion über $n \in \mathbb{N}$. Ist die Idee erst einmal geboren, so ist die Ausführung recht leicht.

Zusatz: Formulieren und lösen Sie das dreidimensionale Puzzle. Es wirkt zunächst noch komplizierter, gelingt aber ebenso leicht!

Induktion: Beweisen ist leicht. Finden ist schwer.

C423
Erläuterung

Scherzhafte Frage: Wie lautet zu $g(x) = \mathrm{e}^x$ die 100te Ableitung?

Ernsthafte Frage: Wie lautet zu $f(x) = x\,\mathrm{e}^x$ die 100te Ableitung?

🙂 Selbst wenn weder Frage noch Antwort von Induktion sprechen, kann es dennoch helfen, eine geeignete Induktion einzuführen!

Anleitung: (1) Berechnen Sie einige Ableitungen f', f'', f''', …
(2) Formulieren Sie eine Vermutung für die $n$te Ableitung $f^{(n)}$.
(3) Beweisen Sie Ihre Vermutung per Induktion über $n \in \mathbb{N}$.
(4) Spezialisieren Sie schließlich zu dem Fall $n = 100$.

Lösung: (1) Wir finden $f'(x) = (x+1)\,\mathrm{e}^x$, dann $f''(x) = (x+2)\,\mathrm{e}^x$, dann $f'''(x) = (x+3)\,\mathrm{e}^x$. (2) Wir vermuten daher $f^{(n)}(x) = (x+n)\,\mathrm{e}^x$.
(3) Der Beweis per Induktion ist nun leicht. Formulieren Sie dies aus!
(4) Speziell für $n = 100$ finden wir $f^{(100)}(x) = (x+100)\,\mathrm{e}^x$. Voilà!

🙂 Meist läuft dieser Prozess weniger formell ab: Nach den ersten drei Beispielen wollen Sie vermutlich ausrufen „Ja, klar, und immer so weiter bis 100.“ Dahinter steckt, wenn Sie ehrlich sind, eine Induktion!

Induktion: Beweisen ist leicht. Finden ist schwer.

C424
Erläuterung

Die beiden vorigen und auch die nachfolgenden Aufgaben illustrieren ein wichtiges Prinzip: Liegt eine geeignet formulierte Vermutung erst einmal vor uns, so ist ihr Induktionsbeweis meist leicht: Rechnen! Das gilt selbstverständlich nicht immer, aber doch erstaunlich oft.

Ungleich schwieriger dagegen kann es sein, eine geeignete Vermutung überhaupt erst zu finden, zu formulieren und dabei auszubalancieren.

Nicht im Beweis einer gegebenen Konstruktion,
sondern in der Erfindung der Konstruktion liegt
in den meisten Fällen die eigentliche Schwierigkeit.
Hermann Weyl (1885–1955)

Lassen Sie sich nicht davon einlullen, dass viele Lehrbücher die ersten Induktionsaufgaben meist sehr stereotyp und allzu einfach formulieren. Das ist selbstverständlich sinnvoll und hilfreich für die ersten Schritte, aber kein realistisches Vorbild für selbständige mathematische Arbeit.

Induktion ist im Wesentlichen nicht stumpfsinniges, formales Rechnen, sondern eine filigrane Kunst. Probieren Sie es, Sie werden es erleben!

Die Summe $1+3+5+\cdots+(2n-1)$

Aufgabe: Finden und beweisen Sie eine geschlossene Formel für die Summe s_n der ersten n ungeraden Zahlen:

$$s_n := \sum_{k=1}^{n}(2k-1) = 1+3+5+\cdots+(2n-1)$$

(0) Berechnen Sie kleine Beispiele und formulieren Sie eine Vermutung. Beweisen Sie Ihre Vermutung (1) per Induktion und (2) geometrisch.

Lösung: (0) Wir finden $s_0=0$, $s_1=1$, $s_2=4$, $s_3=9$, $s_4=16$, ...
Die naheliegende Vermutung ist daher: Es gilt $s_n=n^2$ für alle $n\in\mathbb{N}$.

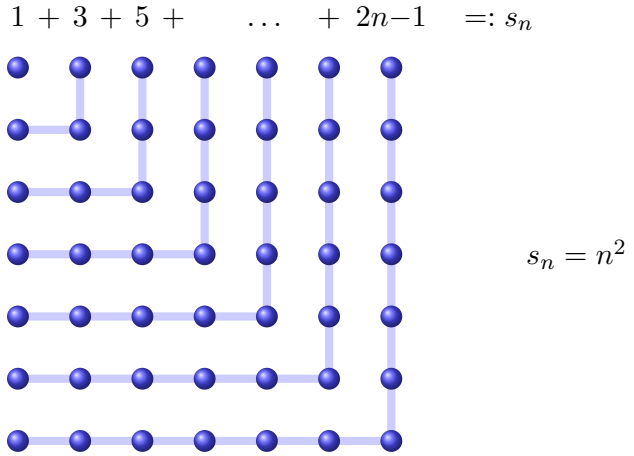
(1) Wir beweisen die Aussage $A(n): s_n=n^2$ per Induktion.
Für $n=0$ gilt $s_0=0$, daher ist die Aussage $A(0): s_0=0^2$ wahr.
Angenommen, es gilt $A(n): s_n=n^2$. Damit zeigen wir nun $A(n+1)$:

$$s_{n+1} \overset{\text{Def}}{=} s_n+(2n+1) \overset{\text{IV}}{=} n^2+2n+1 \overset{\text{N}}{=} (n+1)^2$$

Per vollständiger Induktion (Satz C4A) schließen wir daraus:
Für jede natürliche Zahl $n\in\mathbb{N}$ gilt die vermutete Gleichung $s_n=n^2$.

Die Summe $1+3+5+\cdots+(2n-1)$

(2) Hier ein geometrischer Beweis, als Bild ganz ohne Worte:

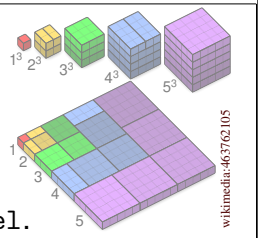


L Geometrische Beweise wie dieser oder zum kleinen Gauß (C408) sind wunderschönes Material für die Schule und bereits früh zugänglich. Sie bauen spielerisch eine Brücke zur algebraisch-formalen Induktion.

Weitere Induktionsbeweise zu Summen

Aufgabe: Finden Sie die Summenformeln zu

$$\sum_{k=0}^{n-1}1,\quad \sum_{k=0}^{n-1}k,\quad \sum_{k=0}^{n-1}k^2,\quad \sum_{k=0}^{n-1}k^3,\quad \dots$$



Siehe `de.wikipedia.org/wiki/Faulhabersche_Formel`.
Auch für $\sum_{k=0}^{n-1}k^3=(\sum_{k=0}^{n-1}k)^2$ existiert ein geometrischer Beweis!

Lösung: Wir kennen bzw. finden bzw. vermuten die Summenformeln

$$\sum_{k=0}^{n-1}1=n, \qquad \sum_{k=0}^{n-1}k=\frac{n(n-1)}{2},$$
$$\sum_{k=0}^{n-1}k^2=\frac{n(n-1)(2n-1)}{6}, \qquad \sum_{k=0}^{n-1}k^3=\frac{n^2(n-1)^2}{4}.$$

Übung: Beweisen Sie diese Vermutungen nun durch Induktion über n.
Liegt eine solche Formel $\sum_{k=0}^{n-1}f(k)=[F]_0^n$ erst einmal (als Vermutung) vor, so gelingt der Beweis leicht durch folgende „diskrete Ableitung“.

Hauptsatz zu Differenzen und Summen / HDS

Satz C4E: Hauptsatz zu Differenzen und Summen / HDS

Für $f,F:\mathbb{Z}\to\mathbb{R}$ gelte $f(k)=F(k+1)-F(k)$ für alle $k\in\mathbb{Z}$.
Durch Summation erhalten wir hieraus die Teleskopsumme

$$\sum_{k=a}^{b-1}f(k)=\sum_{k=a}^{b-1}\big[F(k+1)-F(k)\big]=F(b)-F(a)=:\big[F\big]_a^b.$$

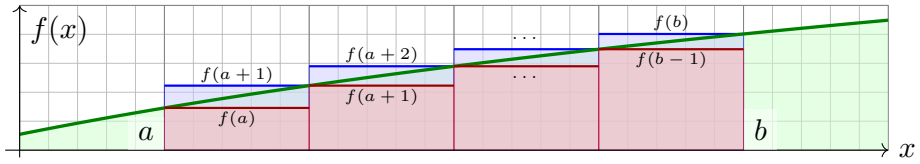
Beispiele sind $f(k)=1$, $F(k)=k$ und $f(k)=k$, $F(k)=k(k-1)/2$ etc. wie oben angegeben. Man rechnet dies nun leicht / mechanisch nach.

Das ist das diskrete Analogon zum HDI / Hauptsatz der Differential- und Integralrechnung $\int_a^b f(x)\,\mathrm{d}x=[F]_a^b$ für $f,F:[a,b]\to\mathbb{R}$ stetig und $F'=f$.
In beiden Fällen ist Differenzieren leichter als Summieren / Integrieren, und der Hauptsatz schlägt die enorm nützliche Brücke zwischen beiden!

Übung: Beweisen Sie den obigen Satz per Induktion über b.
(Alles ist sehr leicht und steht eigentlich schon da.)

Monotoner Vergleich von Summe und Integral

C429
Übung



Satz C4F: monotoner Vergleich von Reihe und Integral

Sei $f : \mathbb{R} \to \mathbb{R}$ monoton wachsend. Für alle $a \le b$ in $\mathbb{Z}$ gilt dann:

$$\sum_{k=a}^{b-1} f(k) \quad \le \quad \int_{x=a}^{b} f(x)\,\mathrm{d}x \quad \le \quad \sum_{k=a+1}^{b} f(k)$$

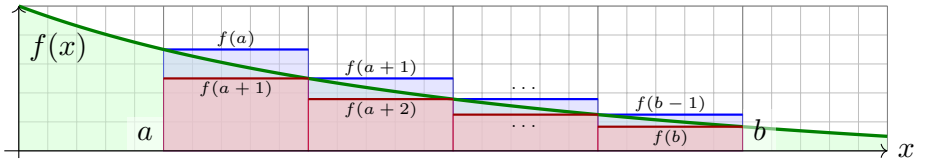
Durch Umstellung ist dies äquivalent zu:

$$f(a) + \int_{x=a}^{b-1} f(x)\,\mathrm{d}x \quad \le \quad \sum_{k=a}^{b-1} f(k) \quad \le \quad \int_{x=a}^{b} f(x)\,\mathrm{d}x$$

Übung: Beweisen Sie diesen Satz sorgsam per Induktion über b.

Monotoner Vergleich von Summe und Integral

C430
Übung



Satz C4G: monotoner Vergleich von Integral und Reihe

Sei $f : \mathbb{R} \to \mathbb{R}$ monoton fallend. Für alle $a \le b$ in $\mathbb{Z}$ gilt dann:

$$\sum_{k=a+1}^{b} f(k) \quad \le \quad \int_{x=a}^{b} f(x)\,\mathrm{d}x \quad \le \quad \sum_{k=a}^{b-1} f(k)$$

Durch Umstellung ist dies äquivalent zu:

$$\int_{x=a}^{b} f(x)\,\mathrm{d}x \quad \le \quad \sum_{k=a}^{b-1} f(k) \quad \le \quad f(a) + \int_{x=a}^{b-1} f(x)\,\mathrm{d}x$$

Übung: Beweisen Sie diesen Satz sorgsam per Induktion über b.

Die harmonische Reihe und der natürliche Logarithmus

C431
Übung

🙂 Für die vorigen beiden Übungen und die folgenden beiden Aufgaben benötigen Sie etwas Integration, wie Sie es in der Schule gelernt haben.

Aufgabe: Wir untersuchen die **harmonische Reihe**

$$H_n := \sum_{k=1}^{n} \frac{1}{k}.$$

(1) Schachteln Sie den Wert H_n ein durch den Logarithmus $\ln(n)$.
(2) Folgern Sie das Konvergenzverhalten von H_n für $n \to \infty$.
(3) Bei welchem Index n überschreitet H_n den Wert 1000?

Lösung: (1) Für die Funktion $f(x) = 1/x$ erhalten wir dank Satz C4G:

$$\ln(n+1) \quad \le \quad \sum_{k=1}^{n} \frac{1}{k} \quad \le \quad 1 + \ln(n)$$

🙂 Die harmonische Reihe wächst wie der natürliche Logarithmus!
(2) Insbesondere erhalten wir die Divergenz $\sum_{k=1}^{n} \frac{1}{k} \to \infty$ für $n \to \infty$.
(3) Bei $n \approx \mathrm{e}^{1000} \approx 2 \cdot 10^{434}$. Wir werden das also sicher nie erleben!

Approximation einer Dirichlet–Reihe durch Integrale

C432
Übung

Aufgabe: Berechnen Sie durch Summation näherungsweise den Wert

$$\zeta(3) := \sum_{k=1}^{\infty} \frac{1}{k^3} \quad \text{der Riemannschen Zeta–Funktion} \quad \zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$$

bis auf einen Fehler $\le \varepsilon = 0.5 \cdot 10^{-6}$, also sechs Nachkommastellen.
Wie kontrollieren Sie den Fehler? Wie weit müssen Sie summieren?

Lösung: Wir berechnen die endlichen Summen $s_n = \sum_{k=1}^{n} k^{-3}$ und wählen n so, dass der Rest $\zeta(3) - s_n = \sum_{k=n+1}^{\infty} k^{-3}$ kleiner als ε ist:

$$0 \;<\; \int_{x=n+1}^{\infty} x^{-3}\,\mathrm{d}x \;<\; \sum_{k=n+1}^{\infty} k^{-3} \;<\; \int_{x=n}^{\infty} x^{-3}\,\mathrm{d}x \;=\; \frac{1}{2n^2} \;\overset{!}{\le}\; \varepsilon$$

Die Wahl $n = 1000$ garantiert einen Fehler $\le 0.5 \cdot 10^{-6} = 0.0000005$.
Wir finden $s_{1000} = 1.20205640\ldots$, also $1.202055 < \zeta(3) < 1.202057$.
🙂 Noch besser: $s_n + (n+1)^{-2}/2 \le \zeta(3) \le s_n + n^{-2}/2$, Fehler $\le n^{-3}$.
Mit diesem raffinierten Trick genügt schon die Summation bis $n = 100$.

Beispiel einer Klausuraufgabe (2020)

Aufgabe: Zeigen Sie per vollständiger Induktion,
dass die folgende Aussage $A(n)$ für alle $n \in \mathbb{N}$ gilt.

$$A(n): \quad \text{Die Zahl } 5^{2n} - 2^n \text{ ist in } \mathbb{Z} \text{ durch } 23 \text{ teilbar.}$$

Induktionsanfang: Für $n = 0$ beweisen wir $A(0)$ direkt:

$$5^{2\cdot 0} - 2^0 = 1 - 1 = 0 = 23 \cdot 0.$$

Induktionsschritt: Sei $n \in \mathbb{N}$. Wir setzen voraus, dass $A(n)$ gilt,
es existiert also $k \in \mathbb{Z}$ mit $5^{2n} - 2^n = 23k$, somit $5^{2n} = 2^n + 23k$.
Daraus folgern wir nun die Behauptung $A(n+1)$:

$$\begin{aligned} 5^{2(n+1)} - 2^{n+1} &\overset{\mathbb{Z}}{=} 25 \cdot 5^{2n} - 2^{n+1} \\ &\overset{\text{IV}}{=} 25 \cdot (2^n + 23k) - 2 \cdot 2^n \\ &\overset{\mathbb{Z}}{=} 23 \cdot 2^n + 25 \cdot 23 \cdot k \qquad \overset{\mathbb{Z}}{=} 23(2^n + 25k) \end{aligned}$$

Das beweist den Induktionsschritt $A(n) \Rightarrow A(n+1)$ für alle $n \geq 0$.
Per vollständiger Induktion folgt die Behauptung $A(n)$ für alle $n \in \mathbb{N}$.

Beispiel einer Klausuraufgabe (2020)

☺ Die Induktion ist ein Standardverfahren und oft einfache Routine.
Für die vorliegende Aufgabe müssen Sie vor allem sorgfältig rechnen.

Hinweis: Wenn Sie diese Aufgabe selbst versuchen und aufmerksam betrachten, dann merken Sie: Es ist nicht immer offensichtlich, wo und wie Sie die Induktionsvoraussetzung nutzbringend einsetzen können. Hier hilft Ihnen letztlich Ihre Erfahrung. Übung macht die Meisterin!

Alternative: Sie können die gesamte Rechnung modulo 23 ausführen.
Diese nützliche Rechentechnik lernen Sie in Kapitel E ab Seite E341:
Auf $\mathbb{Z}$ nutzen wir die Kongruenz $a \equiv b \mod m$, hier für $m = 23$.
Es gilt $25 \equiv 2$. Damit wird die Induktion gänzlich überflüssig:

$$5^{2(n+1)} \overset{\mathbb{Z}}{=} 25^{n+1} \equiv 2^{n+1}$$

☺ Die Rechnung modulo 23 ist einfacher, kürzer und klarer,
genau dazu führen wir diese wunderbare und nützliche Technik ein.
Beide Rechnungen tun dasselbe; gute Notation vereinfacht Ihre Arbeit.

Eine zweite Induktion zur Teilbarkeit

Aufgabe: Zeigen Sie per vollständiger Induktion,
dass die folgende Aussage $A(n)$ für alle $n \in \mathbb{N}_{\geq 1}$ gilt.

$$A(n): \quad \text{Die Zahl } 3^{2n+4} - 2^{n-1} \text{ ist durch } 7 \text{ teilbar.}$$

Induktionsanfang: Für $n = 1$ beweisen wir $A(1)$ direkt:

$$3^{2\cdot 1+4} - 2^0 = 3^6 - 1 = 728 = 7 \cdot 104.$$

Induktionsschritt: Sei $n \in \mathbb{N}_{\geq 1}$. Wir setzen voraus, dass $A(n)$ gilt,
es existiert also $k \in \mathbb{Z}$ mit $3^{2n+4} - 2^{n-1} = 7k$, somit $3^{2n+4} = 7k + 2^{n-1}$.
Daraus folgern wir nun die Behauptung $A(n+1)$:

$$\begin{aligned} 3^{2(n+1)+4} - 2^n &\overset{\mathbb{Z}}{=} 3^{2n+4} \cdot 9 - 2^n \\ &\overset{\text{IV}}{=} (7k + 2^{n-1}) \cdot 9 - 2^n \\ &\overset{\mathbb{Z}}{=} 7k + 2^{n-1}(9 - 2) \qquad \overset{\mathbb{Z}}{=} 7(k + 2^{n-1}) \end{aligned}$$

Das beweist den Induktionsschritt $A(n) \Rightarrow A(n+1)$ für alle $n \geq 1$.
Per vollständiger Induktion folgt die Behauptung $A(n)$ für alle $n \in \mathbb{N}_{\geq 1}$.

Eine zweite Induktion zur Teilbarkeit

☺ Auch hier müssen Sie vor allem sorgfältig rechnen,
anfangs mit konkreten Zahlen in $\mathbb{Z}$, dann auch mit Variablen.

☺ Wenn Sie diesen Aufgabentyp zum ersten Mal selbst versuchen, ist es noch schwer. Wenn Sie die vorige Aufgabe schon gelöst haben, denn zahlt sich diese Erfahrung hier bereits aus: Übung macht die Meisterin!

Alternative: Sie können die gesamte Rechnung modulo 7 ausführen.
Diese nützliche Rechentechnik lernen Sie in Kapitel E ab Seite E341:
Auf $\mathbb{Z}$ nutzen wir die Kongruenz $a \equiv b \mod m$, hier für $m = 7$.
Es gilt $9 \equiv 2$ und $2^3 = 8 \equiv 1$. Damit wird die Induktion überflüssig:

$$3^{2n+4} \overset{\mathbb{Z}}{=} 3^{2(n-1)+6} \overset{\mathbb{Z}}{=} 9^{n-1} \cdot 9^3 \equiv 2^{n-1} \cdot 2^3 \equiv 2^{n-1}$$

☺ Die Rechnung modulo 7 ist einfacher, kürzer und klarer,
genau dazu führen wir diese wunderbare und nützliche Technik ein.
Beide Rechnungen tun dasselbe; gute Notation vereinfacht Ihre Arbeit.

Aufgabe: Zeigen Sie per vollständiger Induktion, dass die Aussage $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq 1$ gilt.

$$A(n): \quad \prod_{k=2}^{n} \left(1 - \frac{2}{k(k+1)}\right) = \frac{1}{3}\left(1 + \frac{2}{n}\right)$$

Induktionsanfang: Wir betrachten den ersten Fall $n = 1$. Auf der linken Seite der Gleichung steht das leere Produkt

$$\prod_{k=2}^{1} \left(1 - \frac{2}{k(k+1)}\right) = 1.$$

Auf der rechten Seite der Gleichung steht

$$\frac{1}{3}\left(1 + \frac{2}{1}\right) = 1.$$

Also gilt die Behauptung $A(1)$.

Induktionsschritt: Sei $n \geq 1$. Wir setzen voraus, dass die Behauptung $A(n)$ gilt. Daraus folgern wir nun die nächste Behauptung $A(n+1)$:

$$\begin{aligned}
\prod_{k=2}^{n+1} \left(1 - \frac{2}{k(k+1)}\right) &\overset{\text{Def}}{=} \left[\prod_{k=2}^{n} \left(1 - \frac{2}{k(k+1)}\right)\right] \cdot \left(1 - \frac{2}{(n+1)(n+2)}\right) \\
&\overset{\text{IV}}{=} \frac{1}{3}\left(1 + \frac{2}{n}\right) \cdot \left(1 - \frac{2}{(n+1)(n+2)}\right) \\
&\overset{\mathbb{Q}}{=} \frac{1}{3} \cdot \frac{n+2}{n} \cdot \frac{n^2+3n}{(n+1)\cdot(n+2)} \\
&\overset{\mathbb{Q}}{=} \frac{1}{3} \cdot \frac{n+3}{n+1} \overset{\mathbb{Q}}{=} \frac{1}{3}\left(1 + \frac{2}{n+1}\right)
\end{aligned}$$

Das beweist den Induktionsschritt $A(n) \Rightarrow A(n+1)$ für alle $n \geq 1$.

Zur Betonung fasse ich zusammen: Aus dem Induktionsanfang $A(1)$ und dem Induktionsschritt $A(n) \Rightarrow A(n+1)$ für alle $n \geq 1$ folgt der **Induktionsschluss:** Die Behauptung $A(n)$ gilt für alle $n \geq 1$.

Die Fibonacci–Folge

Die Fibonacci–Folge $(f_n)_{n\in\mathbb{N}}$ ist definiert durch die Startwerte $f_0 = 0$ und $f_1 = 1$ sowie die Rekursionsvorschrift $f_n = f_{n-1} + f_{n-2}$ für $n \in \mathbb{N}_{\geq 2}$. (Leonardo Fibonacci beschrieb damit im Jahr 1202 das Wachstum einer Kaninchenpopulation; in der Natur ist sie ein recht häufiges Muster.)

Aufgabe: (0) Vergleichen Sie f_n und 2^{n-1} für kleine Werte von n.
(1) Formulieren Sie zu (0) eine Vermutung und beweisen Sie diese.
(2) Was ist für die Ungleichung $f_n \leq c^{n-1}$ die optimale Konstante c?

Lösung: (0) Für kleine Werte $n = 0, 1, 2, 3, \dots$ finden wir

n	0	1	2	3	4	5	6	7	8	9	…
f_n	0	1	1	2	3	5	8	13	21	34	…
2^{n-1}	$1/2$	1	2	4	8	16	32	64	128	256	…

Die naheliegende Vermutung ist daher $f_n \leq 2^{n-1}$ für alle $n \in \mathbb{N}$.
Dies beweisen wir nun per Induktion (1). Diese Ungleichung ist noch allzu verschwenderisch, daher verfeinern wir sie anschließend in (2).

Die Fibonacci–Folge

(1) Wir beweisen die Aussage $A(n) : f_n \leq 2^{n-1}$ per Induktion über n.
Wir haben $f_0 = 0 < 2^{-1}$ und $f_1 = 1 = 2^0$, also gelten $A(0)$ und $A(1)$.
Angenommen, es gilt $A(n-1)$ und $A(n-2)$. Damit zeigen wir nun $A(n)$:

$$f_n \overset{\text{Def}}{=} f_{n-1} + f_{n-2} \overset{\text{IV}}{\leq} 2^{n-2} + 2^{n-3} < 2^{n-2} + 2^{n-2} = 2^{n-1}$$

Per vollständiger Induktion (C4C) gilt $f_n \leq 2^{n-1}$ für alle $n \in \mathbb{N}$.

(2) Wir wollen die induktive Ungleichung $A(n) : f_n \leq c^{n-1}$ optimieren.
Für jede Konstante $c \in \mathbb{R}_{>0}$ gilt zunächst $f_0 = 0 < c^{-1}$ und $f_1 = 1 = c^0$.
Angenommen, es gilt $A(n-1)$ und $A(n-2)$. Damit zeigen wir nun $A(n)$:

$$f_n \overset{\text{Def}}{=} f_{n-1} + f_{n-2} \overset{\text{IV}}{\leq} c^{n-2} + c^{n-3} = c^{n-3} \cdot (c+1) \overset{!}{\leq} c^{n-3} \cdot c^2$$

Wir suchen also $c \in \mathbb{R}_{>0}$ mit $1 + c \leq c^2$. Die kleinste solche Konstante ist die positive Lösung der quadratischen Gleichung $c^2 - c - 1 = 0$, also

$$\phi := (1 + \sqrt{5})/2.$$

Damit gelingt unsere Induktion und beweist $f_n \leq \phi^{n-1}$ für alle $n \in \mathbb{N}$.

Die Fibonacci–Folge

Wir betrachten weiterhin die Fibonacci–Folge $(f_n)_{n\in\mathbb{N}}$, definiert durch $f_0 = 0$ und $f_1 = 1$ und die Rekursionsvorschrift $f_{n+2} = f_{n+1} + f_n$.

Aufgabe: Beweisen Sie für alle $n \in \mathbb{N}$ die **Binet–Formel**

$$A(n): \qquad f_n = \frac{\phi^n - \psi^n}{\phi - \psi}$$

wobei $\phi = \frac{1}{2}(1 + \sqrt{5})$ und $\psi = \frac{1}{2}(1 - \sqrt{5})$ die Nullstellen von $x^2 - x - 1$ sind. Explizit ausgeschrieben ergibt dies die phantastische Formel

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Ist zum Beweis die einfache oder die starke Induktion geschickter?

Induktionsanfang: Offensichtlich gelten $A(0)$ und $A(1)$:

$$\frac{\phi^n - \psi^n}{\phi - \psi} = \frac{1-1}{\phi - \psi} = 0, \qquad \frac{\phi^1 - \psi^1}{\phi - \psi} = \frac{\phi - \psi}{\phi - \psi} = 1$$

Die Fibonacci–Folge

Induktionsschritt: Die einfache Induktion passt hier nicht direkt.
Wir nutzen die starke Induktion in der Form $A(n) \wedge A(n+1) \Rightarrow A(n+2)$.
Wir setzen also $A(n)$ und $A(n+1)$ voraus und folgern daraus $A(n+2)$:

$$f_{n+2} \overset{\text{Def}}{=} f_{n+1} + f_n \overset{\text{IV}}{=} \frac{\phi^{n+1} - \psi^{n+1}}{\phi - \psi} + \frac{\phi^n - \psi^n}{\phi - \psi}$$

$$\overset{\mathbb{R}}{=} \frac{\phi^n(\phi+1) - \psi^n(\psi+1)}{\phi - \psi} \overset{\mathbb{R}}{=} \frac{\phi^n\phi^2 - \psi^n\psi^2}{\phi - \psi} \overset{\mathbb{R}}{=} \frac{\phi^{n+2} - \psi^{n+2}}{\phi - \psi}$$

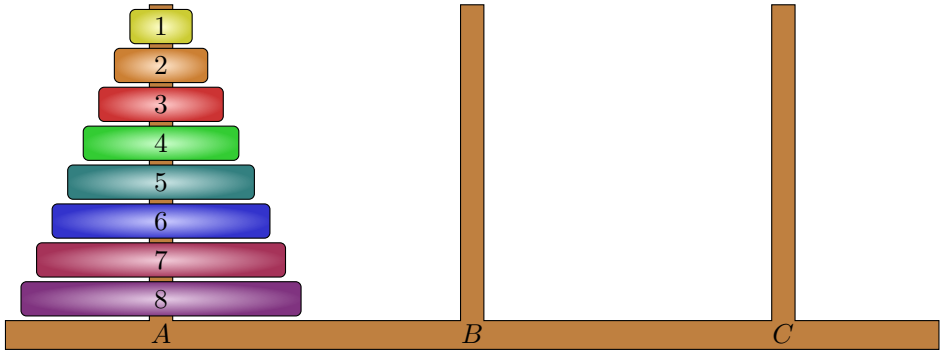
Die Induktion ist ein Standardverfahren und oft einfache Routine.
Auch für diese Aufgabe müssen Sie vor allem sorgfältig rechnen.

Die Induktion sagt uns, wie wir die Gleichung *beweisen* können.
Sie sagt uns jedoch nicht, wie wir die Gleichung *finden* können.

Übung: Finden Sie die Binet–Formel mit folgender **Ansatzmethode**:
Für welche $x \in \mathbb{R}$ erfüllt $f_n = x^n$ die Rekursion $f_{n+2} = f_{n+1} + f_n$?
Gilt dies dann auch für jede Linearkombination $f_n = \lambda\phi^n + \mu\psi^n$?
Für welche Koeffizienten λ, μ gilt $f_0 = 0$ und $f_1 = 1$? (siehe M249)

Die Türme von Hanoi

C445
Ergänzung



Das Spiel **die Türme von Hanoi** besteht aus drei Stäben A, B, C und darauf die Scheiben $1, \ldots, n$ wachsender Größe. Zu jedem Zeitpunkt des Spiels sind die Scheiben auf jedem Stab der Größe nach geordnet.

Zu Beginn liegen alle Scheiben auf Stab A. Ziel des Spiels ist es, alle Scheiben von A nach C zu versetzen. Bei jedem Zug wird die oberste Scheibe von einem Stab auf einen anderen versetzt, vorausgesetzt, dass sich dort nicht schon eine kleinere Scheibe befindet.

Die Türme von Hanoi

C446
Ergänzung

Als **Lösung** bezeichnen wir jede Folge legaler Züge, die den Turm mit n Scheiben von A nach C bewegt.

Aufgabe: Lösen Sie dieses Logik-Puzzle in vier Härtegraden:
P_n: Für den Turm der Höhe n existiert (mind.) eine Lösung.
Q_n: ... der Länge $2^n - 1$. R_n: ... aber nicht mit weniger.
S_n: Es gibt genau eine kürzeste Lösung, mit $2^n - 1$ Zügen.

Strategie: Lösen Sie zunächst die kleinen Fälle $n = 0, 1, 2, 3, \ldots$.
Sie können hierzu Bücher oder Münzen geeigneter Größe stapeln.
Lösen Sie anschließend den allgemeinen Fall per Induktion über n.

I Es ist eine klassische Programmieraufgabe, die (!) optimale Lösung zu programmieren, etwa einfach-elegant als eine rekursive Funktion.

L Für die menschlich-manuelle Lösung, etwa für $n = 5$ Scheiben, ist eine iterative Formulierung leichter: Sehen Sie, wie dies geht?

Wenn Sie dies als wunderschöne Videos bewundern wollen, dann bei Grant Sanderson alias 3Blue1Brown, `youtu.be/2SUvWfNJSsM`, und Burkard Polster alias Mathologer, `youtu.be/MbonokcLbNo`.

Die Türme von Hanoi

C447
Ergänzung

Lösung: Für den 0–Turm sind die Aussagen P_0, Q_0, R_0, S_0 trivial.
Für den 1–Turm sind die Aussagen P_1, Q_1, R_1, S_1 offensichtlich wahr.

$P_n \Rightarrow P_{n+1}$ und $Q_n \Rightarrow Q_{n+1}$: Dank P_n versetzen wir den n–Turm von A nach B mit $2^n - 1$ Zügen. Wir versetzen die Scheibe $n+1$ von A nach C mit einem Zug. Dank P_n versetzen wir den n–Turm von B nach C mit $2^n - 1$ Zügen. Insgesamt gelingt diese Lösung also mit $2^{n+1} - 1$ Zügen.

$R_n \Rightarrow R_{n+1}$: Die größte Schreibe $n+1$ wird mindestens einmal bewegt. Dank R_n gehen dem ersten Mal mindestens $2^n - 1$ Züge voraus und ebenso folgen dem letzten Mal noch mindestens $2^n - 1$ weitere Züge. Insgesamt sind demnach mindestens $2^{n+1} - 1$ Züge notwendig.

Aus Q_n und R_n folgt: Jede optimale Lösung für den n–Turm hat genau die Länge $2^n - 1$ und bewegt die größte Scheibe genau einmal.

$S_n \Rightarrow S_{n+1}$: Jede kürzeste Lösung, der Länge $2^{n+1} - 1$, versetzt den n–Turm von A nach B mit $2^n - 1$ Zügen, dann die Scheibe $n+1$ von A nach C mit einem Zug, und schließlich den n–Turm von B nach C mit $2^n - 1$ Zügen. Dank S_n gelingt dies auf genau eine Weise, also gilt S_{n+1}.

Die Türme von Hanoi

C448
Ergänzung

Dieses Logikspiel wurde 1883 vom französischen Mathematiker Édouard Lucas erfunden. Es erfreut sich seither großer Beliebtheit und führt immer wieder zu überraschenden mathematischen Fragen.

Das Problem mit 3 Stäben ist leicht. H.E. Dudeney fragte 1908 nach optimalen Lösungen bei 4 Stäben. Seine Vermutung blieb über hundert Jahre lang offen und wurde erst 2014 bewiesen von Thierry Bousch: *La quatrième tour de Hanoï*, Bull. Belg. Math. Soc. 21 (2014) 895–912.

Allgemein für $k \geq 3$ Stäbe gibt es eine elegante, rekursive Lösung von J.S. Frame und B.M. Stewart (Amer. Math. Monthly, 1941). Im Falle $k = 3$ ist dies die eindeutige optimale Lösung mit $2^n - 1$ Zügen. Auch im Falle $k = 4$ ist die Frame–Stewart–Lösung optimal, wie Thierry Bousch zeigte. Für $k \geq 5$ hingegen ist die Optimalität weiterhin eine offene Vermutung.

📖 Mehr hierzu finden Sie im Buch von A.M. Hinz, S. Klavžar, C. Petr: *The Tower of Hanoi – Myths and Maths*, 2nd ed., Birkhäuser 2018.

🙂 Scheinbar einfache Probleme, selbst Kinderspiele, führen schnell zu tiefliegenden mathematischen Fragen – wenn wir nur genau hinsehen.

PORC: Finde ein Muster! Dann beweise es per Induktion!

Wir definieren die Folge $a_1, a_2, a_3, \ldots \in \mathbb{N}$ rekursiv (dank Satz F2B) durch den Startwert $a_1 = 1$ und für alle $n \geq 2$ die Rekursionsvorschrift:

$$a_n = \begin{cases} a_{n-1} + n + 1 & \text{falls } d := \mathrm{ggT}(a_{n-1}, n) = 1, \\ a_{n-1}/d & \text{falls } d := \mathrm{ggT}(a_{n-1}, n) > 1. \end{cases}$$

Aufgabe: (0) Berechnen Sie (per Hand) die ersten zehn Folgenwerte.

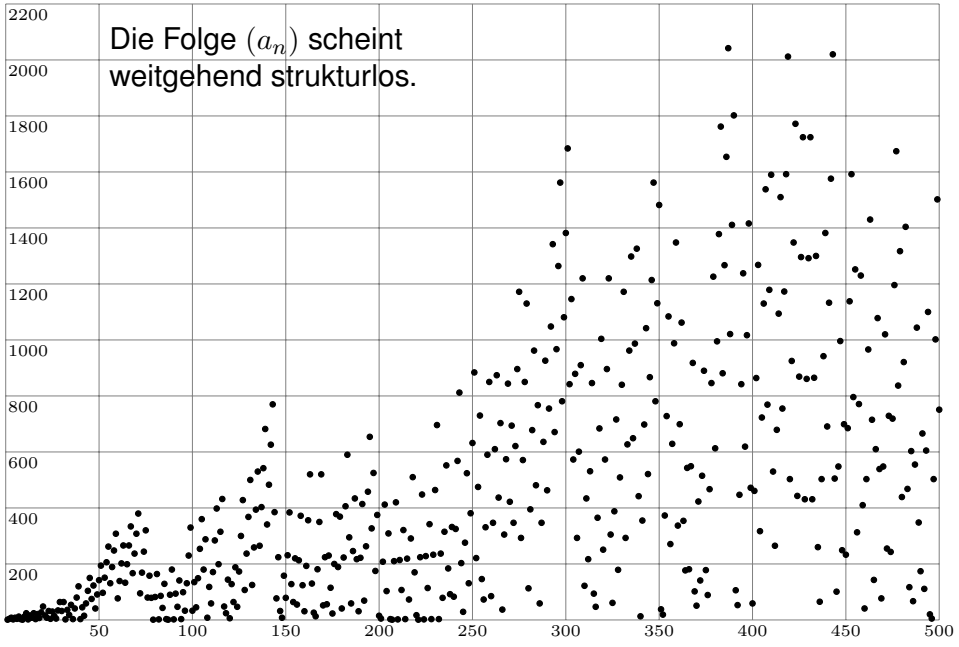
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a_n	1	4	8	2	8	4	12	3	1	12	24	2	16	8	24	3

Aufgabe: Erlaubt die Zuordnung $n \mapsto a_n$ eine geschlossene Formel? Sobald Sie ein Muster erkennen, formulieren und beweisen Sie es!

(1) Plotten Sie (per Computer) die ersten 500 Folgenwerte.
(2) Plotten Sie (per Computer) die ersten 1000 Folgenwerte.

⚠ Das ist in der Realität die typische Situation: Die Aussage ist noch nicht vorformuliert, sondern muss erst gefunden werden: Dies gelingt durch **Exploration** und dann **Konsolidierung** in Form eines Beweises.

PORC: Finde ein Muster! Dann beweise es per Induktion!



PORC: Finde ein Muster! Dann beweise es per Induktion!

Um uns einen graphischen Überblick zu verschaffen, berechnen und plotten wir die ersten 500 Folgenwerte. Hier in Python und LaTeX/TikZ:

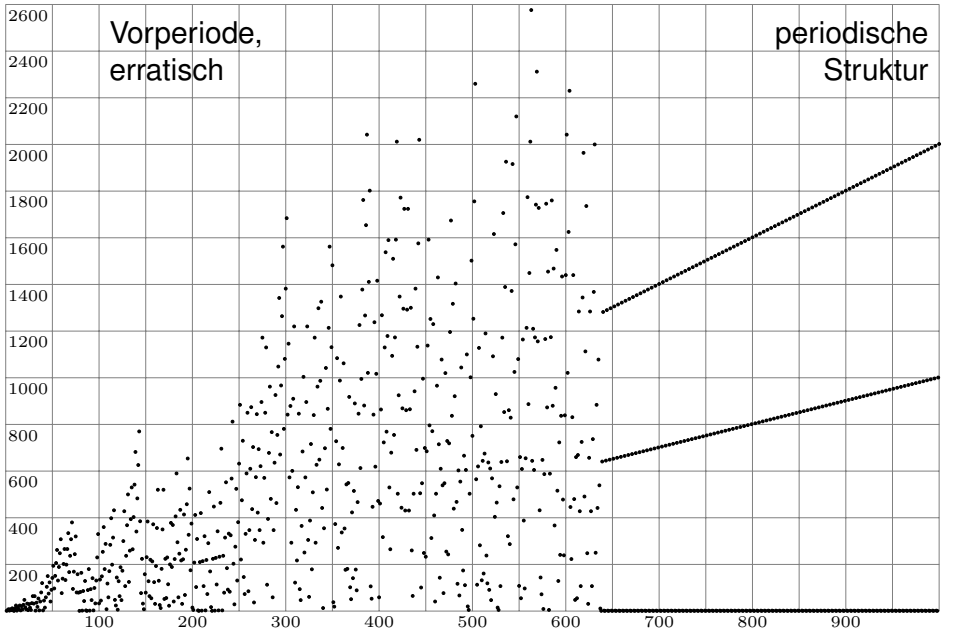
```
from math import gcd
a = 1; max = 500
for n in range(1, max):
    print(str(n) + '/' + str(a) + ', ', end='')
    d = gcd(a, n+1)
    if d > 1: a = a // d
    else:     a = a + n+2
print(str(max) + '/' + str(a))
```

Dies berechnet und druckt die ersten 500 Folgenwerte: `1/1, 2/4, 3/8, 4/2, 5/8, 6/4, 7/12, 8/3, 9/1, 10/12, 11/24, ..., 500/751`

Diese Liste von Koordinaten (x, y) habe ich oben mit TikZ geplottet. Diese Daten sehen zunächst völlig strukturlos aus, doch dann...

☺ Sehen Sie selbst! Bei $n = 638$ geschieht plötzlich ein Wunder...

PORC: Finde ein Muster! Dann beweise es per Induktion!



PORC: Finde ein Muster! Dann beweise es per Induktion!

C453 Übung

Lösung: Die Folge $(a_n)_{n\in\mathbb{N}}$ scheint anfangs weitgehend strukturlos. Die Graphik bis $n = 500$ verschafft uns einen ersten groben Überblick. In der zweiten Graphik bis $n = 1000$ geschieht etwas Unerwartetes, ein Wunder: Die Folge wird plötzlich vollkommen regelmäßig.

Wie entsteht dieses Wunder? Der Wert $a_n = 1$ wird immer wieder angenommen, zunächst an den Stellen $n = 1, 9, 79, 87, 207, 221, 638$. Dies ist der erste *gerade* Index n mit $a_n = 1$. Für alle $n \geq 638$ gilt dann:

$$a_n = \begin{cases} 1 & \text{für } n = 4k+2, \\ n+2 & \text{für } n = 4k+3, \\ 2n+2 & \text{für } n = 4k+4, \\ 2 & \text{für } n = 4k+5. \end{cases}$$

Für $n \geq 638$ ist $n \mapsto a_n$ *polynomial on residue classes*, kurz *PORC*.

Aufgabe: (3) Beweisen Sie diese Gleichungen per Induktion über n.

🙂 Steht diese Aussage einmal vor Ihnen, so ist der Nachweis leicht: Als bewährtes Standardverfahren greift hier die vollständige Induktion!

PORC: Finde ein Muster! Dann beweise es per Induktion!

C454 Übung

Lösung: Wir beweisen die obige Behauptung per Induktion.

Induktionsanfang: Für $n = 638 = 4 \cdot 159 + 2$ gilt die Aussage $a_n = 1$.

⚠ Oft ist der Induktionsanfang leicht und der Induktionsschritt knifflig. Hier ist es umgekehrt: Der Induktionsanfang bei $n = 638$ erfordert die explizite Berechnung aller vorhergehenden Werte $a_1, a_2, a_3, \ldots, a_{638}$. Per Hand ist diese Rechnung zwar möglich, doch lang und monoton, recht mühselig und fehleranfällig. Zum Glück haben wir Computer!

Induktionsschritt: Wir wenden die Rekursionsvorschrift an:

$$a_n = \begin{cases} a_{n-1} + n + 1 & \text{falls } d := \operatorname{ggT}(a_{n-1}, n) = 1, \\ a_{n-1}/d & \text{falls } d := \operatorname{ggT}(a_{n-1}, n) > 1. \end{cases}$$

Sei nun $n > 638$. Wir nutzen die Induktionsvoraussetzung für a_{n-1}:
Für $n = 4k+3$ gilt $a_{n-1} = 1$, daraus folgt $d = 1$ und $a_n = n + 2$.
Für $n = 4k+4$ gilt $a_{n-1} = n + 1$, also $d = 1$ und $a_n = 2n + 2$.
Für $n = 4k+5$ gilt $a_{n-1} = 2n$, also $d = n$ und somit $a_n = 2$.
Für $n = 4k+2$ gilt $a_{n-1} = 2$, also $d = 2$ und somit $a_n = 1$.

PORC: Finde ein Muster! Dann beweise es per Induktion!

C455 Übung

Im Rückblick betrachtet ist die Struktur des Beweises klar und einfach: Steht die zu beweisende Aussage erst einmal ausformuliert vor uns, so führen wir, wie so oft, routiniert eine vollständige Induktion durch. Hierzu genügt eine sorgsame Rechnung und Fallunterscheidung.

Und die Moral von der Geschicht? An dieser Aufgabe erkennen und erfahren Sie einige wichtige Phänomene, die für die mathematische Arbeit typisch sind, aber in Lehrbüchern meist unterrepräsentiert und in Klausuren wenn überhaupt nur in Miniatur möglich:

🙂 Oft ist noch keine Aussage vorformuliert, sondern mögliche Muster müssen erst gefunden werden: (1) Diese **Exploration** erfordert meist Ausprobieren, geschickt gewählte Beispiele, kritische Beobachtung, usw. (2) Ist eine Beobachtung / Aussage / Vermutung bereits formuliert, so suchen wir eine **Konsolidierung** in Form eines Beweises.

🙂 Beide Phasen erfordern mathematisches Geschick und Kreativität! In Ihren Hausaufgaben haben Sie Zeit für beides, bitte nutzen Sie dies. Nur so können Sie mathematische Arbeit selbst erfahren und erlernen.

PORC: Finde ein Muster! Dann beweise es per Induktion!

C456 Übung

🙂 Der Computer ist das Teleskop / Mikroskop der Mathematik. Nutzen Sie seine Möglichkeiten und kennen Sie seine Limitationen. Lernen Sie frühzeitig, dieses mächtige Hilfsmittel effizient anzuwenden!

Der Computer unterstützt Ihre Arbeit. Er nimmt Ihnen zwar nicht die Beobachtungen / Formulierungen / Beweise ab, aber er erledigt für Sie lästige Rechnungen, klaglos und zuverlässig. Dank der Ergebnisse dieser Rechnungen können Sie den Kern des Problems erfassen, Muster erkennen, Aussagen formulieren und anschließend beweisen!

🙂 Wie im obigen Beispiel zeigen sich Muster oft erst auf großer Skala, die für Handrechnungen nur schwer oder gar nicht zugänglich ist. Hierzu programmieren und nutzen Sie einen Computer!

Sie sehen dies eindrücklich im obigen Beispiel: Ohne die Graphiken hätten Sie das Muster nicht erkannt. Ohne die Berechnung von a_{638} hätten Sie den Induktionsanfang nicht beweisen können.

Solche Weisheiten lernen Sie nur durch Erfahrung. Diese Erfahrung gewinnen Sie nur durch das eigenständige Lösen von Aufgaben.

Welche Rolle spielt Logik im Alltag?

C501
Erläuterung

Mathematiker/innen wird gerne vorgeworfen, dass sie alles zu genau nehmen. Umgekehrt wird von ihnen verlässliche Präzision gefordert.

Which one is it? You cannot have it both ways!
Everybody gangsta until the equations start lying.

Zu Beginn des Kapitels habe ich einfache Alltagsbeispiele aufgeführt, für die präzise Formulierung und unbestechliche Logik wesentlich sind.

Für viele Anwendungen ist diese Klarheit wünschenswert, gar essentiell: Wirtschaft und Verträge: Wurde fristgerecht geliefert / überwiesen? Naturwissenschaft und Technik: Hat das Instrument angeschlagen? Gesellschaft: Hat Kandidat X die Wahl gewonnen? Sport: Gilt das Tor?

Im Rückblick auf dieses Kapitel komme ich auf dieses Spannungsfeld zwischen mathematischer Logik und alltäglichen Anwendungen zurück. Hierzu möchte ich Sie mit ein paar provokanten Beispielen konfrontieren und zum kritischen Nachdenken anregen. Es lohnt sich.

Welche Rolle spielt Induktion im Alltag?

C502
Erläuterung

Ich frage offen: **Spielt Induktion im Alltag überhaupt eine Rolle?** Für die formal ausgeführte, vollständige Induktion lautet die ehrliche Antwort wohl: fast nie! Doch bei genauerem Hinsehen erweist sich dann das Gegenteil: fast überall! Wie kann beides gleichzeitig wahr sein?

Diese **paradoxe Wahrnehmung** gilt für nahezu alle mathematischen Sätze und Techniken: Sie treten meist nicht als allgemeiner Sachverhalt in Erscheinung, sondern werfen lediglich einen Schatten in Form von konkreten Rechnungen und speziellen Anwendungen.

Für die mathematische Kennerin sind die logischen Grundlagen und dazu die mathematischen Werkzeuge klar und ihr Nutzen offensichtlich. Der mathematisch Unerfahrene jedoch verkennt jegliche Verbindung von Theorie und Anwendung und bestreitet vehement ihren Nutzen.

Der häufig wiedergekäute Vorwurf „Das ist reine Theorie ohne konkrete Anwendung“ ist daher meist keine Aussage über den mathematischen Gegenstand, sondern vielmehr ein Bekenntnis des Sprechers zu seiner eigenen Ignoranz. Bitte achten Sie in Zukunft bewusst darauf.

Wo finden wir Induktion / Rekursion im Alltag?

C503
Erläuterung

Nun will ich meine kühnen Thesen mit konkreten Beispielen belegen. Logik und Präzision treten besonders deutlich dort in Erscheinung, wo es um etwas geht: bei strategischen Überlegungen, zum Beispiel bei finanziellen Entscheidungen, oder etwas lockerer in Spielen.

Dabei verwenden wir ständig Induktion, ganz intuitiv und allgegenwärtig. Es ist meist keine *vollständige* Induktion, diese ist auch gar nicht nötig, für viele Anwendungen genügen endlich viele, gar wenige Schritte. Sobald die Anzahl unübersichtlich wird, machen wir schnell Fehler.

Nichtsdestotrotz ist das Prinzip der Induktion hier klar und deutlich: Wir zerlegen das gegebene Problem schrittweise in kleinere Probleme. In Blickrichtung von klein zu groß spricht man von Induktion, umgekehrt von groß zurück zu klein von Rekursion oder auch Rückwärtsinduktion.

Die folgenden erstaunlichen Beispiele stammen aus der Spieltheorie; ihre Lösung ist elementar, erfordert aber etwas Geduld und Sorgfalt. Sie illustrieren wunderbar, wie häufig uns (endliche) Induktion nützt. Es lohnt sich also, diese Technik zu erlernen und anzuwenden.

Wo finden wir Induktion / Rekursion im Alltag?

C504
Erläuterung

Verstehen kann man das Leben nur rückwärts,
leben muss man es aber vorwärts.
Søren Kierkegaard (1813–1855)

In den folgenden Beispielen wird die Induktion nicht formal ausgeführt; mit Ihren Kenntnissen können Sie das anschließend leicht nachholen. Stattdessen wird rekursiv argumentiert und damit informell gerechnet; hier wird Induktion *praktiziert*, und zwar meist etwas versteckt.

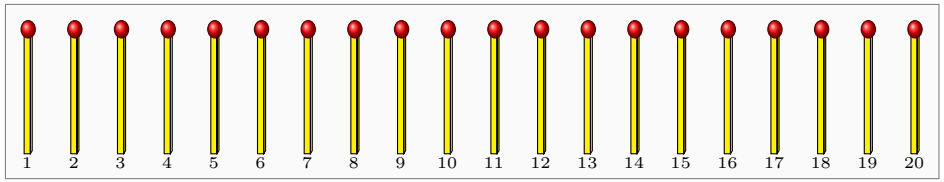
Richard Bellman (1920–1984) war ein US-amerikanischer Mathematiker. Er entwickelte 1953 die Kernidee der **Dynamischen Programmierung**. Das traditionelle Wort „Programmierung“ bedeutet dabei so viel wie „Planung“ oder „Optimierung“, hier rekursiv / induktiv angewendet.

Ökonomen bezeichnen die Dynamische Programmierung schlicht als **Rekursionsmethode**. Sie tritt bei zahlreichen Optimierungsproblemen natürlich auf und wird gerne und erfolgreich angewendet. Sie ist daher ein beliebtes Universalwerkzeug der Wirtschaftswissenschaften.

Einzeiliges Nim und Rekursion / Induktion

C505

Auf dem Tisch liegen anfangs $x \in \mathbb{N}$ Streichhölzer / Münzen / Steine.
Die Spieler ziehen abwechselnd, jeder entfernt ein oder zwei Hölzer.
Normalspiel / Misèrespiel: Wer nicht mehr ziehen kann, verliert / gewinnt.



Bevor Sie weiterlesen sollten Sie dieses Spiel einige Male durchspielen, am besten zu zweit. Folgen Sie Ihrer Neugier: Es macht Spaß!

Beobachten Sie dabei ihren Lernprozess vom *Whaaa?* bis zum *Aha!* Anfangs werden Sie vermutlich wenig Struktur erkennen. Mit Erfahrung ahnen Sie gewisse Regelmäßigkeiten. Diese können Sie in folgender Aufgabe ausarbeiten und schließlich die allgemeine Regel formulieren.

Am Ende steht ein mathematischer Satz als Extrakt Ihrer Erfahrungen. Diesen können Sie induktiv beweisen und zukünftig getrost anwenden!

Einzeiliges Nim und Rekursion / Induktion

C506
Übung

Aufgabe: (0) Schreiben Sie eine Funktion zur rekursiven Berechnung: Der Wert 0 steht für eine Verlustposition und 1 für eine Gewinnposition.

Lösung: (0a) Misèrespiel μ: Wer nicht mehr ziehen kann, gewinnt.

```
def mu(x):
    if x == 0: return 1   # Wer nicht mehr ziehen kann, gewinnt.
    return 1 - min( mu(y) for y in range(max(0,x-2), x) )
```

(0b) Normalspiel ν: Wer nicht mehr ziehen kann, verliert.

```
def nu(x):
    if x == 0: return 0   # Wer nicht mehr ziehen kann, verliert.
    return 1 - min( nu(y) for y in range(max(0,x-2), x) )
```

Aufgabe: Bestimmen Sie die Anzahl $f(x)$ der Funktionsaufrufe.

Lösung: Wir finden $f(0) = 0$ und $f(1) = 1$ sowie für alle $x \in \mathbb{N}_{\geq 2}$ rekursiv $f(x) = f(x-1) + f(x-2)$. Dies ist die Fibonacci–Folge!

⚠ Bei dieser naiven Methode wächst der Aufwand exponentiell mit x!

Einzeiliges Nim und Rekursion / Induktion

C507

Aufgabe: (1) Was sind Verlustpositionen? Was sind Gewinnzüge?

Lösung: (1) Wir berechnen rekursiv Gewinn 1 und Verlust 0 für das Misèrespiel μ bzw. das Normalspiel ν und erhalten folgende Tabelle:

$x=$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\mu=$	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
$\nu=$	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1

Quidquid agis, prudenter agas et respice finem!
[Was immer du tust, handele klug und bedenke das Ende!]

(2) Wie lautet die allgemeine Regel? Damit krönen wir unsere Analyse:

Satz C5A: einzeiliges Nim mit Zugoptionen $S = \{1, 2, \ldots, n-1\}$

Misèrespiel: Genau dann ist x eine Verlustposition, wenn $x \bmod n = 1$.
Normalspiel: Genau dann ist x eine Verlustposition, wenn $x \bmod n = 0$.

Übung: Beweisen Sie diesen Satz per Induktion über $x \in \mathbb{N}$.

Einzeiliges Nim und Rekursion / Induktion

C508
Übung

Der naiv-rekursive Algorithmus (0) benötigt exponentiellen Aufwand in x. Die Tabelle (1) berechnen wir ebenso rekursiv. Da wir jedoch die zuvor berechneten Ergebnisse speichern, ist der Aufwand nur noch linear in x. Das ist eine dramatische Verbesserung! Berechnen Sie so etwa $\nu(100)$.

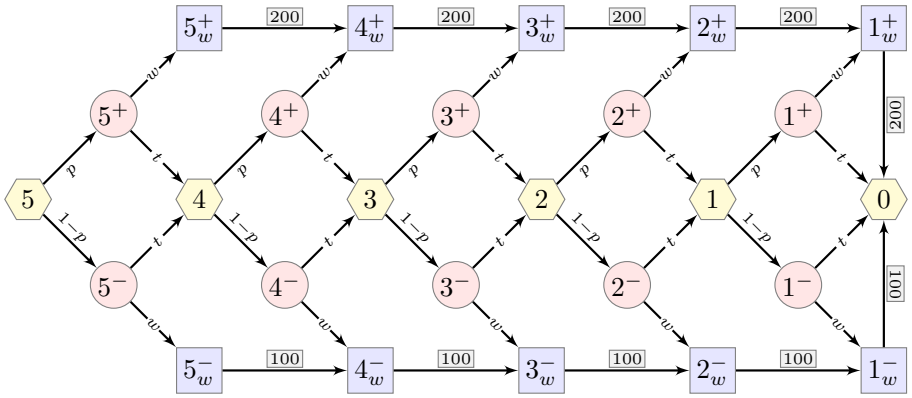
☹ Rekursion hat unter Anfänger/innen meist einen schlechten Ruf: Zuerst sind Denkweise und Progammiertechnik nicht leicht zu erlernen. Ist diese Hürde genommen, so folgt gleich die erste Ernüchterung: Naive Implementierung führt meist zu exponentiellem Aufwand.

🙂 Rekursion entfaltet ihre wahre Kraft erst durch raffiniert-effiziente Implementierung: Die genial-einfache Idee hierzu heißt **Memoisation**, das geschickte Speichern der zuvor berechneten Zwischenergebnisse, von lat. **Memorandum**, kurz **Memo**, *das zu Erinnernde*.

🙂 Im vorliegenden Falle vollendet Satz C5A unsere Lösung durch eine weitere dramatische Optimierung: Die Berechnung von $x \bmod n$ benötigt nur noch logarithmischen Aufwand, gemäß Ziffernzahl $\text{len}(x) \sim \log_2(x)$. Sie ist zudem so einfach, dass wir sie im Kopf ausführen können!

Optimierung durch Rekursion / Induktion

Aufgabe: Ihr Work&Travel endet in 5 Wochen. Zu Beginn jeder Woche erhalten Sie ein Jobangebot: mit Wkt $p = 0.4$ ist es gut für 200€, mit Wkt $1 - p = 0.6$ schlecht für 100€. Wenn Sie es annehmen, bleiben Sie für die restliche Zeit dabei. Andernfalls reisen Sie eine Woche umher.



Wie viel können Sie erwarten? Ist 700€ möglich? Geht mehr? optimal?

Optimierung durch Rekursion / Induktion

Sie sehen hier den sorgsamen Übergang von der realen Fragestellung zu einem **mathematischen Modell**: Dies nennen wir **Modellierung**.

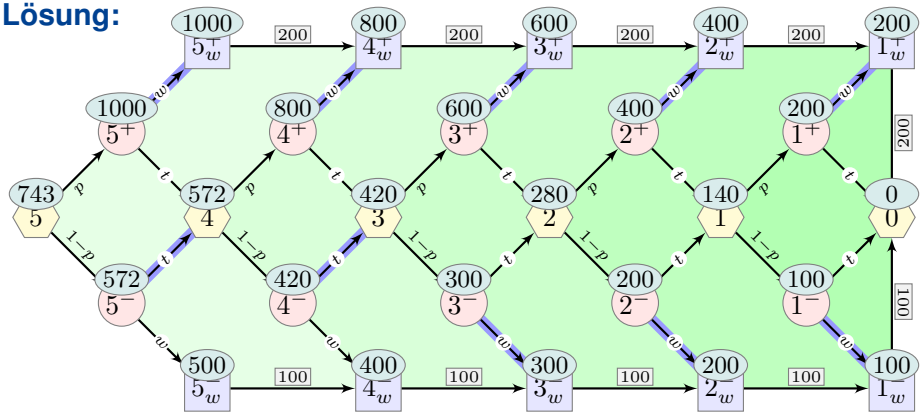
Meist gibt es mehrere mögliche Modelle zur gegebenen Fragestellung: Der umgangssprachliche Text ist wunderbar anschaulich und hoffentlich motivierend. Leider ist er in manchen Details noch nicht explizit, sondern appelliert an Weltwissen und Konventionen. Die Übersetzung in einen Graphen ist kurz und zudem präzise: Hier bleiben keine Fragen offen. Zum Beispiel: Reisen und Arbeiten kostet gleich viel Lebensunterhalt. Andernfalls codieren wir Reisekosten und Lebensunterhalt im Graphen.

Der hier gezeigte Graph ist ein **Markov–Graph**, denn er enthält neben den Spielzügen als möglichen Aktionen des Spielers realistischerweise auch Zufallszüge, auf die der Spieler keinen Einfluss hat. *That's life.*

In jeder der zehn Entscheidungssituationen $5^\pm, 4^\pm, 3^\pm, 2^\pm, 1^\pm$ muss eine Entscheidung für $w =$ work oder $t =$ travel getroffen werden. Es gibt also $2^{10} = 1024$ Strategien. Die optimale finden Sie durch Rekursion!

Optimierung durch Rekursion / Induktion

Lösung:



In Worten: Einen guten Job nehmen Sie immer an, einen schlechten nur in den letzten 3 Wochen. Bei ≥ 4 Wochen lohnt sich noch abzuwarten.

Diese quantitative Analyse erfordert vor allem Sorgfalt und Geduld. Die entscheidende Idee ist, vom Ende aus rekursiv vorzugehen.

☺ Gespielt wird vorwärts, optimiert wird rückwärts: per Induktion!

Optimierung durch Rekursion / Induktion

⚠ Wenn Sie diese Art von Problemstellung zum ersten Mal erkunden, sind Sie vermutlich versucht, in der Zeit wie üblich *vorwärts* zu denken.

☺ Wir lösen das Problem rekursiv, indem wir *rückwärts* argumentieren. Das führt zum Erfolg: Rekursives Denken ist zielgerichtetes Denken!

Das Thema Rekursion ist ebenso wichtig wie sagenumwoben. Dazu gibt es zahlreiche Weisheiten, teils ernst, teils scherzhaft:

Um Rekursion zu verstehen, muss man klein anfangen
und zunächst einmal Rekursion verstehen.

Insbesondere in der Programmierung ist Rekursion allgegenwärtig. Sie ist ein Universalwerkzeug zum Lösen komplexer Probleme.

Recursion makes good programmers better
and bad programmers obvious.

Übung: Probieren Sie einige der anderen 1023 Strategien aus.
Gibt es bessere? gleich gute? Die Sachlage erweist sich als knifflig!
Warum spreche ich dennoch kurzerhand von *der* optimalen Strategie?
Ist wenigstens die optimale Gewinnerwartung eindeutig / wohldefiniert?

Übung: Vorwärts gelesen scheinen nach den Entscheidungen $2^{\pm} \mapsto w$ alle folgenden Entscheidungen $\{3^{\pm}, 4^{\pm}\} \to \{w, t\}$ ganz überflüssig!
Warum müssen Sie sich dennoch ebenso genau damit befassen?
Sind diese Züge wichtig für das Spiel? oder für die Analyse?

Unser kunstvoller Graph hilft uns zunächst einmal zur Anschauung, aber dann auch ganz praktisch zur Organisation unserer Rechnung.
Die Rechnung kann automatisiert werden! **Topologische Sortierung** heißt in der Informatik jede geschickte Reihenfolge der Positionen, so dass jedes Teilproblem nur kleinere nutzt, die bereits berechnet wurden.

Übung: Implementieren Sie die Rechnung in einer Tabellenkalkulation.
Sie finden eine einfache Lösung in der Datei `Work-and-Travel.ods`.

	A	B	C	D	E	F	G	H	I	J	K
1	**Work and Travel**		Week -5		Week -4		Week -3		Week -2		Week -1
2			1000,00		800,00		600,00		400,00		200,00
3	0,400	1000,00	0,400	800,00	0,400	600,00	0,400	400,00	0,400	200,00	
4	743,20	maximize	572,00	maximize	420,00	maximize	280,00	maximize	140,00	maximize	0,00
5	0,600	572,00	0,600	420,00	0,600	300,00	0,600	200,00	0,600	100,00	
6			500,00		400,00		300,00		200,00		100,00

Übung: Variieren Sie die Konstanten, berechnen Sie weitere Beispiele.
Durch solche *Erfahrung* entwickeln Sie ein *Gefühl* für das Problem.

Verfeinerungen: (a) Mit Wkt $q^{\pm}$ wird Ihnen zu Wochenbeginn gekündigt.
(b) Reisen / Arbeiten kostet Geld, zur Vereinfachung einen festen Betrag.
(c) Sie benötigen mindestens 400€, ansonsten maximieren Sie.
Das erweitert den Graphen, die Lösungsmethode bleibt gleich.

🙂 Der Mensch ist fähig, meist jedoch widerwillig, komplexe logische Zusammenhänge zu durchdringen, insbesondere Rekursion / Induktion.

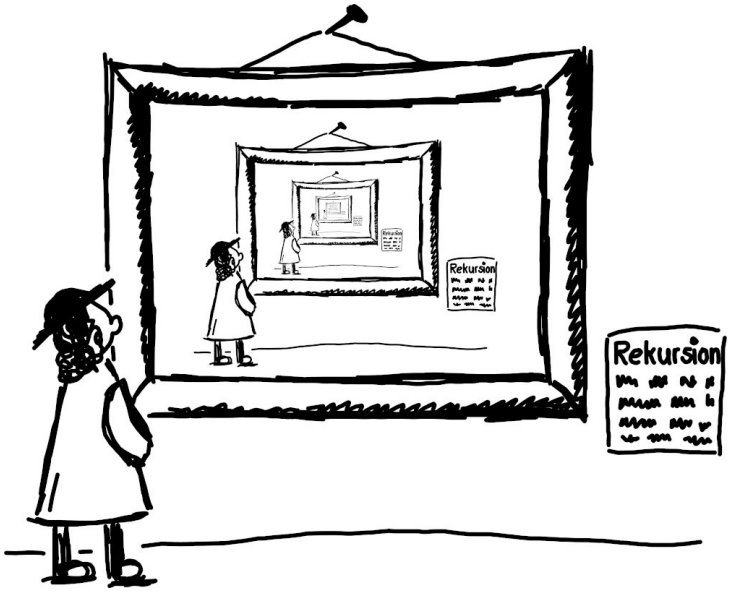
Thinking fast and slow von Daniel Kahneman, Wirtschaftsnobelpreis 2002, unterscheidet zwei verschiedene Arbeitsweisen unseres Gehirns:

1. Schnell, automatisch, immer aktiv, emotional, stereotyp, unbewusst
2. Langsam, anstrengend, selten aktiv, logisch, berechnend, bewusst

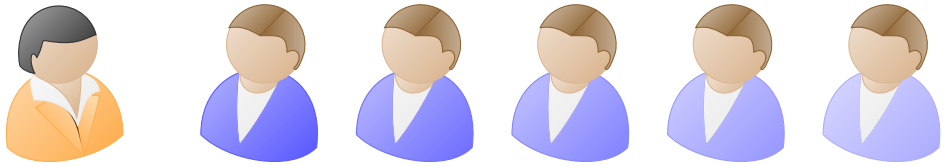
Sie vertrauen oft Ihrem Instinkt, Bauchgefühl oder Erfahrung, insb. wenn Sie keine genaue Information haben oder keine Zeit, sie auszuwerten.

Ihr Verstand braucht wesentlich länger, um zu einem Urteil zu kommen. Das lohnt sich, wenn Sie die Muße haben und das Ziel wichtig genug ist.

In Ihrem Mathematikstudium lernen Sie diese zweite Vorgehensweise. Dies hilft zu umsichtiger Analyse und vorausschauendem Handeln.



Marriage problem: When to stop dating and start to get married?



Alice begegnet im Laufe ihres Lebens n potentiellen Ehemännern.
Bei Kandidat $k = 1, 2, 3, \ldots, n$ stellt sie die Eignung $X_k \in [0, 1]$ fest.

Er verliebt sich in die bezaubernde Alice, sie kann ihn nun heiraten oder zurückweisen. Diese Entscheidung ist in jedem Falle endgültig.

Aufgabe: Wie anspruchsvoll soll Alice sein? Was ist optimal?
Welche Eignung ihres Ehepartners kann Alice maximal erwarten?

Die Zufallsvariablen $X_1, \ldots, X_n$ seien unabhängig und gleichverteilt.
(Übung für Hartgesottene: Andere Verteilungen sind ebenso möglich.)

Lösung: Alice ermittelt die optimale Strategie durch Rekursion wie folgt:
Sie heiratet den letzten Kandidaten n auf jeden Fall. Erwartete Eignung:

$$\mu_n = \mathbf{E}(X_n) = 1/2$$

Sie heiratet Kandidat $n-1$, falls $X_{n-1} > \mu_n$. Erwartete Eignung:

$$\mu_{n-1} = \mathbf{E}(\max(X_{n-1}, \mu_n)) = 1/2 \cdot 1/2 + 1/2 \cdot 3/4 = 5/8$$

Sie heiratet Kandidat $n-2$, falls $X_{n-2} > \mu_{n-1}$. Erwartete Eignung:

$$\mu_{n-2} = \mathbf{E}(\max(X_{n-2}, \mu_{n-1})) = 5/8 \cdot 5/8 + 3/8 \cdot 13/16 = 89/128$$

☺ Alice' Ansprüche steigen, je mehr Kandidaten noch warten.
Ihre Ansprüche sinken, je weniger Kandidaten noch bleiben.

Das ist anschaulich klar und entspricht der Alltagserfahrung.
Nun können wir es begründen und genauer quantifizieren.

Vielleicht klingt das alles recht herzlos und übertrieben formal,
aber so ganz unrealistisch ist es dann auch wieder nicht!

Für den folgenden Satz kehren wir die Nummerierung um:
Die „Rückwärtsinduktion" ist eine ganz normale Induktion!

Satz C5B: optimale Partnerwahl: Looking for Mr. Right

Alice optimiert die Partnerwahl wie folgt. Sie setzt $a_0 = 0$ und rekursiv

$$a_{n+1} = (1 + a_n^2)/2 \qquad \text{für alle } n \in \mathbb{N}.$$

Warten noch genau $n+1$ Kandidaten, so heiratet Alice den nächsten Kandidaten genau dann, wenn seine Eignung größer als a_n ist.

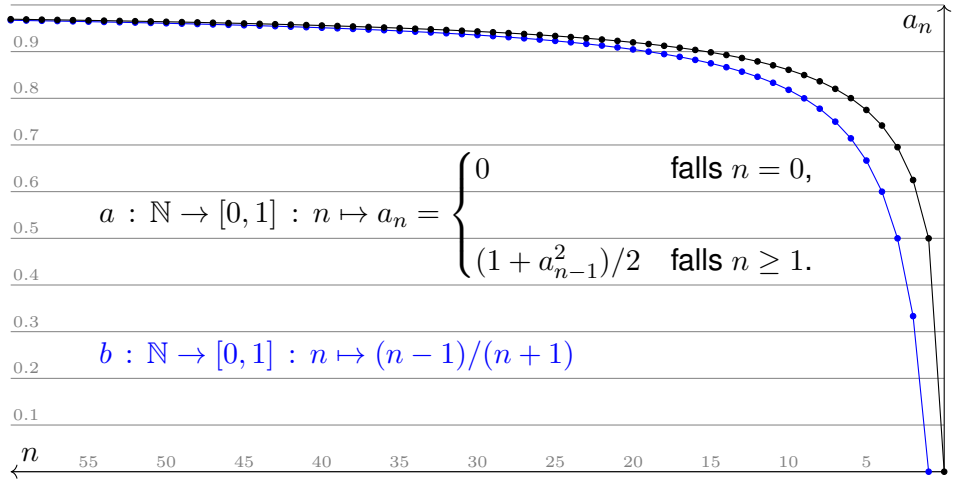
Mit dieser optimalen Strategie erwartet Alice die Eignung a_{n+1}.
Die Folge $(a_n)_{n\in\mathbb{N}}$ wächst streng monoton und konvergiert gegen 1.

Übung: Beweisen Sie diesen Satz per Induktion über $n \in \mathbb{N}$.

☺ Die ungefähre Form der Kurve $n \mapsto a_n$ ist anschaulich plausibel.
Die genauen Werte können wir wie oben berechnen – und beweisen.

☺ Steht diese Aussage einmal vor Ihnen, so ist der Nachweis leicht:
Als bewährtes Standardverfahren greift hier die vollständige Induktion!

Alice' Erwartung bzw. Anspruch a_n als Funktion der Kandidatenzahl n:

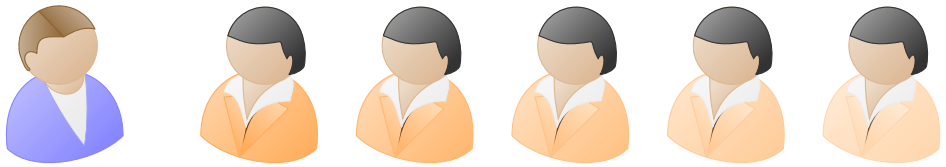


Fun fact: b_n ist die Erwartung des *zweithöchsten* Wertes in $X_1, \ldots, X_n$.
Alice optimiert erfolgreich, doch es bleibt etwas Wehmut: Eines Tages begegnet ihr Mr. Right, doch sie ist schon mit Mr. Almost verheiratet.

Optimales Stoppen: das Sekretärinnen-Problem

C521
Erläuterung

Secretary problem: When to stop interviewing and start hiring?



Bob 1 2 3 ... n

Bob möchte eine Sekretärinnen einstellen. Dazu sind n Bewerberinnen eingeladen, in zufälliger Reihenfolge. Bob sucht die beste Kandidatin, doch nur im Interview mit Kandidatin k kann er feststellen, ob sie besser ist als alle vorigen. Er kann sie nun sofort einstellen oder ihr absagen. Diese Entscheidung ist in jedem Falle endgültig.

Aufgabe: Wie soll Bob vorgehen? Wie maximiert er seine Trefferwkt?

Die 37%–Regel: Interviewe zunächst n/e Kandidatinnen mit Absage; dann wähle die nächste Kandidatin, die besser ist als alle vorigen.
Das klingt verrückt? Es ist nachweislich die beste Strategie!

Optimales Stoppen: der Bruss–Algorithmus

C522
Erläuterung

Problem: Sie bekommen n Angebote zu Zeiten $t = 1, 2, 3, \ldots, n$.
Wir setzen $X_t = 1$, falls Angebot t besser ist als alle vorigen $1, \ldots, t-1$.

Sie können solch ein Angebot entweder annehmen ($s =$ select $=$ stop) oder dieses Angebot ein für alle Mal ablehnen ($r =$ reject $=$ resume).

Sie wollen unter allen Angeboten das beste auswählen,
also das letzte Angebot t mit $X_t = 1$ annehmen.

Beispiele: Eine optimale Online-Auktion mit sofortiger Zu- oder Absage. Den besten Gebrauchtwagen kaufen. Die beste Tankstelle entlang einer langen Straße auswählen. Die beste Sekretärin einstellen. Heiraten?

(a) Die Zufallsvariablen $X_1, X_2, \ldots, X_n$ seien unabhängig
mit den Wkten $\mathbf{P}(X_t{=}1) = p_t$ und $\mathbf{P}(X_t{=}0) = q_t = 1 - p_t$.

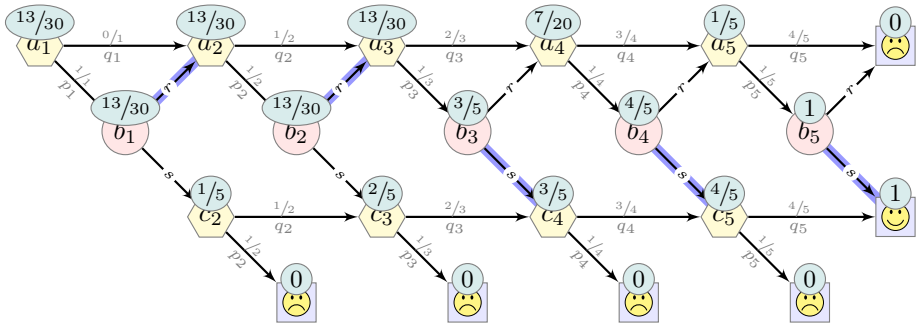
(b) Speziell betrachten wir n unterschiedlich gute Angebote in zufälliger Reihenfolge, mit Gleichverteilung der $n!$ Anordnungen, also $p_t = 1/t$.

Aufgabe: (1) Formulieren Sie dieses Spiel als einen Markov–Graphen.
(2) Was ist die beste Strategie? (3) Was ist die optimale Erfolgswkt?

Optimales Stoppen: der Bruss–Algorithmus

C523
Erläuterung

Beispiel: Wir untersuchen $n = 5$ mit $p_k = 1/k$ und $q_k = 1 - p_k$.



Aufgabe: Wie gelingt dies allgemein? Beweisen Sie folgenden Satz:

Satz C5c: optimales Stoppen, Bruss 2000

Sei $s \in \{1, \ldots, n\}$ der größte Index mit $R_s := \sum_{k=s}^{n} p_k/q_k \geq 1$. Dann ist folgende Strategie optimal: Wähle das erste Angebot $k \geq s$ mit $X_k = 1$.

Die optimale Gewinnwkt ist dabei gleich $R_s Q_s$ mit $Q_s = q_s \cdots q_n$.

Anwendung: Für $p_k = 1/k$ gilt $s \gtrapprox n/\mathrm{e}$ und $R_s Q_s \gtrapprox 1/\mathrm{e} \gtrapprox 0.367$.

Optimales Stoppen: der Bruss–Algorithmus

C524
Erläuterung

☺ Dieser Satz ist wunderbar effizient und sein Beweis ebenso elegant.
Der Algorithmus stammt aus dem wunderschönen Artikel von F.T. Bruss:
Sum the odds to one and stop. Ann. of Prob. 28 (2000) 1384–1391.

Beweis: Wir berechnen die Gewinnwkt w in jedem Zustand a_k, b_k, c_k bei optimaler Strategie. Wie immer gehen wir hierzu rekursiv vor:

Im Zustand c_k ist die Gewinnwkt offensichtlich $w(c_k) = Q_k := q_k \cdots q_n$.
Wir setzen $R_k := p_k/q_k + \cdots + p_n/q_n$ und finden s mit $R_s \geq 1 > R_{s+1}$.
Terminal, für $k = n+1$, gilt $w(c_k) = 1 = Q_k$ und $w(a_k) = 0 = R_k Q_k$.

(1) Im Falle $R_k < 1$ gilt $w(a_k) = R_k Q_k$ und $w(a_{k-1}) = R_{k-1} Q_{k-1}$:
Im Zustand b_{k-1} wählen wir zwischen $w(a_k) = R_k Q_k$ und $w(c_k) = Q_k$.
Da wir $R_k < 1$ voraussetzen, entscheiden wir uns optimal für c_k.
Daraufhin gilt $w(a_{k-1}) = p_{k-1} Q_k + q_{k-1} R_k Q_k = R_{k-1} Q_{k-1}$.

(2) Im Falle $R_k \geq 1$ hingegen entscheiden wir uns optimal für a_k.
(Für $R_k = 1$ herrscht Indifferenz, die Wahl c_k wäre genauso gut.)
Die Gewinnwkt ist dann $w(a_{k-1}) = w(a_k)$, wie oben gezeigt.
Für alle $k = 1, \ldots, s$ gilt daher $w(a_k) = w(a_s) = R_s Q_s$. QED

Optimales Stoppen: der Bruss–Algorithmus

Die optimale Stoppzeit s_n und die Gewinnwkt w_n für $n = 1, \ldots, 40$:

n	1	2	3	4	5	6	7	8	9	10
s_n	1	2	2	2	3	3	3	4	4	4
w_n	1	$1/2$	$1/2$	$11/24$	$13/30$	$77/180$	$29/70$	...	...	...
$\approx$	1.000	0.500	0.500	0.458	0.433	0.428	0.414	0.410	0.406	0.399

n	11	12	13	14	15	16	17	18	19	20
s_n	5	5	6	6	6	7	7	7	8	8
w_n	0.398	0.396	0.392	0.392	0.389	0.388	0.387	0.385	0.385	0.384

n	21	22	23	24	25	26	27	28	29	30
s_n	9	9	9	10	10	10	11	11	11	12
w_n	0.383	0.383	0.382	0.381	0.381	0.380	0.380	0.379	0.379	0.379

n	31	32	33	34	35	36	37	38	39	40
s_n	12	13	13	13	14	14	14	15	15	16
w_n	0.378	0.378	0.378	0.377	0.377	0.377	0.376	0.376	0.376	0.376

Optimales Stoppen: der Bruss–Algorithmus

Übung: Wählen Sie einen kleinen Wert n und berechnen Sie das Paar (s_n, w_n) von Hand. Vorbild: Der Fall $n = 5$ ist oben detailliert ausgeführt. Kontrolle: Für $n \leq 7$ finden Sie den exakten Wert w_n in obiger Tabelle.

Aufgabe: Schreiben Sie ein Programm zur Berechnung von (s_n, w_n). Kontrolle: Vergleichen Sie Ihre Werte mit der obigen Tabelle.

Lösung: In Python sieht eine mögliche Lösung wie folgt aus:

```
1 def bruss(n):
2     k = n; r = 0
3     while r < 1: k -= 1; r += 1/k
4     return k+1, r*k/n
```

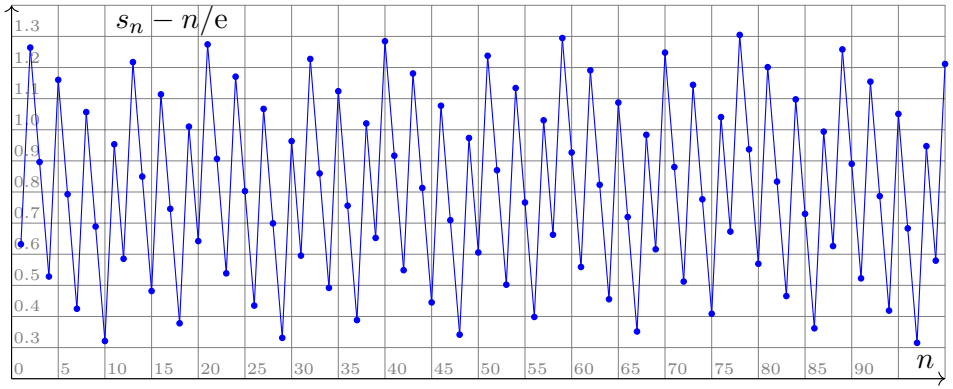
Der Aufruf `bruss(5)` liefert als Ergebnis das Wertepaar `3, 0.433`.
Auf diese Weise wurden die Werte für die obige Tabelle berechnet.

🙂 Die Korrektheit dieser Rechnung verdanken wir dem obigen Satz:
Grundlagen / Theorie und Programmierung / Anwendung ergänzen sich!

Optimales Stoppen: der Bruss–Algorithmus

Aufgabe: Vergleichen Sie die Stoppzeit s_n mit der Faustformel n/e.

Lösung: Die Berechnung übernimmt bequem unser obiges Programm.
Die folgende Graphik zeigt die Differenz $s_n - n/\mathrm{e}$ für $n = 1, \ldots, 100$:



Somit gilt $s_n = \lceil n/\mathrm{e} \rceil$ oder $s_n = \lceil n/\mathrm{e} \rceil + 1$, zumindest für alle $n \leq 100$.
Das bietet eine einfache, doch recht genaue Näherungsformel für s_n.

Optimales Stoppen: der Bruss–Algorithmus

🙂 Wenn Sie die logische Entwicklung dieser Aufgabe nachvollziehen, werden Sie ein interessantes Wechselspiel erkennen und verstehen:

- Wir beginnen mit einem **konkreten Beispiel**, nämlich der Analyse des Spiels für den Fall $n = 5$.
- Dadurch erkennen wir das **allgemeine Muster** und können dies anschließend als Satz C5C beweisen.
- Mit dem so gewonnenen Algorithmus können wir **weitere Beispiele** lösen und mehr Daten erschließen.
- Daran beobachten wir ein **genaueres Muster**. Dies wollen wir nun als Satz C5D beweisen!

Dieses Wechselspiel von theoretischen Grundlagen und praktischen Anwendungen, von mathematischen Sätze und numerischen Experimenten, ist durchaus typisch und überaus erfolgreich.

🙂 So können wir uns langsam auf unbekanntes Terrain vortasten, Muster erkennen, Vermutungen formulieren und Ergebnisse beweisen.

Optimales Stoppen: der Bruss–Algorithmus

Zu $n \in \mathbb{N}_{\geq 2}$ suchen wir die Stoppzeit s_n. Unsere numerischen Experimente lassen uns die folgende einfache Regel vermuten:

Satz C5D: die 37%–Regel

Das Sekretärinnen-Problem wird durch folgende Faustformel gelöst:

(1) Für alle $n \in \mathbb{N}_{\geq 2}$ gilt $s_n = \lceil n/\mathrm{e} \rceil$ oder $s_n = \lceil n/\mathrm{e} \rceil + 1$, kurzum:

$$\boxed{s_n \approx n/\mathrm{e}}$$

(2) Die Gewinnerwkt ist $w_n = R_s Q_s$ mit $R_s \gtrapprox 1$ und $Q_s = (s-1)/n$, also:

$$\boxed{w_n \approx 1/\mathrm{e}}$$

Für $n \to \infty$ gilt $s_n/n \to 1/\mathrm{e}$ und $w_n \to 1/\mathrm{e}$. Als numerische Werte haben wir $\mathrm{e} \approx 2.718$ und $1/\mathrm{e} \approx 0.368$, daher der Name „$37\%$–Regel“.

Aufgabe: Beweisen Sie diese Näherungen. *Tipp:* Approximieren Sie hierzu die Summe durch ein Integral, $\sum_{k=s}^{n-1} \frac{1}{k} \gtrapprox \int_s^n \frac{1}{x}\,\mathrm{d}x = \ln(n/s)$.

Optimales Stoppen: der Bruss–Algorithmus

Lösung: (1) Vorgegeben ist die natürliche Zahl $n \in \mathbb{N}_{\geq 2}$.
Wir suchen die Lösung $s \in \{1, \dots, n\}$ zu folgender Ungleichung:

$$(*) \qquad \sum_{k=s+1}^{n} \frac{1}{k-1} \;<\; 1 \;\leq\; \sum_{k=s}^{n} \frac{1}{k-1}$$

Der Vergleich von Summe und Integral liefert hier:

$$\sum_{k=s}^{n-1} \frac{1}{k} \;\geq\; \int_{x=s}^{n} \frac{1}{x}\,\mathrm{d}x \;=\; \ln\Big(\frac{n}{s}\Big)$$

$$\sum_{k=s-1}^{n-1} \frac{1}{k} \;\leq\; \int_{x=s-2}^{n-1} \frac{1}{x}\,\mathrm{d}x \;=\; \ln\Big(\frac{n-1}{s-2}\Big)$$

Wir setzen dazu stillschweigend $s \geq 3$ voraus, also $n \geq 5$.
Die kleinen Fälle $n \leq 4$ lösen wir direkt, wie oben gezeigt.

Optimales Stoppen: der Bruss–Algorithmus

Wir nutzen nun die Doppelungleichung $(*)$ und schließen:

$$\ln\Big(\frac{n}{s}\Big) < 1 \quad\Longrightarrow\quad s > n/\mathrm{e}$$

$$\ln\Big(\frac{n-1}{s-2}\Big) \geq 1 \quad\Longrightarrow\quad s \leq n/\mathrm{e} + 2 - 1/\mathrm{e}$$

Da s eine ganze Zahl ist, folgt durch Auf/Abrunden:

$$\lceil n/\mathrm{e} \rceil \leq s \leq \lfloor n/\mathrm{e} + 2 - 1/\mathrm{e} \rfloor$$

Das bedeutet $s = \lceil n/\mathrm{e} \rceil$ oder $s = \lceil n/\mathrm{e} \rceil + 1$, oder zusammengefasst:

$$\boxed{s \in \lceil n/\mathrm{e} \rceil + \{0, 1\}}$$

Für große n ist die kleine verbleibende Unsicherheit $\{0, 1\}$ unerheblich.
Für kleine n können wir mühelos eine Tabelle anlegen, wie oben erklärt.
Allgemeiner Satz und numerische Rechnung ergänzen sich wunderbar!

Optimales Stoppen: der Bruss–Algorithmus

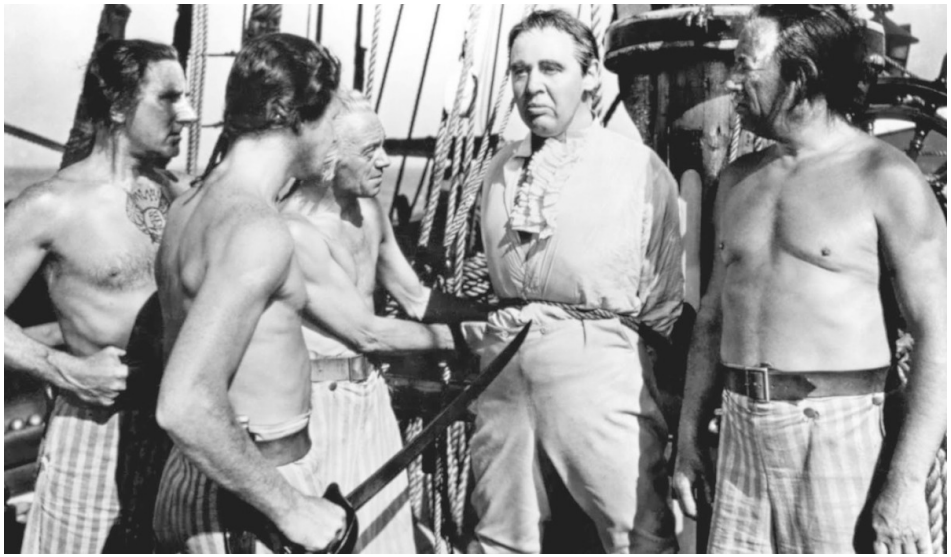
Damit ist das Sekretärinnen-Problem gelöst, theoretisch und praktisch.
Es ist ein Paradebeispiel für die rekursive Lösung komplexer Probleme.
In der schön konkreten Geschichte steckt abstrakt allgemeine Wahrheit.
Solche Modelle werden tatsächlich genutzt für Online-Auktionen u.ä.

Das ist nur die Spitze des Eisbergs, damit beginnt erst das Abenteuer!
Fragen des **optimalen Stoppens** finden sich nahezu überall in der Stochastik, insbesondere der Ökonomik und der Finanzmathematik, zum Beispiel beim Börsenhandel mit Aktien oder Optionen.

Die Frage lautet allgemein: Wie wählen wir den optimalen Zeitpunkt für eine Aktion? Unser Ziel ist es, den erwarteten Gewinn zu maximieren oder die erwarteten Kosten zu minimieren. Viele solche Probleme können rekursiv gelöst werden, so wie in unserem Beispiel.

Diese Knobelaufgabe ist also nicht nur lehrreich für den Themenkreis Induktion / Rekursion / Rückwärtsinduktion, sondern zugleich ein erstes Anwendungsbeispiel, ein motivierender Startpunkt für die Optimierung, hier einer Stoppzeit, die weitreichende Anwendungen erschließt.

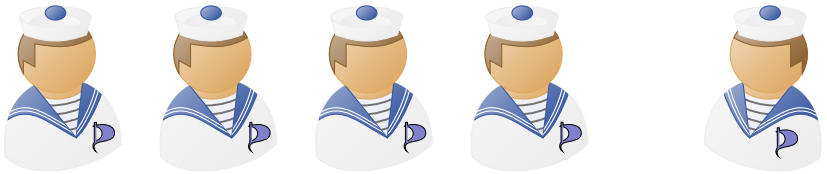
Meuterei auf der Bounty (1935)



Mutiny on the Bounty mit Clark Gable und Charles Laughton
unter der Regie von Frank Lloyd. Oscar 1936 als bester Film.

Fünf gierige Piraten [*the pirate game*]

Fünf basisdemokratische Piraten $1, 2, 3, 4, 5$ teilen sich 100 Dukaten.
(nach Ian Stewart: *A Puzzle for Pirates.* Scientific American 5/1999)



Der ranghöchste Pirat 5 schlägt eine Zuteilung zur Abstimmung vor.
Stimmt mindestens die Hälfte dafür, so wird diese Zuteilung ausgeführt.
Bei Ablehnung wird der Vorschlagende über Bord ins Meer geworfen,
und die verbleibenden Piraten beginnen das Spiel von vorn.

Präzisierung: Ein Dukat ist unteilbar. Jeder Pirat will A: selbst überleben, B: möglichst viel Gold, C: bei Indifferenz lieber andere ins Meer werfen, D: lieber rangniedrige bestechen als ranghohe. Jeder Pirat ist rational. Absprachen sind unmöglich, denn jeder misstraut jedem anderen und würde Absprachen brechen. Diese Fakten sind gemeinsames Wissen.

Fünf gierige Piraten [*the pirate game*]

Naiv könnte man vermuten, der ranghöchste Pirat muss um sein Leben fürchten und daher all sein Gold hergeben. Das Gegenteil ist der Fall!

Aufgabe: Lösen Sie das Piratenrätsel für $n = 5$, sowie für alle $n \in \mathbb{N}$.

Lösung: Wir nutzen Induktion über $n = 1, 2, 3, 4, 5, \ldots$ und finden:

	1	2	3	4	5	…	197	198	199	200	201	202
	100	☠	☠	☠	☠	…	☠	☠	☠	☠	☠	☠
$\mathscr{R}_1$	0	100	☠	☠	☠	…	☠	☠	☠	☠	☠	☠
$\mathscr{R}_2$	1	0	99	☠	☠	…	☠	☠	☠	☠	☠	☠
$\mathscr{R}_3$	0	1	0	99	☠	…	☠	☠	☠	☠	☠	☠
$\mathscr{R}_4$	1	0	1	0	98	…	☠	☠	☠	☠	☠	☠
⋮												
$\mathscr{R}_{197}$	0	1	0	1	0	…	0	2	☠	☠	☠	☠
$\mathscr{R}_{198}$	1	0	1	0	1	…	1	0	1	☠	☠	☠
$\mathscr{R}_{199}$	0	1	0	1	0	…	0	1	0	1	☠	☠
$\mathscr{R}_{200}$	1	0	1	0	1	…	1	0	1	0	0	☠
$\mathscr{R}_{201}$	0	1	0	1	0	…	0	1	0	1	0	0

Fünf gierige Piraten [*the pirate game*]

🙂 Scharfsinn, Systematik & Induktion liefern die erstaunliche Antwort!
Wir nutzen die Prioritäten A–C und strenge Rationalität, insb. Egoismus ohne Kooperation. Real beobachtetes Verhalten kann davon abweichen.

⚠ Im Spiel mit $n \geq 201$ Piraten geht es nur noch ums Überleben!
Der Vorschlagende $n = 201, 202, 204, 208, \ldots$ kann überleben,
der Verschlagende $n = 203, 205, 206, 207, \ldots$ leider nicht.

Zur Analyse zerlegen wir $n = 200 + 2^k + r$ mit $k, r \in \mathbb{N}$ und $0 \leq r < 2^k$.

Im Falle $0 < r < 2^k$ geht Pirat n über die Planke, egal was er vorschlägt:
Er kann nur 100 Piraten bestechen. Dazu bekommt er alle r Stimmen der Todgeweihten (inklusive seiner selbst). Das bleibt eine Minderheit.

Im Falle $r = 0$ überlebt Pirat $n = 200 + 2^k$ durch folgende Strategie:

- Falls k gerade ist, gibt er allen Ungeraden $1, 3, \ldots, 199$ je ein Dukat.
- Falls k ungerade ist, gibt er allen Geraden $2, 4, \ldots, 200$ je ein Dukat.

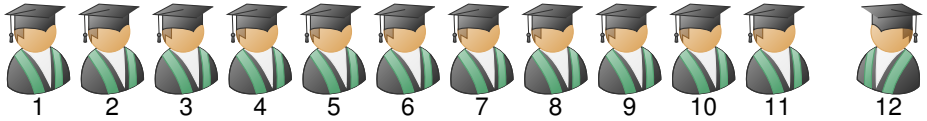
So bekommt er alle 100 Stimmen der Bestochenen und zusätzlich noch alle $2^k - 2^{k-1} = 2^{k-1}$ Stimmen der Geretteten (inklusive seiner selbst).

🙂 Prioritäten A–D lösen Indifferenzen und garantieren Eindeutigkeit.

Ein Komitee zur Verbesserung der Hochschullehre

C537
Übung

Die chronisch unterfinanzierte Hochschullehre soll mit einer Förderung von $50\,\text{k€}$ exzellent werden. (Das ist aberwitzig, aber besser als nichts.) Ein Komitee von zwölf Professoren teilt die Fördersumme unter sich auf.



Der dienstälteste Professor 12 legt eine Zuteilung zur Abstimmung vor. Bei Ablehnung wird der Vorschlagende als befangen ausgeschlossen, und die verbleibenden Professoren beginnen das Komiteespiel von vorn. Präzisierung: Ein k€ ist unteilbar. Weiter gelten obige Piratenregeln.

Aufgabe: Welcher Professor erhält wie viel von der Fördersumme? Lösen Sie das Komiteespiel mit folgenden Abstimmungsregeln:
(1) Annahme erfordert mehr als die Hälfte der Stimmen.
(2) Annahme erfordert mindestens zwei Drittel der Stimmen.
(3) Annahme gilt erst bei höchstens einer Gegenstimme.

Das Komiteespiel: mehr als die Hälfte

C538
Übung

Lösung: (1) Wir nutzen Induktion über $n = 1, 2, \ldots, 12$ und finden:

n	q	1	2	3	4	5	6	7	8	9	10	11	12
1	1	50	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠
2	2	50	0	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠
3	2	0	1	49	☠	☠	☠	☠	☠	☠	☠	☠	☠
4	3	1	2	0	47	☠	☠	☠	☠	☠	☠	☠	☠
5	3	2	0	1	0	47	☠	☠	☠	☠	☠	☠	☠
6	4	0	1	2	1	0	46	☠	☠	☠	☠	☠	☠
7	4	1	2	0	0	1	0	46	☠	☠	☠	☠	☠
8	5	2	0	1	1	0	1	0	45	☠	☠	☠	☠
9	5	0	1	2	0	1	0	1	0	45	☠	☠	☠
10	6	1	2	0	1	0	1	0	1	0	44	☠	☠
11	6	2	0	1	0	1	0	1	0	1	0	44	☠
12	7	0	1	2	1	0	1	0	1	0	1	0	43

Jeder Vorsitzende n kann sich das Quorum $q = 1 + \lfloor n/2 \rfloor$ billig erkaufen und sich selbst den Löwenanteil des zu verteilenden Geldes sichern.

Das Komiteespiel: mindestens zwei Drittel

C539
Übung

Lösung: (2) Wir nutzen Induktion über $n = 1, 2, \ldots, 12$ und finden:

n	q	1	2	3	4	5	6	7	8	9	10	11	12
1	1	50	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠
2	2	50	0	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠
3	2	0	1	49	☠	☠	☠	☠	☠	☠	☠	☠	☠
4	3	1	2	0	47	☠	☠	☠	☠	☠	☠	☠	☠
5	4	2	3	1	0	44	☠	☠	☠	☠	☠	☠	☠
6	4	3	0	2	1	0	44	☠	☠	☠	☠	☠	☠
7	5	0	1	3	2	1	0	43	☠	☠	☠	☠	☠
8	6	1	2	0	3	2	1	0	41	☠	☠	☠	☠
9	6	2	3	1	0	0	2	1	0	41	☠	☠	☠
10	7	3	0	2	1	1	0	2	1	0	40	☠	☠
11	8	0	1	3	2	2	1	0	2	1	0	38	☠
12	8	1	2	0	3	0	2	1	0	2	1	0	38

Jeder Vorsitzende n kann sich das Quorum $q = \lfloor 3n/2 \rfloor$ billig erkaufen und sich selbst den Löwenanteil des zu verteilenden Geldes sichern.

Das Komiteespiel: höchstens eine Gegenstimme

C540
Übung

Lösung: (3) Wir nutzen Induktion über $n = 1, 2, \ldots, 12$ und finden:

n	q	1	2	3	4	5	6	7	8	9	10	11	12
1	1	50	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠
2	1	0	50	☠	☠	☠	☠	☠	☠	☠	☠	☠	☠
3	2	1	0	49	☠	☠	☠	☠	☠	☠	☠	☠	☠
4	3	2	1	0	47	☠	☠	☠	☠	☠	☠	☠	☠
5	4	3	2	1	0	44	☠	☠	☠	☠	☠	☠	☠
6	5	4	3	2	1	0	40	☠	☠	☠	☠	☠	☠
7	6	5	4	3	2	1	0	35	☠	☠	☠	☠	☠
8	7	6	5	4	3	2	1	0	29	☠	☠	☠	☠
9	8	7	6	5	4	3	2	1	0	22	☠	☠	☠
10	9	8	7	6	5	4	3	2	1	0	14	☠	☠
11	10	9	8	7	6	5	4	3	2	1	0	5	☠
12	11	0	9	8	7	6	5	4	3	2	1	5	0

Professor 12 kann sich nicht genug Unterstützung erkaufen. Professor 11 hingegen bringt seinen Vorschlag mit überwältigender Mehrheit durch.

Tanz der Vampire: Wissen und gemeinsames Wissen

In Transsylvanien treffen sich einmal jedes Jahr 100 Vampire zum Tanz.
Anschließend verharren sie den Rest des Jahres schlafend in der Gruft.

Vampire altern nicht, sind untrüglich intelligent und vollkommen rational.
Jeder weiß dies. Auch dies weiß jeder. Selbst dies weiß jeder. Usw.

Jeder Vampir trägt ein Schandmal deutlich sichtbar auf seiner Stirn.
Dies weiß keiner von sich selbst, da Vampire kein Spiegelbild werfen.
Erführe er es, er suchte den Freitod im nächsten Sonnenaufgang.
(Diese Vampire verbrennen im Sonnenlicht. *Wear sunscreen!*)

Hingegen sieht jeder Vampir das Schandmal bei jedem anderen.
Jeder sieht es. Jeder weiß es. Auch dies weiß jeder. Usw. usw. usw.
Höfliche Rücksicht gebietet jedoch strenges Stillschweigen darüber.
(Tabuisierte Kommunikation der Vampire ist ihre große Schwäche.)

Im Jahr 2001 platzt der Vampirjäger Professor Abronsius in das Fest:
„Mindestens einer von Euch trägt ein Schandmal!“ schreit er und flieht.
Die Vampire sehen keinen Grund, seiner Aussage zu widersprechen:
Er sagt ihnen nur, was ohnehin jeder heimlich weiß. Oder etwa nicht?

Tanz der Vampire: Wissen und gemeinsames Wissen

Vampire werfen bekanntlich kein Spielbild.
Das führt zu komplizierten Verwicklungen.

Aufgabe: Was geschieht? Nichts? Plötzliche Erkenntnis? Wann?

Lösung: Nach dem Fest 2100 sterben alle Vampire im Sonnenaufgang.
Führen Sie sorgfältig einen Beweis per Induktion: Was ist die Aussage?
Wie ist das möglich? Welche Neuigkeit hat der Professor verraten?

Tanz der Vampire: Wissen und gemeinsames Wissen

Hier geht es um gemeinsames Wissen / *common knowledge*.
Nur weil eine Aussage wahr ist, weiß dies noch längst nicht jeder!
Nur weil es jeder weiß, ist es noch kein gemeinsames Wissen!

Die untrügliche Intelligenz der Vampire ist gemeinsames Wissen:
$\mathscr{R}_1$: Jeder Vampir ist untrüglich intelligent und vollkommen rational.
$\mathscr{R}_k$: Es gilt $\mathscr{R}_{k-1}$, und jeder Vampir weiß $\mathscr{R}_{k-1}$. (Stufe $k \in \mathbb{N}_{\geq 2}$)
$\mathscr{R}_\infty$: Es gilt $\mathscr{R}_k$ für alle $k \in \mathbb{N}_{\geq 1}$. (gemeinsames Wissen)

Die Anzahl der Schandmale hingegen ist kein gemeinsames Wissen:
$\mathscr{S}_1$: Jeder ehrbare Vampir sieht alle n Schandmale der anderen,
jeder Schandmalträger jedoch sieht genau $n-1$ Schandmale.
$\mathscr{S}_k$: Es gilt $\mathscr{S}_{k-1}$, und jeder Vampir weiß $\mathscr{S}_{k-1}$. (Stufe $k \in \mathbb{N}_{\geq 2}$)
$\mathscr{S}_\infty$: Es gilt $\mathscr{S}_k$ für alle $k \in \mathbb{N}_{\geq 1}$. (gemeinsames Wissen)

Professor Abronsius' Aussage hingegen liefert stärkere Information:
$\mathscr{A}_1$: Jeder Vampir weiß, dass es mindestens ein Schandmal gibt.
$\mathscr{A}_k$: Es gilt $\mathscr{A}_{k-1}$, und jeder Vampir weiß $\mathscr{A}_{k-1}$. (Stufe $k \in \mathbb{N}_{\geq 2}$)
$\mathscr{A}_\infty$: Es gilt $\mathscr{A}_k$ für alle $k \in \mathbb{N}_{\geq 1}$. (gemeinsames Wissen)

Tanz der Vampire: Wissen und gemeinsames Wissen

Es lohnt sich, diese berüchtigte Rätsel sorgfältig zu durchleuchten!
Wir nehmen hierzu an, genau n Vampire tragen ein Schandmal,
und behaupten: Diese sterben am Morgen nach Fest $2000+n$.

Im Falle $n=1$ ahnt der Träger zunächst nichts vom Schandmal.
Durch Abronsius' Aussage erkennt er seine Schande und stirbt bei
Sonnenaufgang. (Wir nutzen die Voraussetzungen $\mathscr{A}_1$, $\mathscr{S}_1$ und $\mathscr{R}_1$.)

Im Falle $n=2$ erwarten die beiden Träger den Freitod des anderen.
Beim Fest 2002 treffen sie sich jedoch wieder, völlig unerwartet.
Dadurch erkennt jeder der beiden klar seine Schande und stirbt.
(Wir nutzen hierzu die Voraussetzungen $\mathscr{A}_2$, $\mathscr{S}_2$, $\mathscr{R}_2$ und den Fall 1.)

Per Induktion gilt dieses Argument für jede natürliche Zahl $n \in \mathbb{N}_{\geq 2}$:
Jeder der n Träger sieht genau $n-1$ Schandmale und geht davon aus,
dass er keines trägt. Er erwartet daher den Freitod der $n-1$ anderen
nach dem Fest $2000+n-1$. Alle treffen sich jedoch beim Fest $2000+n$
unerwartet wieder. Dadurch erkennt jeder zweifelsfrei seine Schande.
(Wir nutzen hierzu die Voraussetzungen $\mathscr{A}_n$, $\mathscr{S}_n$, $\mathscr{R}_n$ und den Fall $n-1$.)

Schmutzige Gesichter: eigenes und gegenseitiges Wissen

C545
Übung

Hier ein berühmtes Logikrätsel aus der Folklore der Talmudschulen als Zentren jüdischer Gelehrsamkeit. (de.wikipedia.org/wiki/Jeschiwa) Es handelt von eigenem Wissen und von gegenseitigem Wissen...

(1) Rabbi: „Zwei Männer klettern durch einen Kamin. Der eine kommt mit sauberem Gesicht heraus, der andere mit schmutzigem. Wer von beiden geht sich nun waschen?“ — Schüler: „Na wohl der mit dem schmutzigen Gesicht!“ — „Falsch! Der Schmutzige sieht den Sauberen und denkt, sein Gesicht sei auch sauber. Der Saubere sieht den Schmutzigen und denkt, sein Gesicht sei auch schmutzig, also geht er sich waschen.“

(2) Rabbi: „Zwei Männer klettern durch einen Kamin. Der eine kommt mit sauberem Gesicht heraus, der andere mit schmutzigem. Wer von beiden geht sich nun waschen?“ — Schüler: „Aber wir haben doch eben schon festgestellt: der mit dem sauberen Gesicht!“ — „Falsch: Beide gehen sich waschen. Überlege logisch: Der Saubere sieht den Schmutzigen und geht sich waschen. Der Schmutzige sieht das und versteht, dass sein Gesicht schmutzig ist, also geht auch er sich waschen.“

Schmutzige Gesichter: eigenes und gegenseitiges Wissen

C546
Übung

(3) Rabbi: „Zwei Männer klettern durch einen Kamin. Der eine kommt mit sauberem Gesicht heraus, der andere mit schmutzigem. Wer von beiden geht sich nun waschen?“ — Schüler: „Na, beide gehen sich waschen.“ — „Falsch: Keiner von beiden. Der Schmutzige sieht den Sauberen und geht sich nicht waschen. Der Saubere sieht das und versteht, dass sein Gesicht sauber ist, also geht auch er sich nicht waschen.“

(4) „Zwei Männer klettern durch einen Kamin...“ — „Ich weiß, keiner von beiden wird sich waschen.“ — „Falsch! Sage mir: Wie kann es sein, dass zwei Männer durch denselben Kamin klettern, und der eine macht sein Gesicht schmutzig, der andere aber nicht? Die ganze Frage ist unsinnig. Wenn du dein Leben dazu verwendest, sinnlose Fragen zu beantworten, werden auch alle deine Antworten sinnlos sein.“

Aufgabe: Wie lösen Sie den Widerspruch zwischen (2) und (3)?

Lösung: Zur Festlegung dieses Spiels fehlen uns noch Informationen: Wir benötigen die genaue Reihenfolge der Züge / Signale / Folgerungen! Erst zieht Spieler 1, dann Spieler 2 mit dem Wissen des vorigen Zuges.

Schmutzige Gesichter: eigenes und gegenseitiges Wissen

C547
Übung

Schmutzige Gesichter gibt es in vielen Rätseln, hier etwa in der Bahn:

Das Mathematische Forschungsinstitut Oberwolfach liegt wunderbar idyllisch mitten im Schwarzwald, etwa zweidrittelwegs von Stuttgart nach Freiburg. Im Zug zu unserem fiktiven Workshop „Mathematical Logic“ sitzen 12 berühmte Logiker, manche davon mit schmutzigem Gesicht. Alle können sich gegenseitig sehen, es gibt jedoch keinen Spiegel, und diese überaus schüchternen Menschen reden nicht miteinander.

Der Schaffner erklärt der Gruppe höflich: „Mindestens zwei von Ihnen haben schmutzige Gesichter. Diese sollten schnellstmöglich aussteigen und sich waschen.“ An den nächsten Bahnhöfen $1, 2, 3, 4, 5$ passiert noch nichts. Erst am sechsten Bahnhof steigen einige der Passagiere aus, um sich das Gesicht zu waschen. Wie viele sind es?

Aufgabe: Lösen Sie dieses Logikrätsel. Präzisieren Sie alle hierzu nötigen Annahmen. Warum ist der Takt der Bahnhöfe wichtig?

Lösung: Genau sieben Personen haben ein schmutziges Gesicht. (Die Zahl 12 ist hier vollkommen beliebig und überflüssig.)

Schmutzige Gesichter: eigenes und gegenseitiges Wissen

C548
Übung

Angenommen, es gibt genau $n \in \{2, 3, \dots, 12\}$ schmutzige Gesichter.

Im Falle $n = 2$ wissen die beiden Betroffenen sofort Bescheid: Jeder der beiden sieht nur ein schmutziges Gesicht. Nach Aussage des Schaffners gibt es jedoch mindestens zwei. Daraus schließt jeder Betroffene richtig, das sein Gesicht schmutzig ist, und steigt am 1. Bahnhof aus.

Im Falle $n = 3$ sieht jeder Betroffene genau zwei schmutzige Gesichter und erwartet daher, dass diese am 1. Bahnhof aussteigen werden, wie zuvor im Fall $n = 2$ erklärt. Da dies jedoch nicht geschieht, folgert er richtig, das sein Gesicht schmutzig ist, und steigt am 2. Bahnhof aus.

Das Argument setzt sich per Induktion für alle n fort. Dazu muss gelten: $\mathscr{R}_2$: Jeder kann richtig sehen und logisch schließen, wie oben erklärt. $\mathscr{R}_3$: Es gilt $\mathscr{R}_2$, und jeder weiß es. $\mathscr{R}_n$: Es gilt $\mathscr{R}_{n-1}$, und jeder weiß es.

Konkretes Beispiel: Alle Betroffenen steigen am sechsten Bahnhof aus. Demnach gibt es genau sieben Personen mit schmutzigem Gesicht.

Der vorgegebene Takt der Bahnhöfe ist wesentlich, damit allen klar ist, wann eine Aktion ausgeführt werden kann oder unterlassen wurde.

Das Problem der Stuttgarter Mathematiker

Das folgende Rätsel stammt aus *Forschung und Lehre* (5/2019, S.503):

An der Universität Stuttgart gibt es 17 Professoren (m/w) im Fachbereich Mathematik. Sie treffen sich einmal im Monat bei Sitzungen. Bei einer früheren Sitzung haben sie die Regel eingeführt, dass jeder Professor, der von einem Fehler in einer von ihm selbst publizierten Arbeit erfährt, sein Amt bei der nächsten Sitzung niederlegen muss. Noch nie ist ein Professor zurückgetreten. Das bedeutet aber nicht, dass keiner der Professoren je einen Fehler publiziert hat. Im Gegenteil, jeder Professor hat schon Fehler publiziert, und jeder andere hat das bemerkt. Man könnte auch so sagen: Jeder Professor weiß, dass jeder andere Professor schon Fehler gemacht hat, weiß aber nichts von eigenen Fehlern. Eines Tages besucht der Rektor der Universität den Fachbereich und hält eine kleine Ansprache, in der er einen denkwürdigen Satz spricht: „Ich muss Ihnen mitteilen, dass ein Professor unter Ihnen bemerkt hat, dass ein anderer Professor einen Fehler publiziert hat." Was passiert als Reaktion auf die Bekanntgabe des Rektors? […] Der Rektor sagt natürlich die Wahrheit. Und alle Professoren sind perfekte Logiker. Sowie absolut fehlerfrei bei der Beurteilung, ob ein anderer einen Fehler begangen hat. Zwei Alternativen möchte ich Ihnen anbieten: Antwort 1: […] Nichts passiert. Antwort 2: Recht lange passiert gar nichts. Aber dann, in der 17-ten Sitzung nach der Rede des Rektors treten alle 17 Professoren zurück.

Das Problem der Stuttgarter Mathematiker

Zur Antwort 2 wird folgende Erklärung geboten (F&L 5/2019, S.471):

Was passiert, wenn es unter den 17 Professoren nur einen gäbe, der einen Fehler publiziert hat? Nennen wir ihn schwarzes Schaf. Da er von keinem schwarzen Schaf weiß, muss er aufgrund der Rede des Rektors schließen, dass er selbst ein schwarzes Schaf ist. Also muss er in der 1. Sitzung nach der Rede zurücktreten.

Wie ist es bei zwei schwarzen Schafen A und B? Beide treten in der 1. Sitzung nicht zurück, da zwar jeder weiß, dass der andere ein schwarzes Schaf ist, aber nichts über sich selbst erschließen kann. Doch da B in der 1. Sitzung nicht zurücktritt, muss A schlussfolgern, dass er selbst ein schwarzes Schaf ist. Denn andernfalls hätte B nach der Rede gewusst, dass er ein schwarzes Schaf ist und wäre in der 1. Sitzung zurückgetreten. Also muss A in der 2. Sitzung zurücktreten. B führt denselben Gedankengang durch, und auch er tritt in der 2. Sitzung zurück. […]

So kann man sich bis zur Situation mit 17 schwarzen Schafen vorarbeiten. Alle werden auf der 17. Sitzung zurücktreten. […] Der Rektor hat den Professoren doch Information vermittelt. Offensichtlich gibt es in einer Gruppe verschiedene Formen des Wissens. Jeder kann eine Tatsache T wissen. Zusätzlich kann jeder wissen, dass jeder andere auch T weiß. Ferner kann jeder wissen, dass jeder weiß, dass jeder T weiß. Usw.

Das Problem der Stuttgarter Mathematiker

Aufgabe: Lesen Sie aufmerksam das obige Rätsel. Leider gingen bei der Übertragung dieses Rätselklassikers auf Stuttgarter Mathematiker wesentliche Voraussetzungen verloren. Ist Antwort 1 weiterhin möglich?

Lösung: Hier geht es um gemeinsames Wissen / *common knowledge*. Nur weil eine Aussage wahr ist, weiß dies noch längst nicht jeder! Nur weil es jeder weiß, ist es noch kein gemeinsames Wissen!

Die Antwort 2 nutzt Aussage P: *Alle Professoren sind perfekte Logiker und absolut fehlerfrei bei der Beurteilung, ob ein anderer einen Fehler publiziert hat.* Die Gültigkeit der Aussage P allein genügt jedoch nicht, es muss auch jeder wissen, dass P gilt, usw. Denkbar wäre folgendes:

1. Nehmen wir an, jeder Professor ist ein perfekter Logiker und absolut fehlerfrei bei der Beurteilung, ob ein anderer einen Fehler publiziert hat, doch mindestens ein Professor hält manch anderen für fehleranfällig. Die Aussage des Rektors, ein Professor habe eines anderen Fehler entdeckt, lässt ihn daher kalt, denn auf die Meinung dieses Kollegen gibt er nicht viel. Daher scheitert schon der Induktionsanfang.

Das Problem der Stuttgarter Mathematiker

Zahlreiche weitere Varianten sind denkbar und in der hier angegebenen Formulierung des Rätsels nicht geklärt, weder bejaht noch verneint.

2. Nehmen wir weiterhin P an: Jeder Professor ist ein perfekter Logiker und absolut fehlerfrei bei der Beurteilung, ob ein anderer einen Fehler publiziert hat. Zudem gelte P': Jeder Professor weiß die Tatsache P. Jeder Professor glaubt also an die perfekte Urteilskraft jedes Kollegen. Er weiß allerdings nicht, ob die anderen dies ebenfalls glauben.

Hier gelingt noch der Induktionsanfang: Gibt es nur ein schwarzes Schaf, so erkennt es durch die Aussage des Rektors seinen eigenen Fehler.

Der Schluss von einem auf zwei schwarze Schafe hingegen misslingt. Die beiden schwarzen Schafe A und B treten in der 1. Sitzung nicht zurück. Kann A nun schlussfolgern, dass er ein schwarzes Schaf ist? Leider nein: A kann / muss befürchten, dass B nicht an die perfekte Urteilskraft jedes Kollegen glaubt; die Aussage des Rektors ließe dann B völlig kalt, da B auf die Meinung seiner Kollegen nichts gibt. Daher scheitert hier der Induktionsschritt von 1 auf 2.

Der unerwartete Abischerz: Wie ist das möglich?

Das folgende Paradox existiert in vielen Varianten, etwa als unerwartete Hinrichtung, `en.wikipedia.org/wiki/Unexpected_hanging_paradox`, Feueralarmübung oder Klassenarbeit, hier umgedreht als Abischerz.

Darum wachet! Denn ihr wisst weder Tag noch Stunde.
(Matthäus 25,13, Lutherbibel 2017)

Nach einer wahren Begebenheit: Die Abiturienten eines Gymnasiums planen ihren Abischerz. Aus Termingründen kommen dafür genau fünf Tage, Montag bis Freitag, in Frage. Die ängstliche Schulleiterin möchte den Termin wissen. Die Schüler verweigern dies mit der Begründung, der Abischerz müsse für die Lehrer vollkommen überraschend sein.

Die Schulleiterin denkt sich daher folgendes: „Der Abischerz kann sicher nicht am Freitag stattfinden, denn das ist der letzte mögliche Termin. Wäre bis Freitag Morgen nichts geschehen, dann wüssten wir, dass der Abischerz an diesem Tag stattfindet. Das wäre nicht überraschend.“

Der unerwartete Abischerz: Wie ist das möglich?

Die Schulleiterin folgert sofort weiter: „Der Abischerz kann auch nicht am Donnerstag stattfinden. Freitag haben wir bereits ausgeschlossen. Wäre bis Donnerstag Morgen nichts geschehen, dann wüssten wir, dass der Abischerz an diesem Tag stattfindet. Das wäre nicht überraschend.“

Ebenso schließt die Schulleiterin Mittwoch, Dienstag und Montag aus und kommt zu dem Schluss: „Es wird gar kein Abischerz stattfinden.“ Alle Lehrer bewundern die logischen Ausführungen der Schulleiterin.

Die Abiturienten veranstalten ihren Abischerz am Mittwoch.
Wie vorhergesagt sind alle Lehrer vollkommen überrascht.

Aufgabe: Alle Argumente scheinen logisch. Was also geht schief?

Lösungsidee: Die Eigenschaft „vollkommen überraschend“ ist kritisch; sie ist nicht präzise definiert und wird daher unterschiedlich interpretiert. Weitere Probleme sind Selbstbezüglichkeit und evtl. Widersprüchlichkeit. Wie das Paradoxon aufzulösen ist, darüber wird anhaltend diskutiert; hierzu gibt es ungefähr so viele Lösungsvorschläge wie Autoren.

Der unerwartete Abischerz: Wie ist das möglich?

Es ist sehr wichtig, keine unbewiesenen Annahmen zu treffen,
aber noch wichtiger ist es, keine Worte zu benutzen,
hinter denen sich kein klarer Sinn verbirgt.
(William Kingdon Clifford, 1845–1879)

Lösung: Wir können das Paradoxon auflösen, indem wir der vagen Formulierung „vollkommen überraschend“ einen präzisen Sinn geben. Hierzu betrachten wir wie zuvor verschiedene Stufen des Wissens:

$\mathscr{R}_0$: Der Abischerz findet höchstens an einem der fünf Tage Mo, Di, Mi, Do, Fr statt. Im Falle vertrödelter Planung gibt es keinen Abischerz.

$\mathscr{R}_1$: Es gilt $\mathscr{R}_0$, die Schulleiterin weiß dies, kann aber am Morgen des Abischerzes nicht sicher vorhersagen, dass er an diesem Tag stattfindet.

$\mathscr{R}_2$: Es gilt $\mathscr{R}_1$, die Schulleiterin weiß dies, kann aber am Morgen des Abischerzes nicht sicher vorhersagen, dass er an diesem Tag stattfindet.

$\mathscr{R}_n$: Es gilt $\mathscr{R}_{n-1}$, die Schulleiterin weiß dies, kann aber am Morgen des Abischerzes nicht sicher vorhersagen, dass er an diesem Tag stattfindet.

Der unerwartete Abischerz: Wie ist das möglich?

Dank Aussage $\mathscr{R}_0$ kann die Schulleiterin den Termin des Abischerzes immerhin auf die fünf fraglichen Tage Mo, Di, Mi, Do, Fr eingrenzen.
Mit $\mathscr{R}_1$ kann sie Fr ausschließen, es bleiben nur Mo, Di, Mi, Do.
Mit $\mathscr{R}_2$ kann sie Fr, Do ausschließen, es bleiben nur Mo, Di, Mi.
Mit $\mathscr{R}_3$ kann sie Fr, Do, Mi ausschließen, es bleiben nur Mo, Di.
Mit $\mathscr{R}_4$ kann sie Fr, Do, Mi, Di ausschließen, es bleibt also nur Mo.
Mit $\mathscr{R}_5$ kann sie alle fünf Tage ausschließen: Es gibt keinen Abischerz.

Die Schulleiterin interpretiert die Aussage „vollkommen überraschend“ im stärksten Sinne als $\mathscr{R}_5$ oder noch höher. Aus dieser starken Annahme folgert sie zurecht, dass es dieses Jahr keinen Abischerz geben kann.

Die Abiturienten interpretieren „vollkommen überraschend“ nur als $\mathscr{R}_1$. Ihr Abischerz am Mittwoch ist so gesehen vollkommen überraschend.

⚠ Diese Beispiele zeigen eindringlich: In strategischen Situationen sind Wissen und Nichtwissen oft entscheidend, sowohl eigenes als auch gegenseitiges und gemeinsames. Eine sichere Analyse setzt präzise Formulierung voraus und erfordert mathematische Sorgfalt und Disziplin.

Kapitel D

Mengen, Abbildungen und Relationen

This is not to say that the contents of this book are unusually difficult or profound. What is true is that the concepts are very general and very abstract, and that, therefore, they may take some getting used to. [. . .]

The student's task in learning set theory is to steep himself in unfamiliar but essentially shallow generalities till they become so familiar that they can be used with almost no conscious effort.

Paul Halmos (1916–2006), *Naive set theory*

Inhalt dieses Kapitels D

Zielsetzung

In den ersten beiden Kapiteln ging es vor allem ums Rechnen, zunächst mit Zahlen $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, dann mit Matrizen.

Damit Sie effizient arbeiten können, mussten wir auch theoretische Grundlagen klären. Dazu haben wir erste Sätze formuliert und auch Beweise geführt. Dabei haben Sie deutlich gespürt, dass Sie dringend grundlegende mathematische Werkzeuge benötigen, insbesondere Logik und Beweistechniken sowie Mengen und Abbildungen.

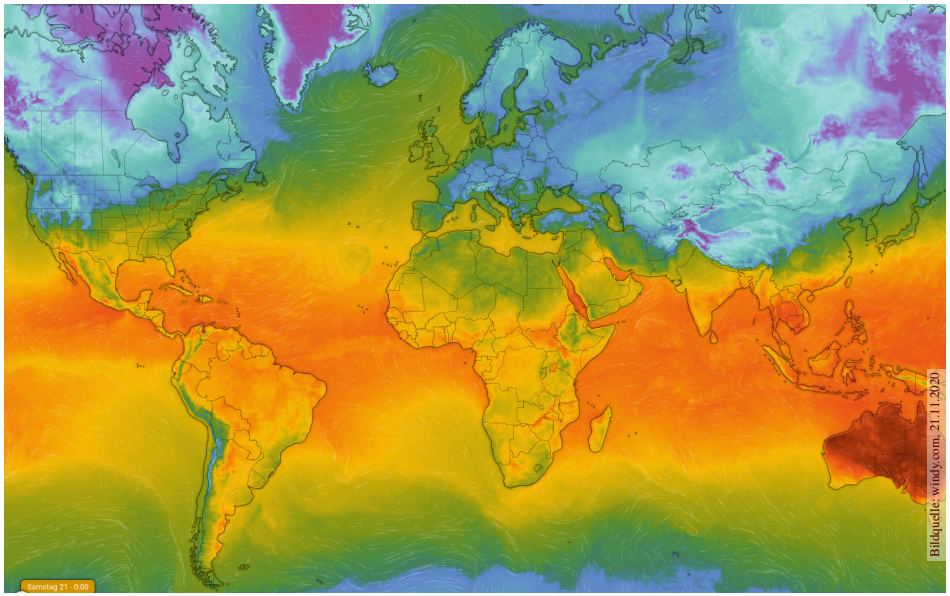
Diese Grundlagen erarbeiten wir uns nun Schritt für Schritt.

Zielsetzung

Im vorigen Kapitel C haben Sie gelernt, mit Aussagen und Wahrheitswerten zu rechnen, insbesondere Beweise zu führen. In diesem Kapitel D wollen wir nun ebenso gründlich klären, wie Sie mit Mengen effizient arbeiten und rechnen können.

Wir wollen dabei folgende Fragen klären: Was sind Mengen? Bescheidener: Nach welchen Regeln verhalten sich Mengen? Oder noch konkreter: Nach welchen Regeln nutzen wir Mengen? Unser Ziel ist also: *Set theory for the working mathematician.*

Mengen und Funktionen



Temperatur, Luftdruck, etc. $f : \mathbb{R}^2 \supseteq U \to \mathbb{R} \;\; : (x,y) \mapsto f(x,y)$

Windgeschwindigkeit, etc. $g : \mathbb{R}^2 \supseteq U \to \mathbb{R}^2 : (x,y) \mapsto g(x,y)$

Mengen und Funktionen

☺ Funktionen begegnen Ihnen alltäglich überall, zum Beispiel bereits in den Wetternachrichten. Diese Daten wollen Sie verstehen und nutzen!

Beispiel: Welche Temperatur, Luftdruck und Windgeschwindigkeit herrschen heute um 12 Uhr? „Das hängt davon ab!“, sagen Sie und denken zurecht an eine Funktion: Die fraglichen Daten bestehen nicht nur aus einer Zahl oder einem Vektor, sondern hängen vom Ort x ab!

Aus Sicht der **Physik** ist das eine zentrale und raffinierte Konstruktion: Die Beschreibung der Wirklichkeit oder gar die Vorhersage erfordert eine extrem präzise Begriffsbildung und auch abstrakte Denkweise. Anders sind erfolgreiche physikalische Anwendungen nicht möglich.

Die Schwierigkeiten beginnen bereits mit konkreten **Messvorschriften**. Was bedeutet Temperatur $f(x)$ in einem Punkt x? Wie messen wir das? Ist dies überhaupt in jedem Punkt eine eindeutige wohldefinierte Größe? Selbst wenn wir praktisch nicht in jedem Punkt nachschauen können?

Mengen und Funktionen

Aus Sicht der **Informatik** sind Funktionen ebenfalls überaus interessant: Wie speichern, verarbeiten und berechnen wir die relevanten Daten?

Auch hier ist unser Beispiel der Wetterdaten erhellend und illustrativ: Es zeigt, wie knifflig selbst einfachste Anwendungsfragen sind.

Es ist ganz sicher unmöglich, *alle* Werte in *allen* Punkten zu speichern: Ein realer, binärer Computer kann nur endlich viele Werte speichern!

Damit stellt sich sofort die Frage nach einer geeigneten **Approximation** der gedachten Funktion und einer **Kompression** der gegebene Daten.

Sodann stellt sich die Frage nach der möglichst präzisen **Berechnung**. Das ist bereits für „einfache“ Wetterdaten notorisch schwierig (D240).

Das alles sind wichtige Fragen, überaus praktisch aber auch schwierig. Um diese schwierigen Fragen soll es hier deshalb zunächst nicht gehen.

Vereinfachung: Wir beginnen mit den mathematischen Grundlagen. Darauf aufbauend können Sie später komplizierte Modelle untersuchen.

Mengen und Funktionen

Das obige Wetterbeispiel lässt bereits die Schwierigkeiten erahnen. Der mathematische Begriff einer **Funktion** ist dagegen sehr einfach: Er bietet eine dramatische Idealisierung und hilfreiche Vereinfachung. Es ist wie so oft in der Mathematik: Abstraktion hilft und vereinfacht!

Aus Sicht der **Mathematik** müssen wir zunächst zwei Fragen klären:

- Welche Daten benötigen wir zur Festlegung einer Funktion f?
- Praktische Anwendung: Wann sind Funktionen f und g gleich?

Damit blenden wir Fragen der Physik (Messung, Ungenauigkeit) oder der Informatik (Speicherung, Verarbeitung, Näherung) vorläufig aus. Das wird später wichtig, ist aber eine klar getrennte Fragestellung. Sie dürfen diese Vereinfachung begrüßen und nutzen lernen!

Alles sollte so einfach wie möglich gemacht werden
— aber nicht noch einfacher.
Albert Einstein (1879–1955)

Mengen und Elemente

D101

Die Mathematik nutzt die Sprache der Mengen, bewusst und erfolgreich.
Anschaulich: Eine Menge ist die Zusammenfassung ihrer Elemente.

$$\mathbb{N} = \{\, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \,\}$$
$$\mathbb{Z} = \{\, \dots, -3, -2, -1, 0, 1, 2, 3, \dots \,\}$$
$$\mathbb{Q} = \{\, z/n \mid z, n \in \mathbb{Z},\ n \neq 0 \,\}$$
$$\mathbb{R} = \text{„}\mathbb{Q} \text{ und alle Grenzwerte“}$$
$$\mathbb{C} = \{\, x + \mathrm{i}y \mid x, y \in \mathbb{R} \,\}$$

Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen.
Georg Cantor: *Beiträge zur Begründung der transfiniten Mengenlehre.*
Mathematische Annalen 46 (1895), p. 481

Eine Menge entsteht durch Zusammenfassung von Einzeldingen zu einem Ganzen. Eine Menge ist eine Vielheit, als Einheit gedacht.
Felix Hausdorff: *Mengenlehre* (1927), p. 11

Mengen und Elemente

D102
Erläuterung

Cantor und Hausdorff haben die Grundidee schön formuliert.

Ist damit alles klar? Wohl kaum. Es ist bemerkenswert schwierig zu sagen was eine Menge *ist*, doch viel einfacher, was eine Menge *tut*. Wir werden daher ganz bescheiden klären, wie sich Mengen *verhalten*, also wie wir damit *arbeiten* können. Das soll und muss uns genügen.

🙂 Trösten Sie sich mit einer vertrauen, ähnlich traurigen Wahrheit: Man kann nie genau wissen, wer ein Mensch wirklich *ist* oder was in ihm vorgeht, aber Sie können sehr wohl sehen, wie er sich *verhält*.
Für alle pragmatischen Zwecke des sozialen Umgangs genügt das.

Die Mengenlehre wurde vom deutschen Mathematiker Georg Cantor (1845–1918) zwischen 1870 und 1900 begründet, und zwar zunächst, um damit ganz konkrete Probleme der Analysis zu lösen, speziell der Fourier–Reihen. Erst nach und nach entstand aus der Mengenlehre eine eigene Theorie, die von anderen dann ausgebaut wurde.

Diese Entwicklung hält bis heute an.

Mengen und Elemente

D103
Erläuterung

Die *gesamte* Mathematik gründet, sofern sie formal betrieben wird, auf dem Fundament der Mengenlehre. Daher ist zu erwarten, dass die Mengenlehre ein mächtiges, geschärftes Werkzeug ist.
Es ist gut und richtig, sich von Anfang an daran zu gewöhnen!

Einfache Beispiele sind zwar sofort und leicht zu verstehen, doch für die nachhaltigen Bedürfnisse des Mathematikstudiums müssen wir tiefer graben, um ein solides Fundament zu legen.
Das kostet wie immer Zeit und Mühe, doch es lohnt sich.

Für AnfängerInnen ist der streng axiomatische Mengenbegriff schwer zugänglich; das gelingt erst in einem zweiten oder dritten Durchgang. Daher wähle ich in diesem Kapitel einen weniger strengen Zugang. Man spricht dann von *naiver Mengenlehre*.

Für Mengen nutzen wir Aussagen der Form $x \in M$, $A = B$, $A \subseteq B$, $A \supseteq B$, etc. Die logischen Operatoren $\wedge, \vee, \Rightarrow, \Leftrightarrow, \dots$ binden stets schwächer als diese Mengenrelationen $\in, =, \subseteq, \supseteq, \dots$. Wir kürzen also $(((x \in A) \wedge (A \subseteq B)) \Rightarrow (x \in B))$ ab durch $x \in A \wedge A \subseteq B \Rightarrow x \in B$.

Mengen und Elemente

D104

Anschaulich: Eine Menge M ist die Zusammenfassung ihrer Elemente.
Wir erklären nun, ausführlich und schrittweise, wie man damit rechnet.

Ist x ein **Element** von M, so sagen wir auch die Menge M enthält x, geschrieben $x \in M$ oder $M \ni x$, andernfalls $x \notin M$ oder $M \not\ni x$.

Zwei Mengen A und B sind **gleich**, $A = B$, falls sie dieselben Elemente enthalten: Für jedes Element x gilt $x \in A$ genau dann, wenn $x \in B$ gilt.

Jede endliche Menge lässt sich **aufzählen** gemäß $M = \{\, a_1, a_2, \dots, a_n \,\}$.
Diese Schreibweise bedeutet: $x \in M \Leftrightarrow x = a_1 \vee x = a_2 \vee \dots \vee x = a_n$.

Beispiel: Demnach gilt $\{1, 2, 3\} = \{3, 1, 2\} = \{1, 2, 2, 3, 3, 2, 1\}$.
Ebenso gilt $\{\clubsuit, \heartsuit, \diamondsuit\} = \{\heartsuit, \clubsuit, \clubsuit, \diamondsuit, \diamondsuit, \clubsuit, \heartsuit, \diamondsuit, \heartsuit, \diamondsuit, \diamondsuit, \diamondsuit, \diamondsuit, \diamondsuit\}$.
Viele verschiedene Schreibweisen definieren ein und dieselbe Menge!
Hingegen gilt $\{1, 2, 4\} \neq \{1, 3, 4\}$, denn $2 \in \{1, 2, 4\}$, aber $2 \notin \{1, 3, 4\}$.

Die Aussage $x \in M$ hat den Wahrheitswert $0 =$ falsch oder $1 =$ wahr.
Die Menge M zählt also nicht „wie oft“ sie x enthält, sondern nur „ob“.
Entweder x gehört zu M oder nicht, mehr lässt sich dazu nicht sagen.
(Wo immer die Anzahl wichtig ist, benötigen wir ein verfeinertes Modell.)

Teilmengen

D105

Wir nennen A eine **Teilmenge** von B, geschrieben $A \subseteq B$, falls jedes Element von A auch in B liegt. Das bedeutet $\forall x : x \in A \Rightarrow x \in B$.
Wir schreiben auch $B \supseteq A$, die Negation ist $A \not\subseteq B$ bzw. $B \not\supseteq A$.

Beispiel: Es gilt $\{1,3\} \subseteq \{1,2,3\}$, aber $\{1,2,3\} \not\subseteq \{1,3\}$.

🙂 Die Relation $\subseteq$ erfüllt folgende Regeln für alle Mengen A, B, C:

Reflexivität,	**Refl**$(\subseteq)$:	$A \subseteq A$.
Antisymmetrie,	**Asym**$(\subseteq)$:	Aus $A \subseteq B$ und $B \subseteq A$ folgt $A = B$.
Transitivität,	**Tran**$(\subseteq)$:	Aus $A \subseteq B$ und $B \subseteq C$ folgt $A \subseteq C$.

Die leere Menge $\emptyset = \{\}$ enthält keine Elemente: $x \in \emptyset \Leftrightarrow x \neq x$.
Ausführlich heißt das $M = \emptyset \Leftrightarrow \forall x : x \notin M$ und $M \neq \emptyset \Leftrightarrow \exists x : x \in M$.

Beispiel: Demnach gilt $\emptyset \subseteq M$ für jede Menge M.
Die leere Menge $\emptyset$ ist die einzige mit dieser Eigenschaft.

Beweis: Ist E eine Menge mit $E \subseteq M$ für jede Menge M, so haben wir insbesondere $E \subseteq \emptyset$ und zudem $\emptyset \subseteq E$. Wir schließen daraus $E = \emptyset$.

🙂 Die leere Menge wird durch diese Eigenschaft eindeutig bestimmt.

Teilmengen

D106

Die Inklusion $A \subseteq B$ bedeutet $x \in A \Rightarrow x \in B$; insbesondere gilt $B \subseteq B$.
Eine **echte** oder **strikte Teilmenge** $A \subsetneq B$ erfüllt $A \subseteq B$, aber $A \neq B$.

⚠ In der Literatur existieren hierzu konkurrierende Schreibweisen:
Bitte prüfen Sie bei der Lektüre die jeweils verwendete Definition!

	beliebige Teilmenge	strikte Teilmenge
(0)	$A \subseteq B$	$A \subsetneq B$
(1)	$A \subseteq B$	$A \subset B$
(2)	$A \subset B$	$A \subsetneq B$

Die Notation (1) ist wohl die ästhetisch schönste, analog zu $\leq$ und $<$.
Leider ist auch (2) weit verbreitet, auch unter Einfluss von Bourbaki, *Théorie des ensembles*. Dieses legendäre Autorenkollektiv hat mit seinen Grundlagen viel Gutes und Klärendes geleistet, hier haben sie meines Erachtens leider nur die zweitbeste Wahl getroffen.

Die Betonung (0) ist nicht so schön wie (1), aber narrensicher.
Wo es keiner Betonung oder Klärung bedarf, verwende ich auch (1).
Ich schreibe zum Beispiel ohne Skrupel $\{0,1\} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Auch Mengen wollen Elemente sein!

D107

Die Zusammenfassung von Objekten $a_1, a_2, \ldots, a_n$ zu einer Menge $M = \{a_1, a_2, \ldots, a_n\}$ liefert ein neues, eigenständiges Objekt M.

🙂 Eine Menge darf selbst Element einer anderen Mengen sein!

Der Mengenbegriff ist *iterativ* und extrem *flexibel*, jede Menge b kann nicht nur rechts in $a \in b$ auftreten, sondern auch links in $b \in c$.

Beispiel: Die Menge $A = \{\emptyset\}$ ist nicht leer, sie enthält das Element $\emptyset$.
Die Menge $B = \{\, 1, 2, \{1,2\} \,\}$ enthält drei Elemente: 1 und 2 und $\{1,2\}$.
Wie viele Elemente enthält die Menge $C = \{1, \{1\}, \{1,2\}, \{1,2,1\}\}$?

🙂 Eine Menge M darf sich nicht selbst enthalten: Nie gilt $M \ni M$.
Insbesondere gibt es keine „Allmenge“ oder „Menge aller Mengen“.
Auch $A = \{B\}$ und $B = \{A\}$ verbieten wir, dann wäre $A \ni B \ni A$.
Allgemein verbieten wir unendliche Ketten $M_0 \ni M_1 \ni M_2 \ni \ldots$.

Beispiel: Die Mengen M und $\{M\}$ und $\{\{M\}\}$ sind verschieden.
Wäre nämlich $M = \{M\}$, so hätten wir die Kette $M \ni M \ni M \ni \ldots$.
Wäre $\{M\} = \{\{M\}\}$, so hätten wir $M = \{M\}$, also $M \ni M \ni M \ldots$.
Wäre $M = \{\{M\}\}$, so hätten wir $M \ni \{M\} \ni M \ni \{M\} \ni M \ni \ldots$.

Potenzmenge

D108

Alle Teilmengen von M fassen wir zu ihrer **Potenzmenge** zusammen:

$$\mathfrak{P}(M) = \mathscr{P}(M) = \mathbb{P}(M) = \{\, A \subseteq M \,\} := \{\, A \mid A \subseteq M \,\}$$

Das bedeutet $A \in \mathfrak{P}(M) \Leftrightarrow A \subseteq M$. **Beispiele:**

$$\begin{aligned}
\mathfrak{P}(\{1\}) &= \{\, \emptyset,\ \{1\} \,\} \\
\mathfrak{P}(\{1,2\}) &= \{\, \emptyset,\ \{1\}, \{2\},\ \{1,2\} \,\} \\
\mathfrak{P}(\{1,2,3\}) &= \{\, \emptyset,\ \{1\}, \{2\}, \{3\},\ \{1,2\}, \{1,3\}, \{2,3\},\ \{1,2,3\} \,\}
\end{aligned}$$

🙂 Wenn M genau n Elemente besitzt, dann besitzt $\mathfrak{P}(M)$ genau 2^n.

Beweis: Jede Teilmenge $A \subseteq M$ entsteht durch n unabhängige Wahlen: Jedes Element $x \in M$ liegt entweder in A oder nicht, und diese Wahlen bestimmen A. Insgesamt gibt es $2^n = 2 \cdot 2 \cdots 2$ Möglichkeiten. QED

$$\begin{aligned}
\mathfrak{P}(\emptyset) &= \{\, \emptyset \,\} \\
\mathfrak{P}(\{\emptyset\}) &= \{\, \emptyset,\ \{\emptyset\} \,\} \\
\mathfrak{P}(\{\emptyset, \{\emptyset\}\}) &= \{\, \emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\emptyset, \{\emptyset\}\} \,\}
\end{aligned}$$

Aussonderung

D109

Beispiel: Es gilt $\{ x \in \mathbb{N} \mid \text{unzerlegbar}(x) \} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$.

Vorgelegt sei eine Menge M und ein Prädikat $p(x)$ für Elemente $x \in M$. Wir können die Elemente $x \in M$ mit der Eigenschaft $p(x)$ **aussondern**:

$$A = \{ x \in M \mid p(x) \}$$

Das bedeutet $x \in A \Leftrightarrow x \in M \wedge p(x)$. Die Teilmenge A von M besteht aus allen Elementen $x \in M$ mit der hier geforderten Eigenschaft $p(x)$. Ist die Grundmenge M im Kontext unmissverständlich klar, so können wir ihre explizite Notation weglassen und schreiben kurz $\{ x \mid p(x) \}$.

Beispiel: Es gilt $\{ x \in \mathbb{Z} \mid (x-3)(x-7) \leq 0 \} = \{ 3, 4, 5, 6, 7 \}$.
„$\supseteq$“: Jedes Element $x \in \{3, 4, 5, 6, 7\}$ erfüllt $x \in \mathbb{Z}$ und $(x-3)(x-7) \leq 0$.
„$\subseteq$“: Aus $x \in \mathbb{Z}$ und $(x-3)(x-7) \leq 0$ folgt umgekehrt $x \in \{3, 4, 5, 6, 7\}$.
Warum? Dies sehen Sie an der Parabel dank Fallunterscheidung!

Beispiel: Wir definieren zwei Teilmengen der Potenzmenge:

$$\mathfrak{P}'(M) := \{ A \in \mathfrak{P}(M) \mid A \neq M \} = \{ A \subsetneq M \},$$
$$\mathfrak{P}(M)^* := \{ A \in \mathfrak{P}(M) \mid A \neq \emptyset \} = \{ A \subseteq M \mid A \neq \emptyset \}.$$

Beispiel: reelle Intervalle

D110

Für $a \leq b$ in $\mathbb{R}$ haben wir die **endlichen Intervalle** $\emptyset = \{\}$ und

$$[a,b] := \{ x \in \mathbb{R} \mid a \leq x \leq b \}, \qquad]a,b[:= \{ x \in \mathbb{R} \mid a < x < b \},$$
$$[a,b[:= \{ x \in \mathbb{R} \mid a \leq x < b \}, \qquad]a,b] := \{ x \in \mathbb{R} \mid a < x \leq b \}.$$

Zudem haben wir die **unendlichen Intervalle** $\mathbb{R} =]-\infty, +\infty[$ und

$$[a,+\infty[:= \{ x \in \mathbb{R} \mid a \leq x \}, \qquad]a,+\infty[:= \{ x \in \mathbb{R} \mid a < x \},$$
$$]-\infty,b] := \{ x \in \mathbb{R} \mid x \leq b \}, \qquad]-\infty,b[:= \{ x \in \mathbb{R} \mid x < b \}.$$

Sei $(X, \leq)$ eine geordnete Menge, wir denken an $(\mathbb{Q}, \leq)$ oder $(\mathbb{R}, \leq)$. Eine Teilmenge $I \subseteq X$ heißt **Intervall** in X, wenn für alle $a < x < b$ in X mit $a, b \in I$ auch $x \in I$ gilt, kurz: I erfüllt die Zwischenwerteigenschaft.

Übung: Die obigen Mengen in $\mathbb{R}$ sind tatsächlich Intervalle. Warum?

Ist jedes Intervall in $\mathbb{R}$ von dieser Form? Ja, dank Vollständigkeit von $\mathbb{R}$! Wir nutzen $a = \inf I$ und $b = \sup I$ in $\bar{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$, damit gelingt es.

Rationale Intervalle schreiben wir $]a,b[_{\mathbb{Q}}$ etc; $I = \{ x \in \mathbb{Q} \mid x^2 \leq 2 \}$ ist ein rationales Intervall, lässt sich aber nicht so schreiben mit $a, b \in \mathbb{Q}$.

Beispiel: die Gruppe der invertierbaren Elemente

D111

Sei $(M, \cdot, 1)$ ein Monoid. Die Menge aller invertierbaren Elemente ist

$$M^\times = (M,\cdot)^\times = (M,\cdot,1)^\times := \{ a \in M \mid \exists b \in M : a \cdot b = b \cdot a = 1 \}.$$

Wir sondern hier also alle invertierbaren Elemente zur Menge $M^\times$ aus. Diese Teilmenge von M bildet eine Gruppe $(M^\times, \cdot, 1)$, siehe Satz B1C.

Speziell in jedem Ring $(R, +, 0, \cdot, 1)$ definieren wir

$$R^* := \{ a \in R \mid a \neq 0 \} \qquad \text{und} \qquad R^\times := (R, \cdot, 1)^\times.$$

Beispiele: Im Ring $(\mathbb{Z}_n, +_n, \cdot_n)$ gilt $\mathbb{Z}_n^\times = \{ a \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1 \}$.
Genau dann gilt $\mathbb{Z}_n^\times = \mathbb{Z}_n^*$, wenn $n \in \mathbb{N}_{\geq 2}$ prim ist.

Im Ring $(\mathbb{Z}, +, \cdot)$ gilt $\mathbb{Z}^\times = \{-1, 1\}$. Im Körper $(\mathbb{Q}, +, \cdot)$ gilt $\mathbb{Q}^\times = \mathbb{Q}^*$.
Für jeden Ring $(R, +, 0, \cdot, 1)$ mit $0 \neq 1$ gilt $R^\times \subseteq R^*$, denn $0 \notin \mathbb{R}^\times$.
Genau dann gilt $R^\times = R^*$, wenn R ein Divisionsring ist.

Die allgemeine lineare Gruppe ist $\text{GL}_n(R) := (R^{n \times n}, \bullet, 1_{n \times n})^\times$.
Sie besteht aus der Menge der invertierbaren $n \times n$–Matrizen über R.

Ersetzungsmenge

D112

Beispiel: Es gilt $\{ x^2 \mid x \in \mathbb{Z} \} = \{ 0, 1, 4, 9, 16, 25, \ldots \}$. Allgemein:

Vorgelegt sei eine Menge M. Jedem Element $x \in M$ werde genau ein Objekt $y = f(x)$ zugeordnet. Daraus bilden wir die **Ersetzungsmenge**:

$$E = \{ f(x) \mid x \in M \}$$

Das bedeutet $y \in E \Leftrightarrow \exists x \in M : f(x) = y$. Die Ersetzungsmenge E besteht aus allen Elementen $f(x)$, wobei x die Menge M durchläuft.

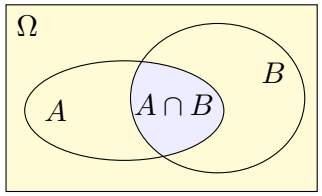
Beispiel: Es gilt $2\mathbb{N} := \{ 2n \mid n \in \mathbb{N} \} = \{ 0, 2, 4, 6, 8, 10, 12, \ldots \}$
und ebenso $2\mathbb{N}+1 := \{ 2n+1 \mid n \in \mathbb{N} \} = \{ 1, 3, 5, 7, 9, 11, 13 \ldots \}$.

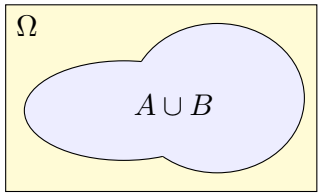
Beispiel: Es gilt $\{ x^2 \mid x \in \mathbb{Q} \} \subsetneq \mathbb{Q}_{\geq 0}$: „$\subseteq$“ aber nicht „$\supseteq$“! (Satz A1F)
Reell hingegen gilt $\{ x^2 \mid x \in \mathbb{R} \} = \mathbb{R}_{\geq 0}$: „$\subseteq$“ und „$\supseteq$“ dank $\sqrt{}$ (ZWS)

Aufgabe: Explizieren Sie die Menge $E = \{ \mathfrak{P}(A) \mid A \subseteq \{1, 2\} \}$.
Lösung: Die Schreibweise bedeutet $E = \{ \mathfrak{P}(A) \mid A \in \mathfrak{P}(\{1, 2\}) \}$.
Wir finden die Menge $E = \{ \{\emptyset\}, \{\emptyset, \{1\}\}, \{\emptyset, \{2\}\}, \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \}$.

Schnittmenge und Vereinigung

D113





Die **Schnittmenge** „A und B“ ist

$$A \cap B = \{\, x \mid x \in A \wedge x \in B \,\}.$$

Sie besteht aus den Elementen, die sowohl in A als auch in B liegen.

Die **Vereinigungsmenge** „A oder B“ ist

$$A \cup B = \{\, x \mid x \in A \vee x \in B \,\}.$$

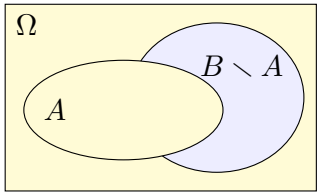
Sie besteht aus den Elementen, die in A oder B liegen (oder in beiden).

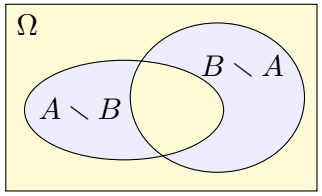
Zwei Mengen A, B heißen **disjunkt** (punktfremd), falls $A \cap B = \emptyset$ gilt.
In diesem Spezialfall ist die Vereinigung eine **disjunkte Vereinigung**:

$$A \sqcup B := A \cup B \quad \text{mit} \quad A \cap B = \emptyset$$

Restmenge und symmetrische Differenz

D114





Die **Restmenge** oder **Differenzmenge** „B ohne A“ ist

$$B \setminus A := \{\, x \in B \mid x \notin A \,\}.$$

Sie besteht aus allen Elementen, die in B liegen, aber nicht in A.

Die **symmetrische Differenz** „entweder A oder B“ ist

$$\begin{aligned} A \triangle B &:= \{\, x \mid x \in A \mathbin{\dot\vee} x \in B \,\} \\ &= (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A). \end{aligned}$$

Sie besteht aus allen Elementen, die entweder in A oder in B liegen, aber nicht in beiden zugleich. Dies entspricht dem exklusiven Oder.

Rechenregeln für Vereinigung ∪ und Schnitt ∩

D115

Satz D1A: Rechenregeln für Mengen

Folgende Rechenregeln gelten für alle $A, B, C \subseteq \Omega$ und $\overline{A} = \Omega \setminus A$.
(0) Neutralität, Absorbtion, Idempotenz, Komplemente:

$$\begin{aligned} A \cup \emptyset &= A, & A \cup \Omega &= \Omega, & A \cup A &= A, & A \cup \overline{A} &= \Omega \\ A \cap \Omega &= A, & A \cap \emptyset &= \emptyset, & A \cap A &= A, & A \cap \overline{A} &= \emptyset \end{aligned}$$

(1) Kommutativität:

$$A \cup B = B \cup A, \qquad A \cap B = B \cap A$$

(2) Assoziativität:

$$A \cup (B \cup C) = (A \cup B) \cup C, \qquad A \cap (B \cap C) = (A \cap B) \cap C$$

(3) Distributivität:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Insbesondere ist $(\mathfrak{P}(\Omega), \cup, \emptyset, \cap, \Omega)$ demnach ein kommutativer Halbring.

Rechenregeln für Komplement und Restmenge

D116

Satz D1A: Rechenregeln für Mengen

Weiterhin seien $A, B, C \subseteq \Omega$. Das Komplement von A in Ω ist

$$\overline{A} = \complement A = \complement_\Omega A = \Omega \setminus A := \{\, x \in \Omega \mid x \notin A \,\}.$$

(4) Es gilt $\overline{\Omega} = \emptyset$ und $\overline{\emptyset} = \Omega$ sowie $\overline{\overline{A}} = A$. Für die Restmenge gilt:

$$B \setminus A = B \cap \overline{A}$$

(5) Für je zwei Mengen $A, B \subseteq \Omega$ gilt nach De Morgan:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}$$

(6) Allgemein, für je drei Mengen A, B, C gilt:

$$\begin{aligned} C \setminus (A \cup B) &= (C \setminus A) \cap (C \setminus B), \\ C \setminus (A \cap B) &= (C \setminus A) \cup (C \setminus B). \end{aligned}$$

☺ Später sagen wir: Die Halbringe $(\mathfrak{P}(\Omega), \cup, \cap)$ und $(\mathfrak{P}(\Omega), \cap, \cup)$ sind isomorph durch Komplementbildung $(\complement, \complement) : (\mathfrak{P}(\Omega), \cup, \cap) \cong (\mathfrak{P}(\Omega), \cap, \cup)$.

Rechenregeln für Mengen

D117

Aufgabe: Beweisen Sie diese Regeln (mit Kapitel C).

Lösung: Dies folgt aus den entsprechenden Regeln der Logik.
Ich führe dies hier in zwei typischen Fällen exemplarisch vor.

(3) $$\begin{aligned} x \in A \cap (B \cup C) &\overset{\text{Def}}{\iff} x \in A \wedge (x \in B \cup C) \\ &\overset{\text{Def}}{\iff} x \in A \wedge (x \in B \vee x \in C) \\ &\overset{\substack{\text{Distr}\\ \text{C135}}}{\iff} (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\overset{\text{Def}}{\iff} (x \in A \cap B) \vee (x \in A \cap C) \\ &\overset{\text{Def}}{\iff} x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

(6) $$\begin{aligned} x \in C \smallsetminus (A \cup B) &\overset{\text{Def}}{\iff} x \in C \wedge \neg(x \in A \vee x \in B) \\ &\overset{\substack{\text{DeM}\\ \text{C135}}}{\iff} x \in C \wedge (x \notin A \wedge x \notin B) \\ &\overset{\substack{\cdots\\ \text{C135}}}{\iff} (x \in C \wedge x \notin A) \wedge (x \in C \wedge x \notin B) \\ &\overset{\text{Def}}{\iff} x \in (C \smallsetminus A) \cap (C \smallsetminus B) \end{aligned}$$

Vereinigung und Schnittmenge: endlich und unendlich

D118

Vereinigung und Schnitt einer endlichen Familie von Mengen:

$$\bigcup_{k=1}^{n} A_k := A_1 \cup A_2 \cup \cdots \cup A_n \quad \text{und} \quad \bigcap_{k=1}^{n} A_k := A_1 \cap A_2 \cap \cdots \cap A_n$$

🙂 Dank Assoziativität dürfen wir beliebig klammern
und dank Kommutativität zudem beliebig umordnen.

Sei $I \neq \emptyset$ eine Menge und $(A_i)_{i \in I}$ eine Familie von Mengen A_i indiziert durch $i \in I$, das heißt, jedem Index $i \in I$ ist eine Menge A_i zugeordnet.

$$\bigcup_{i \in I} A_i := \{\, x \mid \exists i \in I : x \in A_i \,\} \quad \text{und} \quad \bigcap_{i \in I} A_i := \{\, x \mid \forall i \in I : x \in A_i \,\}$$
$$= \{\, x \mid \bigvee_{i \in I} x \in A_i \,\} \qquad = \{\, x \mid \bigwedge_{i \in I} x \in A_i \,\}$$

🙂 Im Spezialfall $I = \emptyset$ erhalten wir die leere Vereinigung $\bigcup_{i \in \emptyset} X_i = \emptyset$.

☹ Der leere Durchschnitt $\bigcap_{i \in \emptyset} X_i$ ist im Allgemeinen nicht definiert.
Dies wäre wörtlich interpretiert die Menge *aller* Elemente und logisch problematisch (D107, D127). Arbeiten wir jedoch innerhalb einer festen Grundmenge Ω, so können und werden wir $\bigcap_{i \in \emptyset} X_i = \Omega$ vereinbaren.

Vereinigung und Schnitt: allgemein über Mengensysteme

D119

Beispiel: Wir haben $\mathbb{R} = \bigcup_{a \in \mathbb{Z}} [a, a+1]$ und $\mathbb{R} = \mathbb{R}_{<0} \sqcup \{0\} \sqcup \mathbb{R}_{>0}$.

Die Familie $(A_i)_{i \in I}$ heißt **disjunkt**, falls $A_i \cap A_j = \emptyset$ für alle $i \neq j$ in I.
In diesem Spezialfall ist die Vereinigung eine **disjunkte Vereinigung**:

$$\bigsqcup_{i \in I} A_i := \bigcup_{i \in I} A_i \quad \text{mit} \quad A_i \cap A_j = \emptyset \quad \text{für alle } i \neq j$$

Jedes Element der Vereinigung liegt in genau einer der Mengen A_i.

Beispiel: Es gilt $\mathbb{R} = \bigsqcup_{x \in \mathbb{R}} \{x\}$ und $\mathbb{R} = \bigsqcup_{a \in \mathbb{Z}} [a, a+1[$ (abrunden).

Beispiel: Wir haben $\bigcup \{\, \{1,2\}, \{1,3\} \,\} = \{1,2\} \cup \{1,3\} = \{1,2,3\}$
und entsprechend $\bigcap \{\, \{1,2\}, \{1,3\} \,\} = \{1,2\} \cap \{1,3\} = \{1\}$.

Ist $U \neq \emptyset$ eine Menge von Mengen, so definieren wir:

$$\bigcup U = \bigcup_{A \in U} A := \{\, x \mid \exists A \in U : x \in A \,\}$$
$$\bigcap U = \bigcap_{A \in U} A := \{\, x \mid \forall A \in U : x \in A \,\}$$

Beispiel: Für jede Menge M gilt $\bigcup \mathfrak{P}(M) = M$ und $\bigcap \mathfrak{P}(M) = \emptyset$.

🙂 Im Sonderfall $U = \emptyset$ gilt $\bigcup \emptyset = \emptyset$, ☹ aber $\bigcap \emptyset$ ist nicht definiert.
Dies wäre die Menge *aller* Elemente und problematisch (D107, D127).

Vereinigung und Schnitt: allgemein über Mengensysteme

D120
Erläuterung

Wir haben also drei Operationen in aufsteigender Allgemeinheit:

- paarweise Schnitte und Vereinigungen
- endliche Schnitte und Vereinigungen
- beliebige Schnitte und Vereinigungen

Letztere formulieren wir schließlich besonders bequem, wie oben,
als Schnitt $\bigcap U$ und Vereinigung $\bigcup U$ eines Mengensystems U.

Das ist schwindelerregend allgemein. Zum Glück haben Sie präzise Definitionen und erhellende Beispiele, daran können Sie sich halten.

Überdeckungen und Zerlegungen

D121

Beispiel: Die Menge $\{\{1,2\},\{2,3\}\}$ ist eine Überdeckung von $\{1,2,3\}$.
Zur Menge $M = \{1,2,3,4,5,6,7\}$ ist $Z = \{\{1,4\},\{2,3,6,7\},\{5\}\}$ eine Überdeckung durch disjunkte nicht-leere Teilmengen: eine Zerlegung.

Eine **Überdeckung** von M ist eine Menge $U \subseteq \mathfrak{P}(M)$ mit $\bigcup U = M$:

$$\forall x \in M \;\; \exists A \in U \;:\; x \in A$$

Wir nennen U **disjunkt**, falls gilt $\forall A, B \in U : A \neq B \Rightarrow A \cap B = \emptyset$.
Dann ist die Vereinigung eine **disjunkte Vereinigung** $M = \bigsqcup U$:

$$\forall x \in M \;\; \exists! A \in U \;:\; x \in A$$

Eine **Zerlegung** $M = \bigsqcup Z$ ist eine disjunkte Überdeckung $Z \subseteq \mathfrak{P}(M)^*$:

$$\bigcup Z = M \;\; \wedge \;\; \forall A, B \in Z \;:\; A = B \;\dot\vee\; A \cap B = \emptyset$$

In Worten: Z ist ein System von Teilmengen von M, alle Mengen in Z sind nicht-leer und paarweise disjunkt, und ihre Vereinigung ist M.

Beispiel: Es gilt $\mathbb{R} = \bigsqcup\{\, \{x\} \mid x \in \mathbb{R} \,\}$ und $\mathbb{R} = \bigsqcup\{\, [a, a+1[\mid a \in \mathbb{Z} \,\}$.

Überdeckungen und Zerlegungen

D122
Erläuterung

Überdeckungen und Zerlegungen spielen in vielen Bereichen der Mathematik eine wichtige Rolle, in immer neuen Variationen, hier begegnen Sie uns zunächst als Grundbegriffe der Mengenlehre. Nützliche Konzepte verdienen einen guten Namen.

Leider bedeutet das auch, dass Sie am Anfang Ihres Studiums mit vielen neuen Begriffen konfrontiert werden. Diese müssen Sie lernen wie Vokabeln im Sprachunterricht, ohne geht es nicht. Jeder einzelne Fall ist nicht schwer, aber insgesamt erfordert es viel Disziplin.

Hier helfen einfache und illustrative Beispiele,
... und anschließend gute Übungen!

Auswahlmenge aka Repräsentantensystem

D123

Beispiel: Zu $M = \{1,2,3,4,5,6,7\}$ und $Z = \{\{1,4\},\{2,3,6,7\},\{5\}\}$ ist $R = \{4,3,5\}$ eine Auswahl, ebenso $\{1,6,5\}$ oder $\{1,2,5\}$ etc.
Es gibt hier $2 \cdot 4 \cdot 1 = 8$ mögliche Auswahlen. Allgemein:

Sei $M = \bigsqcup Z$ eine Zerlegung. Eine Teilmenge $R \subseteq M$ heißt **Auswahlmenge** oder **Repräsentantensystem** zu Z, falls gilt:

$$\forall A \in Z \;\; \exists! x \in R \;:\; x \in A$$

Das bedeutet: Die Repräsentantenmenge R wählt aus jeder Menge $A \in Z$ der vorgegebenen Zerlegung Z genau ein Element $a \in A$.

Beispiel: Die Menge $M = \bigsqcup\{A_1, \ldots, A_n\}$ der SchülerInnen teilt sich in Klassen auf und $R = \{a_1, \ldots, a_n\}$ enthält die KlassensprecherInnen.

Einige mathematische Konstruktionen nutzen das **Auswahlaxiom (AC)**:
Zu jeder Zerlegung $M = \bigsqcup Z$ existiert eine Auswahlmenge $R \subseteq M$.
Eine solche Auswahl ist überaus nützlich, doch leider nicht eindeutig!

Beispiel: In $(\mathbb{N}, \leq)$ hat jede nicht-leere Teilmenge $A \subseteq \mathbb{N}$ ein kleinstes Element; wir können daher $a = \min A$ als Repräsentanten wählen.

Auswahlmenge aka Repräsentantensystem

D124
Erläuterung

All unsere bisherigen Konstruktionen sind konkret, präzise, eindeutig: Aus gegebenen Mengen konstruieren wir eine wohldefinierte neue Menge, etwa die Potenzmenge $M \mapsto \mathfrak{P}(M)$ oder die Aussonderung $(M, p) \mapsto \{\, x \in M \mid p(x) \,\}$ oder die Ersetzung $(M, f) \mapsto \{\, f(x) \mid x \in M \,\}$, ebenso Schnitt $(A, B) \mapsto A \cap B$ und Vereinigung $(A, B) \mapsto A \cup B$ etc.

☹ Bei der Auswahl eines Repräsentantensystems ist dies anders!

Im Allgemeinen gibt es viele mögliche Auswahlen, und keine ist schöner als die andere. Wir müssen daher „irgendwie“ und „willkürlich“ wählen. Das unterscheidet das Auswahlaxiom von den vorigen Konstruktionen.

Beispiel: Für jede *endliche* Zerlegung $Z = \{A_1, \ldots, A_n\}$ ist das Auswahlaxiom weitgehend unproblematisch: Wir wählen willkürlich Repräsentanten $a_1 \in A_1, \ldots, a_n \in A_n$. Bei *unendlichen* Zerlegungen ist dies kritisch: Nach welchem Muster soll unsere Willkür verfahren?

Wo dies möglich und sinnvoll ist, versuche ich konstruktiv vorzugehen. Das macht die Wahl eindeutig, weniger willkürlich, gar kanonisch.

John von Neumanns Modell der natürlichen Zahlen

Ausgehend von der leeren Menge $\emptyset$ können wir weitere Mengen bilden, etwa $\{\emptyset\}$ und $\{\emptyset, \{\emptyset\}\}$. Zur Fortsetzung betrachten wir die Zuordnung

$$s : n \mapsto n' = n \cup \{n\}.$$

Daraus erhalten wir John von Neumanns Modell der natürlichen Zahlen:

$$\left\{\begin{array}{l} 0 := \emptyset \\ 1 := \{0\} \\ 2 := \{0,1\} \\ 3 := \{0,1,2\} \\ 4 := \{0,1,2,3\} \\ 5 := \{0,1,2,3,4\} \\ \quad \dots \end{array}\right\} =: \omega$$

Hier ist jede natürliche Zahl n die Menge all ihrer Vorgängerinnen.
So können wir die natürlichen Zahlen als Mengen implementieren.

🙂 Dieses Modell $(\omega, \emptyset, s)$ erfüllt die Dedekind–Peano–Axiome (A109).

John von Neumanns Modell der natürlichen Zahlen

Die Gesamtmenge $\omega = \{ 0, 1, 2, 3, \dots \}$ definieren wir wie folgt:

- Die Menge ω ist **induktiv**: Es gilt $\emptyset \in \omega$ und $\forall n \in \omega : s(n) \in \omega$.
- Ist M eine beliebige induktive Menge, so gilt $\omega \subseteq M$.

Beides zusammengefasst: ω ist die kleinste induktive Menge.

Aufgabe: (1) Für alle $n \in \omega$ gilt $\bigcup s(n) = n$.
(2) Für je zwei Elemente $m \neq n$ in ω gilt $s(m) \neq s(n)$.
(3) Das Tripel $(\omega, \emptyset, s)$ erfüllt die Dedekind–Peano–Axiome.

Lösung: (1) Wir betrachten $M = \{ n \in \omega \mid \bigcup s(n) = n \}$.
Es gilt $\emptyset \in M$, denn für $n = \emptyset$ finden wir $\bigcup s(\emptyset) = \bigcup\{\emptyset\} = \emptyset$.
Gilt $n \in M$, also $\bigcup s(n) = n$, so folgt $s(n) \in M$, denn:

$$\begin{aligned} \bigcup s(s(n)) = \bigcup\big[s(n) \cup \{s(n)\}\big] &= \big[\bigcup s(n)\big] \cup s(n) \\ = n \cup (n \cup \{n\}) \qquad = n \cup \{n\} \qquad &= s(n) \end{aligned}$$

(2) Kontraposition: Gilt $s(m) = s(n)$ so folgt $m = \bigcup s(m) = \bigcup s(n) = n$.
(3) Dies fasst die bisherigen Rechnungen zu $(\omega, \emptyset, s)$ zusammen.
So können wir die natürlichen Zahlen als Mengen implementieren.

Die Russelsche Antinomie

Das Barbier-Paradoxon: Im Dorf rasiert der Barbier genau die Männer, die sich nicht selbst rasieren. Frage: Rasiert der Barbier sich selbst?

Bertrand Russel (1872–1970, Literaturnobelpreis 1950) veröffentlichte 1903 folgendes Paradoxon der naiven Mengenlehre: Wir untersuchen

$$\mathscr{R} = \{ x \mid x \notin x \}.$$

Das heißt, $\mathscr{R}$ enthält alle Mengen x, die sich nicht selbst enthalten.
Ist dieses Objekt $\mathscr{R}$ selbst eine Menge? Gilt dann $\mathscr{R} \in \mathscr{R}$ oder $\mathscr{R} \notin \mathscr{R}$?
Gilt $\mathscr{R} \in \mathscr{R}$, so folgt $\mathscr{R} \notin \mathscr{R}$. Gilt $\mathscr{R} \notin \mathscr{R}$, so folgt $\mathscr{R} \in \mathscr{R}$. Katastrophe!

🙂 Einzig möglicher Ausweg: Dieses Objekt $\mathscr{R}$ ist keine Menge!
Nicht alles, was wir naiv hinschreiben können, ist tatsächlich sinnvoll.

Beispiel: Gibt es eine Menge $\mathscr{A}$ aller Mengen? Nein, denn dann wäre $\mathscr{R} = \{ x \in \mathscr{A} \mid x \notin x \} \subseteq \mathscr{A}$ durch Aussonderung ebenfalls eine Menge.

⚠ Wir müssen die Konstruktion von Mengen reglementieren!

- So restriktiv wie nötig, um Paradoxien wie die obige zu vermeiden.
- So expressiv wie möglich, um alles zu formulieren, was wir brauchen.

Lösung der Antinomie durch Zermelo–Fraenkel

This is not to say that the contents of this book are unusually difficult or profound. What is true is that the concepts are very general and very abstract, and that, therefore, they may take some getting used to. […]
Paul Halmos (1916–2006), *Naive set theory*

Wir kennen nun für Mengen alle Operationen, die wir je benötigen.
Daher halten wir Rückschau und fassen das Wesentliche zusammen.

Die folgende Zusammenfassung und Präzisierung geht zurück auf Ernst Zermelo (1871–1953) und Abraham Fraenkel (1891–1965).

Wir einigen uns auf eine Handvoll grundlegender Konstruktionen:
Diese und nur diese wollen wir im Folgenden verwenden!

Die Erfahrung zeigt, dass diese Wahl gut ist: Sie vermeidet Paradoxien!
Es ist nicht die einzig mögliche Wahl, aber eine allgemeine Grundlage.

🙂 Kurz gesagt: Die Zermelo–Fraenkel–Axiome (kurz ZF–Axiome) sind die **Rechenregeln für Mengen**, kurz und gut, präzise und bequem.

Die Zermelo–Fraenkel Axiome: ZF und ZFC = ZF+AC

D129
Erläuterung

Um Widersprüche und Paradoxien wie die Russelsche Antinomie D127 zu vermeiden, müssen wir die Konstruktion von Mengen reglementieren. Die folgenden Axiome von Zermelo und Fraenkel leisten genau dies. Sie extrahieren eine Handvoll von Konstruktionen, die im Folgenden für den Aufbau der gesamten (klassischen) Mathematik genügen.

Wir betrachten hierzu ein Universum Ω aller Mengen. Hier ist Ω selbst keine Menge, siehe D107 und D127, sondern benennt nur den Rahmen, in dem wir uns bewegen. Im Folgenden ist Ω unser Diskursuniversum, darauf beziehen sich uneingeschränkte Quantoren wie $\forall x$ und $\exists x$.

Alle Objekte von Ω sind Mengen. Für diese haben wir die Relation „$\in$“, die wir als Elementrelation interpretieren: Zu je zwei Mengen A, B gilt entweder $A \in B$ oder nicht, genau das nutzen wir, und mehr nicht. Aus diesen primitiven Daten $(\Omega, \in)$ allein leiten wir alles Weitere ab, etwa die Teilmengenrelation $A \subseteq B$ durch $\forall x : x \in A \Rightarrow x \in B$.

Die ZF–Axiome erklären alle grundlegenden Rechenregeln für Mengen; zusammen mit dem Auswahlaxiom D123 erhalten wir ZFC (für *choice*).

Die Zermelo–Fraenkel Axiome: ZF und ZFC = ZF+AC

D130

0 **Extensionalität:**
Zwei Mengen A und B sind gleich, falls $A \subseteq B$ und $A \supseteq B$ gilt.

1 **Fundierung:**
Mengen erlauben keine unendlichen Ketten $M_0 \ni M_1 \ni M_2 \ni \dots$.

2 **Leere Menge:**
Es existiert eine Menge $\emptyset$ ohne Elemente, also $x \in \emptyset \Leftrightarrow x \neq x$.

3 **Potenzmenge:**
Zu jeder Menge M existiert $\mathfrak{P}(M)$, also $A \in \mathfrak{P}(M) \Leftrightarrow A \subseteq M$.

4 **Vereinigung:**
Zu jeder Menge M existiert $\bigcup M$, also $x \in \bigcup M \Leftrightarrow \exists A \in M : x \in A$.

5 **Aussonderung:**
Zu jeder Menge M und jedem Prädikat p existiert $\{ x \in M \mid p(x) \}$.

6 **Ersetzung:**
Zu jeder Menge M und jeder Zuordnung f existiert $\{ f(x) \mid x \in M \}$.

7 **Unendlichkeit:**
Es existiert eine Menge ω mit $\emptyset \in \omega$ und $(n \in \omega) \Rightarrow (n \cup \{n\} \in \omega)$.

Die Zermelo–Fraenkel Axiome: ZF und ZFC = ZF+AC

D131
Erläuterung

Axiome (0) und (1) klären zunächst die Beschaffenheit von Mengen: Vergleich und Fundierung. Die Fundierung lässt sich so formulieren: Ist $M \neq 0$ eine nicht-leere Menge, so existiert $A \in M$ mit $M \cap A = \emptyset$. Das verhindert unendliche Ketten $M_0 \ni M_1 \ni M_2 \ni \dots$, andernfalls enthielte $M = \{ M_0, M_1, M_2, \dots \}$ kein Element $A \in M$ mit $M \cap A = \emptyset$.

Axiom (2) stellt sicher, dass überhaupt irgendeine Menge in Ω existiert. Dieses Axiom wird redundant mit (7) und (5), denn $\emptyset = \{ x \in \omega \mid x \neq x \}$.

Mit dem Potenzmengenaxiom (3) generieren wir nun weitere Mengen, etwa $\mathfrak{P}(\emptyset) = \{\emptyset\}$ und $\mathfrak{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$, zusammen mit Aussonderung (5) und Ersetzung (6). Zu A erhalten wir $\{A\}$ durch Ersetzung aus $\{\emptyset\}$. Zu A, B erhalten wir $\{A, B\}$ durch Ersetzung aus $\{\emptyset, \{\emptyset\}\}$.

Wir fordern die allgemeine Vereinigung als Axiom (4). Die Bildung von Schnittmengen folgt aus der Aussonderung (5): Ist $M \neq \emptyset$ eine Menge, so sei $G \in M$ und wir erhalten $\bigcap M = \{ x \in G \mid \forall A \in M : x \in A \}$.

Soweit konstruieren wir mit (2–6) allein nur endliche Mengen. Axiom (7) garantiert, dass es in Ω auch unendliche Mengen gibt.

Die Zermelo–Fraenkel Axiome: ZF und ZFC = ZF+AC

D132
Erläuterung

Zur Aussonderung $\{ x \in M \mid p(x) \}$ ist $p(x)$ ein Prädikat für Elemente $x \in M$, also eine Formel in der Sprache der Mengen und Aussagenlogik. Im Beispiel $B \smallsetminus A = \{ x \in B \mid x \notin A \}$ ist p das Prädikat $p(x) = (x \notin A)$.

Zur Ersetzung $\{ f(x) \mid x \in M \}$ ist $F(x, y)$ ein zweistelliges Prädikat, sodass zu jedem Element $x \in M$ genau eine Menge y existiert, für die $F(x, y)$ wahr ist. Diese eindeutige Menge y schreiben wir $y = f(x)$. Im Beispiel $\{ \mathfrak{P}(x) \mid x \in M \}$ ist $F(x, y) = (\forall z : z \subseteq x \Leftrightarrow z \in y)$.

Das Aussonderungsaxiom (5) ist redundant, es folgt aus Vereinigung (4) und Ersetzung (6): Zu M und p wollen wir $\{ x \in M \mid p(x) \}$ konstruieren. Hierzu definieren wir $F(x, y) = (p(x) \wedge y = \{x\}) \vee (\neg p(x) \wedge y = \emptyset)$, also $f(x) = \{x\}$, falls $p(x)$ wahr ist, und $f(x) = \emptyset$, falls $p(x)$ falsch ist. Damit erhalten wir $\{ x \in M \mid p(x) \} = \bigcup \{ f(x) \mid x \in M \}$ wie ersehnt.

☺ Wir benötigen für ZF neben den Axiomen (0,1) zum Aufbau ganz sparsam nur die vier Konstruktionen (3,4,6,7). Für ZFC nehmen wir das Auswahlaxiom AC hinzu. Eine Handvoll von Konstruktionen genügt uns! Das ist bemerkenswert kurz und effizient, bequem und flexibel.

Paare und kartesische Produktmenge

D133

Aus Elementen $x \in X$ und $y \in Y$ bilden wir das geordnete **Paar** (x, y).
Die Gleichheit $(x, y) = (x', y')$ soll äquivalent sein zu $(x = x') \wedge (y = y')$.
Das ist die charakteristische Eigenschaft, die wir von Paaren verlangen.

☹ Die Paarmenge $\{x, y\}$ ist dazu ungeeignet, denn $\{x, y\} = \{y, x\}$.

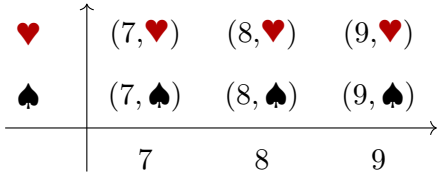
🙂 Es gelingt jedoch mit Kuratowskis Kniff $(x, y) := \{\{x\}, \{x, y\}\}$.
Hieraus lassen sich $\mathrm{pr}_1(x, y) = x$ und $\mathrm{pr}_2(x, y) = y$ extrahieren.

Das kartesische **Produkt** von X und Y ist die Menge aller Paare:

$$X \times Y := \{\, (x, y) \mid x \in X \wedge y \in Y \,\}$$

Beispiel: $\{7, 8, 9\} \times \{\spadesuit, \heartsuit\} = \{(7, \spadesuit), (7, \heartsuit), (8, \spadesuit), (8, \heartsuit), (9, \spadesuit), (9, \heartsuit)\}$.

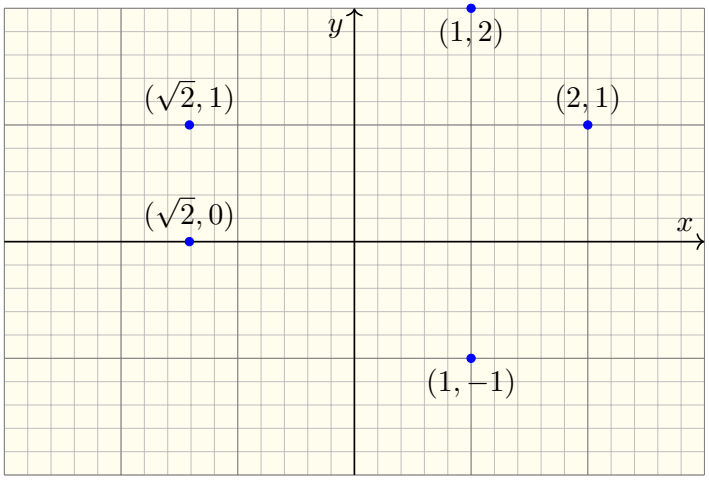
Graphisch:



Ist X eine endliche Menge mit n Elementen, so schreiben wir $\sharp X = n$.
Es gilt $\sharp(X \cup Y) = \sharp X + \sharp Y - \sharp(X \cap Y)$ und $\sharp(X \times Y) = (\sharp X) \cdot (\sharp Y)$.

Paare und kartesische Produktmenge

D134



Beispiel: Aus der Menge $\mathbb{R}$ der reellen Zahlen erhalten wir das Produkt

$$\mathbb{R}^2 \;:=\; \mathbb{R} \times \mathbb{R} \;=\; \{\, (x, y) \mid x, y \in \mathbb{R} \,\}.$$

Wir visualisieren $\mathbb{R}$ als Gerade und $\mathbb{R}^2$ als Ebene; dies sind die **kartesischen Koordinaten** nach René Descartes (1596–1650).

Paare und kartesische Produktmenge

D135
Erläuterung

Aus den Elementen x, y bilden wir das geordnete **Paar**

$$p = (x, y) := \{\{x\}, \{x, y\}\}.$$

Hieraus lassen sich $\mathrm{pr}_1(x, y) = x$ und $\mathrm{pr}_2(x, y) = y$ extrahieren:

$$\mathrm{Pr}_1(p, x) \;=\; \big[\textstyle\bigcap p = \{x\}\big]$$

Zu p existiert genau ein x mit $\mathrm{Pr}_1(p, x)$; dies schreiben wir $\mathrm{pr}_1(p) := x$ und nennen dies die **erste Koordinate** oder den ersten Eintrag von p.
Auch die **zweite Koordinate** y erhalten wir aus $p = \{\{x\}, \{x, y\}\}$ dank

$$\mathrm{Pr}_2(p, y) \;=\; \big[\textstyle\bigcup p = \{y\} \cup \bigcap p\big].$$

Zu p existiert genau ein y mit $\mathrm{Pr}_2(p, y)$; dies schreiben wir $\mathrm{pr}_2(p) := y$.

🙂 Mit diesem einfachen Kniff können wir also jedes Paar (x, y) als eine geeignete Menge implementieren. Die Konstruktionen von Mengen à la Zermelo–Fraenkel sind bemerkenswert effizient, bequem und flexibel. Sie liefern alles, was wir für die Mathematik benötigen werden.

Paare und kartesische Produktmenge

D136
Erläuterung

Die **Produktmenge** $P = X \times Y$ wird charakterisiert durch

$$p \in P \quad\Leftrightarrow\quad \exists x \in X \;\; \exists y \in Y \;:\; p = (x, y).$$

Somit ist P die Menge aller Paare (x, y) mit $x \in X$ und $y \in Y$.
Wir schreiben dies kurz und bequem so wie oben eingeführt:

$$X \times Y := \{\, (x, y) \mid x \in X \wedge y \in Y \,\}$$

Können wir diese Menge allein mit den ZF–Axiomen konstruieren?
Zunächst stellen wir fest: Für alle Elemente $x \in X$ und $y \in Y$ gilt

$$(x, y) = \{\{x\}, \{x, y\}\} \subseteq \mathfrak{P}(X \cup Y).$$

denn $\{x\} \subseteq X \subseteq X \cup Y$ und $\{x, y\} \subseteq X \cup Y$. Demnach erhalten wir

$$X \times Y := \{\, p \in \mathfrak{P}(\mathfrak{P}(X \cup Y)) \mid \exists x \in X \;\; \exists y \in Y \;:\; p = (x, y) \,\}$$

🙂 Hierzu nutzen wir die Vereinigung (4), zweimal die Potenz (3) und dann die Aussonderung (5). Die ZF–Axiome reglementieren zwar streng, doch glücklicherweise gelingen uns alle gewünschten Konstruktionen!

Paare, Tripel und n–Tupel

Aus $x \in X$ und $y \in Y$ und $z \in Z$ bilden wir das **Tripel** (x, y, z).
Als charakterisierende Eigenschaft verlangen wir lediglich:

$$(x, y, z) = (x', y', z') \quad \Longleftrightarrow \quad (x = x') \wedge (y = y') \wedge (z = z')$$

Eine erste mögliche Implementierung ist $(x, y, z) := ((x, y), z)$.
Die Rechtsklammerung $(x, (y, z))$ wäre eine andere Möglichkeit.
Wir lernen später noch weitere Möglichkeiten kennen und nutzen.

Das kartesische **Produkt** der Mengen X, Y, Z ist die Menge aller Tripel:

$$X \times Y \times Z := \{\, (x, y, z) \mid x \in X \wedge y \in Y \wedge z \in Z \,\}$$

Beispiel: Aus $\mathbb{R}$ erhalten wir so

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{\, (x, y, z) \mid x, y, z \in \mathbb{R} \,\}.$$

☺ Die Konstruktionen von Mengen à la Zermelo–Fraenkel sind flexibel und effizient. Sie liefern alles, was wir für die Mathematik benötigen.

Paare, Tripel und n–Tupel

Ebenso definieren wir für $n \in \mathbb{N}$ und $x_1 \in X_1, \ldots, x_n \in X_n$ das **n–Tupel**:

$$(x_1, \ldots, x_n) = (x_1', \ldots, x_n') \quad \Longleftrightarrow \quad (x_1 = x_1') \wedge \cdots \wedge (x_n = x_n')$$

Eine mögliche Implementierung ist $(x_1, x_2, \ldots, x_n) := ((x_1, x_2), \ldots, x_n)$.
Jede beliebige andere Klammerung wäre ebenso eine Möglichkeit.
Wir lernen später noch weitere Möglichkeiten kennen und nutzen.

Das kartesische **Produkt** der Mengen $X_1, \ldots, X_n$ ist dann:

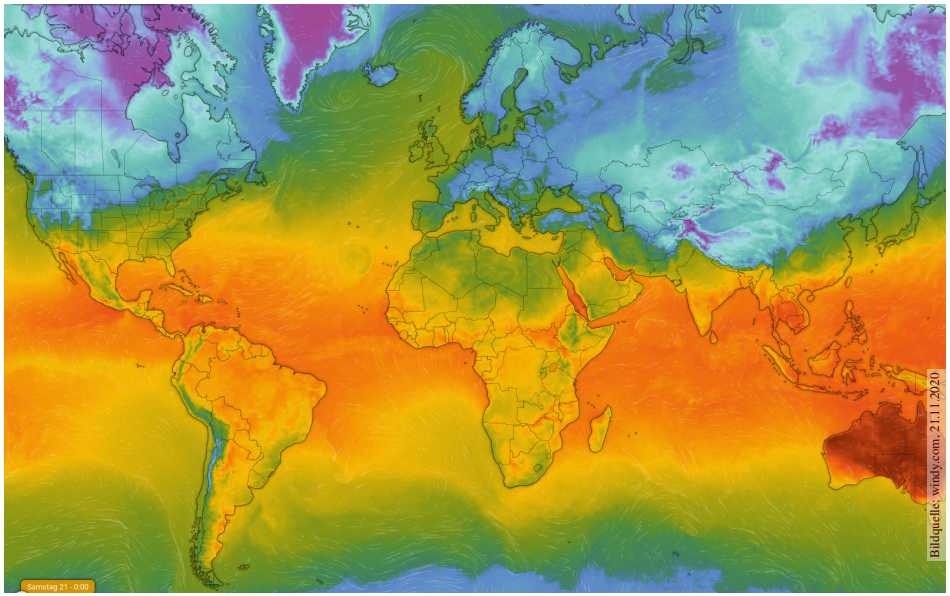
$$X_1 \times \cdots \times X_n := \{\, (x_1, \ldots, x_n) \mid x_1 \in X_1 \wedge \cdots \wedge x_n \in X_n \,\}$$

Beispiel: Aus $\mathbb{R}$ erhalten wir $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$ (mit n Faktoren):

$$\mathbb{R}^n = \{\, (x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R} \,\}$$

Auf dem Campus höre ich manchmal: „Der Raum $\mathbb{R}^4$ existiert gar nicht!“
Tatsächlich können wir uns dieses Objekt schwer räumlich vorstellen.
Ob er in der „physikalischen Realität“ existiert, ist schwer zu sagen,
als Modell ist er jedenfalls sehr erfolgreich in der Relativitätstheorie.
Mathematisch existiert er garantiert: Wir haben ihn gerade konstruiert!
Das genügt, um damit zu arbeiten, also in Koordinaten zu rechnen.

Paare, Tripel und n–Tupel



Temperatur, Luftdruck, etc. $\quad f : \mathbb{R}^2 \supseteq U \to \mathbb{R} \;\; : (x, y) \mapsto f(x, y)$
Windgeschwindigkeit, etc. $\quad g : \mathbb{R}^2 \supseteq U \to \mathbb{R}^2 : (x, y) \mapsto g(x, y)$

Paare, Tripel und n–Tupel

Damit kommen wir unserem Ziel einen wichtigen ersten Schritt näher:
Wir benötigen und konstruieren geeignete mathematische Werkzeuge
zur Beschreibung, Untersuchung und Lösung von realen Problemen.
Die Sprache der Mengen ist hierfür eine universelle Grundlage.

Die Mengenlehre ist abstrakt, zugegeben. Das ist gut und richtig so,
denn sie soll ja gerade eine *allgemeine* gesicherte Grundlage bilden!
Die Sprache der Mengen ist kein „abstrakter Unsinn“, sondern Sinn!
Wir werden alles weitere auf diesem Fundament aufbauen können.

Hierzu sind insbesondere Funktionen ein allgegenwärtiges Werkzeug.
Wir können jetzt bereits Teilmengen $U \subseteq \mathbb{R}^2$ der Ebene betrachten.
Eine Funktion $f : U \to \mathbb{R}$ ordnet jedem Punkt $(x, y) \in U$ eine reelle Zahl
$f(x, y) \in \mathbb{R}$ zu. Dieses Konzept untersuchen wir als nächstes.

Funktionen: Anschauung und Motivation

D201

Funktionen sind ein zentraler Grundbegriff der Mathematik!

$$\begin{aligned}
\mathrm{sq} &: \mathbb{R} \to \mathbb{R}_{\geq 0} : x \mapsto x^2 \\
\mathrm{sqrt} &: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto \sqrt{x} \\
\mathrm{sqrt} \circ \mathrm{sq} &: \mathbb{R} \to \mathbb{R}_{\geq 0} : x \mapsto \sqrt{x^2} \\
\mathrm{abs} &: \mathbb{R} \to \mathbb{R}_{\geq 0} : x \mapsto |x| = \begin{cases} x & \text{falls } x \geq 0, \\ -x & \text{falls } x \leq 0. \end{cases} \\
h &: \mathbb{R} \to \mathbb{R} : x \mapsto |x|
\end{aligned}$$

Eine Funktion $f : X \to Y$ bildet die Startmenge X in die Zielmenge Y ab: Jedem Element $x \in X$ ordnet f ein eindeutiges Bildelement $y \in Y$ zu; dies schreiben wir $y = f(x)$ oder $x \mapsto y = f(x)$. Zusammengefasst:

$$f : X \to Y : x \mapsto y = f(x)$$

Die **Gleichheit** von zwei Funktionen $f : X \to Y$ und $f' : X' \to Y'$ ist definiert durch $X = X'$ und $Y = Y'$ sowie $f(x) = f'(x)$ für alle $x \in X$.

Aufgabe: Welche obigen Funktionen sind gleich? Nur $\mathrm{sqrt} \circ \mathrm{sq} = \mathrm{abs}$.

Funktionen: Anschauung und Motivation

D202

Jede Funktion $f : X \to Y$ besteht demnach aus drei Daten (X, F, Y): der **Startmenge** X, der **Zielmenge** Y und dem **Funktionsgraphen**

$$F = \{\, (x, y) \in X \times Y \mid y = f(x) \,\} \subseteq X \times Y.$$

☺ Die Menge F codiert demnach die **vollständige Wertetabelle**:

$f : \{0, 1, \ldots, 10\} \to \mathbb{R}$ mit folgender Zuordnung

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	4	8	13	27	34	29	60	83	95

$F = \{\, (0,0),\ (1,1),\ (2,4),\ (3,8),\ (4,13),\ \ldots,\ (10,95) \,\}$

☺ Genau so wurden früher und werden auch heute noch Funktionen tabelliert, zum Beispiel Logarithmentafeln. Mit Computerhilfe geht es heutzutage noch bequemer, aber letztlich leistet er genau dasselbe.

☺ Alle modernen Programmiersprachen bieten dies als Datentyp. Dank der Sprache der Mengen können wir dies genauso problemlos nun für alle Mengen X, Y formulieren, egal ob endlich oder unendlich.

Funktionen: formale Definition

D203
Erläuterung

Eine Funktion $f : X \to Y$ ordnet jedem Element $x \in X$ eindeutig ein Element $y \in Y$ zu; hierfür schreiben wir kurz $y = f(x)$. Dies nennt man die **Präfix-Notation**: Das Funktionssymbol steht *vor* dem Argument. Die **Postfix-Notation** $y = (x)f$ ist seltener, kommt aber durchaus vor, etwa bei Transposition $A \mapsto A^\intercal$ oder Fakultät $n \mapsto n! = 1 \cdot 2 \cdot 3 \cdots n$.

In den obigen Beispielen sehen Sie bereits, dass Funktionsvorschriften, Formeln und Algorithmen einerseits sehr nützlich und praktisch sind, andererseits aber nicht das Wesen einer Funktion ausmachen.

Für jede Funktion $f : X \to Y$ zählen nur drei Daten: die Startmenge X, die Zielmenge Y und der Graph $F \subseteq X \times Y$ (Wertetabelle, Zuordnung). Wir kehren die Sichtweise um und erheben diese Daten zur Definition!

Das ist ein sehr kühner doch konsequenter Schritt der Abstraktion. Ganz allgemein folgt dies einem mathematischen Grundprinzip: *Finde, was wirklich wichtig ist, und mache es zur Definition!*

Funktionen: formale Definition

D204

Definition D2A: Abbildung / Funktion / Zuordnung

Eine **Abbildung** / **Funktion** / **Zuordnung** $f : X \to Y$ ist durch drei Daten $f = (X, F, Y)$ gegeben: die Startmenge X und die Zielmenge Y sowie den Funktionsgraphen $F \subseteq X \times Y$.

Dabei muss f jedem Startpunkt $x \in X$ aus der Startmenge genau einen Zielpunkt $y \in Y$ in der Zielmenge zuordnen:

$$\mathbf{Fun}(f) \quad :\Longleftrightarrow \quad \forall x \in X\ \exists! y \in Y : (x, y) \in F$$

Zu jedem Paar $(x, y) \in F$ sagen wir, f ordnet dem Element $x \in X$ das Bildelement $y \in Y$ zu, kurz $x \mapsto y =: f(x)$ Präfix oder $y =: (x)f$ Postfix.

Die **Gleichheit** von Abbildungen $f : X \to Y$ und $f' : X' \to Y'$ bedeutet somit $(X, F, Y) = (X', F', Y')$, also $X = X'$ und $Y = Y'$ und $F = F'$. Letzteres heißt $f(x) = f'(x)$ für jeden Startpunkt $x \in X$.

Zu $f : X \to Y$ und $g : Y \to Z$ ist die **Komposition** $h = f \bullet g = g \circ f$ die Abbildung $h : X \to Z$ durch Hintereinanderausführung $h(x) = g(f(x))$.

Funktionen: Schluss mit schlampig!

D205
Erläuterung

Aufgabe: (0) Was ist falsch an der (verbreiteten aber schlampigen) Sprechweise „die Funktion $f(x) = x^2$“ oder „die Funktion $y = x^2$“? Nennen Sie mindestens zehn unterschiedliche Interpretationen!

(1) Ist „die Funktion $f(x) = x^2$“ monoton? (2) Ist sie umkehrbar? (3) Ist „die Funktion $f(x) = x^2$“ gleich $g(x) = |x|$? gleich $h(x) = x$?

Lösung: (0) Zur Bearbeitung fehlen uns wesentliche Informationen: Aus welcher Startmenge kommt x? In welcher Zielmenge landet y?

$$
\begin{array}{llll}
f_1 : \mathbb{R} \to \mathbb{R} : x \mapsto x^2, & f_1^{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q} : x \mapsto x^2, \\
f_2 : \mathbb{R} \to \mathbb{R}_{\geq 0} : x \mapsto x^2, & f_2^{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}_{\geq 0} : x \mapsto x^2, \\
f_3 : \mathbb{R}_{\geq 0} \to \mathbb{R} : x \mapsto x^2, & f_3^{\mathbb{Q}} : \mathbb{Q}_{\geq 0} \to \mathbb{Q} : x \mapsto x^2, \\
f_4 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto x^2, & f_4^{\mathbb{Q}} : \mathbb{Q}_{\geq 0} \to \mathbb{Q}_{\geq 0} : x \mapsto x^2, \\
f_5 : \mathbb{R}_{\leq 0} \to \mathbb{R} : x \mapsto x^2, & f_5^{\mathbb{Q}} : \mathbb{Q}_{\leq 0} \to \mathbb{Q} : x \mapsto x^2, \\
f_6 : \mathbb{R}_{\leq 0} \to \mathbb{R}_{\geq 0} : x \mapsto x^2, & f_6^{\mathbb{Q}} : \mathbb{Q}_{\leq 0} \to \mathbb{Q}_{\geq 0} : x \mapsto x^2, \\
f_7 : \{0,1\} \to \{0,1\} : x \mapsto x^2, & f_8 : \{0,\pm 1\} \to \{0,1\} : x \mapsto x^2.
\end{array}
$$

⚠ Nur mit diesen Daten können wir (1,2,3) überhaupt erst angehen!

Funktionen: Schluss mit schlampig!

D206
Erläuterung

🙂 Müssen MathematikerInnen es immer so genau nehmen? Ja, sicher! Die „Funktion $f(x) = x^2$“ ergibt keinen rechten Sinn: Die Startmenge ist hier vollkommen unklar! Welche x sind dabei zugelassen? rational? reell? komplex? Und was ist die Zielmenge? Für die Monotonie (1), die Umkehrfunktion (2) und die Gleichheit (3) ist dies wesentlich!

Start- und Zielmenge einer Funktion müssen immer klar sein!
Am besten geben Sie diese Daten immer möglichst explizit an.
Notfalls müssen wir sie implizit aus dem Kontext erschließen:
„In der Schule bilden alle Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ ab.“
Nein, eben nicht alle, selbst dort gibt es Ausnahmen!

Eine Funktion f schreiben wir möglichst explizit wie folgt:

$$f : X \to Y : x \mapsto y = f(x)$$

Das bündelt die Information *Name*: *Start und Ziel*: *Abbildungsvorschrift*.
Gesprochen: Die Abbildung f bildet die Menge X in die Menge Y ab, indem sie jedem Element $x \in X$ sein Bild $y = f(x) \in Y$ zugeordnet.

Funktionen: Schluss mit schlampig!

D207
Erläuterung

⚠ **Funktionen** und **Formeln** sind grundsätzlich verschiedene Dinge! Häufig definieren wir eine Funktion mit Hilfe einer geeigneten Formel. Verschiedene Formeldarstellungen können jedoch dieselbe Funktion definieren, und manche Funktionen erlauben überhaupt keine Formel.

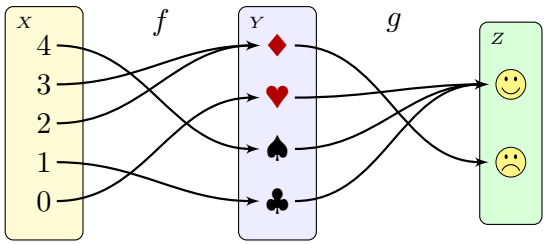
🙂 **Black-Box-Prinzip:** Wichtig ist für f nur das *Was*, nicht das *Wie*. Wir fassen daher alle Rechenwege zur selben Funktion f zusammen. Diese geschickte Abstraktion ist eine dramatische Vereinfachung.

🙂 Die Untersuchung möglicher Berechnungen ist wichtig, aber es ist eine klar getrennte Fragestellung. Erst wenn Sie f konkret auswerten, etwa auf dem Computer implementieren, zählt der genaue Rechenweg. Beispiel: Berechnen Sie $|x|$ und $\sqrt{x^2}$ mit Stift und Papier für $x = -12345$.

🙂 Wir trennen daher die Funktion von ihren diversen Darstellungen, Schreibweisen durch Formeln, Rechenvorschriften durch Algorithmen. Das lässt uns für später viele Freiheiten, denn dieselbe Funktion kann auf verschiedenen Wegen implementiert werden; je nach Bedarf suchen wir einen möglichst günstigen (einfach, effizient, schnell, genau, etc.).

Die Komposition zweier Funktionen ergibt eine Funktion.

D208



Zu $f : X \to Y$ und $g : Y \to Z$ definieren wir ihre **Komposition**

$$h = f \bullet g = g \circ f : X \to Z : x \mapsto h(x) = g(f(x)).$$

Beispiel: In der oben gezeigten Graphik gilt

$$h(0) = 🙂,\quad h(1) = 🙂,\quad h(2) = ☹,\quad h(3) = ☹,\quad h(4) = 🙂.$$

Datenbanken nutzen Funktionen, z.B. $f : M \to N$: Matrikelnr $\mapsto$ Name.
⚠ Vorsicht! Die Umkehrung $f^{\mathsf{T}} : N \to M$: Name $\mapsto$ Matrikelnr ist leider keine Funktion, sondern nur eine Relation. Auch das ist sehr nützlich...

Relationen und ihre Komposition

Definition D2B: Relation zwischen zwei Mengen

Vorgelegt seien Mengen X und Y. Eine **Relation zwischen X und Y** oder ein **Relationsgraph** ist eine Teilmenge $F \subseteq X \times Y$ des Produkts.

(1) Zu jeder Menge X definieren wir ihre **Diagonale**

$$\Delta_X = \{\, (x,x) \mid x \in X \,\} \subseteq X \times X.$$

(2) Zu $F \subseteq X \times Y$ definieren wir ihre **Inverse** oder **Umkehrrelation**

$$F^{-1} = F^{\mathsf{T}} = \{\, (y,x) \mid (x,y) \in F \,\} \subseteq Y \times X.$$

(3) Zu $F \subseteq X \times Y$ und $G \subseteq Y \times Z$ definieren wir ihre **Komposition**

$$H =: F \bullet G = G \circ F \subseteq X \times Z \quad (\text{„}F \text{ vor } G\text{“ bzw. „}G \text{ nach } F\text{“}),$$
$$H = \{\, (x,z) \in X \times Z \mid \exists y \in Y \,:\, (x,y) \in F \wedge (y,z) \in G \,\}.$$

Für $(x,y) \in F$ schreiben wir auch bequem $x\,F\,y$ in **Infix-Notation** und kürzen $(x,y) \in F \wedge (y,z) \in G$ ab zu $x\,F\,y\,G\,z$ (wie „$x \le y \le z$“). Somit ist die Komposition $x\,(F \bullet G)\,z$ definiert durch $\exists y \in Y : x\,F\,y\,G\,z$.

Relationen und ihre Komposition

☺ Uns interessieren meist vor allem Funktionen / Abbildungen / Zuordnungen: Das sind spezielle, besonders schöne Relationen. Gerade deshalb ist es praktisch nützlich und didaktisch hilfreich, Relationen zu betrachten: Sie bieten den allgemeinen Rahmen.

Zur Betonung nennen wir $F \subseteq X \times Y$ auch **zweistellige** oder **binäre Relation**. Wenn nicht ausdrücklich etwas anderes präzisiert wird, verstehen wir unter Relation immer eine zweistellige Relation.

Eine n–stellige Relation hat die Form $F \subseteq X_1 \times X_2 \times \cdots \times X_n$. Für $n = 1$ ist dies eine Teilmenge, für $n = 2$ eine binäre Relation.

Im Falle $(x,y) \in F$ sagen wir auch „x und y stehen in der Relation F“ oder „x korrespondiert zu y bezüglich F“ , abgekürzt $x\,F\,y$ als Infix.

Diese Infix-Schreibweise ist vor allem für Ordnungsrelation $\le$ und Äquivalenzrelationen $\sim$ üblich, da sehr bequem und suggestiv.

Die Komposition $H = F \bullet G$ erfüllt $x\,H\,z$ genau dann, falls es ein Bindeglied y mit $x\,F\,y$ und $y\,G\,z$ gibt, abgekürzt $x\,F\,y\,G\,z$.

Graphisches Beispiel zur Diagonalen

Zu der Menge $X = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$ ist die Diagonale

$$\Delta = \Delta_X = \{\, (\clubsuit,\clubsuit), (\spadesuit,\spadesuit), (\heartsuit,\heartsuit), (\diamondsuit,\diamondsuit) \,\} \subseteq X \times X.$$

Graphisch sieht diese Teilmenge $\Delta_X \subseteq X \times X$ so aus:

Δ	$\clubsuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$
$\clubsuit$	1	0	0	0
$\spadesuit$	0	1	0	0
$\heartsuit$	0	0	1	0
$\diamondsuit$	0	0	0	1

Der Eintrag $1\,/\,0$ an der Stelle (x,y) bedeutet $(x,y) \in \Delta$ bzw. $(x,y) \notin \Delta$.

☺ Die Darstellung durch 0 und 1 erinnert uns an die **Einheitsmatrix**. Der Name „Diagonale“ für die Menge $\Delta_X \subseteq X \times X$ ist sprechend.

Graphisches Beispiel zur Umkehrrelation

F	5	6	7
$\clubsuit$	1	0	1
$\spadesuit$	1	1	0
$\heartsuit$	0	1	0
$\diamondsuit$	0	0	0

$\longleftrightarrow$

F^{T}	$\clubsuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$
5	1	1	0	0
6	0	1	1	0
7	1	0	0	0

Zwischen den Mengen $X = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$ und $Y = \{5,6,7\}$ betrachten wir die obige Relation $F \subseteq X \times Y$. Die zugehörige Umkehrrelation ist

$$F^{-1} = F^{\mathsf{T}} = \{\, (y,x) \mid (x,y) \in F \,\} \subseteq Y \times X.$$

Das erinnert uns an die **Transposition einer Matrix** aus Kapitel B: Dort wird die Matrix $A \in \mathbb{K}^{m \times n}$ zu $A^{\mathsf{T}} \in \mathbb{K}^{n \times m}$ transponiert, hier die Relation $F \subseteq X \times Y$ zu $F^{\mathsf{T}} \subseteq Y \times X$ gespiegelt.

Graphisches Beispiel zur Komposition

D213

F	♠	♥	♦
5	0	0	1
6	1	1	0
7	0	0	0
8	0	1	0
9	1	0	1

$\bullet$

G	🙂	☹
♠	1	0
♥	1	1
♦	0	0

$=$

H	🙂	☹
5	0	0
6	1	1
7	0	0
8	1	1
9	1	0

Wir betrachten die Mengen $X = \{5, 6, 7, 8, 9\}$ und $Y = \{♠, ♥, ♦\}$ und $Z = \{🙂, ☹\}$ sowie obige Relationen $F \subseteq X \times Y$ und $G \subseteq Y \times Z$ und

$$H = F \bullet G = \{\, (x, z) \in X \times Z \mid \exists y \in Y : (x, y) \in F \wedge (y, z) \in G \,\}.$$

Das ist die **Matrixmultiplikation** über dem Halbring $(\{0, 1\}, \vee, 0, \wedge, 1)$.

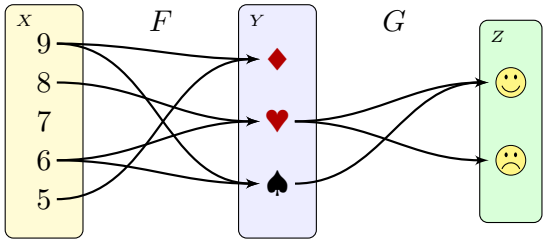
Für die Komposition $H = F \bullet G$ gilt demnach $(x, z) \in H$ genau dann, wenn es einen Weg von $x \in X$ nach $z \in Z$ gibt mit Zwischenstopp in Y.

Wenn wir stattdessen über dem Halbring $(\mathbb{N}, +, 0, \cdot, 1)$ rechnen, so erhalten wir die **Anzahl** der Wege, wie im nächsten Bild.

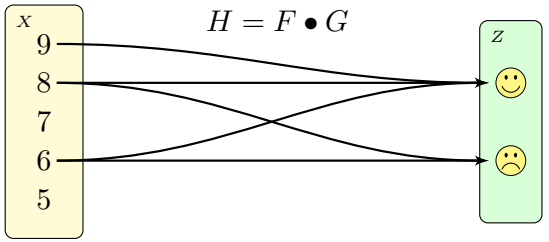
Graphisches Beispiel zur Komposition

D214

Dasselbe Beispiel in anderer Darstellung, diesmal in Pfeilschreibweise:



Die Komposition $F \bullet G$ codiert Verbindungen von X über Y nach Z:



Relationen und ihre Komposition

D215
Erläuterung

Ist das abstrakt und unnütz? Abstrakt ja, unnütz nein! Diese Strukturen sind abstrakt, und deshalb vielseitig anwendbar und universell nutzbar. In der Mathematik nutzen wir Mengen, insbesondere Funktionen und Relationen, um gewisse Informationen zu codieren, zu speichern und zu verarbeiten. Das hat eine direkte Entsprechung in der Informatik:

Eine **relationale Datenbank** speichert und verarbeitet Informationen als Relationen in Tabellenform. Sie wurden um 1970 von Edgar Codd bei IBM entwickelt und sind ein etablierter, weit verbreiteter Standard, etwa in Form der Datenbanksprache SQL (Structured Query Language). Sie wird nahezu überall eingesetzt, nicht zuletzt in Webanwendungen.

Relationale Datenbanken nutzen Mengen und Relationen. Sie eignen sich besonders für strukturierte Daten. In den letzten Jahrzehnten widmet sich **Big Data** zunehmend unstrukturierten und sehr große Datenmengen. Hier müssen die klassischen Konzepte erweitert und angepasst werden, auch dies gelingt auf Grundlage der Mengenlehre!

Relationen und ihre Komposition

D216
Erläuterung

⚠ Für die meisten Zwecke ist es wichtig zu der Relation $F \subseteq X \times Y$ immer auch die Startmenge X und die Zielmenge Y zu kennen.

Allein aus $F \subseteq X \times Y$ können wir nämlich die Mengen X und Y nicht immer rekonstruieren, sondern nur die eventuell kleineren Teilmengen

$$X' = \mathrm{pr}_1 F = \{\, x \mid \exists y : (x, y) \in F \,\},$$
$$Y' = \mathrm{pr}_2 F = \{\, y \mid \exists x : (x, y) \in F \,\}.$$

☹ Im traurigen Extremfall der leeren Relation $F \subseteq X \times Y$ gilt $F = \emptyset$, und hier geben $X' = Y' = \emptyset$ überhaupt keine Auskunft über X und Y.

Um alle nötigen Informationen parat zu halten, ist es sinnvoll und nötig, der Relation $F \subseteq X \times Y$ explizit die Mengen X und Y mitzugeben.

🙂 Die vollständige Information bietet das Tripel $f = (X, F, Y)$.
Diese Überlegung führt uns zu der folgenden Definition D2C.

Prominente Beispiele: Ordnungsrelationen

D217

Auf der Menge $X = \{0, 1, 2, 3, 4\} \subset \mathbb{N}$ betrachten wir die Relationen $R = \{\, (x, y) \in X \times X \mid x \leq y \,\}$ und $S = \{\, (x, y) \in X \times X \mid x < y \,\}$.

In Infix-Notation schreiben wir kurz $x\, R\, y \Leftrightarrow x \leq y$ und $x\, S\, y \Leftrightarrow x \leq y$.

R	0	1	2	3	4
0	1	1	1	1	1
1	0	1	1	1	1
2	0	0	1	1	1
3	0	0	0	1	1
4	0	0	0	0	1

S	0	1	2	3	4
0	0	1	1	1	1
1	0	0	1	1	1
2	0	0	0	1	1
3	0	0	0	0	1
4	0	0	0	0	0

Reflexivität,	**Refl**(X, R):	$\Delta_X \subseteq R$,	$x\, R\, x$ für alle $x \in X$.
Antisymmetrie,	**Asym**(X, R):	$R \cap R^{\mathsf{T}} \subseteq \Delta_X$,	$x\, R\, y \wedge y\, R\, x \Rightarrow x = y$.
Transitivität,	**Tran**(X, R):	$R \bullet R \subseteq R$,	$x\, R\, y \wedge y\, R\, z \Rightarrow x\, R\, z$.

Eine Relation mit diesen drei Eigenschaften heißt **Ordnungsrelation**.

$R^{\mathsf{T}} = \{\, (x, y) \in X \times X \mid x \geq y \,\}$ und $S^{\mathsf{T}} = \{\, (x, y) \in X \times X \mid x > y \,\}$.

Prominente Beispiele: Ordnungsrelationen

D218 Erläuterung

Dies sind zunächst zwei schöne, konkrete Beispiele für Relationen. Hier illustrieren sie Relationen als einfache und flexible Grundstruktur. Den allgemeinen und zentral wichtigen Begriff der Ordnungsrelation werden wir im übernächsten Kapitel F ausführlich behandeln.

Allgemein betrachten wir Relationen $F \subseteq X \times Y$ zwischen zwei Mengen X und Y wie in Definition D2B. Hier hingegen haben wir den Spezialfall $X = Y$ und gelangen zu Relationen $R \subseteq X \times X$ auf einer Menge X. Dabei ergeben sich neue interessante Phänomene und Fragen wie Reflexivität, Symmetrie / Antisymmetrie, Transitivität.

Für Relationen (wie zuvor für Matrizen) haben wir drei Grundobjekte: Die Diagonale $\Delta_X \subseteq X \times X$, die Umkehrrelation $F \mapsto F^{\mathsf{T}}$ und die Komposition $(F, G) \mapsto F \bullet G = G \circ F$, wie oben erklärt und illustriert. Es ist lehrreich und auch amüsant, dass sich Reflexivität, Symmetrie / Antisymmetrie, Transitivität damit überaus elegant formulieren lassen.

Prominente Beispiele: Äquivalenzrelationen

D219

Auf der Menge $X = \{0, -1, +1, -\mathrm{i}, +\mathrm{i}\} \subset \mathbb{C}$ haben wir die Relationen $R = \{\, (x, y) \in X \times X \mid x^2 = y^2 \,\}$ und $S = \{\, (x, y) \in X \times X \mid |x| = |y| \,\}$.

In Infix-Notation schreiben wir $x\, R\, y \Leftrightarrow x^2 = y^2$ und $x\, S\, y \Leftrightarrow |x| = |y|$.

R	0	-1	$+1$	$-\mathrm{i}$	$+\mathrm{i}$
0	1	0	0	0	0
-1	0	1	1	0	0
$+1$	0	1	1	0	0
$-\mathrm{i}$	0	0	0	1	1
$+\mathrm{i}$	0	0	0	1	1

S	0	-1	$+1$	$-\mathrm{i}$	$+\mathrm{i}$
0	1	0	0	0	0
-1	0	1	1	1	1
$+1$	0	1	1	1	1
$-\mathrm{i}$	0	1	1	1	1
$+\mathrm{i}$	0	1	1	1	1

Reflexivität,	**Refl**(X, R):	$\Delta_X \subseteq R$,	$x\, R\, x$ für alle $x \in X$.
Symmetrie,	**Sym**(X, R):	$R = R^{\mathsf{T}}$,	$x\, R\, y \Rightarrow y\, R\, x$.
Transitivität,	**Tran**(X, R):	$R \bullet R \subseteq R$,	$x\, R\, y \wedge y\, R\, z \Rightarrow x\, R\, z$.

Eine Relation mit diesen drei Eigenschaften heißt **Äquivalenzrelation**.

Diese zerlegen $X = \bigsqcup\{\, \{0\}, \{-1, 1\}, \{-\mathrm{i}, \mathrm{i}\} \,\} = \bigsqcup\{\, \{0\}, \{-1, 1, -\mathrm{i}, \mathrm{i}\} \,\}$.

Prominente Beispiele: Äquivalenzrelationen

D220 Erläuterung

Dies sind zunächst zwei schöne, konkrete Beispiele für Relationen; Hier illustrieren sie Relationen als einfache und flexible Grundstruktur. Den allgemeinen und zentral wichtigen Begriff der Äquivalenzrelation werden wir im nächsten Kapitel E ausführlich behandeln.

Relationen im realen / digitalen Alltag


Alice


Bob


Chuck

Beispiel: Wir betrachten $X = \{ A{=}\text{Alice}, B{=}\text{Bob}, C{=}\text{Chuck} \}$.
Wer duzt wen? Relationen sind extrem flexibel:

G_0	A	B	C
A	0	0	0
B	0	0	0
C	0	0	0

G_1	A	B	C
A	1	1	1
B	1	1	1
C	1	1	1

G_2	A	B	C
A	1	1	1
B	1	0	0
C	0	0	1

Unser realer / digitaler Alltag ist voller Relationen:

- soziale Netzwerke, Likes, Abonnenten, Follower, ...
- Webseiten und gegenseitige Links, Google PageRank, ...
- Corona-Warn-App, Kontaktgraph mit weiteren relevanten Daten ...

Relationen im realen / digitalen Alltag

🙂 Unsere drei einfachen Beispiele G_0, G_1, G_2 illustrieren das Prinzip.
Extremfälle sind G_0: Niemand duzt irgendwen, G_1: Jeder duzt jeden.
Alle weiteren Relationen liegen dazwischen, im Sinne der Inklusion.
Unser Beispiel G_2 scheint recht plausibel und typisch:

G_2: Alice duzt Chuck, aber nicht umgekehrt: G_2 *ist nicht symmetrisch*.
Alice duzt sich in Selbstgesprächen, Bob niemals: G_2 *ist nicht reflexiv*.
Bob duzt Alice und Alice duzt Chuck, aber Bob duzt nicht Chuck:
Die Relation G_2 ist demnach auch *nicht transitiv*.

Beobachten und (er)finden Sie weitere Beispiele dieser Art!
Wenn Sie erst einmal auf die Idee gekommen sind und die nötigen mathematischen Begriffe kennen, so entdecken Sie überall Relationen!

Viele der aktuell großen Internetkonzerne gründen ihren Erfolg auf der mathematisch-algorithmischen Auswertung von sozalen Relationen.
Dies ist ein wichtiges Anwendungsbeispiel von **Big Data**.

Kleine-Welt-Phänomen / *Six degrees of separation*

Die Redewendung **Six degrees of separation** bezeichnet die Idee, dass je zwei Menschen auf der Erde über sechs Zwischenstationen miteinander bekannt sind. Das scheint tatsächlich häufig zuzutreffen, siehe `en.wikipedia.org/wiki/Small-world_experiment`.

Der Begriff **Kleine-Welt-Phänomen** wurde 1967 von Stanley Milgram geprägt. Der Hypothese nach ist jeder Mensch mit jedem anderen über eine überraschend kurze Kette von Bekanntschaften verbunden; zwar ist die soziale Vernetzung eher dünn, erlaubt aber viele Abkürzungen.

Wie kann man daraus eine präzise, überprüfbare Aussage machen? Hierzu müssen wir zunächst die Aussage „x und y sind verbunden“ päzisieren, etwa (0) x kennt y beim Namen oder (1) x und y kennen sich gegenseitig oder (2) x und y haben sich die Hand geschüttelt, etc.

Für eine deutschsprachige Testgruppe könnte man auch „x dutzt y“ betrachten, wie im obigen Beispiel. Im der Relation G_2 ist Chuck mit niemand anderem verbunden, hier wäre die Hypothese also falsch.

Kleine-Welt-Phänomen / *Six degrees of separation*

Aufgabe: Angenommen, die Relation $R \subseteq X \times X$ codiert „x kennt y“.
Wie würden Sie die Aussage *six degrees of separation* formulieren?

Lösung: Wir können Reflexivität $\Delta_X \subseteq R$ annehmen oder fordern.
Auch Symmetrie $R = R^\intercal$ ist nach manchen Definitionen automatisch.
Die Behauptung ist nun $R \bullet R \bullet R \bullet R \bullet R \bullet R \overset{!}{=} X \times X$: Je zwei Menschen sind über höchstens sechs Zwischenstationen verbunden.

🙂 Auch hier ist es lehrreich zu sehen, wie sich die ursprünglich vage Idee präzisieren lässt. Dies ist dringend notwendig, wenn konkrete Daten erhoben und Experimente durchgeführt werden sollen.

🙂 Mit konkreten Daten lässt sich die Hypothese nun überprüfen, je nach Datenlage also entweder bestätigen oder widerlegen!
Das ist das typische Vorgehen in den Naturwissenschaften.

Relationen mit Start und Ziel

Definition D2c: Relation mit Start und Ziel

Eine **Relation** $f = (X, F, Y)$ besteht aus ihrer **Startmenge** X und ihrer **Zielmenge** Y sowie ihrem **Relationsgraphen** $F \subseteq X \times Y$.

Definitionsmenge	$\mathrm{Def}(f) := \mathrm{pr}_1 F = \{\, x \in X \mid \exists y \in Y : (x,y) \in F \,\},$
Bildmenge	$\mathrm{im}(f) := \mathrm{pr}_2 F = \{\, y \in Y \mid \exists x \in X : (x,y) \in F \,\}.$

(1) Zu jeder Menge X definieren wir ihre **Identität(sabbildung)**

$$\mathrm{id}_X = (X, \Delta_X, X) \quad \text{mit} \quad \Delta_X = \{\, (x,x) \mid x \in X \,\}.$$

(2) Zu $f = (X, F, Y)$ definieren wir ihre **Inverse** oder **Umkehrrelation**

$$f^{-1} = f^\intercal = (Y, F^\intercal, X) \quad \text{mit} \quad F^\intercal = \{\, (y,x) \mid (x,y) \in F \,\}.$$

(3) Zu $f = (X, F, Y)$ und $g = (Y, G, Z)$ definieren wir ihre **Komposition**

$$h = (X, H, Z) =: f \bullet g = g \circ f \quad (\text{„}f \text{ vor } g\text{“ bzw. „}g \text{ nach } f\text{“}),$$
$$H = \{\, (x,z) \in X \times Z \mid \exists y \in Y : (x,y) \in F \wedge (y,z) \in G \,\}.$$

Relationen mit Start und Ziel

Die **Startmenge** X, engl. *source*, heißt auch **Quelle** oder **Linksmenge**.
Die **Zielmenge** Y, engl. *target*, heißt auch **Ziel** oder **Rechtsmenge**.

Die Definitionsmenge $\mathrm{Def}(f) \subseteq X$ heißt auch **Urbildmenge** von f, seltener auch **Argumentbereich** oder **Vorbereich** der Relation f.

Die Bildmenge $\mathrm{im}(f) \subseteq Y$ heißt auch **Wertemenge** oder **Wertebereich**. In diesem Kontext ist das Wort „Bereich“ synonym mit (Teil-)Menge.

🙂 Das Tripel $f = (X, F, Y)$ bietet die vollständige Information.
Wie zuvor motiviert wollen wir für $F \subseteq X \times Y$ alle nötigen Informationen parat halten, daher geben wir F explizit die Mengen X und Y mit.

Die Definition von Relationen als Tripel hat wichtige Konsequenzen.
Die Gleichheit von $f = (X, F, Y)$ und $f' = (X', F', Y')$ bedeutet:

$$f = f' \quad \Longleftrightarrow \quad X = X' \ \wedge\ Y = Y' \ \wedge\ F = F'$$

Zur Betonung nochmal in Worten: Nicht nur der Graph $F = F'$ ist gleich, sondern auch die Startmenge $X = X'$ und die Zielmenge $Y = Y'$.

Rechenregeln für die Komposition

Aufgabe: Für $f = (X, F, Y)$ und $g = (Y, G, Z)$ und $h = (Z, H, W)$ gilt:
(1) Neutralität $\mathrm{id}_X \bullet f = f \bullet \mathrm{id}_Y = f$ bzw. $f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f$.
(2) Umkehrung $(f \bullet g)^\intercal = g^\intercal \bullet f^\intercal$ bzw. $(g \circ f)^\intercal = f^\intercal \circ g^\intercal$.
(3) Assoziativität $(f \bullet g) \bullet h = f \bullet (g \bullet h)$ bzw. $(h \circ g) \circ f = h \circ (g \circ f)$.

Lösung: (1) Die passende Identität ist links- / rechtsneutral:

$$(x,y) \in \Delta_X \bullet F \overset{\text{Def}}{\Longleftrightarrow} \exists x' \in X : x\, \Delta_X\, x' \wedge x'\, F\, y \overset{\Delta}{\Longleftrightarrow} (x,y) \in F$$
$$(x,y) \in F \bullet \Delta_Y \overset{\text{Def}}{\Longleftrightarrow} \exists y' \in Y : x\, F\, y' \wedge y'\, \Delta_Y\, y \overset{\Delta}{\Longleftrightarrow} (x,y) \in F$$

(2) Die Umkehrung vertauscht die Faktoren:

$$(z,x) \in (F \bullet G)^\intercal \overset{\text{Def}}{\Longleftrightarrow} (x,z) \in F \bullet G \overset{\text{Def}}{\Longleftrightarrow} \exists y \in Y : x\, F\, y \wedge y\, G\, z$$
$$(z,x) \in G^\intercal \bullet F^\intercal \overset{\text{Def}}{\Longleftrightarrow} \exists y \in Y : z\, G^\intercal\, y \wedge y\, F^\intercal\, x$$

(3) Wir setzen die Definition ein und rechnen es nach!

$$(x,w) \in F \bullet (G \bullet H) \overset{\text{Def}}{\Longleftrightarrow} \exists y \in Y : x\, F\, y \wedge \big[\exists z \in Z : y\, G\, z \wedge z\, H\, w\big]$$
$$(x,w) \in (F \bullet G) \bullet H \overset{\text{Def}}{\Longleftrightarrow} \exists z \in Z : \big[\exists y \in Y : x\, F\, y \wedge y\, G\, z\big] \wedge z\, H\, w$$

🙂 Zum Glück haben wir die Logik in Kapitel C gründlich vorbereitet!

Rechenregeln für die Komposition

⚠ Die Komposition $f \bullet g$ bzw. $g \circ f$ zweier Relationen ist nur dann definiert, wenn das Ziel von f mit dem Start von g übereinstimmt!

In diesem Fall heißen f und g **komponierbar** oder **verknüpfbar**.

Die **Komposition** heißt auch **Verknüpfung** oder **Verkettung** oder **Hintereinanderschaltung** oder **Hintereinanderausführung**.

Als Schreibweise vereinbaren hier zwei nützliche Konventionen:
Die Linkskomposition $\circ$ ist üblich, die Rechtskomposition $\bullet$ natürlich.

🙂 Der obige Beweis gelingt sofort, indem Sie die Definition einsetzen.
Eine solche Überprüfung heißt **trivial**, da sie rein mechanisch ist.
Sie erfordert allein gewissenhafte Sorgfalt, aber keine neuen Ideen,
da alles Notwendige (Definitionen, Sätze, etc.) bereits vorbereitet ist.

🙂 Bitte vergleichen Sie dies mit der Multiplikation von Matrizen.
Dabei drängen sich bemerkenswerte Parallelen und Analogien auf.
Dort haben wir zahlreiche triviale Rechnung sorgsam ausgeführt.
Auch und gerade triviale Beweise sollten Sie routiniert durchführen!

Von Relationen zu Funktionen

D229

Vorgelegt sei eine Relation $f = (X, F, Y)$ mit Graph $F \subseteq X \times Y$.
Wir nennen f **linkstotal**, falls gilt:

$$\forall x \in X \;\; \exists y \in Y \;:\; (x, y) \in F$$

Wir nennen f **rechtstotal**, falls gilt:

$$\forall y \in Y \;\; \exists x \in X \;:\; (x, y) \in F$$

Wir nennen f **linkseindeutig**, falls gilt:

$$\forall y \in Y \;\; \forall x, x' \in X \;:\; (x, y) \in F \wedge (x', y) \in F \Rightarrow x = x'$$

Wir nennen f **rechtseindeutig**, falls gilt:

$$\forall x \in X \;\; \forall y, y' \in Y \;:\; (x, y) \in F \wedge (x, y') \in F \Rightarrow y = y'$$

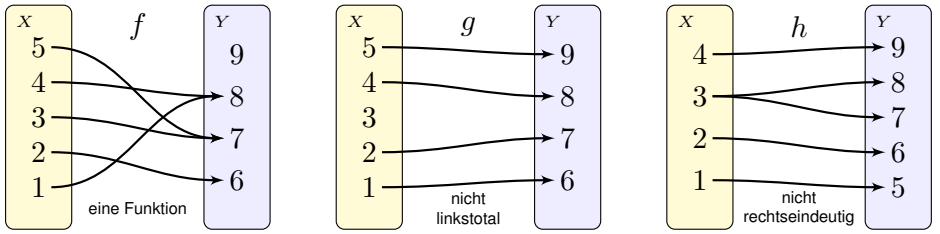
Die Relation $f = (X, F, Y)$ ist eine **Abbildung** / **Funktion** / **Zuordnung**, falls sie linkstotal und rechtseindeutig ist. Ausgeschrieben bedeutet das:

$$\mathbf{Fun}(f) \quad :\Longleftrightarrow \quad \forall x \in X \;\; \exists! y \in Y \;:\; (x, y) \in F$$

Zu jedem Paar $(x, y) \in F$ sagen wir dann, f ordnet dem Element $x \in X$ das Element $y \in Y$ zu, und schreiben hierfür $f(x) = y$ oder $f : x \mapsto y$.

Funktion oder nicht?

D230



Die Tatsache, dass die Relation $f = (X, F, Y)$ eine Funktion ist, also das Prädikat $\mathbf{Fun}(f)$ erfüllt, schreiben wir kurz und bequem:

$$f : X \to Y$$

Zusätzlich können wir eine Abbildungsvorschrift angeben:

$$f \;:\; X \to Y \;:\; x \mapsto y = f(x)$$

Das bündelt die Information *Name* : *Start und Ziel* : *Abbildungsvorschrift*.

Beispiel $f : \{1, 2, 3, 4, 5\} \to \{6, 7, 8, 9\} : 1 \mapsto 8, 2 \mapsto 6, 3 \mapsto 7, 4 \mapsto 8, 5 \mapsto 7$
oder $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0} : x \mapsto 1/x$ oder $f : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto \sqrt{x^2 + y^2}$

Eigenschaften von Abbildungen: injektiv, surjektiv, bijektiv

D231

Sei $f : X \to Y$ eine Abbildung, also $f = (X, F, Y)$ mit $F \subseteq X \times Y$ und

$$\mathbf{Fun}(f) \quad :\Longleftrightarrow \quad \forall x \in X \;\; \exists! y \in Y \;:\; (x, y) \in F$$

Die Abbildung $f : X \to Y$ heißt **injektiv**, falls sie linkseindeutig ist:

$$\forall x, x' \in X \;:\; f(x) = f(x') \Rightarrow x = x'$$

Jedes Zielelement $y \in Y$ wird höchstens einmal getroffen.
Per Kontraposition ist das äquivalent zu: $x \neq x' \Rightarrow f(x) \neq f(x')$.

Die Abbildung $f : X \to Y$ heißt **surjektiv**, falls sie rechtstotal ist:

$$\forall y \in Y \;\; \exists x \in X \;:\; f(x) = y$$

Jedes Zielelement $y \in Y$ wird mindestens einmal getroffen.
Die Bildmenge $\mathrm{im}(f) = \{\, f(x) \mid x \in X \,\} \subseteq Y$ ist die ganze Menge Y.

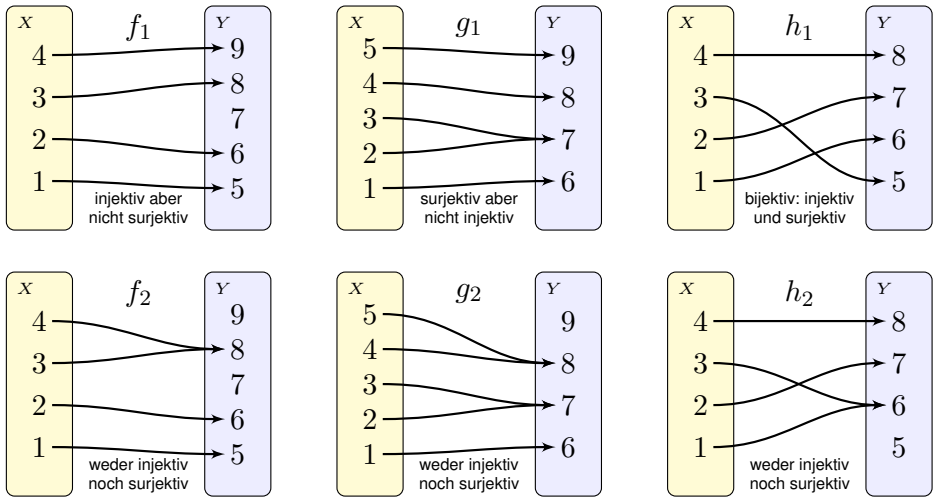
Die Abbildung $f : X \to Y$ heißt **bijektiv**, falls sie injektiv und surjektiv ist:

$$\forall y \in Y \;\; \exists! x \in X \;:\; f(x) = y$$

Zu jedem Ziel $y \in Y$ existiert genau ein Start $x \in X$ mit $f(x) = y$.

Eigenschaften von Abbildungen: injektiv, surjektiv, bijektiv

D232



Eine **Bijektion** $f : X \xrightarrow{\sim} Y$ ist eine bijektive Abbildung $f : X \to Y$.
Eine **Injektion** $f : X \hookrightarrow Y$ ist eine injektive Abbildung $f : X \to Y$.
Eine **Surjektion** $f : X \twoheadrightarrow Y$ ist eine surjektive Abbildung $f : X \to Y$.

Bildmenge

D233

Sei $f : X \to Y$ eine Abbildung, $f = (X, F, Y)$ mit Graph $F \subseteq X \times Y$.
Zu jeder Teilmenge $A \subseteq X$ definieren wir ihre **Bildmenge unter** f durch

$$\begin{aligned} f(A) = f_*(A) &= \{\, f(x) \mid x \in A \,\} \\ &= \{\, y \in Y \mid \exists x \in A : (x, y) \in F \,\}. \end{aligned}$$

Genau dann gilt $y \in f_*(A)$, wenn ein $x \in A$ existiert mit $f(x) = y$.
So induziert $f : X \to Y$ die Abbildung $f_* : \mathfrak{P}(X) \to \mathfrak{P}(Y) : A \mapsto f_*(A)$.

Beispiele: (In bequem-schludriger Schreibweise f statt f_*)
Für $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ gilt $f_*([-2, 3]) = [0, 9]$ und $f_*(\mathbb{R}) = \mathbb{R}_{\geq 0}$.
Für $g : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ gilt $g_*([-2, 3]) = [-8, 27]$ und $g_*(\mathbb{R}) = \mathbb{R}$.

Die **Bildmenge** der Abbildung $f : X \to Y$ ist

$$\operatorname{im}(f) = f_*(X) = \{\, f(x) \mid x \in X \,\} \subseteq Y.$$

Genau dann ist die Abbildung f surjektiv, wenn $f_*(X) = Y$ gilt.
(Für jedes $y \in Y$ hat die Faser $f^*(\{y\})$ mindestens ein Element.)

Vorsicht bei Überladung der Notation

D234
Erläuterung

Die Abbildung $f : X \to Y$ schickt jedes Startelement $x \in X$ auf sein Bildelement $y = f(x)$. Gegeben sei nun eine Teilmenge $A \subseteq X$.
Wir schicken jedes ihrer Elemente $x \in A$ auf sein Bild $y = f(x)$
und fassen diese Bildelemente zusammen zu der Bildmenge

$$f(A) = f_*(A) = \left\{\, f(x) \;\middle|\; x \in A \,\right\}.$$

⚠ Die Schreibweise $f(A)$ ist schludrig, aber verlockend bequem und daher weit verbreitet. Die Abbildungen $f : X \to Y$ und $f_* : \mathfrak{P}(X) \to \mathfrak{P}(Y)$ sind verschiedene Dinge! Gerade am Anfang sollten Sie beide gründlich unterscheiden, wenn schon nicht in der Notation, so in der Bedeutung.

Einige Autoren bemühen sich um Notation und Klärung des Problems, doch in der Literatur begegnet Ihnen vermutlich häufiger die Lässigkeit. Ich führe daher zunächst eine formal korrekte Bezeichnung ein, werde dann aber die bequem fahrlässige Schreibweise nutzen.

🙂 Hier gilt ausnahmsweise: *Do as I say, not as I do.* (Man kann seine Kinder noch so gut erziehen, sie machen einem doch alles nach.)

Urbildmenge

D235

Sei $f : X \to Y$ eine Abbildung, $f = (X, F, Y)$ mit $F \subseteq X \times Y$.
Zu jeder Teilmenge $B \subseteq Y$ definieren wir ihr **Urbild unter** f durch

$$\begin{aligned} f^{-1}(B) = f^*(B) &= \{\, x \in X \mid f(x) \in B \,\} \\ &= \{\, x \in X \mid \exists y \in B : (x, y) \in F \,\}. \end{aligned}$$

In Worten: Für $x \in X$ gilt $x \in f^*(B)$ genau dann, wenn $f(x) \in B$ gilt.
So induziert $f : X \to Y$ die Abbildung $f^* : \mathfrak{P}(Y) \to \mathfrak{P}(X) : B \mapsto f^*(B)$.

Beispiele: (In bequem-schludriger Schreibweise f^{-1} statt f^*)
Für $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ gilt $f^{-1}(\{2\}) = \{-\sqrt{2}, +\sqrt{2}\}$.
Für $g : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ gilt $g^{-1}(\{2\}) = \{\sqrt[3]{2}\}$.

Die **Faser** über dem Zielpunkt $y \in Y$ ist die Urbildmenge

$$f^*(\{y\}) = \{\, x \in X \mid f(x) = y \,\}.$$

Genau dann ist f injektiv / surjektiv / bijektiv, wenn für jedes $y \in Y$ die Faser $f^*(\{y\})$ höchstens / mindestens / genau ein Element hat.

Vorsicht bei Überladung der Notation

D236
Erläuterung

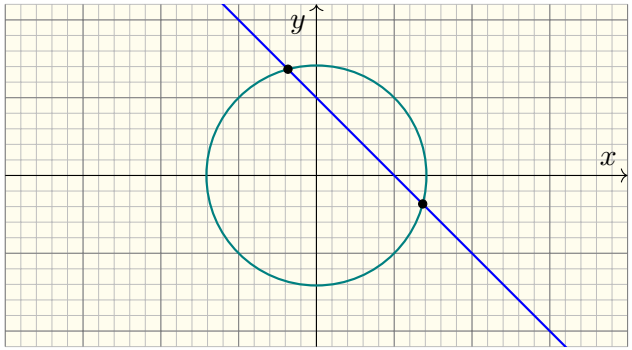
⚠ Zu jeder Abbildung $f : X \to Y$ existiert $f^* : \mathfrak{P}(Y) \to \mathfrak{P}(X)$, doch die Umkehrabbildung $f^{-1} : Y \to X$ existiert dagegen nur, falls f bijektiv ist. Beides sind verschiedene Dinge! Die Schreibweise $f^{-1}(B)$ statt $f^*(B)$ ist schludrig, aber verlockend bequem und daher sehr weit verbreitet. Gerade am Anfang sollten Sie beide gründlich unterscheiden.

Nun mag man einwenden, dass der Kontext jeweils eindeutig erklärt, was gemeint ist. Das ist oft tatsächlich der Fall: Wir können Elemente $y \in Y$ und Teilmengen $B \subseteq Y$ unterscheiden, also können wir auch $f^{-1}(y)$ und $f^{-1}(B) = f^*(B)$ auseinanderhalten. Aus diesem Grund erzeugt dieser **Missbrauch der Notation** (engl. *abuse of notation*) vermutlich selten wirklichen Schaden. Didaktisch klug ist es nicht.

Es gibt noch eine Steigerung: Die Faser über $y \in Y$ wird oft mit $f^{-1}(y)$ bezeichnet. Das kann man nun wirklich nicht von der Umkehrabbildung unterscheiden. Das ist akzeptabel, solange alle Beteiligten wissen, was gemeint ist, zum Beispiel weil weit und breit keine Umkehrabbildungen vorkommen. Achten Sie in der Literatur auf die jeweilige Bedeutung.

Beispiel zu Urbildmengen: Lösung von Gleichungen

Beispiel: Wir wollen $x^2 + y^2 = 2$ und $x + y = 1$ für $(x, y) \in \mathbb{R}^2$ lösen.

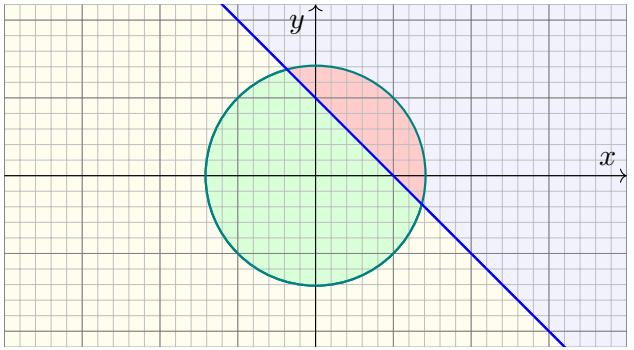


Die erste Gleichung besagt $f(x, y) = a$ mit $f : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto x^2 + y^2$.
Die zweite Gleichung besagt $g(x, y) = b$ mit $g : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto x + y$.
Ihre Lösungsmengen sind jeweils $f^{-1}(\{a\})$ und $g^{-1}(\{b\})$. Wir suchen

$$L = f^{-1}(\{a\}) \cap g^{-1}(\{b\}).$$

Beispiel zu Urbildmengen: Lösung von Ungleichungen

Beispiel: Wir wollen $x^2 + y^2 \leq 2$ und $x + y \geq 1$ für $(x, y) \in \mathbb{R}^2$ lösen.

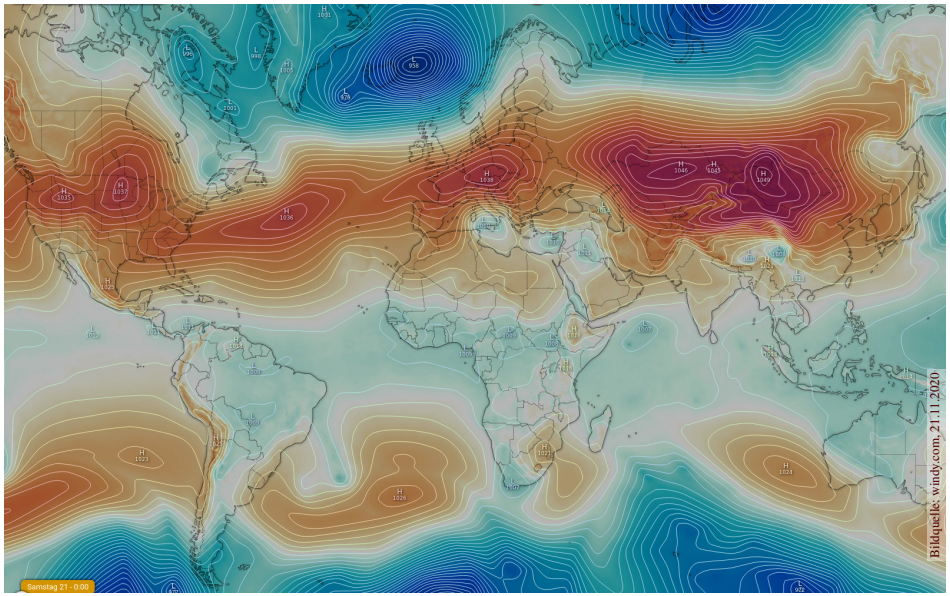


Diese Ungleichungen besagen $f(x, y) \leq a$ und $g(x, y) \geq b$.
Ihre Lösungsmengen sind jeweils $f^{-1}([0, a])$ und $g^{-1}([b, \infty[)$.

$$L = f^{-1}([0, a]) \cap g^{-1}([b, \infty[).$$

Graphische Lösung: Wir schneiden Kreisscheibe und Halbebene.

Beispiel zu Urbildmengen: Isobaren, Tiefdruck, Hochdruck



Luftdruck $f : \mathbb{R}^2 \supseteq U \to \mathbb{R} : (x, y) \mapsto f(x, y)$, Isobaren $f^{-1}(\{c\})$,
Tiefdruckgebiete $f^{-1}(\mathbb{R}_{\leq a})$ und Hochdruckgebiete $f^{-1}(\mathbb{R}_{\geq b})$

Bewegung von Fluiden

Die Bewegung von Fluiden, etwa strömenden Flüssigkeiten oder Gasen, wird beschrieben durch die Navier–Stokes–Gleichungen. Wir können sie hier noch nicht verstehen, aber schon bewundern:

Massenerhaltung:
$$\sum_{k=1}^{n} \frac{\partial v_k}{\partial x_k} = 0$$

Impulserhaltung:
$$\underbrace{\frac{\partial v_i}{\partial t}}_{\text{Änderung}} + \underbrace{\sum_{k=1}^{n} v_k \frac{\partial v_i}{\partial x_k}}_{\text{Konvektion}} = \underbrace{\nu \Delta v_i}_{\text{Diffusion}} - \underbrace{\frac{1}{\varrho} \frac{\partial p}{\partial x_i}}_{\text{intern}} + \underbrace{f_i}_{\text{extern}}$$

Diese $1 + n$ Gleichungen beschreiben die Strömungsgeschwindigkeit $v : I \times \Omega \to \mathbb{R}^n$ einer Flüssigkeit zur Zeit $t \in I \subseteq \mathbb{R}$ am Ort $x \in \Omega \subseteq \mathbb{R}^n$ in der Ebene (n=2) oder im Raum (n=3), mit konstanter Dichte $\varrho \in \mathbb{R}$ und Viskosität $\nu \in \mathbb{R}$, Druck $p : I \times \Omega \to \mathbb{R}$ und äußerer Kraft $f : I \times \Omega \to \mathbb{R}^n$.

Die mathematischen Grundlagen zur Lösbarkeit dieser Gleichungen sind ein weiteres der sieben Millennium-Probleme.

Satz D2D: Ur/Bilder und Mengenoperationen

Sei $f : X \to Y$ eine Abbildung sowie $A, A', A_i \subseteq X$ und $B, B', B_i \subseteq Y$.

$$f^{-1}(B) := \{\, x \in X \mid f(x) \in B \,\}, \qquad f(A) := \{\, f(x) \mid x \in A \,\}$$

Aus dieser Definition ergeben sich folgenden Rechenregeln:

$$\begin{aligned}
f^{-1}\big(\textstyle\bigcap_{i\in I} B_i\big) &= \textstyle\bigcap_{i\in I} f^{-1}(B_i), & f\big(\textstyle\bigcap_{i\in I} A_i\big) &\;\dot\subseteq\; \textstyle\bigcap_{i\in I} f(A_i),\\
f^{-1}\big(\textstyle\bigcup_{i\in I} B_i\big) &= \textstyle\bigcup_{i\in I} f^{-1}(B_i), & f\big(\textstyle\bigcup_{i\in I} A_i\big) &= \textstyle\bigcup_{i\in I} f(A_i),\\
f^{-1}(Y) &= X,\ f^{-1}(\emptyset) = \emptyset, & f(X) &\;\ddot\subseteq\; Y,\ f(\emptyset) = \emptyset,\\
B \subseteq B' &\Rightarrow f^{-1}(B) \subseteq f^{-1}(B'), & A \subseteq A' &\Rightarrow f(A) \subseteq f(A'),\\
f^{-1}(B \setminus B') &= f^{-1}(B) \setminus f^{-1}(B'), & f(A \setminus A') &\;\dot\supseteq\; f(A) \setminus f(A'),\\
f\big(f^{-1}(B)\big) &= B \cap f(X) \;\ddot\subseteq\; B, & f^{-1}\big(f(A)\big) &\;\dot\supseteq\; A.
\end{aligned}$$

Für jede injektive / surjektive Abbildung f gilt statt „$\dot\subseteq$“ / „$\ddot\subseteq$“ stärker „$=$“.

Beweis: Ich führe die ersten beiden Aussagen aus. Hierzu sei $I \neq \emptyset$.

$$\boxed{f^{-1}\big(\textstyle\bigcap_{i\in I} B_i\big) = \textstyle\bigcap_{i\in I} f^{-1}(B_i)}$$

Wir nutzen die Definition von Urbild und Schnittmenge:

$$x \in f^{-1}\big(\textstyle\bigcap_{i\in I} B_i\big) \overset{\text{Def}}{\underset{\text{D235}}{\iff}} f(x) \in \textstyle\bigcap_{i\in I} B_i \overset{\text{Def}}{\underset{\text{D118}}{\iff}} \textstyle\bigwedge_{i\in I} f(x) \in B_i$$

$$\overset{\text{Def}}{\underset{\text{D235}}{\iff}} \textstyle\bigwedge_{i\in I} x \in f^{-1}(B_i) \overset{\text{Def}}{\underset{\text{D118}}{\iff}} x \in \textstyle\bigcap_{i\in I} f^{-1}(B_i)$$

Für die Bildmenge gilt zunächst nur „$\subseteq$“, erst bei Injektivität auch „$\supseteq$“:

$$\boxed{f\big(\textstyle\bigcap_{i\in I} A_i\big) \;\dot\subseteq\; \textstyle\bigcap_{i\in I} f(A_i)}$$

„$\subseteq$“: Sei $y \in f\big(\bigcap_{i\in I} A_i\big)$. Das bedeutet, es gibt $x \in \bigcap_{i\in I} A_i$ mit $f(x) = y$. Für alle $i \in I$ gilt $x \in A_i$, also $y = f(x) \in f(A_i)$, somit $y \in \bigcap_{i\in I} f(A_i)$.

„$\supseteq$“: Sei $y \in \bigcap_{i\in I} f(A_i)$, also $y \in f(A_i)$ für jedes $i \in I$, somit $y = f(x_i)$ für ein $x_i \in A_i$. Da f injektiv ist, haben wir $f^{-1}(\{y\}) = \{x\}$. Für alle $i \in I$ gilt demnach $x = x_i \in A_i$, also $x \in \bigcap_{i\in I} A_i$ und $y = f(x) \in f\big(\bigcap_{i\in I} A_i\big)$.

Ist $f : X \to Y$ nicht injektiv, dann gibt es Familien $(A_i)_{i\in I}$ mit

$$\boxed{f\big(\textstyle\bigcap_{i\in I} A_i\big) \;\subsetneq\; \textstyle\bigcap_{i\in I} f(A_i).}$$

Angenommen zwei Elemente $x_1 \neq x_2$ in X erfüllen $f(x_1) = f(x_2) = y$.
Für $A_1 = \{x_1\}$ und $A_2 = \{x_2\}$ gilt $A_1 \cap A_2 = \emptyset$, also $f(A_1 \cap A_2) = \emptyset$.
Wegen $f(A_1) = f(A_2) = \{y\}$ gilt jedoch $f(A_1) \cap f(A_2) = \{y\} \supsetneq \emptyset$.

Übung: Führen Sie die verbleibenden Fälle aus, nach obigem Vorbild:
(a) Zeigen Sie jede der gültigen Inklusionen in D2D durch einen Beweis.
(b) Belegen Sie jede ungültige Inklusion durch ein Gegenbeispiel.

🙂 Das erfordert sowohl (a) Sorgfalt als auch (b) Kreativität.
Es kostet etwas Zeit, aber diese Mühe ist gut investiert:
So lernen Sie Ur/Bilder und Mengenoperationen!

Warnung: Zu $f : X \to Y$ erfüllen die Abbildungen $f_* : \mathfrak{P}(X) \to \mathfrak{P}(Y)$ und $f^* : \mathfrak{P}(Y) \to \mathfrak{P}(X)$ nur $f_*(f^*(B)) \;\ddot\subseteq\; B$ und $f^*(f_*(A)) \;\dot\supseteq\; A$.
Im Allgemeinen sind f_* und f^* nicht invers zueinander!

Die Lösungsmenge der Gleichung $f(x) = y$ ist die Urbildmenge $f^{-1}(\{y\})$, die Lösungsmenge von $f(x) \in B$ ist entsprechend $f^{-1}(B)$.
In dieser Form treten Urbildmengen überall in der Mathematik und ihren Anwendungen auf. Hier lernen Sie, die Definitionen präzise zu nutzen.

In einigen Gebieten der Mathematik wird besonders hemmungslos mit Mengen und Abbildungen gearbeitet, so wie hier im Satz zu sehen:

- Maß- und Integrationstheorie
- Wahrscheinlichkeitstheorie
- Fraktale Geometrie
- Topologie

Für diese Art von Fragestellung hat sich das „Rechnen mit Mengen“ als die allgemeine und effiziente Arbeitsweise herauskristallisiert.

Ich sage dies hier vor allem zur Ermutigung und als Ausblick.
Solide Grundlagen zahlen sich dort und überall aus!

Vereinigung von Relationen

Gegeben seien Relationen

$$f_1 = (X_1, F_1, Y_1) \quad \text{mit} \quad F_1 \subseteq X_1 \times Y_1,$$
$$f_2 = (X_2, F_2, Y_2) \quad \text{mit} \quad F_2 \subseteq X_2 \times Y_2.$$

Dann definieren wir ihre Vereinigung $f = f_1 \cup f_2$ als die Relation

$$f = (X, F, Y) \quad \text{mit} \quad X = X_1 \cup X_2,\ Y = Y_1 \cup Y_2,\ F = F_1 \cup F_2.$$

Gleiches gilt für jede Familie $f_i = (X_i, F_i, Y_i)$ von Relationen, mit $i \in I$: Wir definieren die **Vereinigungsrelation** $f = \bigcup_{i\in I} f_i$ durch

$$f = (X, F, Y) \quad \text{mit} \quad X = \bigcup_{i\in I} X_i,\ Y = \bigcup_{i\in I} Y_i,\ F = \bigcup_{i\in I} F_i.$$

🙂 Da wir für Relationen nichts weiter als diese Daten verlangen, gelingt diese Konstruktion immer. Meist jedoch wollen wir weitere Eigenschaften erhalten, etwa für Funktionen: sie sind linkstotal und rechtseindeutig. Dazu schauen wir nun genauer hin.

Anwendung: stückweise definierte Funktionen

Oft wollen wir Funktionen stückweise definieren, wie zum Beispiel:

$$f : \mathbb{R} \to \mathbb{R}_{\geq 0} : x \mapsto |x| = \begin{cases} +x & \text{falls } x \geq 0, \\ -x & \text{falls } x \leq 0. \end{cases}$$

Das ist die Vereinigung von zwei Funktionen, nämlich

$$f_1 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto +x,$$
$$f_2 : \mathbb{R}_{\leq 0} \to \mathbb{R}_{\geq 0} : x \mapsto -x.$$

Im vorliegenden Falle ist ihre Vereinigung die Funktion

$$f_1 \cup f_2 = f : \mathbb{R} \to \mathbb{R}_{\geq 0}.$$

Nach Konstruktion ist f linkstotal, denn es gilt $\mathbb{R}_{\geq 0} \cup \mathbb{R}_{\leq 0} = \mathbb{R}$. Zudem ist f rechtseindeutig, dank $f_1(0) = f_2(0)$ auf der Überlappung $\mathbb{R}_{\geq 0} \cap \mathbb{R}_{\leq 0} = \{0\}$. Das ist auch schon alles, was wir prüfen müssen!

🙂 Dahinter steckt das folgende allgemeine Konstruktionsprinzip.

Vereinigung von Funktionen

Satz D2E: Vereinigung von Funktionen

Zu $i \in I$ sei $f_i : X_i \to Y_i$ eine Funktion, gegeben durch $f_i = (X_i, F_i, Y_i)$. Wir können dann die Vereinigungsrelation $f = \bigcup_{i\in I} f_i$ betrachten:

$$f = (X, F, Y) \quad \text{mit} \quad X = \bigcup_{i\in I} X_i,\ Y = \bigcup_{i\in I} Y_i,\ F = \bigcup_{i\in I} F_i$$

Genau dann ist $f = \bigcup_{i\in I} f_i$ eine Funktion, geschrieben $f : X \to Y$, wenn die folgende **Schnittbedingung** erfüllt ist:

Für alle $i, j \in I$ und $x \in X_i \cap X_j$ gilt $f_i(x) = f_j(x)$.

Sind die Startmengen paarweise disjunkt, also $X_i \cap X_j = \emptyset$ für alle $i \neq j$, so schreiben wir dies zur Betonung als disjunkte Summe $f = \bigsqcup_{i\in I} f_i$.

Beweis: Nach Konstruktion ist f linkstotal: Zu jedem $x \in X$ existiert mindestens ein Index $i \in I$ mit $x \in X_i$. Da $f_i : X_i \to Y_i$ eine Funktion ist, existiert genau ein $y \in Y_i$ mit $(x, y) \in F_i$, und somit gilt $(x, y) \in F$. Die Schnittbedingung garantiert, dass f rechtseindeutig ist. QED

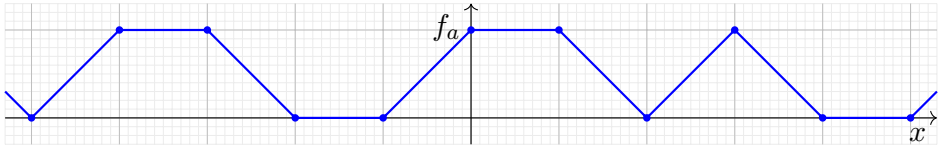
Anwendung: stückweise definierte Funktionen

🙂 Satz D2E erklärt die Konstruktion von stückweise definierten Funktionen; das ist überall sehr bequem und flexibel.

Beispiele: Wir konstruieren so die folgenden Funktionen:

$$f : \mathbb{R} \to \mathbb{R} : x \mapsto \begin{cases} 1 \text{ falls } x \in \mathbb{Q} \\ 0 \text{ falls } x \in \mathbb{R} \setminus \mathbb{Q} \end{cases}, \qquad g : \mathbb{Q} \to \mathbb{Q} : x \mapsto \begin{cases} 0 \text{ für } x^2 > 2 \\ 1 \text{ für } x^2 < 2 \end{cases},$$

$$h : \mathbb{R} \to \mathbb{R} : x \mapsto \begin{cases} 0 \text{ für } x < 0 \\ 1 \text{ für } x \geq 0 \end{cases}, \qquad k : \mathbb{R} \to \mathbb{R} : x \mapsto \begin{cases} \sqrt{x} \text{ für } x \geq 0 \\ -\sqrt{-x} \text{ für } x \leq 0 \end{cases}.$$



Zu jeder Folge $a : \mathbb{Z} \to \{0, 1\}$ sei $f_a : \mathbb{R} \to [0, 1]$ die affine Interpolation mit $f_a(x) = (1 - t)a_k + ta_{k+1}$ für $x = k + t$ mit $k \in \mathbb{Z}$ und $t \in [0, 1]$.

Zusammenfassung: Komposition von Relationen

Die **Menge aller Relationen zwischen X und Y** bezeichnen wir mit

$$\mathrm{Rel}(X,Y) := \{\, f = (X,F,Y) \mid F \subseteq X \times Y \,\}.$$

Für je drei Mengen X, Y, Z haben wir

$$\begin{aligned}
&\mathrm{id}_X \in \mathrm{Rel}(X,X),\\
&{}^{\intercal} : \mathrm{Rel}(X,Y) \to \mathrm{Rel}(Y,X) : f \mapsto f^{\intercal},\\
&\circ : \mathrm{Rel}(Y,Z) \times \mathrm{Rel}(X,Y) \to \mathrm{Rel}(X,Z) : (g,f) \mapsto h = g \circ f,\\
&\bullet : \mathrm{Rel}(X,Y) \times \mathrm{Rel}(Y,Z) \to \mathrm{Rel}(X,Z) : (f,g) \mapsto h = f \bullet g.
\end{aligned}$$

Die Linkskomposition $\circ$ ist üblich, die Rechtskomposition $\bullet$ natürlich.
Die Komposition ist assoziativ, und die passende Identität ist neutral.
Es gilt $\mathrm{id}_X^{\intercal} = \mathrm{id}_X$ sowie $(g \circ f)^{\intercal} = f^{\intercal} \circ g^{\intercal}$ und $(f \bullet g)^{\intercal} = g^{\intercal} \bullet f^{\intercal}$.

Übung: Sind f und g beide links- / rechtseindeutig / links- / rechtstotal / Funktionen / Injektionen / Surjektionen / Bijektionen, so auch $g \circ f = f \bullet g$.

Zusammenfassung: Komposition von Abbildungen

Die **Menge aller Abbildungen von X nach Y** bezeichnen wir mit

$$\begin{aligned}
&\mathrm{Abb}(X,Y) = \mathrm{Fun}(X,Y) = \mathrm{Map}(X,Y) = Y^X = \{\, f : X \to Y \,\}\\
&:= \{\, f = (X,F,Y) \mid F \subseteq X \times Y \text{ linkstotal und rechtseindeutig} \,\}.
\end{aligned}$$

Beispiel: Es gilt $\mathrm{Abb}(\emptyset, Y) = \{(\emptyset, \emptyset, Y)\}$ und $\mathrm{Abb}(X, \emptyset) = \{\}$ für $X \neq \emptyset$.

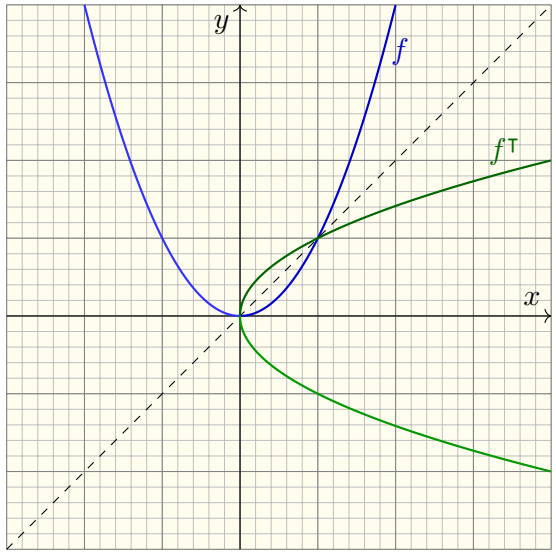
Die (Links/Rechts)Komposition definiert hierauf die Verknüpfungen

$$\begin{aligned}
&\circ : \mathrm{Abb}(Y,Z) \times \mathrm{Abb}(X,Y) \to \mathrm{Abb}(X,Z) : (g,f) \mapsto h = g \circ f,\\
&\bullet : \mathrm{Abb}(X,Y) \times \mathrm{Abb}(Y,Z) \to \mathrm{Abb}(X,Z) : (f,g) \mapsto h = f \bullet g.
\end{aligned}$$

Die Komposition ist assoziativ, und die passende Identität ist neutral.
Gleiches gilt für $\mathrm{Bij}(X,Y),\ \mathrm{Inj}(X,Y),\ \mathrm{Sur}(X,Y) \subseteq \mathrm{Abb}(X,Y)$.

⚠ Ist f eine Funktion, so ist $f^{\intercal}$ im Allgemeinen nur eine Relation.
Genau dann ist auch $f^{\intercal}$ eine Funktion, wenn f bijektiv ist.
In diesem Falle ist $f^{\intercal} = f^{-1}$ die Umkehrfunktion (D3A).

Die Umkehrrelation ist im Allgemeinen keine Funktion!



Hier ist f die Funktion $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$, also $f = (\mathbb{R}, F, \mathbb{R})$ mit $F = \{\, (x, x^2) \mid x \in \mathbb{R} \,\}$.

Die Umkehrrelation $f^{\intercal} = (\mathbb{R}, F^{\intercal}, \mathbb{R})$ mit $F^{\intercal} = \{\, (x^2, x) \mid x \in \mathbb{R} \,\}$ ist keine Funktion:

Sie ist weder linkstotal noch rechtseindeutig!

🙂 Dies gelingt erst durch eine geeinete Einschränkung, etwa auf einen Parabelzweig zu $g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto x^2$ oder $h : \mathbb{R}_{\leq 0} \to \mathbb{R}_{\geq 0} : x \mapsto x^2$.

Die Umkehrrelation ist im Allgemeinen keine Funktion!

Aus der Schule kennen Sie die Merkregel: *Die Umkehrfunktion f^{-1} entsteht aus f durch Spiegelung an der (Haupt-)Diagonalen.*
Für umkehrbare Funktionen stimmt dies tatsächlich!
Das ist der Inhalt des folgenden Satzes D3A.

Sie wissen auch, dass dies nicht immer so einfach funktioniert, hier sehen Sie ein einfaches, aber recht eindrückliches Beispiel: Die ersehnte Spiegelung $f \mapsto f^{\intercal}$ ergibt hier leider keine Funktion, aber immerhin eine Relation. Wir haben das passende Vokabular!

Das ist einer der Gründe, auch allgemein über Relationen zu sprechen: Dieser universelle Rahmen verlangt wenig, und viele grundlegende Konstruktionen gelingen hier immer. Selbst wenn wir vorrangig an Funktionen interessiert sind, so sind Relationen ein gutes Habitat.

Ein weiterer wichtiger Grund ist, dass wir ohnehin Äquivalenzrelationen und Ordnungsrelationen nutzen wollen. Am Relationsbegriff sollten wir also nicht zwanghaft sparen, er ist in jeder Hinsicht hilfreich und nützlich.

Einschränkung von Relationen

D305

Sei $f = (X, F, Y)$ eine Relation sowie $A \subseteq X$ und $B \subseteq Y$ Teilmengen.
Dies definiert die **Einschränkung in Startmenge und Zielmenge**

$$f|_A^B := (A, E, B) \qquad \text{mit} \qquad E := F \cap (A \times B)$$

Diese Einschränkung von $X \times Y$ auf $A \times B$ definiert die Abbildung

$$\mathrm{Rel}(X, Y) \to \mathrm{Rel}(A, B) \;:\; f \mapsto f|_A^B.$$

Zwei Spezialfälle sind die Einschränkung in der Startmenge $f|_A := f|_A^Y$
und entsprechend die Einschränkung in der Zielmenge $f|^B := f|_X^B$.

Zu jeder Teilmenge $A \subseteq X$ definieren wir ihre **Inklusion(sabbildung)**

$$\iota_A = \iota_A^X := (A, \Delta_A, X) \quad \text{also} \quad \iota_A^X \;:\; A \to X \;:\; a \mapsto a.$$

Damit gilt dann $f|_A = \iota_A \bullet f$ und $f|^B = f \bullet \iota_B^\intercal$, also $f|_A^B = \iota_A \bullet f \bullet \iota_B^\intercal$,
gleichbedeutend $f|_A = f \circ \iota_A$ und $f|^B = \iota_B^\intercal \circ f$, also $f|_A^B = \iota_B^\intercal \circ f \circ \iota_A$.

Übung: Schreiben Sie die Kompositionen aus und prüfen Sie es nach.

Einschränkung von Abbildungen

D306

Gegeben sei eine Abbildung $f : X \to Y$ sowie $A \subseteq X$ und $B \subseteq Y$.

$$\begin{array}{ccc} X & \xrightarrow[x \mapsto f(x)]{f} & Y \\ {\scriptstyle \iota_A^X}\uparrow & & \uparrow{\scriptstyle \iota_B^Y} \\ A & \xrightarrow{\quad f|_A^B \quad} & B \end{array}$$

Genau dann ist die Einschränkung $f|_A^B$ eine Funktion, wenn $f(A) \subseteq B$:

$$f|_A^B \;:\; A \to B \;:\; x \mapsto f(x), \qquad \iota_B^Y \circ f|_A^B = f \circ \iota_A^X$$

Wichtige Spezialfälle: Immer gilt $f(A) \subseteq Y$ und manchmal $f(X) \subseteq B$:

$$f|_A = f|_A^Y \;:\; A \to Y \;:\; x \mapsto f(x), \qquad f|_A = f \circ \iota_A^X$$
$$f|^B = f|_X^B \;:\; X \to B \;:\; x \mapsto f(x), \qquad f = \iota_B^Y \circ f|^B$$

Beispiel zur Einschränkung von Abbildungen

D307

Beispiel: Wir betrachten die Funktion

$$f \;:\; \mathbb{R} \to \mathbb{R} \;:\; x \mapsto x^2.$$

Die Zielmenge können wir auf $\mathbb{R}_{\geq 0}$ einschränken:

$$g = f|^{\mathbb{R}_{\geq 0}} \;:\; \mathbb{R} \to \mathbb{R}_{\geq 0} \;:\; x \mapsto x^2$$

Die Zielmenge können wir jedoch nicht auf $[0, 5]$ einschränken:

☹ ~~$f|^{[0,5]} \;:\; \mathbb{R} \to [0, 5] \;:\; x \mapsto x^2$~~ .

Die Relation $f|^{[0,5]}$ ist keine Abbildung mehr! Hingegen gilt

$$f([0, 2]) = [0, 4] \subseteq [0, 5].$$

Daher können wir f einschränken zur Abbildung

☺ $h = f|_{[0,2]}^{[0,5]} \;:\; [0, 2] \to [0, 5] \;:\; x \mapsto x^2.$

Die Einschränkung $f|_{[0,2]}^{[0,4]} : [0, 2] \to [0, 4] : x \mapsto x^2$ ist sogar bijektiv.

Beispiel zur Einschränkung von Verknüpfungen

D308

Beispiel: Wir betrachten die Multiplikation der rationalen Zahlen

$$\mu \;:\; \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \;:\; (x, y) \mapsto x \cdot y.$$

Hier können wir die Zielmenge nicht auf $\mathbb{Z}$ einschränken:

☹ ~~$\mu|^{\mathbb{Z}} \;:\; \mathbb{Q} \times \mathbb{Q} \to \mathbb{Z} \;:\; (x, y) \mapsto x \cdot y$~~

Die Relation $\mu|^{\mathbb{Z}}$ ist keine Abbildung mehr! Hingegen gilt

$$\mu(\mathbb{Z} \times \mathbb{Z}) \subseteq \mathbb{Z}.$$

Daher können wir die Multiplikation μ einschränken zu

☺ $\mu|_{\mathbb{Z}\times\mathbb{Z}}^{\mathbb{Z}} \;:\; \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \;:\; (x, y) \mapsto x \cdot y.$

Diese Einschränkung ist genau die übliche Multiplikation auf $\mathbb{Z}$.
Dasselbe gilt für Addition und Multiplikation auf $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
Das ist das **Fortsetzungsprinzip** beim Aufbau des Zahlensystems:
Die Verknüpfungen werden schrittweise erweitert, wie hier gezeigt.

Illustration zu injektiv, surjektiv, bijektiv

Sei $f : X \to Y : x \mapsto f(x)$ eine Abbildung von X nach Y.
Zu gegebenem $y \in Y$ wollen wir folgende Gleichung lösen:

$$f(x) = y$$

Die Abbildung f ist surjektiv / injektiv / bijektiv, wenn zu jedem $y \in Y$ mindestens / höchstens / genau ein $x \in X$ existiert mit $f(x) = y$.

Beispiel: Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, oder ein Ring, wie $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{H}$.
Jede Matrix $A \in \mathbb{K}^{m \times n}$ definiert die zugehörige Abbildung

$$f : \mathbb{K}^n \to \mathbb{K}^m : x \mapsto f(x) = Ax.$$

Die Abbildung f ist surjektiv / injektiv / bijektiv, wenn zu jedem $y \in \mathbb{K}^m$ mindestens / höchstens / genau ein $x \in \mathbb{K}^n$ existiert mit $Ax = y$.

Illustration zu injektiv, surjektiv, bijektiv

🙂 Das Lösen einer Gleichung $f(x) = y$ ist ein typisches, ja universelles Grundproblem in der Mathematik und ihren zahlreichen Anwendungen.

Die zunächst abstrakten Begriffe surjektiv / injektiv / bijektiv werden daher in jeder Anwendung sogleich konkret und praktisch relevant:

Sie regieren die Existenz und Eindeutigkeit von Lösungen!

🙂 Speziell für lineare Gleichungen der Form $Ax = y$ mit $A \in \mathbb{K}^{m \times n}$ betrachten wir die Abbildung $f : \mathbb{K}^n \to \mathbb{K}^m : x \mapsto f(x) = Ax$.

Zur Lösung kennen Sie eine sehr effiziente Methode aus Kapitel B: Der Gauß–Algorithmus B2C bringt jede Matrix auf Zeilenstufenform!

Daran können wir systematisch *alle* Lösungen von $Ax = y$ ablesen und somit auch die Surjektivität / Injektivität / Bijektivität von f klären.

Illustration: Lösungen linearer Gleichungssysteme

♦ Satz B2D: Invertierbarkeitskriterien für Matrizen

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$; es genügt ein Divisionsring, wie $\mathbb{H}$.
Zur Matrix $A \in \mathbb{K}^{m \times n}$ untersuchen wir $f : \mathbb{K}^n \to \mathbb{K}^m : x \mapsto f(x) = Ax$.
Dazu bringen wir A auf Zeilenstufenform A', mit Rang $r \leq \min\{m, n\}$.

(1) Surjektivität. Die folgenden drei Aussagen sind äquivalent:
(a) Zu jedem $y \in \mathbb{K}^m$ existiert mindestens ein $x \in \mathbb{K}^n$ mit $Ax = y$.
(b) Die Matrix A ist rechtsinvertierbar, $\exists C \in \mathbb{K}^{n \times m} : AC = 1_{m \times m}$.
(c) Es gilt $r = m \leq n$, also Rang gleich Zeilenzahl.

(2) Injektivität. Die folgenden drei Aussagen sind äquivalent:
(a) Zu jedem $y \in \mathbb{K}^m$ existiert höchstens ein $x \in \mathbb{K}^n$ mit $Ax = y$.
(b) Die Matrix A ist linksinvertierbar, $\exists B \in \mathbb{K}^{n \times m} : BA = 1_{n \times n}$.
(c) Es gilt $r = n \leq m$, also Rang gleich Spaltenzahl.

(3) Bijektivität. Die folgenden drei Aussagen sind äquivalent:
(a) Zu jedem $y \in \mathbb{K}^m$ existiert genau ein $x \in \mathbb{K}^n$ mit $Ax = y$.
(b) Die Matrix A ist invertierbar, $\exists B \in \mathbb{K}^{n \times m} : BA = 1_{n \times n}$, $AB = 1_{m \times m}$.
(c) Es gilt $r = m = n$, also A quadratisch mit vollem Rang.

Illustration: Lösungen linearer Gleichungssysteme

🙂 Sie kennen diesen schönen Satz bereits aus Kapitel B:

Er ist sehr elegant und effizient, zudem konkret und praktisch.
Daher wollte ich die ganz handfeste Matrizenrechnung voranstellen, damit Sie einerseits möglichst früh effizient arbeiten können und andererseits gute Vorbilder haben für spätere Entwicklungen.

Sie sehen schöne Parallelen zum allgemeinen Fall von Abbildungen.
Matrizen sind in gewisser Weise sehr konkret und noch übersichtlich,
Abbildungen anfangs ungewohnt und schwindelerregend allgemein.
Ich hoffe, die zahlreichen konkreten Parallelen fördern Ihr Zutrauen.

Auch für Abbildungen klären wir nun die Frage der Invertierbarkeit.
Der obige Satz B2D zur Inversion von Matrizen entspricht dem Satz D3A zur Inversion von Abbildungen, wie nachfolgend erklärt.

Invertierbarkeit von Abbildungen

D313

Vorgelegt seien Abbildungen $f : X \to Y$ und $g, h : Y \to X$.
Wir nutzen im Folgenden die Komposition von links:

$$g \circ f \;:\; X \to X \;:\; x \mapsto g(f(x))$$
$$f \circ h \;:\; Y \to Y \;:\; y \mapsto f(h(y))$$

Wir nennen g **linksinvers** zu f, falls $g \circ f = \mathrm{id}_X$ gilt.
Wir nennen h **rechtsinvers** zu f, falls $f \circ h = \mathrm{id}_Y$ gilt.

Ist g linksinvers zu f und h rechtsinvers zu f, so folgt $g = h$, denn

$$g \overset{\text{rNtr}}{=} g \circ \mathrm{id}_Y \overset{\text{rInv}}{=} g \circ (f \circ h) \overset{\text{Ass}}{=} (g \circ f) \circ h \overset{\text{lInv}}{=} \mathrm{id}_X \circ h \overset{\text{lNtr}}{=} h.$$

Wir nennen g **invers** zu f, falls $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$ gilt.
Damit ist g eindeutig durch f bestimmt, und wir schreiben $f^{-1} := g$.

Die Abbildung f heißt **invertierbar**, falls zu f eine Inverse g existiert.

🙂 Genau dieselben Begriffe kennen wir bereits von Matrizen B125.
Wir benötigen dazu nur Assoziativität und Links-/Rechts-Neutrale.
Dieselbe Rechnung gilt daher auch in jedem Monoid, siehe B1C.

Einseitige Inverse sind nicht immer eindeutig.

D314

Die **Quadratfunktion**

$$f \;:\; \mathbb{R} \to \mathbb{R}_{\geq 0} \;:\; x \mapsto x^2$$

hat mehrere Rechtsinverse h, mit $f \circ h = \mathrm{id}_{\mathbb{R}_{\geq 0}}$, zum Beispiel

$$h_1 \;:\; \mathbb{R}_{\geq 0} \to \mathbb{R} \;:\; x \mapsto +\sqrt{x},$$
$$h_2 \;:\; \mathbb{R}_{\geq 0} \to \mathbb{R} \;:\; x \mapsto -\sqrt{x}.$$

Die **Wurzelfunktion**

$$f \;:\; \mathbb{R}_{\geq 0} \to \mathbb{R} \;:\; x \mapsto \sqrt{x}$$

hat mehrere Linksinverse g, mit $g \circ f = \mathrm{id}_{\mathbb{R}_{\geq 0}}$, zum Beispiel

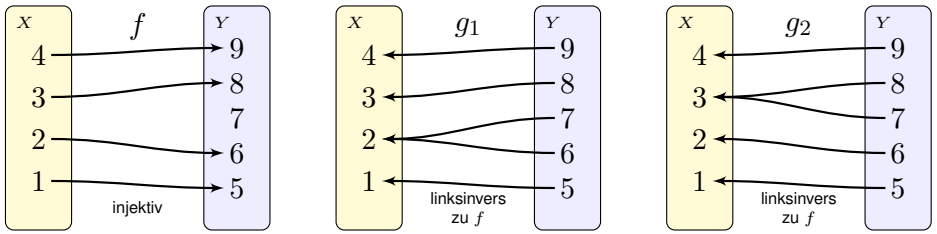
$$g_1 \;:\; \mathbb{R} \to \mathbb{R}_{\geq 0} \;:\; x \mapsto x^2,$$
$$g_2 \;:\; \mathbb{R} \to \mathbb{R}_{\geq 0} \;:\; x \mapsto x \cdot |x|.$$

🙂 Insbesondere kann f in diesen Fällen nicht invertierbar sein:
Wäre f invertierbar, so gäbe es nur genau eine Linksinverse und
nur genau eine Rechtsinverse, nämlich die (eindeutige!) Inverse zu f.

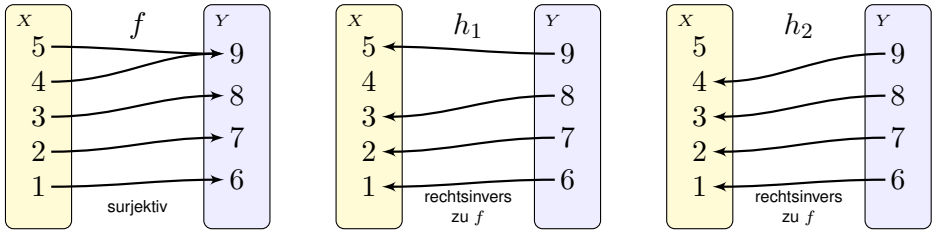
Einseitige Inverse sind nicht immer eindeutig.

D315

Zu $f : X \to Y$ injektiv existiert $g : Y \to X$ mit $g \circ f = \mathrm{id}_X$:



Zu $f : X \to Y$ surjektiv existiert $h : Y \to X$ mit $f \circ h = \mathrm{id}_Y$:



Einseitige Inverse sind nicht immer eindeutig.

D316
Erläuterung

Einseitige Inverse sind im Allgemeinen nicht eindeutig.
Dieses Phänomen kennen Sie bereits von Matrizen (B126).

Die obigen Beispiele illustrieren dies nun für Abbildungen.
In den Bildern erkennen Sie eine allgemeine Konstruktion:

- Jede Surjektion $f : X \twoheadrightarrow Y$ erlaubt (mindestens) eine Rechtsinverse:
  Zu jedem Zielpunkt $y \in Y$ existiert mindestens ein Urbild $x \in X$.
  Im Allgemeinen müssen wir willkürlich wählen, wie skizziert.
- Jede Injektion $f : X \hookrightarrow Y$ erlaubt (mindestens) eine Linksinverse:
  Zu jedem Bildpunkt $y \in \mathrm{im}(f)$ existiert höchstens ein Urbild $x \in X$.
  Im Allgemeinen müssen wir willkürlich ergänzen, wie skizziert.
- Jede Bijektion $f : X \xrightarrow{\sim} Y$ erlaubt eine eindeutige Inverse.
  Zu jedem Zielpunkt $y \in Y$ existiert genau ein Urbild $x \in X$.
  Zu dieser Konstruktion ist keine Wahl nötig oder möglich.

🙂 Der folgende Satz führt diese Beobachtung präzise aus.

Invertierbarkeitskriterien für Abbildungen

D317

Satz D3A: Invertierbarkeitskriterien für Abbildungen

Sei $f : X \to Y$ eine Abbildung.

(1) **Bijektivität**. Die folgenden Aussagen sind äquivalent:
(1a) f ist bijektiv: $\forall y \in Y \;\; \exists! x \in X : f(x) = y$.
(1b) f ist invertierbar: $\exists (g : Y \to X) : g \circ f = \mathrm{id}_X \wedge f \circ g = \mathrm{id}_Y$.
🙂 Die Inverse g zu f ist eindeutig. Wir schreiben $f^{-1} := g$.

(2) **Injektivität**. Mit $X \neq \emptyset$ sind die folgenden Aussagen äquivalent:
(2a) f ist injektiv: $\forall x, x' \in X : f(x) = f(x') \Rightarrow x = x'$
(2b) f ist linksinvertierbar: $\exists (g : Y \to X) : g \circ f = \mathrm{id}_X$.
⚠ Zur Konstruktion „(2a) ⇒ (2b)“ müssen wir $X \neq \emptyset$ voraussetzen.
Linksinverse zu f sind im Allgemeinen nicht eindeutig, siehe oben.

(3) **Surjektivität**. Mit AC sind die folgenden Aussagen äquivalent:
(3a) f ist surjektiv: $\forall y \in Y \;\; \exists x \in X : f(x) = y$.
(3b) f ist rechtsinvertierbar: $\exists (g : Y \to X) : f \circ g = \mathrm{id}_Y$.
⚠ Für „(3a) ⇒ (3b)“ müssen wir aus $X = \bigsqcup_{y \in Y} f^{-1}(\{y\})$ auswählen.
Rechtsinverse zu f sind im Allgemeinen nicht eindeutig, siehe oben.

Bijektiv ⇔ invertierbar

D318

Beweis: (3) f surjektiv ⇔ f rechtsinvertierbar.
„⇐“: Sei $f \circ g = \mathrm{id}_Y$. Zu jedem $y \in Y$ und $x = g(y)$ gilt dann:

$$f(x) = f(g(y)) = (f \circ g)(y) = \mathrm{id}_Y(y) = y$$

(2) f injektiv ⇔ f linksinvertierbar.
„⇐“: Sei $g \circ f = \mathrm{id}_X$. Für alle $x, x' \in X$ gilt dann:

$$f(x) = f(x') \implies g(f(x)) = g(f(x')) \implies x = x'$$

(1) f bijektiv ⇔ f invertierbar.
„⇐“: Dies folgt aus „(2a) ⇐ (2b)“ und „(3a) ⇐ (3b)“.
„⇒“: Ist f bijektiv, so ist $g = f^{\intercal}$ eine Funktion und invers zu f.

$$f = (X, F, Y) \quad \text{mit Graph} \quad F = \{\, (x, f(x)) \mid x \in X \,\}$$
$$g = (Y, G, X) \quad \text{mit Graph} \quad G = \{\, (f(x), x) \mid x \in X \,\}$$

Ausführlich: Wir konstruieren $g : Y \to X$ wie folgt. Zu jedem $y \in Y$ existiert genau ein Urbild $x \in X$, mit $f(x) = y$, und wir setzen $g(y) = x$.
Es gilt dann $f(g(y)) = f(x) = y$ und $g(f(x)) = g(y) = x$.

Injektiv ⇔ linksinvertierbar

D319

(2) f injektiv ⇔ f linksinvertierbar.
„⇒“: Sei $x_0 \in X$; hierzu muss die Menge X nicht-leer sein.
Wir konstruieren $g : Y \to X$ durch Fallunterscheidung:

- Zu jedem $y \in \mathrm{im}(f)$ existiert genau ein Urbild $x \in X$, mit $f(x) = y$. Wir setzen $g(y) = x$.
- Für $y \in Y \setminus \mathrm{im}(f)$ setzen wir $g(y) = x_0$.

Für jedes Element $x \in X$ gilt dann $g(f(x)) = g(y) = x$, also $g \circ f = \mathrm{id}_X$.

⚠ Im Falle $X = \emptyset \neq Y$ gilt $\mathrm{Abb}(\emptyset, Y) = \{(\emptyset, \emptyset, Y)\}$ und $\mathrm{Abb}(Y, \emptyset) = \{\}$.
Hier ist $f = (\emptyset, \emptyset, Y) : X \hookrightarrow Y$ injektiv, aber nicht links-invertierbar:
Es gibt hier keine Abbildung $g : Y \to X$, denn $\mathrm{Abb}(Y, \emptyset) = \{\}$.
Die einzige Relation $g = (Y, \emptyset, \emptyset)$ in $\mathrm{Rel}(Y, \emptyset)$ ist nicht linkstotal.

🙂 Im Sonderfall $X = Y = \emptyset$ ist $f = (\emptyset, \emptyset, \emptyset) : X \xrightarrow{\sim} Y$ eine Bijektion und tatsächlich invertierbar dank $f \circ f = f = \mathrm{id}_\emptyset$. Ist das Haarspalterei?
Wir *können* jetzt genau sein, also *sollten* wir jetzt auch genau sein.

🙂 Manchmal lohnt Nullologie: Nachdenken über die leere Menge.

Surjektiv ⇔ rechtsinvertierbar

D320

(3) f surjektiv ⇔ f rechtsinvertierbar.
„⇒“: Wir konstruieren eine Rechtsinverse $g : Y \to X$ wie folgt.
Zu jedem $y \in Y$ ist die Urbildmenge $f^{-1}(\{y\})$ nicht leer.
Wir wählen ein $x \in f^{-1}(\{y\})$ und setzen $g(y) = x$.
Damit gilt $f(g(y)) = f(x) = y$, also $f \circ g = \mathrm{id}_Y$.

Formale Ausführung: Wir haben die Zerlegung $X = \bigsqcup_{y \in Y} f^{-1}(\{y\})$.
Hierzu existiert eine Repräsentantenmenge R dank Auswahlaxiom.
Damit definieren wir die Abbildung $g : Y \to X$ durch

$$g = (Y, G, X) \quad \text{mit Graph} \quad G = \{\, (f(x), x) \mid x \in R \,\}$$

Diese Relation ist linkstotal und rechtseindeutig, denn zu jedem $y \in Y$ existiert genau ein $x \in R$ mit $x \in f^{-1}(\{y\})$ (Auswahlmenge, D123).
Für jedes Element $y \in Y$ gilt dann $f(g(y)) = f(x) = y$.

🙂 Für diese einfache und grundlegende Konstruktion benötigen wir zum ersten Mal das Auswahlaxiom. Es wird nicht das letzte Mal sein.

Welche Relationen sind invertierbar?

D321
Erläuterung

Aufgabe: Für jede Relation $f = (X, F, Y)$ haben wir $F \bullet F^\intercal \subseteq X \times X$ und $F^\intercal \bullet F \subseteq Y \times Y$. Genauer gelten dabei folgende Äquivalenzen:

$$\begin{aligned} F \bullet F^\intercal \supseteq \Delta_X &\iff f \text{ ist linkstotal} \\ F \bullet F^\intercal \subseteq \Delta_X &\iff f \text{ ist linkseindeutig} \\ F^\intercal \bullet F \supseteq \Delta_Y &\iff f \text{ ist rechtstotal} \\ F^\intercal \bullet F \subseteq \Delta_Y &\iff f \text{ ist rechtseindeutig} \end{aligned}$$

Genau dann gilt $f \bullet f^\intercal = \mathrm{id}_X$ und $f^\intercal \bullet f = \mathrm{id}_Y$, wenn f eine Bijektion ist:

$$\begin{cases} \forall x \in X \ \exists! y \in Y : (x,y) \in F & \text{das heißt } f \text{ ist eine Funktion} \\ \forall y \in Y \ \exists! x \in X : (x,y) \in F & \text{das heißt } f^\intercal \text{ ist eine Funktion} \end{cases}$$

In Worten: Die Relation F zwischen X und Y ordnet jedem $x \in X$ genau ein $y \in Y$ zu und umgekehrt jedem $y \in Y$ genau ein $x \in X$.

Daher heißt F auch **Eins-zu-Eins-Korrespondenz** zwischen X und Y. Diesen älteren Sprachgebrauch finden Sie insbesondere noch in vielen englischsprachigen Büchern und mathematischen Anwendungen.

Welche Relationen sind invertierbar?

D322
Erläuterung

Lösung: Wir setzen direkt die Definition D2B der Komposition ein:
Genau dann gilt $x\,(F \bullet F^\intercal)\,x'$, wenn ein $y \in Y$ existiert mit $x\,F\,y\,F^\intercal\,x'$.

(1) Demnach ist $F \bullet F^\intercal \supseteq \Delta_X$ äquivalent zu: Zu jedem $x \in X$ existiert mindestens ein $y \in Y$ mit $x\,F\,y$. Das bedeutet, F ist linkstotal.

(2) Ebenso ist $F \bullet F^\intercal \subseteq \Delta_X$ äquivalent zu: Zu $x \neq x'$ in X existiert kein $y \in Y$ mit $x\,F\,y$ und $x'\,F\,y$. Das bedeutet, F ist linkseindeutig.

Die letzten beiden Äquivalenzen ergeben sich aus den ersten beiden durch Vertauschen der Rollen. Ich wiederhole sie zur Betonung:

Genau dann gilt $y\,(F^\intercal \bullet F)\,y'$, wenn ein $x \in X$ existiert mit $y\,F^\intercal\,x\,F\,y'$.

(3) Demnach ist $F^\intercal \bullet F \supseteq \Delta_Y$ äquivalent zu: Zu jedem $y \in Y$ existiert mindestens ein $x \in X$ mit $x\,F\,y$. Das bedeutet, F ist rechtstotal.

(4) Ebenso ist $F^\intercal \bullet F \subseteq \Delta_Y$ äquivalent zu: Zu $y \neq y'$ in X existiert kein $x \in X$ mit $x\,F\,y$ und $x\,F\,y$. Das bedeutet, F ist rechtseindeutig.

🙂 Eine Relation f ist also genau dann invertierbar durch $f^\intercal$, wenn f eine Bijektion ist; in diesem Falle ist $f^\intercal = f^{-1}$ die Umkehrfunktion.

Welche Relationen sind invertierbar?

D323
Erläuterung

Aufgabe: Seien $f = (X, F, Y)$ und $g = (Y, G, X)$ Relationen.
Unter welchen Bedingungen gilt $f \bullet g = \mathrm{id}_X$ und $g \bullet f = \mathrm{id}_Y$?
Gilt dies nur, wenn f und g zueinander inverse Bijektionen sind?

Lösung: Wir setzen direkt die Definition D2B der Komposition ein:
Genau dann gilt $x\,(F \bullet G)\,x'$, wenn ein $y \in Y$ existiert mit $x\,F\,y\,G\,x'$.

(1) Sei $F \bullet G \supseteq \Delta_X$: Für jedes $x \in X$ gilt $x\,(F \bullet G)\,x$, das bedeutet:
Es existiert $y \in Y$ mit $x\,F\,y\,G\,x$. Somit ist f linkstotal und g rechtstotal.

(2) Sei $F \bullet G = \Delta_X$: Zu $x \in X$ existiert $y \in Y$ mit $x\,F\,y\,G\,x$.
Aus $x'\,F\,y$ folgt $x'\,(F \bullet G)\,x$, also $x' = x$. Somit ist f linkseindeutig.
Aus $y\,G\,x'$ folgt $x\,(F \bullet G)\,x'$, also $x = x'$. Somit ist g rechtseindeutig.

Wir vertauschen nun die Rollen von f und g. Aus $G \bullet F = \Delta_Y$ folgt:
g ist linkstotal und linkseindeutig, f ist rechtstotal und rechtseindeutig.

Schlussfolgerung: Genau dann gilt $f \bullet g = \mathrm{id}_X$ und $g \bullet f = \mathrm{id}_Y$, wenn $f : X \xrightarrow{\sim} Y$ und $g : Y \xrightarrow{\sim} X$ zueinander inverse Bijektionen sind.

Kurz gesagt: Die invertierbaren Relationen sind genau die Bijektionen.

Projektion einer Relation auf Start und Ziel

D324
Erläuterung

Übung: Sei $f = (X, F, Y)$ eine Relation mit Graph $F \subseteq X \times Y$.
Die Einschränkung der beiden Projektionen definiert die Abbildungen $p_1 : F \to X : (x,y) \mapsto x$ und $p_2 : F \to Y : (x,y) \mapsto y$. Damit erhalten wir:

$$\begin{aligned} p_1 \text{ ist surjektiv} &\iff f \text{ ist linkstotal} \\ p_1 \text{ ist injektiv} &\iff f \text{ ist rechtseindeutig} \\ p_2 \text{ ist surjektiv} &\iff f \text{ ist rechtstotal} \\ p_2 \text{ ist injektiv} &\iff f \text{ ist linkseindeutig} \end{aligned}$$

Genau dann ist f eine Abbildung, wenn die Projektion p_1 bijektiv ist.
In diesem Fall haben wir $p_1^{-1} : X \to F : x \mapsto (x, f(x))$ und $f = p_2 \circ p_1^{-1}$.

🙂 Anhand des Graphen F erklärt dies „graphisch“, ob die Relation f eine Funktion ist: Über jedem Punkt $x \in X$ liegt genau ein Punkt $y \in Y$.

Genau dann ist f eine Bijektion, wenn p_1 und p_2 bijektiv sind.
In diesem Fall gilt $f = p_2 \circ p_1^{-1} : X \to Y$ und $f^{-1} = p_1 \circ p_2^{-1} : Y \to X$.

🙂 Der Graph F vermittelt die Eins-zu-Eins-Übersetzung von X nach Y und zurück, $(F, F^\intercal)$ funktioniert wie ein zweisprachiges Wörterbuch.

Bijektionen und Retrakte als Abbildungspaare

Die suggestive Schreibweise $f : X \hookrightarrow Y$ bzw. $X \twoheadrightarrow Y$ bzw. $X \xrightarrow{\sim} Y$ bedeutet, dass f injektiv / surjektiv / bijektiv ist. Dies dient nur zur Betonung; die Aussage muss jeweils nachgewiesen werden.

Definition D3B: Retrakt und Bijektion als Abbildungspaar

Ein **Retrakt** $(i, r) : X \rightleftarrows Y$, genauer ein **Retraktionspaar**, besteht aus Abbildungen $i : X \to Y$ und $r : Y \to X$ mit $r \circ i = \mathrm{id}_X$. Insbesondere ist r rechtsinvertierbar / surjektiv und i ist linksinvertierbar / injektiv.
(Das jeweilige Gegenstück ist im Allgemeinen nicht eindeutig, wie oben gesehen, daher fassen wir hier beide explizit als ein Paar zusammen.)

Eine **Bijektion** $(f, g) : X \cong Y$, genauer ein **Bijektionspaar**, besteht aus Abbildungen $f : X \to Y$ und $g : Y \to X$ mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$. Das bedeutet, f und g sind zueinander invers, $f^{-1} = g$ und $g^{-1} = f$.
(Es genügt, eine anzugeben, die andere ist dann eindeutig bestimmt. Es ist jedoch oft bequem, das Paar vollständig und explizit anzugeben.)

Existiert eine Bijektion $(f, g) : X \cong Y$, so nennen wir die Mengen X und Y **gleichmächtig** oder **in Bijektion**, abgekürzt $X \cong Y$.

Bijektionen und Retrakte als Abbildungspaare

Beispiele: Folgende Paare sind vertraute Bijektionen bzw. Retrakte:

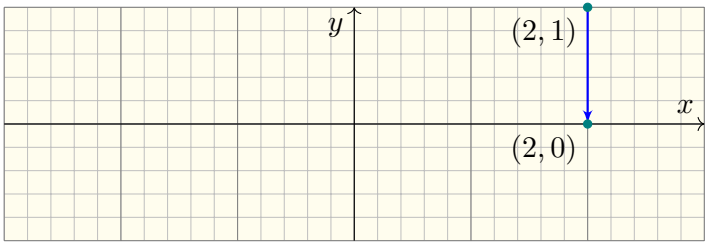
$$(f, g) : \mathbb{R} \rightleftarrows \mathbb{R}_{\geq 0} \quad \text{mit} \quad f(x) = x^2, \quad g(y) = \sqrt{y}$$
$$(h, k) : \mathbb{R}_{\geq 0} \cong \mathbb{R}_{\geq 0} \quad \text{mit} \quad h(x) = x^2, \quad k(y) = \sqrt{y}$$
$$(i, j) : \mathbb{R} \cong \mathbb{R} \quad \text{mit} \quad i(x) = x^3, \quad j(y) = \sqrt[3]{y}$$
$$(\exp, \ln) : \mathbb{R} \cong \mathbb{R}_{>0} \quad \text{dank} \quad \ln(\mathrm{e}^x) = x, \quad \mathrm{e}^{\ln y} = y$$

$$(\mathrm{id}_{\mathbb{R}}, \mathrm{id}_{\mathbb{R}}) : \mathbb{R} \cong \mathbb{R} \quad \text{mit} \quad \mathrm{id}_{\mathbb{R}}(x) = x$$
$$(n, n) : \mathbb{R} \cong \mathbb{R} \quad \text{mit} \quad n(x) = -x$$
$$(i, i) : \mathbb{R}^* \cong \mathbb{R}^* \quad \text{mit} \quad i(x) = x^{-1}$$

$$(\mathsf{T}, \mathsf{T}) : \mathbb{K}^{m \times n} \cong \mathbb{K}^{n \times m} \quad \text{mit} \quad A \leftrightarrow A^{\mathsf{T}}$$
$$(\mathsf{T}, \mathsf{T}) : \mathrm{Rel}(X, Y) \cong \mathrm{Rel}(Y, X) \quad \text{mit} \quad f \leftrightarrow f^{\mathsf{T}}$$

☺ Die Konstruktion eines Paares $(i, r) : X \rightleftarrows Y$ bzw. $(f, g) : X \cong Y$ ist ein elegant-effizienter Beweis der Injektivität / Surjektivität / Bijektivität.

Anwendung: Einbettung und Projektion



Wir können die reelle Gerade $\mathbb{R}$ in die Ebene $\mathbb{R}^2$ einbetten als x–Achse:

$$\iota = \iota_1 : \mathbb{R} \hookrightarrow \mathbb{R}^2 : x \mapsto (x, 0)$$

Wir können jeden Punkt $(x, y) \in \mathbb{R}^2$ auf die x–Achse projizieren:

$$p = \mathrm{pr}_1 : \mathbb{R}^2 \twoheadrightarrow \mathbb{R} : (x, y) \mapsto x$$

Damit gilt $p \circ \iota = \mathrm{id}_{\mathbb{R}}$. Wir erhalten so den Retrakt

$$(\iota, p) : \mathbb{R} \rightleftarrows \mathbb{R}^2.$$

Insbesondere ist ι linksinv'bar / injektiv und p rechtsinv'bar / surjektiv.

Anwendung: Einbettung und Projektion

☺ So gelingt insbesondere die Einbettung $\mathbb{R} \hookrightarrow \mathbb{C} = \mathbb{R}^2 : x \mapsto (x, 0)$.
Die Projektion $\mathrm{pr}_1 = \mathrm{Re}$ ist der Realteil, $\mathrm{pr}_2 = \mathrm{Im}$ ist der Imaginärteil.

☺ Derselbe Trick gelingt für *jedes* kartesische Produkt.
Seien $X_1, \ldots, X_n$ nicht-leer; wir wählen je einen Punkt $a_k \in X_k$.
Wir können X_k in das kartesische Produkt $X = X_1 \times \cdots \times X_n$ einbetten:

$$\iota_k : X_k \hookrightarrow X : x_k \mapsto (a_1, \ldots, a_{k-1}, x_k, a_{k+1}, \ldots, a_n)$$

Wir können jeden Punkt $x \in X$ auf die k–te Koordinate projizieren:

$$p_k = \mathrm{pr}_k : X \twoheadrightarrow X_k : (x_1, \ldots, x_k, \ldots, x_n) \mapsto x_k$$

Damit gilt $p_k \circ \iota_k = \mathrm{id}_{X_k}$. Wir erhalten so den Retrakt

$$(\iota_k, p_k) : X_k \rightleftarrows X.$$

Insbesondere ist ι_k linksinv'bar / injektiv und p_k rechtsinv'bar / surjektiv.

⚠ Ist einer der Faktoren X_k leer, so ist auch das Produkt X leer!

☺ Die Konstruktion eines Paares $(i, r) : X \rightleftarrows Y$ bzw. $(f, g) : X \cong Y$ ist ein eleganter Nachweis der Injektivität / Surjektivität / Bijektivität.

Eine Bijektion zwischen reeller Gerade und offenem Intervall

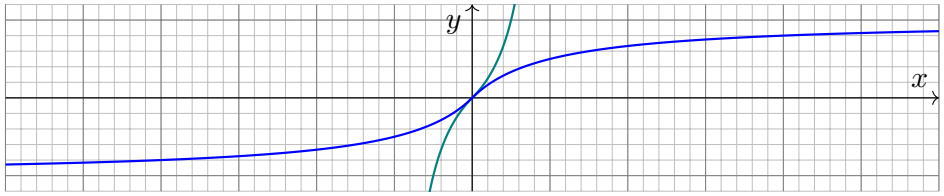
D329

Beispiel D3C: reelle Gerade und offenes Intervall

Es gilt $\mathbb{R} \cong]-1,1[$, genauer $(f,g) : \mathbb{R} \cong]-1,1[$ vermöge

$$f \,:\, \mathbb{R} \to]-1,1[\,:\, x \mapsto x/(1+|x|),$$
$$g \,:\,]-1,1[\to \mathbb{R} \,:\, y \mapsto y/(1-|y|).$$

🙂 Stehen die Abbildungen erst einmal vor uns, so genügt sorgfältiges Nachrechnen! Haben Sie also keine Angst vor expliziten Formeln, sie sind nicht Fluch, sondern Segen. Rechnen reinigt die Seele.



🙂 Unsere beiden Abbildungen f und g sind zudem stetig, sogar stetig differenzierbar. In der Analysis / Topologie ist dies ein schönes Beispiel für einen **Homöomorphismus** bzw. **Diffeomorphismus** $\mathbb{R} \cong]-1,1[$.

Eine Bijektion zwischen reeller Gerade und offenem Intervall

D330

Behauptung: Es gilt $(f,g) : \mathbb{R} \cong]-1,1[$ mit

$$f \,:\, \mathbb{R} \to]-1,1[\,:\, x \mapsto x/(1+|x|),$$
$$g \,:\,]-1,1[\to \mathbb{R} \,:\, y \mapsto y/(1-|y|).$$

Beweis: Nachrechnen!

Ausführlich: Die Abbildungen f und g sind wohldefiniert:

- Für jedes $x \in \mathbb{R}$ gilt $|f(x)| = |x|/(1+|x|) < 1$, also $f(x) \in]-1,1[$.
- Für jedes $y \in]-1,1[$ erfüllt der Nenner die Bedingung $1-|y| \neq 0$.

Zudem sind sie zueinander invers, wie wir geduldig nachrechnen:

$$g(f(x)) = \frac{x/(1+|x|)}{1-\left|x/(1+|x|)\right|} = \frac{x}{1+|x|-|x|} = x, \quad \text{also} \quad g \circ f = \mathrm{id}_{\mathbb{R}}$$

$$f(g(y)) = \frac{y/(1-|y|)}{1+\left|y/(1-|y|)\right|} = \frac{y}{1-|y|+|y|} = y, \quad \text{also} \quad f \circ g = \mathrm{id}_{]-1,1[}$$

Damit haben wir die Behauptung $(f,g) : \mathbb{R} \cong]-1,1[$ bewiesen. QED

Bijektion zwischen Teilmengen und Indikatorfunktionen

D331

Die **Indikatorfunktion** einer Teilmenge $A \subseteq X$ definieren wir durch

$$\mathbf{I}_A = \mathbf{I}_A^X \,:\, X \to \{0,1\} \,:\, x \mapsto \langle\, x \in A \,\rangle = \begin{cases} 1 & \text{falls } x \in A, \\ 0 & \text{falls } x \notin A. \end{cases}$$

Der **Träger** von $f : X \to Y$ bezüglich eines Nullwertes $0 \in Y$ ist

$$\operatorname{supp}(f) := \{\, x \in X \mid f(x) \neq 0 \,\}.$$

Die Bezeichnung supp kommt von engl. *support* und frz. *support*; nicht zu verwechseln mit dem Supremum $\sup M$ in $(X,\leq)$, siehe F1J.

Satz D3D: Bijektion zwischen Teilmengen und Indikatorfunktionen

Wir haben die (übliche, kanonische, natürliche) Bijektion

$$(\mathbf{I}, \operatorname{supp}) \,:\, \mathfrak{P}(X) \;\cong\; \operatorname{Abb}(X,\{0,1\}) \;=\; \{0,1\}^X \;=\; 2^X$$

Beweis: Für jede Teilmenge $A \subseteq X$ gilt $A \mapsto \mathbf{I}_A \mapsto \operatorname{supp}(\mathbf{I}_A) = A$.
Für jede Funktion $f : X \to \{0,1\}$ gilt $f \mapsto \operatorname{supp}(f) \mapsto \mathbf{I}_{\operatorname{supp}(f)} = f$. QED

Präzise Definition und konzise Notation

D332
Erläuterung

🙂 Die Konstruktion eines Paares $(i,r) : X \rightleftarrows Y$ bzw. $(f,g) : X \cong Y$ ist ein eleganter Nachweis der Injektivität / Surjektivität / Bijektivität. Sie sehen dies hier bereits an ersten, noch einfachen Beispielen. Die Erfahrung zeigt, dass diese Sichtweise sehr häufig nützt.

Ich folge weiter einem einfachen, aber erfolgreichen Grundprinzip: Zentrale Ideen verdienen gute Namen und konzise Notation. Daher diskutiere ich hier explizit Retraktspaare $(i,r) : X \rightleftarrows Y$ und Bijektionspaare $(f,g) : X \cong Y$. Es unterstützt Ihre Arbeit.

🙂 Klarheit der Sprache und des Denkens: Wir erschaffen hier eine geeignete Sprache, mit der wir auch komplizierte Sachverhalte klar, kurz und präzise formulieren können. Was wir klar benennen können, das können wir gut begreifen, klar denken und klar kommunizieren.

🙂 Es mag Ihnen zunächst etwas mühsam, gar pedantisch erscheinen, doch präzise Definitionen und konzise Notation erleichtern Ihre Arbeit, zunächst das Lesen und Schreiben, dann das Sprechen und Denken. Das erfordert anfangs eine große Investition, aber es zahlt sich aus!

Kartesische Produkte: allgemeine Konstruktion

Gegeben seien Mengen I und Ω. Eine Abbildung $x : I \to \Omega$ ordnet jedem Startelement $i \in I$ ein Bildelement $x_i = x(i)$ zu. Wir schreiben

$$\mathrm{Abb}(I,\Omega) = \{\, x : I \to \Omega : x \mapsto x_i \,\} = \Omega^I =: \prod_{i\in I} \Omega.$$

Eine Familie $x = (x_i)_{i\in I}$ von Elementen $x_i \in \Omega$ indiziert durch $i \in I$ ist eine Abbildung $I \to \Omega : i \mapsto x_i$. Ebenso ist eine Familie $(X_i)_{i\in I}$ von Teilmengen $X_i \subseteq \Omega$ eine Abbildung $I \to \mathfrak{P}(\Omega) : i \mapsto X_i$.

Definition D3E: kartesisches Produkt, allgemein

Gegeben sei eine Familie $(X_i)_{i\in I}$ von Mengen X_i.
Wir definieren ihr **kartesisches Produkt** durch

$$\begin{aligned} X = \prod_{i\in I} X_i &:= \{\, x = (x_i)_{i\in I} \mid \forall i \in I : x_i \in X_i \,\} \\ &= \{\, x : I \to \textstyle\bigcup_{i\in I} X_i : i \mapsto x_i \mid \forall i \in I : x_i \in X_i \,\}. \end{aligned}$$

Hierzu gehören die **kanonischen Projektionen**

$$p_i = \mathrm{pr}_i \;:\; X \to X_i \;:\; x \mapsto x_i.$$

Kartesische Produkte: allgemeine Konstruktion

Beispiel: Speziell für $I = \{1,\dots,n\}$ erhalten wir wie auf Seite D138:

$$\prod_{i\in I} X_i \cong X_1 \times X_2 \times \cdots \times X_n \;:\; x \rightleftarrows (x_1, x_2, \dots, x_n)$$

Meist schreiben wir kurz $x = (x_1, x_2, \dots, x_n)$: Das Element $x \in \prod_{i\in I} X_i$ wird definiert durch seine Koordinaten $x_1, x_2, \dots, x_n$ mit $x_i \in X_i$.

🙂 Die Definition D3E ist bereits im endlichen Fall vorteilhaft, da sie die Mehrdeutigkeit der möglichen Klammerungen umgeht.

Beispiel: Das Produkt $\prod_{n\in\mathbb{N}} \mathbb{R} = \mathbb{R}^{\mathbb{N}} = \{\, f : \mathbb{N} \to \mathbb{R} : n \mapsto f_n \,\}$ besteht aus allen Folgen $f = (f_0, f_1, f_2, \dots)$ mit $f_0, f_1, f_2, \dots \in \mathbb{R}$.

Das Produkt $\prod_{n\in\mathbb{N}} [0,n] = \{\, f : \mathbb{N} \to \mathbb{R} \mid \forall n \in \mathbb{N} : f_n \in [0,n] \,\}$ enthält die Folgen $f = (f_0, f_1, f_2, \dots)$ mit $f_n \in [0,n]$ für jedes $n \in \mathbb{N}$.

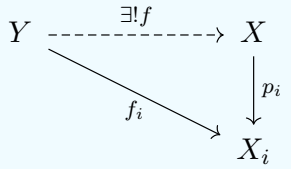
Beispiel: Das Produkt $\prod_{x\in\mathbb{R}} \mathbb{R} = \mathbb{R}^{\mathbb{R}} = \{\, f : \mathbb{R} \to \mathbb{R} : x \mapsto f(x) \,\}$ besteht aus allen Funktionen $f : \mathbb{R} \to \mathbb{R}$, ohne Einschränkung

Das Produkt $\prod_{x\in\mathbb{R}} [-x^2, x^2] = \{\, f : \mathbb{R} \to \mathbb{R} \mid \forall x \in \mathbb{R} : f(x) \in [-x^2, x^2] \,\}$ enthält die Funktionen $f : \mathbb{R} \to \mathbb{R}$ mit $|f(x)| \le x^2$ für jedes $x \in \mathbb{R}$.

Kartesische Produkte: universelle Eigenschaft

Satz D3F: universelle Abbildungseigenschaft (UAE)

Sei $X = \prod_{i\in I} X_i$ das kartesische Produkt der Mengenfamilie $(X_i)_{i\in I}$.



Zu jeder Familie $(f_i : Y \to X_i)_{i\in I}$ von Abbildungen existiert genau eine Abbildung $f : Y \to X$ mit $p_i \circ f = f_i$ für alle $i \in I$, also $f(y) = (f_i(y))_{i\in I}$.

Wir haben somit die kanonische Bijektion

$$\Phi \;:\; \mathrm{Abb}\Big(Y, \prod_{i\in I} X_i\Big) \xrightarrow{\sim} \prod_{i\in I} \mathrm{Abb}(Y, X_i) \;:\; f \mapsto (p_i \circ f)_{i\in I}.$$

Wir schreiben $f = \prod_{i\in I} f_i := \Phi^{-1}((f_i)_{i\in I})$, kurz $f = (f_i : Y \to X_i)_{i\in I}$: Die Funktion f besteht aus ihren Koordinatenfunktionen f_i für $i \in I$.

Beweis: Dies folgt aus der Definition D3E des Produkts. QED

Kartesische Produkte: universelle Eigenschaft

Beispiel: Die Funktion $f : \mathbb{R} \to \mathbb{R}^3 : x \mapsto (x^2, x^4, x^6)$ ist durch ihre drei Koordinatenfunktionen gegeben: $f_1(x) = x^2$, $f_2(x) = x^4$ und $f_3(x) = x^6$. Dies ist jeweils die Projektion von f auf die $i$te Koordinate, $f_i = p_i \circ f$.

Umgekehrt definieren je drei Funktionen $f_1, f_2, f_3 : \mathbb{R} \to \mathbb{R}$ eindeutig die Funktion $f = (f_1, f_2, f_3) : \mathbb{R} \to \mathbb{R}^3$ mit $f(x) = (f_1(x), f_2(x), f_3(x))$. Das ist die universelle Abbildungseigenschaft I2O des Produkts.

🙂 Das kartesische Produkt $X = \prod_{i\in I} X_i$ nutzen wir immer dann, wenn wir unabhängige Koordinaten X_i zusammenfassen wollen.

Genau dies drückt die universelle Abbildungseigenschaft I2O aus. Sie sieht zuerst kompliziert aus, ist aber recht besehen ganz natürlich:

Jede Funktion in ein Produkt wird koordinatenweise festgelegt.

Disjunkte Summen: allgemeine Konstruktion

Gegeben sei eine Familie $(X_i)_{i\in I}$ von Mengen X_i (Teilmengen von Ω). Sie sind **paarweise disjunkt**, wenn $X_i \cap X_j = \emptyset$ für alle $i \neq j$ in I gilt. In diesem Falle haben wir die **(interne) disjunkte Vereinigung**

$$\bigsqcup_{i\in I} X_i := \bigcup_{i\in I} X_i \quad \text{wobei } X_i \cap X_j = \emptyset \text{ für } i \neq j.$$

Falls die Mengen X_i nicht disjunkt sind, können wir sie disjunkt machen: Anschaulich ersetzen wir die Menge X_i durch die Kopie $X_i' = \{i\} \times X_i$; zwischen beiden übersetzen wir durch die Bijektion $\mathrm{pr}_2 : X_i' \xrightarrow{\sim} X_i$.

Definition D3G: disjunkte Summe, kurz Summe

Gegeben sei eine Familie $(X_i)_{i\in I}$ von Mengen X_i. Wir definieren ihre **(disjunkte) Summe** oder **(externe) disjunkte Vereinigung** durch

$$X = \coprod_{i\in I} X_i := \bigcup_{i\in I} \{i\} \times X_i.$$

Der Index $i \in I$ trennt die disjunkten Mengen $X_i' = \{i\} \times X_i$ in X.
Hierzu gehören die **kanonischen Injektionen** $\iota_i : X_i \hookrightarrow X : x \mapsto (i, x)$.

Disjunkte Summen: allgemeine Konstruktion

Beispiel: Falls die gegebene Familie $(X_i)_{i\in I}$ bereits disjunkt ist, so gilt

$$(\mathrm{pr}_2, \sigma) : \coprod_{i\in I} X_i = \bigcup_{i\in I} \{i\} \times X_i \cong \bigcup_{i\in I} X_i = \bigsqcup_{i\in I} X_i$$

durch die Projektion $\mathrm{pr}_2 : (i, x) \mapsto x$ (vergiss den Index i) und umgekehrt $\sigma : x \mapsto (i, x)$ für $i \in I$ mit $x \in X_i$ (suche den Index i): Jedes Element $x \in \bigcup_{i\in I} X_i$ liegt in genau einer der Mengen X_i. Der Index i ist in diesem Falle eine redundante Information.

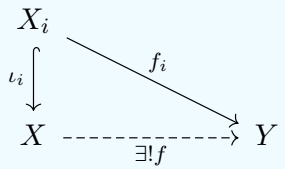
Beispiel: Die Menge $X = \mathbb{R} \amalg \mathbb{R} = (\{1\} \times \mathbb{R}) \cup (\{2\} \times \mathbb{R})$ besteht aus zwei disjunkt gemachten Kopien der reellen Zahlengeraden $\mathbb{R}$.

Wir können uns dies als Teilmenge $X \subseteq \mathbb{R}^2$ der Ebene $\mathbb{R}^2$ vorstellen als die achsenparallele Geraden $X_1' = \{1\} \times \mathbb{R}$ und $X_2' = \{2\} \times \mathbb{R}$.

Disjunkte Summen: universelle Eigenschaft

Satz D3H: universelle Abbildungseigenschaft (UAE)

Sei $X = \coprod_{i\in I} X_i$ die disjunkte Summe der Mengenfamilie $(X_i)_{i\in I}$.



Zu jeder Familie $(f_i : X_i \to Y)_{i\in I}$ von Abbildungen existiert genau eine Abbildung $f : X \to Y$ mit $f \circ \iota_i = f_i$ für alle $i \in I$, also $f(i, x_i) = f_i(x_i)$.

Wir haben somit die kanonische Bijektion

$$\Phi : \mathrm{Abb}\Big(\coprod_{i\in I} X_i, Y\Big) \to \prod_{i\in I} \mathrm{Abb}(X_i, Y) : f \mapsto (f \circ \iota_i)_{\lambda\in I}.$$

Wir schreiben $f = \coprod_{i\in I} f_i := \Phi^{-1}((f_i)_{i\in I})$, alternativ $f = \bigsqcup_{i\in I} f_i'$ als Vereinigung von $f_i' : \{i\} \times X_i \to Y : (i, x_i) \mapsto f_i(x_i)$ wie in Satz D2E.

Beweis: Dies folgt aus der Definition D3G der Summe. QED

Disjunkte Summen: universelle Eigenschaft

Beispiel: Die Menge $X = \mathbb{R} \amalg \mathbb{R} = (\{1\} \times \mathbb{R}) \cup (\{2\} \times \mathbb{R})$ besteht aus zwei disjunkt gemachten Kopien der reellen Zahlengeraden $\mathbb{R}$.

Zu $f_1 : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ und $f_2 : \mathbb{R} \to \mathbb{R} : x \mapsto x^4$ ist demnach die Funktion $f = f_1 \amalg f_2 : \mathbb{R} \amalg \mathbb{R} \to \mathbb{R}$ gegeben durch $f(1, x) = x^2$ und $f(2, x) = x^4$.

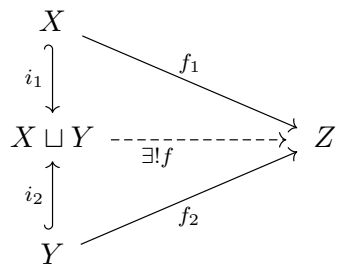
🙂 Die disjunkte Summe $X = \coprod_{i\in I} X_i$ nutzen wir immer dann, wenn wir garantieren wollen, dass die Mengen X_i disjunkt sind.

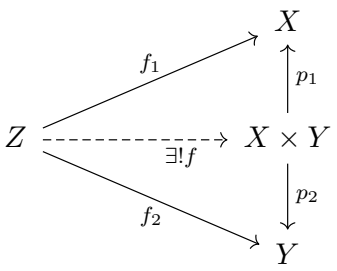
Falls dies bereits der Fall ist, so können wir statt X auch direkt die übliche disjunkte Vereinigung $X \cong \bigsqcup_{i\in I} X_i$ nutzen, wie zuvor

Andernfalls ersetzen wir die Menge X_i durch die Kopie $X_i' = \{i\} \times X_i$ und betrachten die disjunkt gemachte Vereinigung $X = \bigsqcup_{i\in I} X_i'$.

Summen und Produkte von Mengen

D341
Ergänzung





Die universelle Abbildungseigenschaft von Summe und Produkt lautet:

$$\mathscr{C}(X \sqcup Y, Z) \xrightarrow{\sim} \mathscr{C}(X, Z) \times \mathscr{C}(Y, Z) \,:\, f \mapsto (\, f \circ i_1,\ f \circ i_2\,)$$
$$\mathscr{C}(Z, X \times Y) \xrightarrow{\sim} \mathscr{C}(Z, X) \times \mathscr{C}(Z, Y) \,:\, f \mapsto (\, p_1 \circ f,\ p_2 \circ f\,)$$

Die Schreibweise $B^A := \mathscr{C}(A, B)$ und $X + Y := X \sqcup Y$ ist suggestiv:

$$Z^{(X+Y)} \cong Z^X \times Z^Y \quad \text{und} \quad (X \times Y)^Z \cong X^Z \times Y^Z$$

🙂 Das erinnert an die vertrauten Exponentialgesetze für Zahlen.

Summen und Produkte von Mengen

D342
Ergänzung

Die Rechenregeln für Mengen sind wunderbar konkret und praktisch:

$$X \sqcup \emptyset = X = \emptyset \sqcup X, \qquad X \cup \emptyset = X = \emptyset \cup X,$$
$$X \sqcup Y = Y \sqcup X, \qquad X \cup Y = Y \cup X,$$
$$(X \sqcup Y) \sqcup Z = X \sqcup (Y \sqcup Z), \qquad (X \cup Y) \cup Z = X \cup (Y \cup Z).$$

Das kartesische Produkt ist distributiv über die (disjunkte) Vereinigung:

$$X \times (Y \sqcup Z) = (X \times Y) \sqcup (X \times Z) \qquad \text{ebenso für } \cup \text{ und } \cap$$
$$(X \sqcup Y) \times Z = (X \times Z) \sqcup (Y \times Z) \qquad \text{ebenso für } \cup \text{ und } \cap$$

Für die Summe gelten entsprechend kanonische Bijektionen:

$$X \times (Y \amalg Z) \cong (X \times Y) \amalg (X \times Z), \quad (x,(1,y)) \leftrightarrow (1,(x,y)),\ (x,(2,z)) \leftrightarrow (2,(x,z)),$$
$$(X \amalg Y) \times Z = (X \times Z) \amalg (Y \times Z), \quad ((1,x),z) \leftrightarrow (1,(x,z)),\ ((2,y),z)) \leftrightarrow (2,(y,z)).$$

🙂 Hier muss lediglich über die Indizes buchgeführt werden.

Summen und Produkte von Mengen

D343
Ergänzung

Für kartesische Produkte haben wir folgende kanonische Bijektionen:

$$X \times \{a\} \cong X \cong \{a\} \times X, \qquad (x,a) \leftrightarrow x \leftrightarrow (a,x)$$
$$X \times Y \cong Y \times X, \qquad (x,y) \leftrightarrow (y,x)$$
$$(X \times Y) \times Z \cong X \times (Y \times Z), \quad ((x,y),z) \leftrightarrow (x,(y,z))$$

Schließlich gelten die vertrauten Potenzgesetze:

$$Z^{(X \sqcup Y)} \cong Z^X \times Z^Y, \quad f \mapsto (\, f|_X,\ f|_Y\,)$$
$$(X \times Y)^Z \cong X^Z \times Y^Z, \quad f \mapsto (\, \mathrm{pr}_1 \circ f,\ \mathrm{pr}_2 \circ f\,)$$
$$(X^Y)^Z \cong X^{Y \times Z}, \qquad f \mapsto g,\ \ g(y,z) = f(z)(y)$$

Die erste Bijektion entsteht aus Einschränkung $f \mapsto (f|_X, f|_Y)$
und umgekehrt Vereinigung $(g,h) \mapsto f = g \sqcup h$ wie in Satz D2E.

Die zweite Bijektion entsteht aus Projektion $f \mapsto (\mathrm{pr}_1 \circ f, \mathrm{pr}_2 \circ f)$
und umgekehrt $(g,h) \mapsto f$ mit $f : Z \to X \times Y : f(x) = (g(x), h(x))$.

🙂 Das entspricht der universellen Abbildungseigenschaft (I2Q, I2O).

Summen und Produkte von Mengen

D344
Ergänzung

Für jede Bijektion $\varphi : \Lambda \xrightarrow{\sim} \Lambda$ gilt das allgemeine Kommutativgesetz:

$$\coprod_{\lambda \in \Lambda} X_\lambda \cong \coprod_{\lambda \in \Lambda} X_{\varphi(\lambda)} \,:\quad (\varphi(\lambda), x) \leftrightarrow (\lambda, x)$$
$$\prod_{\lambda \in \Lambda} X_\lambda \cong \prod_{\lambda \in \Lambda} X_{\varphi(\lambda)} \,:\quad (x_\lambda)_{\lambda \in \Lambda} \leftrightarrow (x_{\varphi(\lambda)})_{\lambda \in \Lambda}$$

Für jede Summe $\Lambda = \coprod_{i \in I} \Lambda_i$ gilt das allgemeine Assoziativgesetz:

$$\coprod_{\lambda \in \Lambda} X_\lambda \cong \coprod_{i \in I} \Big(\coprod_{\lambda \in \Lambda_i} X_\lambda \Big) \,:\quad ((i,\lambda), x) \leftrightarrow (i, (\lambda, x))$$
$$\prod_{\lambda \in \Lambda} X_\lambda \cong \prod_{i \in I} \Big(\prod_{\lambda \in \Lambda_i} X_\lambda \Big) \,:\quad (x_\lambda)_{\lambda \in \Lambda} \leftrightarrow ((x_\lambda)_{\lambda \in \Lambda_i})_{i \in I}$$

Für jedes Produkt $\Lambda = \prod_{i \in I} \Lambda_i$ gilt das allgemeine Distributivgesetz:

$$\prod_{i \in I} \Big(\coprod_{\lambda_i \in \Lambda_i} X_{\lambda_i} \Big) \cong \coprod_{\lambda \in \Lambda} \Big(\prod_{i \in I} X_{\lambda_i} \Big) \,:\quad (\lambda_i, x_{\lambda_i})_{i \in I} \leftrightarrow ((\lambda_i)_{i \in I}, (x_{\lambda_i})_{i \in I})$$

🙂 Auch hier muss lediglich über die Indizes buchgeführt werden.

Kapitel E

Kombinatorik und Quotienten

Wer hohe Türme bauen will,
muss lange beim Fundament verweilen.

Anton Bruckner (1824–1896)

Inhalt dieses Kapitels E

Kombinatorik und Quotienten

Im vorigen Kapitel D haben wir die Grundlagen erarbeitet für Mengen und Abbildungen, speziell Injektionen, Surjektionen und Bijektionen. Dies wollen wir nun für endliche Mengen $X, Y, \dots$ konkretisieren. Hier gelten besonders starke und nützliche Gesetzmäßigkeiten.

Für Selbstabbildungen $f : X \to X$ führen wir die Listennotation ein. Selbstbijektionen $\sigma : X \xrightarrow{\sim} X$ heißen Permutationen, und hierfür haben wir die sehr effiziente Zykelschreibweise. Permutationen sind überall nützlich, und die konzise Notation hilft in all unseren Rechnungen.

Wir untersuchen damit Abbildungen $f : \{1, \dots, n\} \to \{1, \dots, m\}$. Wir sortieren zur Stufenform (E1E) analog zum Gauß–Algorithmus für Matrizen (B2C). Damit klären wir die Frage der Sur/In/Bijektivität von f durch drei einfache Kennzahlen: n, m und $r = \sharp\,\mathrm{im}(f)$, siehe Satz E1F.

Dieses sorgfältige Vorgehen mag zunächst pedantisch erscheinen, doch der kleinschrittige und umsichtige Aufbau ist eine gute Übung, um mit Sur/In/Bijektionen vertraut zu werden. Als Lohn erhalten wir die Invarianz der Elementezahl E1H und Dirichlets Schubfachprinzip E1I.

Kombinatorik und Quotienten

Der zweite Teil dieses Kapitels behandelt klassische Abzählformeln: (disjunkte) Vereinigungen, kartesisches Produkte und Potenzen, Abbildungsmengen und Potenzmengen. Hier betone ich die expliziten Bijektionspaare: Dies sind schöne Formeln und konkrete Übungen.

Anschließend behandeln wir Binomialkoeffizienten und Teilmengen sowie Zerlegungen und Stirling–Zahlen. Damit können wir die Anzahl $\sharp\,\mathrm{Inj}(X, Y)$ der Injektionen und $\sharp\,\mathrm{Sur}(Y, X)$ der Surjektionen berechnen (Satz E2L). Auch dies ist mathematisch-didaktisch äußerst lehrreich.

Im dritten Teil kommen wir zu Quotienten und Äquivalenzrelationen. Das gilt gemeinhin als abstrakt und schwierig, doch Quotienten sind nichts anderes als Zerlegungen und somit ganz konkret! Hier zahlt sich unsere sorgsame Vorarbeit aus, sie stiftet konkretes Material zur Anschauung und mildert die begrifflichen Schwierigkeiten.

Wir gehen den langen Weg, doch ich bin überzeugt: Er lohnt sich!

Je comprends vite quand on me l'explique lentement.
[Ich verstehe schnell, wenn man es mir langsam erklärt.]

Selbstabbildungen einer Menge X

E101

Wir betrachten eine Menge X und ihre **Selbstabbildungen**:

$$\mathrm{E}_X = \mathrm{End}(X) := \mathrm{Abb}(X,X) = \{\, f : X \to X \,\}$$

Dabei steht End für *Endomorphismus*, hier heißt das *Selbstabbildung*.
Die Komposition definiert das Monoid $(\mathrm{E}_X, \bullet, \mathrm{id}_X)$ bzw. $(\mathrm{E}_X, \circ, \mathrm{id}_X)$.

Am einfachsten ist der Fall einer endlichen Menge $X = \{x_1, x_2, \ldots, x_n\}$:

$$f = \begin{bmatrix} x_1 & x_2 & \ldots & x_n \\ y_1 & y_2 & \ldots & y_n \end{bmatrix} \quad \text{bedeutet} \quad f : X \to X : x_k \mapsto y_k.$$

Bei fester Reihenfolge $(x_1, x_2, \ldots, x_n)$ schreiben wir $f = [y_1, y_2, \ldots, y_n]$.
Wenn wir die freie Wahl haben, denken wir speziell an $X = \{1, 2, \ldots, n\}$.

Die Komposition auf E_X schreiben wir wahlweise rechts oder links:

$$g_1 = \begin{bmatrix} 1&2&3&4 \\ 2&2&3&4 \end{bmatrix} \bullet \begin{bmatrix} 1&2&3&4 \\ 1&3&2&4 \end{bmatrix} = \begin{bmatrix} 1&2&3&4 \\ 3&3&2&4 \end{bmatrix}$$

$$g_2 = \begin{bmatrix} 1&2&3&4 \\ 2&2&3&4 \end{bmatrix} \circ \begin{bmatrix} 1&2&3&4 \\ 1&3&2&4 \end{bmatrix} = \begin{bmatrix} 1&2&3&4 \\ 2&3&2&4 \end{bmatrix}$$

Selbstabbildungen einer Menge X

E102

Wir können jede Abbildung $f : X \to X$ als Wertetabelle / Liste angeben:

$$f_1 = \begin{bmatrix} 1&2&3&4 \\ 2&2&3&4 \end{bmatrix}, \qquad f_2 = \begin{bmatrix} 1&2&3&4 \\ 1&3&2&4 \end{bmatrix}$$

Aufgabe: Wie erkennt man daran, ob $f : X \to X$ eine Bijektion ist?
Lösung: In der Zielzeile tritt jedes Element $x \in X$ genau einmal auf!

Aufgabe: Wie bestimmt man im bijektiven Falle die Inverse f^{-1}?
Lösung: Wir tauschen Startzeile und Zielzeile (und sortieren):

$$f = \begin{bmatrix} 1&2&3&4 \\ 2&3&1&4 \end{bmatrix} \implies f^{-1} = \begin{bmatrix} 2&3&1&4 \\ 1&2&3&4 \end{bmatrix} = \begin{bmatrix} 1&2&3&4 \\ 3&1&2&4 \end{bmatrix}$$

Aufgabe: Ist die Abbildung $f : \mathbb{Z}_7 \to \mathbb{Z}_7 : x \mapsto x^5$ eine Permutation?
Lösung: Wir rechnen die Wertetabelle sorgsam aus:

$$f = \begin{bmatrix} 0&1&2&3&4&5&6 \\ 0&1&4&5&2&3&6 \end{bmatrix} \implies f^{-1} = \begin{bmatrix} 0&1&2&3&4&5&6 \\ 0&1&4&5&2&3&6 \end{bmatrix}$$

Permutationen und die symmetrische Gruppe

E103

Definition E1A: die symmetrische Gruppe S_X

Eine **Permutation** der Menge X ist eine Selbstbijektion $\sigma : X \xrightarrow{\sim} X$.
Die Menge aller Permutationen der Menge X bezeichnen wir mit

$$\mathrm{S}_X = \mathrm{Sym}(X) = \mathrm{Aut}(X) := \mathrm{End}(X)^\times = \mathrm{Bij}(X,X) = \{\, \sigma : X \xrightarrow{\sim} X \,\}.$$

Dabei steht Aut für *Automorphismus*, hier heißt das *Selbstbijektion*.
Die Komposition definiert die Gruppe $(\mathrm{S}_X, \bullet, \mathrm{id}_X)$ bzw. $(\mathrm{S}_X, \circ, \mathrm{id}_X)$.
Wir nennen dies die **symmetrische Gruppe** S_X mit Komposition von rechts bzw. links. Speziell für $X = \{1, 2, \ldots, n\}$ schreiben wir kurz S_n.

Die Komposition auf S_X schreiben wir wahlweise rechts oder links:

$$\pi_1 = \begin{bmatrix} 1&2&3&4 \\ 2&3&1&4 \end{bmatrix} \bullet \begin{bmatrix} 1&2&3&4 \\ 1&2&4&3 \end{bmatrix} = \begin{bmatrix} 1&2&3&4 \\ 2&4&1&3 \end{bmatrix}$$

$$\pi_2 = \begin{bmatrix} 1&2&3&4 \\ 2&3&1&4 \end{bmatrix} \circ \begin{bmatrix} 1&2&3&4 \\ 1&2&4&3 \end{bmatrix} = \begin{bmatrix} 1&2&3&4 \\ 2&3&4&1 \end{bmatrix}$$

Wiederholung der Grundlagen zu Permutationen

E104
Erläuterung

Aufgabe: Was verlangen wir von einem Monoid $(M, \cdot, 1)$? Warum ist $(\mathrm{E}_X, \bullet, \mathrm{id}_X)$ ein Monoid? Was sind hierin die invertierbaren Elemente?

Was verlangen wir von einer Gruppe $(G, \cdot, 1)$? Warum bilden die invertierbaren Elemente in $(M, \cdot, 1)$ eine (Unter)Gruppe? Ganz konkret:

🙂 Die Komposition von zwei Bijektionen ist wieder eine Bijektion; die Komposition ist assoziativ, id_X ist neutral, die Umkehrfunktion ist invers.

Fixpunktmenge und Träger einer Permutation

E105

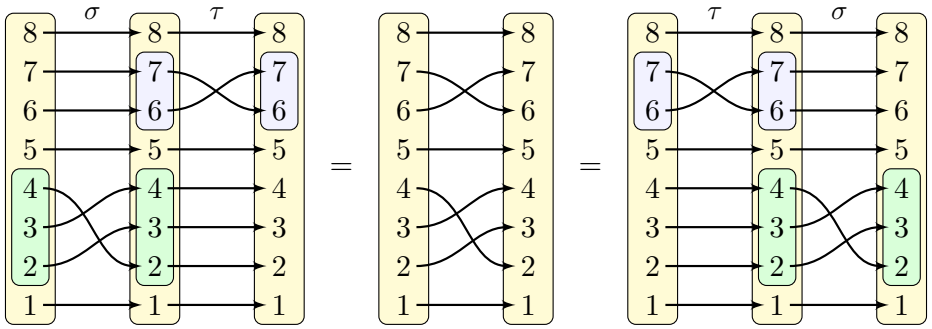
Gegeben sei $\sigma : X \to X$, eine Abbildung der Menge X in sich selbst. Ein Element $x \in X$ mit $\sigma(x) = x$ heißt **Fixpunkt** von σ. Wir setzen $\operatorname{fix}(\sigma) := \{ x \in X \mid \sigma(x) = x \}$ und $\operatorname{supp}(\sigma) := \{ x \in X \mid \sigma(x) \neq x \}$.

Lemma E1B: Disjunkte Permutationen kommutieren.

(0) Für jede Permutation $\sigma : X \xrightarrow{\sim} X$ und $A = \operatorname{supp}(\sigma)$ gilt $\sigma(A) = A$.

(1) Permutationen $\sigma, \tau : X \xrightarrow{\sim} X$ mit disjunkten Trägern kommutieren.

Beweis durch Bild: Es gilt $\sigma \bullet \tau = \tau \bullet \sigma$. Schreiben Sie es aus!



Fixpunktmenge und Träger einer Permutation

E106
Erläuterung

Wir zerlegen $X = \operatorname{fix}(\sigma) \sqcup \operatorname{supp}(\sigma)$. Die **Fixpunktmenge** $\operatorname{fix}(\sigma)$ besteht aus allen Punkten $x \in X$, die von σ festgehalten werden. Der **Träger** $\operatorname{supp}(\sigma)$ besteht aus allen Punkten $x \in X$, die von σ bewegt werden.

Eine Verwechslung mit dem Träger einer Funktion $f : X \to \{0, 1\}$ ist nicht zu befürchten, siehe D331. Hier geht es um Selbstabbildungen.

Zwei Permutationen $\sigma, \tau : X \xrightarrow{\sim} X$ derselben Menge X heißen **disjunkt**, falls ihre Träger disjunkt sind, also $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \emptyset$ erfüllen.

Beweis des Lemmas: (0) Für $x \in \operatorname{supp}(\sigma)$ und $y = \sigma(x)$ gilt $x \neq y$. Wäre $\sigma(y) = y$, so hätte y zwei Urbilder, $x \neq y$, im Widerspruch zur Injektivität von σ. Also gilt $\sigma(y) \neq y$, somit $y \in \operatorname{supp}(\sigma)$, kurz $\sigma(A) \subseteq A$. Für die Umkehrung σ^{-1} gilt $\operatorname{fix}(\sigma^{-1}) = \operatorname{fix}(\sigma)$ und $\operatorname{supp}(\sigma^{-1}) = \operatorname{supp}(\sigma)$.

(1) Gegeben seien Permutationen $\sigma_1, \ldots, \sigma_n : X \xrightarrow{\sim} X$ mit paarweise disjunkten Trägern $A_i = \operatorname{supp}(\sigma_i)$, also $A_i \cap A_j = \emptyset$ für alle $i \neq j$. Dank (0) ist $\sigma = \sigma_1 \bullet \cdots \bullet \sigma_n : X \to X$ gegeben durch $\sigma(x) = \sigma_i(x)$, falls $x \in A_i$ für ein $i \in I$, und $\sigma(x) = x$ sonst, falls $x \in X \setminus \bigcup_i A_i$. Das Ergebnis ist also unabhängig von der Reihenfolge! QED

Zykelschreibweise für Permutationen

E107

Gegeben seien $\ell \geq 2$ verschiedene Elemente $x_1, x_2, \ldots, x_\ell \in X$. Diese definieren eine zyklische Permutation auf X, kurz **ℓ–Zykel**:

$$\sigma = \operatorname{Cyc}_X(x_1, x_2, \ldots, x_\ell) \,:\, X \xrightarrow{\sim} X \,:\, x_1 \mapsto x_2 \mapsto \ldots \mapsto x_\ell \mapsto x_1$$

Ausgeschrieben bedeutet das: $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, …, $\sigma(x_\ell) = x_1$. Für alle anderen Elemente $x \in X \setminus \{x_1, x_2, \ldots, x_\ell\}$ setzen wir $\sigma(x) = x$. Somit ist $\operatorname{supp}(\sigma) = \{x_1, x_2, \ldots, x_\ell\}$ und $\operatorname{fix}(\sigma) = X \setminus \{x_1, x_2, \ldots, x_\ell\}$. Damit ist σ eine Permutation auf X, mit Inverser $\sigma^{-1} = (x_\ell, \ldots, x_2, x_1)$.

Beispiele: Auf der Menge $X = \{1, 2, 3, 4, 5, 6\}$ haben wir

$$(2,5,3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{bmatrix}, \quad (6,5,4,3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 3 & 4 & 5 \end{bmatrix}.$$

Einfachster Fall: Ein 2–Zykel $\operatorname{Cyc}_X(a, b) : a \leftrightarrow b$ heißt **Transposition**. Wir vereinbaren zudem $\operatorname{Cyc}_X(a, a) := \operatorname{id}_X$, das ist oft bequem.

Sonderfall: Für $\ell = 1$ ist $\operatorname{Cyc}_X(a) = \operatorname{id}_X$ die **Identität** auf X. Dies betrachten wir daher nicht als Zykel.

Zykelschreibweise für Permutationen

E108
Erläuterung

Die **Listennotation** können wir für *jede* Abbildung $f : X \to Y$ nutzen. Für Permutationen $f : X \xrightarrow{\sim} X$ haben wir zudem die **Zykelnotation**; diese ist für viele Zwecke und Rechnungen besonders effizient.

Meist lassen wir „Cyc_X“ weg und schreiben kurz $\sigma = (x_1, x_2, \ldots, x_\ell)$. Das bezeichnet nicht das n–Tupel, sondern die Permutation σ auf X.

Wir können jeden ℓ–Zykel auf genau ℓ verschiedene Weisen schreiben: Diese entstehend durch zyklische Rotation der Punkte. Zum Beispiel sind $(2, 5, 3) = (5, 3, 2) = (3, 2, 5)$ die drei Schreibweisen dieses Zykels.

Für beliebige Elemente $a, b \in X$ definieren wir $\tau = (a, b) : X \to X$ durch $\tau(a) = b$ und $\tau(b) = a$ sowie $\tau(x) = x$ für alle $x \in X \setminus \{a, b\}$. Im Falle $a \neq b$ ist dies eine Transposition. Im Falle $a = b$ ist dies die Identität. Dieser Sonderfall $\operatorname{Cyc}_X(a, a) = \operatorname{id}_X$ erweist sich später als bequem.

☺ Permutationen haben überall wichtige Anwendungen, sowohl als nützliches Werkzeug als auch als eigener Untersuchungsgegenstand: Algebra (Determinanten, Darstellungen), Informatik (Sortierverfahren, Kryptographie), Physik (Pauli–Prinzip in der Quantenmechanik).

Die Zykelzerlegung

Beispiel: Von der Listenschreibweise zur Zykelzerlegung:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 7 & 4 & 6 & 2 & 3 & 8 \end{bmatrix} = (1)\ (2,5,4,7)\ (6)\ (3,9,8)$$

Das Inverse ist demnach $\sigma^{-1} = (8,9,3)(7,4,5,2) = (7,4,5,2)(8,9,3)$.
Dank E1B ist die Potenz $\sigma^{2020} = (2,5,4,7)^{2020}(3,9,8)^{2020} = (3,9,8)$.

Satz E1C: eindeutige Zykelzerlegung

Sei X eine endliche Menge. Zu jeder Permutation $\sigma : X \xrightarrow{\sim} X$ existiert genau eine Menge $\{c_1, c_2, \ldots, c_k\} \subseteq \mathrm{S}_X$ disjunkter Zykel $c_1, c_2, \ldots, c_k$, so dass $\sigma = c_1 \bullet c_2 \bullet \cdots \bullet c_k$ gilt. Die Faktoren kommutieren dank E1B.

Beispiel: Komposition nicht-disjunkter Zykel auf $X = \{1, 2, \ldots, 9\}$:

$$\pi_1 = (2,3,4) \bullet (4,5,6,7) = (1)\ (2,3,5,6,7,4)\ (8)\ (9)$$
$$\pi_2 = (2,3,4) \circ (4,5,6,7) = (1)\ (2,3,4,5,6,7)\ (8)\ (9)$$

Bemerkung: Jeder ℓ–Zykel ist ein Produkt von $\ell - 1$ Transpositionen gemäß $(x_1, x_2, \ldots, x_\ell) = (x_1, x_2) \circ (x_2, x_3) \circ \cdots \circ (x_{\ell-1}, x_\ell)$. Dank Satz E1C ist jede Permutation $\sigma \in \mathrm{S}_X$ ein Produkt von Transpositionen.

Die Zykelzerlegung

Aufgabe: Denken Sie sich Permutationen aus und zerlegen Sie diese in Zykel. Formulieren Sie einen Algorithmus. Beweisen Sie Satz E1C.

Algo E1C: Zykelzerlegung

Eingabe: eine Permutation $\sigma : \{1, \ldots, n\} \xrightarrow{\sim} \{1, \ldots, n\}$
Ausgabe: die Zykelzerlegung von σ

```
1: visited ← (0,...,0) ∈ {0,1}^n        // alle Punkte noch unbesucht
2: for i from 1 to n do                 // durchlaufe alle Punkte
3:   if visited[i] = 0 then             // falls neuer Zykel...
4:     j ← i; print( "(", j )           // eröffne den Zykel
5:     repeat                           // durchlaufe den Zykel...
6:       j ← σ(j); visited[j] ← 1       // nächster Punkt des Zykels
7:       if j ≠ i then print( ",", j ) else print( ")" )
8:     until j = i                      // schließe den Zykel
```

Bemerkung: Im folgenden Beweis benötigen wir die Elementezahl von endlichen Mengen. Wir nutzen diesen Begriff weiterhin zunächst naiv; die folgenden Abschnitte werden diese Technik präzisieren.

Die Zykelzerlegung

Beweis des Satzes: Gegeben sei eine endliche Menge X und eine Permutation $\sigma \in \mathrm{S}_X$. Wir suchen eine Menge $C = \{c_1, c_2, \ldots, c_k\} \subseteq \mathrm{S}_X$ disjunkter Zykel, so dass $\sigma = \prod C = \prod_{c \in C} c = c_1 \bullet c_2 \bullet \cdots \bullet c_k$ gilt.

Existenz einer Zykelzerlegung: Wir führen Induktion über die Anzahl $\sharp\,\mathrm{supp}(\sigma)$ der bewegten Punkte. Im Falle $\sharp\,\mathrm{supp}(\sigma) = 0$ gilt $\sigma = \mathrm{id}$ und $C = \emptyset$ ist eine Lösung. Wir nehmen nun $\sharp\,\mathrm{supp}(\sigma) \geq 1$ an und wählen $x \in X$ mit $\sigma(x) \neq x$. Die Folge $x, \sigma(x), \sigma^2(x), \ldots$ in X wiederholt sich irgendwann, da die Menge X endlich ist. Die erste Wiederholung für ein $\ell \in \mathbb{N}$ ist von der Form $\sigma^\ell(x) = x$, denn andernfalls wäre σ nicht injektiv.

Wir setzen $c_1 := \mathrm{Cyc}_X(x, \sigma(x), \sigma^2(x), \ldots, \sigma^{\ell-1}(x))$ und $\sigma' := c_1^{-1} \bullet \sigma$. Der Träger ist demnach $\mathrm{supp}(c_1) = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{\ell-1}(x)\} =: I$. Auf I gilt $\sigma' = \mathrm{id}$, auf $X \smallsetminus I$ gilt $\sigma' = \sigma$. Nach Induktionsvoraussetzung existiert zu σ' eine Zykelzerlegung $C' = \{c_2, \ldots, c_k\}$. Diese ist disjunkt zu c_1. Somit ist $C = \{c_1, c_2, \ldots, c_k\}$ eine Zykelzerlegung zu $\sigma = c_1 \bullet \sigma'$.

Die Zykelzerlegung

🙂 Der obige Algorithmus E1C entrollt diese rekursive Konstruktion in eine Iteration. Dabei wird jeder Punkt nur zweimal durchlaufen. Der Aufwand ist also linear in der Anzahl $\sharp X$ der Punkte.

Eindeutigkeit der Zykelzerlegung: Zu $\sigma \in \mathrm{S}_X$ seien $\sigma = b_1 b_2 \cdots b_j$ und $\sigma = c_1 c_2 \cdots c_k$ zwei Zerlegungen in disjunkte Zykel vorgelegt. Wir haben $\{b_1, b_2, \ldots, b_j\} = \{c_1, c_2, \ldots, c_k\}$ zu zeigen.

Wir können $k \leq j$ annehmen. Wir führen Induktion über k.

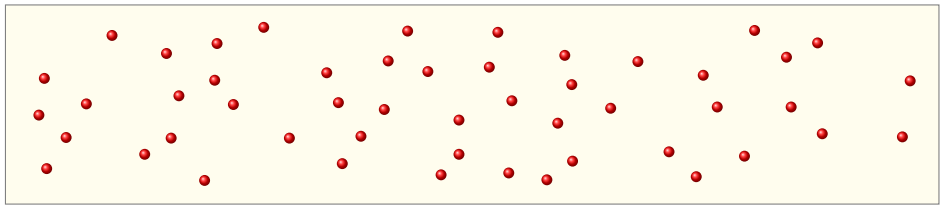
Für $k = 0$ gilt $\sigma = \mathrm{id}_X$, also auch $j = 0$, und die Aussage ist klar.

Sei nun $k \geq 1$ und $x \in \mathrm{supp}(c_1)$. Hierzu existiert b_ν mit $x \in \mathrm{supp}(b_\nu)$. Nach Umordnung können wir $\nu = 1$ annehmen. Da b_1 und c_1 von den anderen Zykeln disjunkt sind, gilt $\sigma^n(x) = b_1^n(x) = c_1^n(x)$ für alle $n \in \mathbb{Z}$, und somit die Gleichheit $b_1 = c_1$ dieser beiden Zykel. Für $\sigma' := c_1^{-1} \bullet \sigma$ haben wir die beiden Zykelzerlegungen $\sigma' = b_2 \cdots b_j$ und $\sigma' = c_2 \cdots c_k$. Nach Induktionsvoraussetzung gilt $\{b_2, \ldots, b_j\} = \{c_2, \ldots, c_k\}$. Daraus folgt $\{b_1, b_2, \ldots, b_j\} = \{c_1, c_2, \ldots, c_k\}$, wie behauptet. QED

Wie viele Elemente hat die vorgelegte Menge?

E113

Wie viele Punkte sehen Sie hier? mindestens? genau?



Definition E1D: die Anzahl der Elemente einer Menge

Sei $n \in \mathbb{N}$. Eine Menge X **besitzt mindestens** n **Elemente**, geschrieben $\sharp X \geq n$, falls eine Injektion $\nu : \{1, \ldots, n\} \hookrightarrow X$ existiert.

Die Menge X **besitzt (genau)** n **Elemente**, geschrieben $\sharp X = n$, falls eine Bijektion $\nu : \{1, \ldots, n\} \xrightarrow{\sim} X$ existiert (siehe Zählsatz E1G).

Existieren $n \in \mathbb{N}$ und $\nu : \{1, \ldots, n\} \xrightarrow{\sim} X$, so nennen wir X **endlich**, kurz $\sharp X < \infty$, andernfalls nennen wir X **unendlich**, kurz $\sharp X = \infty$.

Wir nennen $\sharp X = |X| = \operatorname{card}(X)$ die **Anzahl der Elemente** von X, die **Mächtigkeit** der Menge X, oder die **Kardinalität** der Menge X.

Wie viele Elemente hat die vorgelegte Menge?

E114
Erläuterung

Sei $n \in \mathbb{N}$. Als Referenzmenge mit genau n Elementen nutzen wir hier

$$\underline{n} = \{1, \ldots, n\} = \{\, a \in \mathbb{N} \mid 1 \leq a \leq n \,\}.$$

☺ Das ist sozusagen das Urmeter, der universelle Maßstab, mit dem wir die Größe einer beliebigen (endlichen) Menge messen.

In John von Neumanns Modell (D125) haben wir noch eleganter

$$n = \{0, 1, \ldots, n-1\} = \{\, a \in \mathbb{N} \mid a < n \,\}.$$

Hier ist jede natürliche Zahl n die Menge all ihrer Vorgängerinnen. Zwischen beiden Maßstäben besteht die kanonische Bijektion

$$(s, r) \;:\; n \cong \underline{n} \;:\; s(a) = a + 1,\; r(b) = b - 1.$$

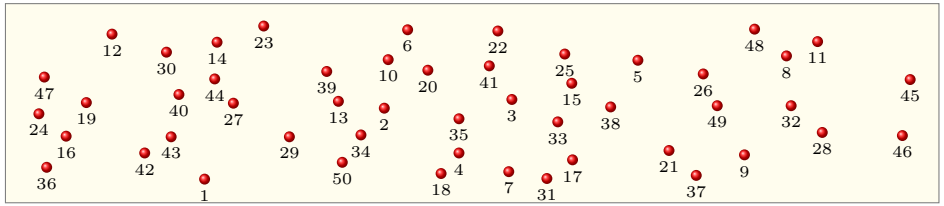
☺ Die Wahl der Referenzmenge ist eine Frage der Tradition und des Geschmacks. Ich nutze meist $\underline{n}$, doch manchmal ist n einfach besser.

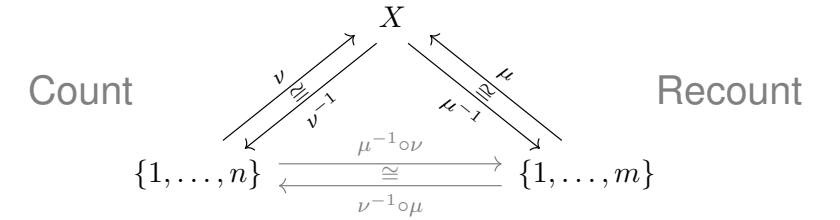
Allgemein können wir $\{\, a \in \mathbb{Z} \mid m \leq a \leq m + n - 1 \,\}$ nutzen mit $m \in \mathbb{Z}$. All diese Maßstäbe stehen kanonisch in Bijektion, alle sind gleich gut.

Wie viele Elemente hat die vorgelegte Menge?

E115

Wie viele Punkte sehen Sie hier? mindestens? genau?





Wir hoffen: Ist $f : \{1, \ldots, n\} \xrightarrow{\sim} \{1, \ldots, m\}$ bijektiv, so gilt $n = m$. Erst dank dieser Garantie ist die Elementezahl $\sharp X$ wohldefiniert!

Beispiel: Wie viele Elemente enthält $X = \{1, \{1\}, \{1, 2\}, \{1, 2, 1\}\}$?

Wie viele Elemente hat die vorgelegte Menge?

E116
Erläuterung

Wir zählen die Elemente einer beliebigen (endlichen) Menge X, indem wir willkürlich eine Nummerierung $\nu : \{1, \ldots, n\} \xrightarrow{\sim} X$ wählen. Kommt jede weitere, unabhängige Zählung μ zum selben Ergebnis?

Im Beispiel haben wir eine Abzählung $\nu : \{1, \ldots, 50\} \xrightarrow{\sim} X$ gefunden. Genügt vielleicht bereits 49 zu einer Bijektion $\mu : \{1, \ldots, 49\} \xrightarrow{\sim} X$? Es gibt $50! \approx 3 \cdot 10^{64}$ Injektionen, das ist eine astronomisch große Zahl. Es ist praktisch unmöglich, jede einzeln auf Bijektivität zu prüfen!

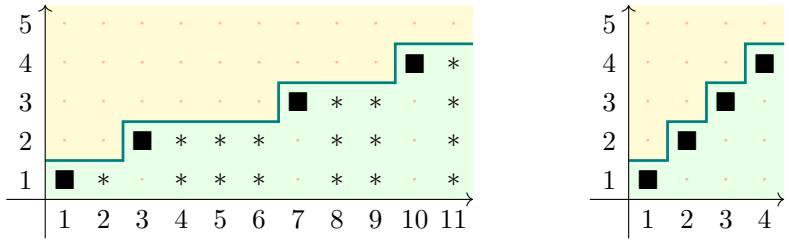
Wir benötigen hier dringend den folgenden grundlegenden **Zählsatz**: Ist eine Abbildung $f : \{1, \ldots, n\} \xrightarrow{\sim} \{1, \ldots, m\}$ bijektiv, so gilt $n = m$. Erst dank dieser Garantie ist die Elementezahl $\sharp X$ wohldefiniert!

Das ist auch politisch hochaktuell. Alle vier Jahre wird in den USA gewählt und gezählt… und nachgezählt! Wir würden hoffen, dass zwei Zählungen derselben Menge immer dasselbe Ergebnis liefern.

Seit Kindheit ist das für Sie eine grundlegende **Erfahrungstatsache**, ebenso wie weitere Rechenregeln (Kommutativität, Assoziativität usw.) Erfahrung ist gut, Intuition ist schön, ein Beweis ist noch besser!

Abbildungen $f : \{1, \dots, n\} \to \{1, \dots, m\}$ in Stufenform

Wir suchen und nutzen die Analogie zum Gauß–Algorithmus B2C:



Die Abbildung $f : \{1, \dots, n\} \to \{1, \dots, m\}$ ist in **Stufenform**, falls gilt:
Wir haben $\operatorname{im}(f) = \{1, \dots, r\}$ und Stufen $s_1 < \cdots < s_r$ in $\{1, \dots, n\}$,
an jeder Stufe s_k gilt $f(s_k) = k$, und für alle $i < s_k$ gilt $f(i) < k$.

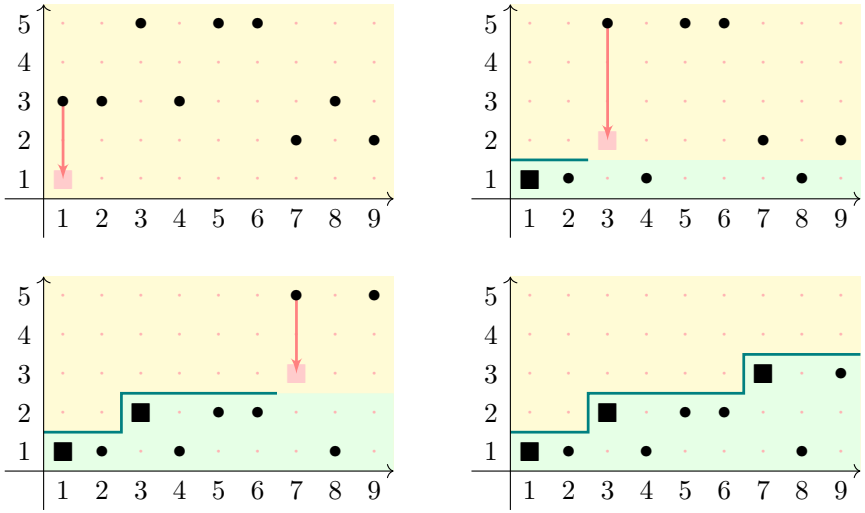
Insbesondere gilt $r \leq m$ und $r \leq n$. Daraus lesen wir ab:

- Genau dann ist f surjektiv, wenn $r = m \leq n$ gilt.
- Genau dann ist f injektiv, wenn $r = n \leq m$ gilt.
- Genau dann ist f bijektiv, wenn $r = n = m$ gilt.

Im Falle $r = n$ gilt $s = (1, 2, \dots, n)$, also ist $f = \iota$ die Inklusion / Identität.

Sortieren zur Stufenform à la Gauß

Wir können jedes $f : \{1, \dots, n\} \to \{1, \dots, m\}$ in Stufenform bringen!
Dies gelingt durch Zeilenvertauschung, wie im Gauß–Algorithmus:



Hier ist $f' = \sigma \circ f$ in Stufenform mit $\sigma = (3,5) \circ (2,5) \circ (1,3) = (1,5,2,3)$.

Sortieren zur Stufenform à la Gauß

Lemma E1E: Sortieren zur Stufenform à la Gauß

Zu jeder Abbildung $f : \{1, \dots, n\} \to \{1, \dots, m\}$ existiert eine Zeilenvertauschung $\sigma \in \mathrm{S}_m$, die $f' = \sigma \circ f$ in Stufenform bringt.

Beweis: Wir sortieren wie im Gauß–Algorithmus B2C:

Algo E1E: Sortieren zur Stufenform à la Gauß

Eingabe: eine Abbildung $f : \{1, \dots, n\} \to \{1, \dots, m\}$
Ausgabe: eine Abbildung $f' = \sigma \circ f$ in Stufenform, wobei $\sigma \in \mathrm{S}_m$
Genauer gilt $\sigma = (r, k_r) \circ \cdots \circ (2, k_2) \circ (1, k_1)$ mit $i \leq k_i \leq m$

1: $r \leftarrow 0$; $\sigma = \mathrm{id}$; $s \leftarrow ()$
2: for ℓ from 1 to n do
3: $\quad k \leftarrow f(\ell)$
4: $\quad$ if $k > r$ then $r \leftarrow r + 1$; $f \leftarrow (r, k) \circ f$; $\sigma \leftarrow (r, k) \circ \sigma$; $s_r \leftarrow \ell$

Die Permutation σ ist die Komposition der Transpositionen (r, k).
Das entspricht genau den elementaren Zeilenoperationen bei Gauß.
Hier ist alles leichter, denn hier entfällt das Aufräumen der Spalten.

Sortieren zur Stufenform à la Gauß

Beachten Sie die wundersam schöne und erstaunlich präzise Analogie zwischen dem Sortieren von Abbildungen $f : \{1, \dots, n\} \to \{1, \dots, m\}$ und dem Gauß–Algorithmus B2C für Matrizen $A \in \mathbb{K}^{m \times n}$ über einem beliebigen Körper oder Divisionsring $\mathbb{K}$:

- Wir können jede Matrix $A \in \mathbb{K}^{m \times n}$ in Zeilenstufenform $A' = SA$ bringen durch elementare Zeilenoperationen, zusammengefasst zu einer invertierbaren Matrix $S \in \mathrm{GL}_m(\mathbb{K})$.
- Wir können jede Abbildung $f : \{1, \dots, n\} \to \{1, \dots, m\}$ in Stufenform $f' = \sigma \circ f$ bringen allein durch Zeilenvertauschungen, auch diese zusammengefasst zu einer Permutation $\sigma \in \mathrm{S}_m$.

🙂 In beiden Fällen nutzen wir (im Prinzip) denselben Algorithmus: Das grundlegende Gauß–Verfahren für Matrizen A und ebenso grundlegend (aber einfacher) die Sortierung für Abbildungen f.

🙂 Auch die Folgerungen sind parallel: Die Invertierbarkeitskriterien B2D für Matrizen entsprechen dem folgenden Satz E1F für Abbildungen. Beide sind überaus praktisch, und die Analogie ist bemerkenswert.

Sur/In/Bijektivität von $f : \{1, \dots, n\} \to \{1, \dots, m\}$

E121

Satz E1F: Sur/In/Bijektivität von $f : \{1, \dots, n\} \to \{1, \dots, m\}$

Vorgelegt sei eine beliebige Abbildung $f : \{1, \dots, n\} \to \{1, \dots, m\}$.
Wir bringen f in Stufenform $f' = \sigma \circ f$ mit Rang $r \leq \min\{m, n\}$.

Genau dann ist f surjektiv / injektiv / bijektiv, wenn dies für f' gilt:

(1) Genau dann ist f surjektiv, wenn $r = m \leq n$ gilt.
(2) Genau dann ist f injektiv, wenn $r = n \leq m$ gilt.
(3) Genau dann ist f bijektiv, wenn $r = n = m$ gilt.

🙂 Das reduziert die Frage auf den Vergleich von drei Kennzahlen!

Zusatz: Ist f injektiv, so ist $f' = \iota$ die Inklusion, somit gilt

$$f = (1, k_1) \circ (2, k_2) \circ \cdots \circ (n, k_n) \circ \iota$$

mit $i \leq k_i \leq m$ für alle i. Dabei ist $(k_1, k_2, \dots, k_n)$ eindeutig.

In Worten: Jede Injektion bzw. Bijektion $f : \{1, \dots, n\} \hookrightarrow \{1, \dots, m\}$ schreibt sich eindeutig als Komposition aufsteigender Transpositionen.

🙂 Das liefert eine effiziente, eindeutige Darstellung jeder Injektion f.

Sur/In/Bijektivität von $f : \{1, \dots, n\} \to \{1, \dots, m\}$

E122
Erläuterung

Beweis: Für f' in Stufenform sind die Aussagen (1–3) klar.
Daraus folgen sie für jede Abbildung $f = \sigma \circ f'$ mit $\sigma \in \mathrm{S}_m$.

Dank dem Sortierlemma E1E gelten die ersehnten Aussagen daher für *jede beliebige* Abbildung $f : \{1, \dots, n\} \to \{1, \dots, m\}$.

Das Sortierlemma liefert weitere wertvolle Informationen:

- Rechtsinverse: Ist f' surjektiv, so ist $k \mapsto s_k$ eine Rechtsinverse. Jedem Bildwert $k \in \{1, \dots, m\}$ wird hierdurch sein *erstes* Urbild $s_k = \min f^{-1}(\{k\})$ zugeordnet. Für $f = \sigma^{-1} \circ f'$ ist demnach $g : \{1, \dots, m\} \to \{1, \dots, n\} : k \mapsto s_{\sigma(k)}$ eine Rechtsinverse.
- Linksinverse: Ist f' injektiv, so ist f dank Stufenform immer die Inklusion $\iota : \{1, \dots, n\} \hookrightarrow \{1, \dots, m\} : i \mapsto i$. Als Linksinverse wählen wir $g' : \{1, \dots, m\} \to \{1, \dots, n\} : j \mapsto \min\{j, n\}$, sodass $g' \circ f' = \mathrm{id}$. Für $f = \sigma^{-1} \circ f'$ ist demnach $g = g' \circ \sigma$ eine Linksinverse.

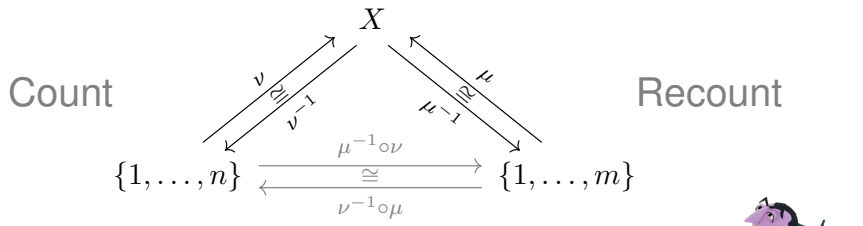
🙂 Zudem erhalten wir eine eindeutige Darstellung jeder Injektion f.

🙂 Unsere allgemeinen Sätze zu Abbildungen aus Kapitel D, wie D3A zur Invertierbarkeit, werden für endliche Mengen algorithmisch-konkret!

Warum ist die Elementezahl einer Menge wohldefiniert?

E123

Wir zählen die Elemente einer beliebigen (endlichen) Menge X, indem wir willkürlich eine Nummerierung $\nu : \{1, \dots, n\} \xrightarrow{\sim} X$ wählen. Kommt jede weitere, unabhängige Zählung μ zum selben Ergebnis?



Korollar E1G: der Zählsatz

Seien $m, n \in \mathbb{N}$ natürliche Zahlen.

(1) Ist $f : \{1, \dots, n\} \hookrightarrow \{1, \dots, m\}$ injektiv, so gilt $n \leq m$.
(2) Ist $f : \{1, \dots, n\} \twoheadrightarrow \{1, \dots, m\}$ surjektiv, so gilt $n \geq m$.
(3) Ist $f : \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, m\}$ bijektiv, so gilt $n = m$.

Somit ist die Elementezahl $\sharp X$ jeder endlichen Menge X wohldefiniert.

Warum ist die Elementezahl einer Menge wohldefiniert?

E124
Erläuterung

Korollar E1G folgt als Satz E1F als **Spezialisierung** der Implikation „⇒“
Die Umkehrung „⇐“ gilt in dieser vereinfachten Form hingegen nicht!

(1) Für $2 \leq n \leq m$ ist nicht jedes $f : \{1, \dots, n\} \to \{1, \dots, m\}$ injektiv!
(2) Für $n \geq m \geq 2$ ist nicht jedes $f : \{1, \dots, n\} \to \{1, \dots, m\}$ surjektiv!
(3) Für $n = m \geq 2$ ist nicht jedes $f : \{1, \dots, n\} \to \{1, \dots, m\}$ bijektiv!

Dies sind zunächst nur **notwendige Bedingungen**, sie werden erst hinreichend mit maximalen Rang r, wie in Satz E1F formuliert.

Bitte vergleichen Sie dies mit dem vollkommen analogen Satz B2D:
Gegeben sei eine Matrix $A \in \mathbb{K}^{m \times n}$ über einem Körper / Divisionsring $\mathbb{K}$.
Dazu bringen wir A auf Zeilenstufenform A', mit Rang $r \leq \min\{m, n\}$.
Für die zugehörige Abbildung $f : \mathbb{K}^n \to \mathbb{K}^m : x \mapsto Ax$ gilt dann:

(1) Genau dann ist f surjektiv, wenn $r = m \leq n$ gilt.
(2) Genau dann ist f injektiv, wenn $r = n \leq m$ gilt.
(3) Genau dann ist f bijektiv, wenn $r = m = n$ gilt.

Auch hier sind $n \geq m$ / $n \leq m$ / $n = m$ nur notwendige Bedingungen für die Sur/In/Bijektivität von f, hinreichend erst mit maximalem Rang r.

Warum ist die Elementezahl einer Menge wohldefiniert?

E125
Erläuterung

Ich erkläre dieses fundamentale Ergebnis hier bewusst ausführlich.
Auf den ersten Blick mag das übertrieben erscheinen. Ich habe Gründe:

- Es handelt sich um eine grundlegende Aussage über Bijektionen.
  Für eine Einführung in die Mathematik ist dies also eine gute Übung.
- Die Analogie zwischen Gauß und Sortierung ist bemerkenswert.
  Diese Parallelen erklären gegenseitig und fördern das Verständnis.
- Sie sollen lernen, präzise zu formulieren und kritisch zu denken.
  Das erfordert ausgiebige Übung und manchmal auch Überwindung.
  Daher scheint es geboten, in einfachen Fällen damit anzufangen.

Ihnen begegnen in der Mathematik sehr oft analoge Situationen:

- Ist „die Lösung“ einer gegebenen Gleichung wohldefiniert?
- Ist die Dimension eines Vektorraums V über $\mathbb{K}$ wohldefiniert?
- Ist das Volumen / Maß einer Menge $A \subseteq \mathbb{R}^n$ wohldefiniert?
- Ist die Euler–Charakteristik eines Polyeders wohldefiniert?

Warum ist die Elementezahl einer Menge wohldefiniert?

E126
Erläuterung

Dahinter steckt ein Grundprinzip: Existenz und Eindeutigkeit!
Sie wollen ein Problem zunächst präzise beschreiben und definieren,
was Sie als Lösung zulassen. Anschließend möchten Sie im Idealfall
garantieren, dass eine Lösung existiert und zudem eindeutig ist.
(Das ist nicht immer möglich, aber es ist das ersehnte Ideal.)

Alle Rechenaufgaben, selbst einfache, beruhen auf diesem Prinzip: Ist
„das Ergebnis“ eindeutig, wohldefiniert, unabhängig vom Rechenweg?
Wir müssten sonst befürchten, dass auf dem einen Rechenweg „das“
Ergebnis $E = 42$ berechnet wird, auf einem anderen Rechenweg jedoch
„das“ Ergebnis $E = 43$. Unsere Definition / Aufgabenstellung / Frage
wäre dann in sich widersprüchlich und somit wertlos.

Solche warnenden Beispiele begegnen uns tatsächlich häufig!

The method of postulating what we want has many advantages;
they are the same as the advantages of theft over honest toil.
Bertrand Russell, 1872–1970, *Introduction to Mathematical Philosophy*

Illustration zur Invarianz: das fehlende Quadrat

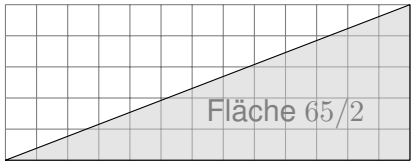
E127
Ergänzung

Wir können jeder messbaren Menge $A \subset \mathbb{R}^2$ ihren Flächeninhalt
$\mathrm{vol}_2(A)$ zuordnen, etwa Rechtecken, Dreiecken, Polygonen, etc.

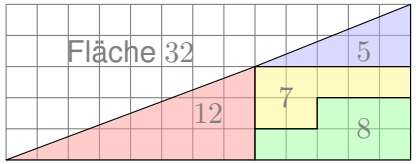
Es ist bemerkenswert, dass das Ergebnis immer eindeutig ist,
insbesondere unabhängig vom Rechenweg! Oder etwa doch nicht?

Wir zerlegen das rechtwinklige Dreieck Δ mit Kathetenlängen 13 und 5
wie skizziert und berechnen den Flächeninhalt $\mathrm{vol}_2(\Delta)$ auf drei Weisen:

Welchen Flächeninhalt hat das Dreieck?



Ist die Antwort eindeutig?



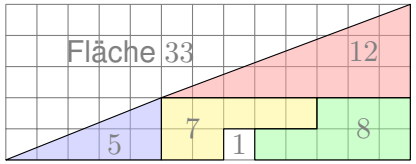


Illustration zur Invarianz: das fehlende Quadrat

E128
Ergänzung

Lösung: Die links gezeigten Mengen nennen wir A_5, A_7, A_8, A_{12}.
Jede hat den angegebenen Flächeninhalt $\mathrm{vol}_2(A_k) = k$. Je zwei sind
fast disjunkt: Ihr Schnitt hat Flächeninhalt $\mathrm{vol}_2(A_k \cap A_\ell) = 0$ für $k \neq \ell$.
Dank unserer Rechenregeln erhalten wir für $A = A_5 \cup A_7 \cup A_8 \cup A_{12}$
demnach den Flächeninhalt $\mathrm{vol}_2(A) = 5 + 7 + 8 + 12 = 32$.

Auf der rechten Seite betrachten wir entsprechend die Mengen
$B_1, B_5, B_7, B_8, B_{12}$. Für ihre Vereinigung $B = B_1 \cup B_5 \cup B_7 \cup B_8 \cup B_{12}$
erhalten wir nach denselben Regeln $\mathrm{vol}_2(B) = 1 + 5 + 7 + 8 + 12 = 33$.

Für das Dreieck Δ hingegen erhalten wir $\mathrm{vol}_2(\Delta) = 65/2 = 32.5$.
Wir erhalten auf drei Rechenwegen also drei verschiedene Ergebnisse!
Ist der Flächeninhalt also in Wirklichkeit gar nicht wohldefiniert?

Was geht hier schief? Die Skizze suggeriert $A = \Delta = B$ und provoziert
den Widerspruch. Bei genauem Hinsehen erkennen Sie $A \subsetneq \Delta \subsetneq B$.
Diese Einschachtelung zeigt $\mathrm{vol}_2(A) = 32 \leq \mathrm{vol}_2(\Delta) \leq 33 = \mathrm{vol}_2(B)$.

Alles wird gut! Der Flächeninhalt vol_2 im $\mathbb{R}^2$ und das Volumen vol_n im $\mathbb{R}^n$
ist tatsächlich wohldefiniert. Freuen Sie sich auf das Lebesgue–Maß!

Invarianz und Dirichlets Schubfachprinzip

E129

Satz E1H: Invarianz der Elementezahl

Seien X und Y endliche Mengen und $f : X \to Y$ eine Abbildung.
Für $r = \sharp\,\mathrm{im}(f)$ gilt dann $r \leq \sharp X$ und $r \leq \sharp Y$, also $r \leq \min\{\sharp X, \sharp Y\}$.

(1) Genau dann ist f surjektiv, wenn $r = \sharp Y \leq \sharp X$ gilt.
(2) Genau dann ist f injektiv, wenn $r = \sharp X \leq \sharp Y$ gilt.
(3) Genau dann ist f bijektiv, wenn $r = \sharp X = \sharp Y$ gilt.

Als Spezialisierung erhalten wir insbesondere:

(1') Ist $f : X \xrightarrow{\sim} Y$ bijektiv, so gilt $\sharp X = \sharp Y$.
(2') Ist $f : X \twoheadrightarrow Y$ surjektiv, so gilt $\sharp X \geq \sharp Y$.
(3') Ist $f : X \hookrightarrow Y$ injektiv, so gilt $\sharp X \leq \sharp Y$.

$$\begin{array}{ccc} X & \xrightarrow{\ f\ } & Y \\ {\scriptstyle\nu}\uparrow\downarrow{\scriptstyle\nu^{-1}}\ {\scriptstyle\cong} & & {\scriptstyle\mu}\uparrow\downarrow{\scriptstyle\mu^{-1}}\ {\scriptstyle\cong} \\ \{1,\dots,n\} & \xrightarrow{\ g\ } & \{1,\dots,m\} \end{array}$$

Per Kontraposition folgt aus (3') sofort:

Korollar E1I: Dirichlets Schubfachprinzip

Sei $f : X \to Y$ eine Abbildung. Gilt $\sharp X > \sharp Y$, so ist f nicht injektiv:
Es existieren zwei Elemente $a \neq b$ in X mit $f(a) = f(b)$ in Y.

Invarianz der Elementezahl

E130
Erläuterung

Sie bestaunen hier die erste und wichtigste Invariante der Mathematik: Die Elementezahl ändert sich nicht unter Anwendung von Bijektionen!

Allgemein versteht die Mathematik unter einer **Invariante** folgendes: Jedem der betrachteten Objekte (hier: endliche Mengen) wird eine Größe zugeordnet (hier: ihre Elementezahl); diese Größe ändert sich nicht unter den betrachteten Umformungen (hier: alle Bijektionen).

Invarianten sind ein wichtiges Hilfsmittel bei Klassifikationsproblemen: Objekte mit unterschiedlichen Invarianten sind wesentlich verschieden. Manchmal gilt sogar die Umkehrung, und Objekte mit gleichen Werten unter der Invariante lassen sich ineinander umformen. Wir sprechen dann von einer **vollständigen Invarianten**. Genau das liegt hier vor:

Korollar E1J: Klassifikation endlicher Mengen bis auf Bijektion

Zwei endliche Mengen X und Y stehen genau dann in Bijektion, kurz $X \cong Y$, wenn sie dieselbe Elementezahl haben, kurz $\sharp X = \sharp Y$.

🙂 Wir sehen dieses Prinzip immer wieder, etwa in Satz J2J bei der Klassifikation endlich-dimensionaler Vektorräume bis auf Isomorphie.

Dirichlets Schubfachprinzip

E131
Erläuterung

Das Schubfachprinzip ist ein einfacher und eleganter **Existenzbeweis**. Trotz seiner Einfachheit hilft Ihnen dieses Prinzip erstaunlich oft! Ehrlicherweise, sollte ich aber auch sagen, was es nicht leistet:

Es sagt uns nicht, *wie* wir ein solches Paar $a \neq b$ in X mit $f(a) = f(b)$ effizient finden, es garantiert nur, *dass* es ein solches Paar gibt.

Eine solche reine Existenzaussage ist zwar leider nicht konstruktiv, doch oft ist eine schwache Aussage besser als gar keine Aussage. Sie ist nicht das Ende der Problemlösung, sondern ein guter Anfang.

Die Existenz einer Lösung hilft in vielen praktischen Anwendungen: Bevor Sie sich auf die lange und mühevolle Suche nach einer Lösung begeben, wollen Sie sicher sein, dass sich Ihre Mühe auch lohnen wird.

Oder noch extremer: Es ist ganz sicher besser frühzeitig zu erkennen, dass es keine Lösung gibt, als jahrelang vergeblich danach zu suchen. Das nachfolgende Beispiel E1K illustriert dies eindrücklich, als Video von Burkard Polster, *The pigeon hole principle*, `youtu.be/TCZ3YwbcDaw`.

Illustration zu Dirichlets Schubfachprinzip

E132

Behauptung: Es gibt in Stuttgart mindestens zwei Personen, die exakt dieselbe Anzahl von Haaren auf dem Kopf haben.

Beweis: Typischerweise hat ein Mensch $100\,000$ bis $200\,000$ Haare, sicher weniger als $500\,000$. Stuttgart hat knapp über $635\,000$ Einwohner. Somit ist die Haarzahl $h : \{\text{Einwohner}\} \to \{0, \dots, 500000\}$ nicht injektiv.

🙂 Das ist ein eleganter Existenzbeweis, wenn auch nicht konstruktiv. Er sagt uns, *dass* wir ein solches Paar finden können, aber nicht *wie*!

Mit solchen Formulierungen lässt sich das Schubfachprinzip schön illustrieren und auch leicht merken. Natürlich gibt es hier zahlreiche mögliche Einwände, wie immer bei allzu anschaulichen Beispielen. Ist die Haarzahl genau bestimmt? Können wir sie praktisch zählen?

Das ist keine ernsthafte *Anwendung*, sondern eher eine scherzhafte *Illustration*. Da es in Stuttgart mindestens zwei Kahlköpfige gibt, ist die hier gemachte Aussage ohnehin trivial. Aber Sie verstehen das Prinzip.

🙂 Die folgende schöne Anwendung ist rein mathematisch, daher viel einfacher, und über jede Haarspalterei erhaben.

Anwendung zu Dirichlets Schubfachprinzip

E133

Aufgabe: Wir nennen $T \subseteq \mathbb{N}$ **teilerfrei**, falls $s \nmid t$ für alle $s \neq t$ in T gilt.

(1) Finden Sie eine teilerfreie Menge $T \subseteq \{1, \dots, 100\}$ mit $\sharp T = 50$.
(2) Finden Sie alle teilerfreien Mengen $T \subseteq \{1, \dots, 100\}$ mit $\sharp T = 51$.

Lösung: (1) Die Menge $T = \{51, \dots, 100\}$ ist teilerfrei. (2) Es gibt keine!
Allgemein gilt hierzu das folgende bemerkenswert elegante Ergebnis:

Beispiel E1K: Anwendung des Schubfachprinzips

Wir betrachten $V = \{1, \dots, 2n\}$ mit $n \in \mathbb{N}_{\geq 1}$. Sei $T \subseteq V$ mit $\sharp T > n$.
Dann existiert mindestens ein Paar $s \neq t$ in T mit $s \mid t$.

Beweis: Die Menge $U := \{1, 3, 5, \dots, 2n-1\}$ hat genau n Elemente.
Wir definieren die Abbildung $f : V \to U : x \mapsto x'$ durch $x = 2^k x'$, $k \in \mathbb{N}$.
Wegen $\sharp T > \sharp U$ ist $f|_T : T \to U$ nicht injektiv dank Schubfachprinzip E1I.
Also existieren zwei verschiedene Elemente $s < t$ in T mit $f(s) = f(t)$.
Für diese gilt $s = 2^k s'$ und $t = 2^\ell s'$ mit $k < \ell$, und somit $s \mid t$. QED

Anwendung zu Dirichlets Schubfachprinzip

E134
Erläuterung

☺ Das ist ein eleganter Existenzbeweis! Wir müssen nur noch suchen.
Der Beweis garantiert, dass wir ein solches Paar in T finden werden.
Anschließend können wir nach effizienten Algorithmen fragen...
Auch dies ist im vorliegenden Beispiel erfreulich einfach.

Schon die „reine Existenzaussage“ ist hier bereits extrem hilfreich!
Die ursprüngliche, ganz praktische Aufgabenstellung lautet ja:
Finden Sie alle teilerfreien Mengen $T \subseteq \{1, \dots, 100\}$ mit $\sharp T = 51$.

Naiv müsste man sich nun daran machen, alle möglichen Teilmengen $T \subseteq \{1, \dots, 100\}$ durchzuprobieren, um nur die teilerfreien zu behalten.
Schon in diesem kleinen Beipsiel ist dies eine lange und mühselige Arbeit: „Die Guten ins Töpfchen, die Schlechten ins Kröpfchen“

Das Schubfachprinzip liefert hier eine schnelle und präzise Antwort:
Es gibt keine einzige teilerfreie Menge $T \subseteq \{1, \dots, 100\}$ mit $\sharp T = 51$.
Damit haben wir unsere Suche schnell und vollständig durchgeführt.
Es lohnt sich daher, in gute Denkwerkzeuge zu investieren.

Jeder endliche Integritätsring ist ein Körper.

E135

Ein **Integritätsring** $(R, +, 0, \cdot, 1)$ ist ein kommutativer Ring mit $1 \neq 0$ ohne Nullteiler. Letzteres heißt: Für alle $a, b \neq 0$ in R gilt $a \cdot b \neq 0$.

Beispiele: Jeder Körper ist ein Integritätsring, etwa $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$.
Die ganzen Zahlen $\mathbb{Z}$ sind ein Integritätsring, aber kein Körper.
Der Ring $\mathbb{Z}_6$ hingegen hat Nullteiler, denn hier gilt $2 \cdot_6 3 = 0$.
Die Ringe $\mathbb{Z}_5$ und $\mathbb{Z}_7$ sind nullteilerfrei... und Körper!

Satz E1L: endliche Integritätsringe

Jeder endliche Integritätsring $(R, +, 0, \cdot, 1)$ ist ein Körper.

Beweis: Zu $a \in R \setminus \{0\}$ betrachten wir die Linksmultiplikation

$$\lambda_a : R \to R : x \mapsto a \cdot x.$$

Diese ist injektiv: Aus $a \cdot x = a \cdot x'$ folgt $a \cdot (x - x') = 0$, also $x = x'$.
Die Menge R ist endlich, also ist λ_a auch surjektiv dank Satz E1H.
Insbesondere existiert zur Gleichung $a \cdot x = 1$ eine Lösung $x \in R$.
Somit ist jedes Element $a \neq 0$ in R invertierbar. QED

Jeder endliche Integritätsring ist ein Körper.

E136
Erläuterung

☺ Aus geringen Voraussetzungen erhalten wir starke Folgerungen, allein dank der Endlichkeit der Menge R! Das ist bemerkenswert.
Es ist eine erste frappierende Anwendung des Invarianzsatzes E1H.

Für endliche Mengen und ihre Abbildungen gelten besonders starke und nützliche Gesetzmäßigkeiten: *Defendit numerus.* [Die Zahl gibt Schutz.]
Dies wollen und werden wir im Folgenden immer wieder nutzen.

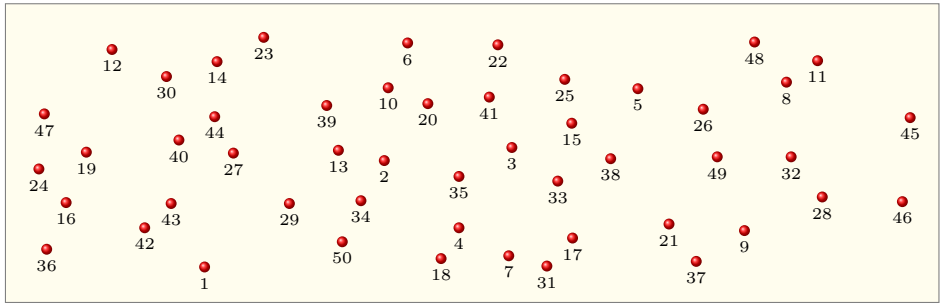
Auch für unendliche Mengen gelten nützliche Gesetzmäßigkeiten, wenn auch deutlich andere und manchmal schockierend paradox.
Damit werden wir uns im folgenden Kapitel genauer beschäftigen.

In diesem Kapitel geht es zunächst um endliche Mengen und die hierbei geltenden Abzählregeln. Vieles davon wird Ihnen sofort einleuchten, vermutlich gar trivial vorkommen. Das ist gut, schauen Sie genau hin!

Ich führe hier bewusst alle Details explizit aus: Es ist eine gute Übung in präziser Formulierung und Argumentation. Zudem bereitet es Sie auf unendliche Mengen vor, die sich deutlich anders verhalten.

Mächtigkeit von Mengen: immer durch Abzählen!

E201
Erläuterung



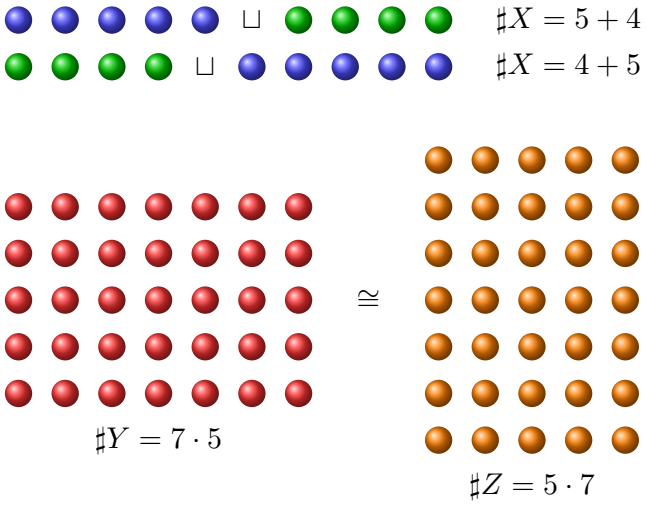
Das Zählen von Dingen ist *die* mathematische Grunderfahrung, sowohl psychologisch-individuell als auch historisch-gesellschaftlich. Das Abzählen spielt eine zentrale Rolle in nahezu jeder Anwendung der Mathematik, vom alltäglichen Handel und Wandel zur Quantenmechanik.

Mengen sind konkret, Zahlen sind abstrakt. Daher nutzt die Didaktik gezielt Mengen, um das Rechnen mit Zahlen zu veranschaulichen. Viele der folgenden Ergebnisse kommen Ihnen daher bekannt vor. Was für Sie neu hinzukommt, ist der formal mathematische Rahmen.

Strukturiertes Abzählen: Grundrechenarten

E202

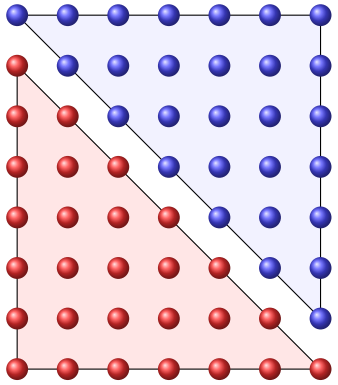
Wir wollen strukturierte Mengen effizient abzählen. Mengenoperationen entsprechen dabei wunderbar Rechenoperationen natürlicher Zahlen:



Doppeltes Abzählen: der kleine Gauß

E203

$$1 + 2 + 3 + \quad \ldots \quad + n =: S(n)$$



$$2S(n) = n(n+1)$$

Dieses genial-einfache Argument zeigt die geschlossene Formel

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Doppeltes Abzählen: der kleine Gauß

E204
Erläuterung

Dahinter stecken einfache Regeln, die wir hier explizit benennen:

1. Doppeltes Abzählen einer Menge ergibt dieselbe Elementezahl in $\mathbb{N}$.
2. Daraus folgt die Invarianz: Jede Bijektion erhält die Elementezahl.
3. Disjunkte Vereinigung von Mengen entspricht der Summe in $\mathbb{N}$.
4. Kartesisches Produkt von Mengen entspricht dem Produkt in $\mathbb{N}$.

Wir wenden dies wie folgt an – meist unbewusst, hier explizit:

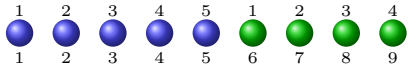
- Das blaue Dreieck Δ hat genau $S(n)$ Elemente dank (3).
- Wir drehen das blaue in das rote Dreieck Δ' und nutzen (2).
- Das Rechteck R ist disjunkte Vereinigung der beiden Dreiecke (3).
- Die Elementezahl des Rechtecks ist das Produkt $n(n+1)$ dank (4).

Wir zählen das Rechteck somit auf zwei Arten (1) und erhalten

$$R = \Delta \sqcup \Delta' \quad \Longrightarrow \quad n(n+1) = S(n) + S(n).$$

Umgestellt erhalten wir die ersehnte Formel $S(n) = n(n-1)/2$.

Mächtigkeit disjunkter Vereinigungen



Satz E2A: Mächtigkeit einer disjunkten Vereinigung

Seien X und Y endliche Mengen mit $X \cap Y = \emptyset$. Dann gilt:

$$\sharp(X \sqcup Y) = (\sharp X) + (\sharp Y)$$

Explizite Konstruktion: Gegeben seien die Abzählungen

$$\mu : \{1, \dots, p\} \xrightarrow{\sim} X,$$
$$\nu : \{1, \dots, q\} \xrightarrow{\sim} Y.$$

Daraus konstruieren wir die Abzählung der disjunkten Vereinigung

$$(\sigma, \tau) : \{1, \dots, p+q\} \cong X \sqcup Y$$

durch $\sigma(k) = \mu(k)$ für $1 \leq k \leq p$ und $\sigma(k) = \nu(k-p)$ für $p < k \leq p+q$ sowie $\tau(x) = \mu^{-1}(x)$ für $x \in X$ und $\tau(y) = \nu^{-1}(y) + p$ für $y \in Y$.

Mächtigkeit disjunkter Vereinigungen

Tatsächlich ist (σ, τ) eine Bijektion. Die Formeln liegen explizit vor, es genügt also nachzurechnen, dass $\tau \circ \sigma = \mathrm{id}$ und $\sigma \circ \tau = \mathrm{id}$ gilt.

Dies beweist die behauptete Gleichung zwischen den Elementzahlen. Es gibt viele Abzählungen, aber das Ergebnis ist eindeutig, siehe E1G.

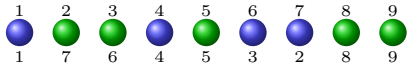
Ist das nicht irgendwie intuitiv klar? Müssen wir es explizit konstruieren? Ja, wenn es so klar ist, dann können wir es leicht explizit konstruieren!

Ist das übertrieben pedantisch? Nein, die Abzählung E1D verlangt eine Bijektion, also sollten wir eine konkrete Bijektion vorweisen.

Dasselbe gilt insbesondere im folgenden Fall einer Teilmenge $X \subseteq Z$. Natürlich ist intuitiv klar, dass $\sharp X \leq \sharp Z$ und $\sharp(Z \smallsetminus X) = (\sharp Z) - (\sharp X)$ gilt.

Aber woher bekommen wir eine geeignete Abzählung, die das belegt? Ganz einfach: Wir müssen sie konstruieren! Es ist zum Glück leicht.

Mächtigkeit von Teilmengen und Vereinigungen



Satz E2B: Mächtigkeit von Teilmengen und Vereinigungen

(0) Ist Z endlich, so auch jede Teilmenge $X \subseteq Z$. Genauer gilt:

$$X \subseteq Z \implies \sharp X \leq \sharp Z, \quad \sharp(Z \smallsetminus X) = (\sharp Z) - (\sharp X)$$

Explizite Konstruktion: Sei $\nu : \{1, \dots, n\} \xrightarrow{\sim} Z$ eine Abzählung. Zu jeder Zerlegung $Z = X \sqcup Y$ existiert eine Sortierung $\sigma \in \mathrm{S}_n$ zu einer angepassten Abzählung $\mu = \nu \circ \sigma : \{1, \dots, n\} \xrightarrow{\sim} Z$ mit $\mu(\{1, \dots, p\}) = X$ und $\mu(\{p+1, \dots, n\}) = Y$.

(1) Für beliebige endliche Mengen X, Y folgt daraus:

$$\sharp(X \cup Y) = \sharp X + \sharp Y - \sharp(X \cap Y)$$

Explizite Konstruktion: Es gilt $X \cup Y = X \sqcup Y'$ mit $Y' = Y \smallsetminus (X \cap Y)$.

Mächtigkeit von Teilmengen und Vereinigungen

Die Aussage $\sharp X \leq \sharp Z$ folgt bereits aus der Invarianz E1H dank Inklusion $\iota : X \hookrightarrow Z$. Auch die Sortierung von ν zum angepassten μ folgt aus dem Sortierlemma E1E. Ich führe es zur Deutlichkeit hier unabhängig aus.

Beweis: (0) Wir können $X \subseteq Z$ nach vorne sortieren:

Algo E2B: Sortiere $X \subseteq Z$ nach vorne

Eingabe: Abzählung $\nu : \{1, \dots, n\} \xrightarrow{\sim} Z$ und Zerlegung $Z = X \sqcup Y$
Ausgabe: (μ, σ, p) mit $\mu = \nu \circ \sigma$ und $\sigma \in \mathrm{S}_n$ und $\mu(\{1, \dots, p\}) = X$

```
1: q ← 1; p ← n; μ ← ν; σ ← id          // μ({1,…,q−1}) ⊆ X
2: while q ≤ p do                        // μ({p+1,…,n}) ⊆ Y
3:     while q ≤ n ∧ μ(q) ∈ X do q ← q+1  // erstes Element in Y
4:     while p ≥ 1 ∧ μ(p) ∈ Y do p ← p−1  // letztes Element in X
5:     if q < p then μ ← μ ∘ (q,p); σ ← σ ∘ (q,p)  // tausche falls nötig
6: return (μ, σ, p)                      // nun liegt X vor Y
```

(1) Wir zerlegen $X \cup Y = X \sqcup Y'$ mit $Y' = Y \smallsetminus (X \cap Y)$. Dank Satz E2A und (0) folgt $\sharp(X \cup Y) = \sharp X + \sharp Y' = \sharp X + \sharp Y - \sharp(X \cap Y)$. QED

Mächtigkeit kartesischer Produkte

Beispiel: Wir wollen kartesische Produkte $X \times Y$ abzählen.
Konkret betrachten wir $X = \{0, \dots, p-1\}$ und $Y = \{0, \dots, q-1\}$.

3	$(0,3)$ $\mapsto 21$	$(1,3)$ $\mapsto 22$	$(2,3)$ $\mapsto 23$	$(3,3)$ $\mapsto 24$	$(4,3)$ $\mapsto 25$	$(5,3)$ $\mapsto 26$	$(6,3)$ $\mapsto 27$
2	$(0,2)$ $\mapsto 14$	$(1,2)$ $\mapsto 15$	$(2,2)$ $\mapsto 16$	$(3,2)$ $\mapsto 17$	$(4,2)$ $\mapsto 18$	$(5,2)$ $\mapsto 19$	$(6,2)$ $\mapsto 20$
1	$(0,1)$ $\mapsto 7$	$(1,1)$ $\mapsto 8$	$(2,1)$ $\mapsto 9$	$(3,1)$ $\mapsto 10$	$(4,1)$ $\mapsto 11$	$(5,1)$ $\mapsto 12$	$(6,1)$ $\mapsto 13$
0	$(0,0)$ $\mapsto 0$	$(1,0)$ $\mapsto 1$	$(2,0)$ $\mapsto 2$	$(3,0)$ $\mapsto 3$	$(4,0)$ $\mapsto 4$	$(5,0)$ $\mapsto 5$	$(6,0)$ $\mapsto 6$
	0	1	2	3	4	5	6

Zeilenweises Abzählen ergibt $(f, g) : X \times Y \cong \{0, \dots, pq-1\}$
mit $f(x, y) = x + yp$ und Umkehrung $g(z) = (z \operatorname{rem} p, z \operatorname{quo} p)$.
Das ist tatsächlich eine Bijektion, denn $g \circ f = \mathrm{id}$ und $f \circ g = \mathrm{id}$.

M Dies iteriert Satz E2A für $X \times Y = X \times \{0\} \sqcup \dots \sqcup X \times \{p-1\}$:
Wir legen die Zeilen hintereinander. (Genauso gelingt es mit Spalten.)

I Auf dem Computer werden Matrizen so konsekutiv gespeichert.
Unsere konkrete Indexumrechnung ist dabei überaus praktisch.

Mächtigkeit kartesischer Produkte

Satz E2C: Mächtigkeit eines kartesischen Produkts

Seien X und Y endliche Mengen. Dann gilt:

$$\sharp(X \times Y) = (\sharp X) \cdot (\sharp Y)$$

Explizite Konstruktion: Gegeben seien

$$\mu : \{0, \dots, p-1\} \xrightarrow{\sim} X,$$
$$\nu : \{0, \dots, q-1\} \xrightarrow{\sim} Y.$$

Daraus konstruieren wir die Abzählung des Produkts

$$(\sigma, \tau) : \{0, \dots, pq-1\} \cong X \times Y$$

durch $\sigma(z) = (\,\mu(z \operatorname{rem} p),\, \nu(z \operatorname{quo} p)\,)$ und $\tau(x, y) = \mu^{-1}(x) + \nu^{-1}(y)p$.

Übung: Das ist tatsächlich eine Bijektion, denn $\tau \circ \sigma = \mathrm{id}$ und $\sigma \circ \tau = \mathrm{id}$.
Stehen die Abbildungen erst einmal vor uns, so genügt Nachrechnen!
Ich betone nochmal: Explizite Formeln sind nicht Fluch, sondern Segen.

Mächtigkeit von Summen und Produkten

Satz E2D: Mächtigkeit von Summen und Produkten

Für (disjunkte) Mengen $X_1, X_2, \dots, X_n$ gilt:

$$X_1 \sqcup X_2 \sqcup \dots \sqcup X_n = (X_1 \sqcup X_2 \sqcup \dots) \sqcup X_n$$
$$X_1 \times X_2 \times \dots \times X_n = (X_1 \times X_2 \times \dots) \times X_n$$

Aus den Sätzen E2B und E2C folgt damit per Induktion:

$$\sharp(X_1 \sqcup X_2 \sqcup \dots \sqcup X_n) = (\sharp X_1) + (\sharp X_2) + \dots + (\sharp X_n).$$
$$\sharp(X_1 \times X_2 \times \dots \times X_n) = (\sharp X_1) \cdot (\sharp X_2) \cdots (\sharp X_n).$$

Übung: (0) Warum gelten die gezeigten Gleichungen für die Mengen?
(1) Beweisen Sie die zugehörigen Gleichungen für die Elementezahlen.
(2) Konstruieren Sie auch hier möglichst explizite Abzählungen.

Mächtigkeit von Summen und Produkten

Lösung: (0) Die erste Gleichheit für die disjunkte Summe ist klar:

$$X_1 \sqcup X_2 \sqcup \dots \sqcup X_n = (X_1 \sqcup X_2 \sqcup \dots) \sqcup X_n$$

Die zweite Gleichheit verdanken wir unserer Definition (Seite D138) des n–fachen kartesischen Produkts durch Linksklammerung:

$$X_1 \times X_2 \times \dots \times X_n = (X_1 \times X_2 \times \dots) \times X_n$$

Andernfalls stünde hier statt strikter Gleichheit „=“ eine geeignete Bijektion „$\cong$“ durch Umklammerung, siehe Seite E223 für ein Beispiel.
Dank Invarianz E1H wäre jede Bijektion für unsere Zwecke genauso gut.

(1) Für $n = 1$ ist die jeweilige Aussage $X_1 = X_1$ und $\sharp X_1 = \sharp X_1$ trivial.
Der Fall $n = 2$ wurde in Satz E2A und E2C konstruktiv ausgeführt.
Diese Konstruktion setzt sich per Induktion für alle $n \in \mathbb{N}$ fort.

(2) Explizite Abzählungen erhalten wir genau nach obiger Vorlage.
Für das Produkt nutzen wir die Zifferndarstellung in gemischter Basis.

Mächtigkeit kartesischer Potenzen

Als Spezialfall des vorigen Satzes E2D erhalten wir $\sharp(X^n) = (\sharp X)^n$.
Wir betrachten diesen Fall hier noch etwas ausführlicher, da Potenzen dieser Art häufig auftreten und zudem interessante Formeln liefern.

Beispiel: Wir wollen kartesische Potenzen X^n abzählen.
Konkret betrachten wir hierzu die Menge $X = \{0, \ldots, p-1\}$.

Wir nutzen die Zifferndarstellung in Basis p (Satz A2B):

$$\begin{aligned}(f,g) &: \{0,\ldots,p-1\}^n \cong \{0,\ldots,p^n-1\},\\ &f(z_0,z_1,\ldots,z_{n-1}) = z_0 + z_1 p + \cdots + z_{n-1}p^{n-1},\\ &g(z) = (z_0,z_1,\ldots,z_{n-1}) \quad \text{mit} \quad z_k = (z \operatorname{quo} p^k) \operatorname{rem} p.\end{aligned}$$

M Die Iteration von Satz E2C ergibt die Zifferndarstellung zur Basis p.
Auch hier ist es besser, bei 0 anzufangen, das vereinfacht die Formeln.

Mächtigkeit kartesischer Potenzen

Satz E2E: Mächtigkeit einer kartesischen Potenz

Sei X eine endliche Menge und $n \in \mathbb{N}$. Dann gilt:

$$\sharp(X^n) = (\sharp X)^n$$

Explizite Konstruktion: Gegeben sei eine Abzählung

$$\mu : \{0,\ldots,p-1\} \xrightarrow{\sim} X.$$

Daraus konstruieren wir die Abzählung der Potenz

$$(\sigma,\tau) : \{0,\ldots,p^n-1\} \cong X^n$$

durch $\sigma(z) = (x_0,x_1,\ldots,x_{n-1})$ mit $x_k = \mu((z \operatorname{quo} p^k) \operatorname{rem} p)$ und
$\tau(x_0,x_1,\ldots,x_{n-1}) = \mu^{-1}(x_0) + \mu^{-1}(x_1)p + \cdots + \mu^{-1}(x_{n-1})p^{n-1}$.

Mächtigkeit und natürliche Zahlen

Auf den ersten Blick mutet es an wie ein Wunder, dass sich die Mengenoperationen $X \sqcup Y$ und $X \times Y$ und X^n so nahtlos übersetzen in die Zahlenoperationen $x + y$ und $x \cdot y$ und x^n. Dieses „Wunder“ hat jedoch eine einfache Erklärung: Die natürlichen Zahlen wurden gerade dafür geschaffen, um solche Phänomene arithmetisch abzubilden.

In der Entwicklung der Menschheit scheint dies recht plausibel:
Zuerst gab es die Objekte selbst, dann erst wurden sie gezählt.
Gerade Vereinigung und Produkt treten im Alltag häufig auf,
und die Zahlen wurden entwickelt, dies wiederzugeben.

Die ganzen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk.
Leopold Kronecker (1823–1891)

In Anbetracht der obigen Zählformeln bin ich versucht zu sagen:
Die Mengen sind das Urmaterial, alles andere ist Menschenwerk.

Mächtigkeit und natürliche Zahlen

Egal ob zahlenmystisches Wunder oder historisch erklärbar,
freuen wir uns an diesem harmonischen Zusammenklang!

Auf der einen Seite haben wir endliche Mengen und ihre Abbildungen,
auf der anderen Seite haben wir die vertrauten natürlichen Zahlen.

In manchen Fällen sind die Zahlen einfacher: Wir begnügen uns dann mit der Anzahl der Elemente und vernachlässigen die Menge selbst.

In anderen Fällen ist die dahinterliegende Menge einfacher oder informativer, dann lohnt es sich, die reichere Struktur zu nutzen.

Mächtigkeit von Abbildungsmengen

E217

Die Menge aller Abbildungen von X nach Y bezeichnen wir mit

$$\mathrm{Abb}(X,Y) := \{\, f : X \to Y \,\} = Y^X.$$

Beispiel Zahlenschloss: Wie viele Abbildungen $f : X \to Y$ gibt es von der Startmenge $X = \{1,2,3,4\}$ in die Zielmenge $Y = \{0,1,\ldots,9\}$?

Satz E2F: Mächtigkeit der Abbildungsmenge

Sind X und Y endlich, so auch die Abbildungsmenge:

$$\sharp\,\mathrm{Abb}(X,Y) = \sharp(Y^X) = (\sharp Y)^{(\sharp X)}$$

Explizite Konstruktion: Jede Abzählung $\mu : \{1,\ldots,n\} \xrightarrow{\sim} X$ beschert uns

$$Y^X \cong Y^n \;:\; f \mapsto \big(\, f(\mu(1)),\, \ldots,\, f(\mu(n)) \,\big).$$

Beweis: Die Bijektion $Y^X \cong Y^n$ ist hier explizit angegeben.
Damit können wir direkt den vorigen Satz E2E anwenden.

Mächtigkeit von Abbildungsmengen

E218
Erläuterung

Für jede natürliche Zahl $n \in \mathbb{N}_{\geq 0}$ haben wir die kanonische Bijektion

$$(\eta,\varepsilon) \;:\; \mathrm{Abb}(\{1,\ldots,n\},Y) \cong Y^n.$$

Für $f : \{1,\ldots,n\} \to Y$ definieren wir $\eta(f) := (f(1),\ldots,f(n))$.
Für $y = (y_1,\ldots,y_n) \in Y^n$ definieren wir $\varepsilon(y) := f$ als die Abbildung $f : \{1,\ldots,n\} \to Y : 1 \mapsto y_1, \ldots, n \mapsto y_n$; diese ist dadurch wohldefiniert.
Damit gilt $\varepsilon \circ \eta = \mathrm{id}$ und $\eta \circ \varepsilon = \mathrm{id}$.

Gegeben sei eine Abzählung $\mu : \{1,\ldots,n\} \xrightarrow{\sim} X$. Dann konstruieren wir

$$(\sigma,\tau) \;:\; \mathrm{Abb}(X,Y) \cong \mathrm{Abb}(\{1,\ldots,n\},Y).$$

Für $f : X \to Y$ definieren wir $\sigma(f) := f \circ \mu : \{1,\ldots,n\} \to Y$.
Für $g : \{1,\ldots,n\} \to Y$ definieren wir $\tau(g) := g \circ \mu^{-1} : X \to Y$.
Damit gilt $\tau(\sigma(f)) = (f \circ \mu) \circ \mu^{-1} = f$, also $\tau \circ \sigma = \mathrm{id}$.
Ebenso gilt $\sigma(\tau(g)) = (g \circ \mu^{-1}) \circ \mu = g$, also $\sigma \circ \tau = \mathrm{id}$.

Satz E2F nutzt die Komposition dieser beiden Bijektionen.

Erinnerung: Tupel über $\{0,1\}$

E219
Erläuterung

Beispiel: Über $\{0,1\}$ lassen sich vier 2–Tupel (Paare) bilden:

$$\{0,1\}^2 = \{\, (0,0),\ (0,1),\ (1,0),\ (1,1) \,\}$$

Ebenso können wir acht 3–Tupel (Tripel) bilden:

$$\{0,1\}^3 = \{\, (0,0,0),\ (0,0,1),\ (0,1,0),\ (0,1,1),\ (1,0,0),\ (1,0,1),\ (1,1,0),\ (1,1,1) \,\}$$

Ebenso können wir sechzehn 4–Tupel (Quadrupel) bilden:

$$\{0,1\}^4 = \{\, (0,0,0,0),\ (0,0,0,1),\ (0,0,1,0),\ (0,0,1,1),\ (0,1,0,0),\ (0,1,0,1),\ (0,1,1,0),\ (0,1,1,1),\ (1,0,0,0),\ (1,0,0,1),\ (1,0,1,0),\ (1,0,1,1),\ (1,1,0,0),\ (1,1,0,1),\ (1,1,1,0),\ (1,1,1,1) \,\}$$

Die Binärdarstellung definiert die Bijektion $\{0,1\}^n \cong \{0,\ldots,2^{n-1}\}$.

Erinnerung: die Potenzmenge $\mathfrak{P}(X)$

E220

Die Potenzmenge $\mathfrak{P}(X) = \{\, A \subseteq X \,\}$ ist die Menge aller Teilmengen:

$$\begin{aligned}
\mathfrak{P}(\emptyset) &= \{\, \emptyset \,\} \\
\mathfrak{P}(\{1\}) &= \{\, \emptyset, \{1\} \,\} \\
\mathfrak{P}(\{1,2\}) &= \{\, \emptyset, \{1\}, \{2\}, \{1,2\} \,\} \\
\mathfrak{P}(\{1,2,3\}) &= \{\, \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} \,\} \\
\mathfrak{P}(\{1,2,3,4\}) &= \{\, \emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \\
&\qquad \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \\
&\qquad \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\} \,\}
\end{aligned}$$

Jede Teilmenge $A \subseteq \{1,2,3,4\}$ entspricht einem Tupel $f \in \{0,1\}^4$:

$$\begin{aligned}
(0,0,0,0) &\leftrightarrow \{1,2,3,4\} \\
(0,1,1,0) &\leftrightarrow \{1,2,3,4\} \\
(1,1,1,0) &\leftrightarrow \{1,2,3,4\} \\
(1,1,1,1) &\leftrightarrow \{1,2,3,4\}
\end{aligned}$$

☺ Dieses Prinzip haben wir in Satz D3D allgemein ausgeführt.

Mächtigkeit von Potenzmengen

Satz E2G: Mächtigkeit der Potenzmenge

Für jede endliche Menge X mit $n = \sharp X$ Elementen gilt:

$$\boxed{\sharp\mathfrak{P}(X) = 2^n}$$

Explizite Konstruktion: Satz D3D beschert uns die Bijektion

$$\begin{aligned}(\mathbf{I}, \operatorname{supp}) \,:\, \mathfrak{P}(X) &\cong \operatorname{Abb}(X, \{0,1\}) \\ A &\mapsto \mathbf{I}_A \\ \operatorname{supp}(f) &\mapsfrom f\end{aligned}$$

Beweis: Anschaulich ist der Satz plausibel, so wie oben illustriert, allzumal wenn es bloß um die vage „gefühlte Elementezahl“ geht.

Eine formale Abzählung gelingt mit der Bijektion aus Satz D3D, dank Satz E2F können wir die Mächtigkeit der Abbildungsmenge ablesen.

Da wir jeweils Bijektionen explizit angeben, erhalten wir auch hier durch Komposition eine explizite Bijektion $\mathfrak{P}(X) \cong \{0, \dots, 2^n - 1\}$. QED

Mächtigkeit von Potenzmengen

Aufgabe: Wie viele Teilmengen hat die Menge $X = \{0, 1, \dots, 9\}$?

Lösung: Die Menge X hat genau $2^{10} = 1024$ verschiedene Teilmengen.

Übung: Konstruieren Sie, etwa im obigen Beispiel für $n = 10$, explizit eine Abzählung $\mu : \{0, \dots, 2^n - 1\} \xrightarrow{\sim} \mathfrak{P}(\{0, \dots, n-1\})$.

Aufgabe: Wie viele Relationen gibt es zwischen $X = \{1, 2, 3\}$ und $Y = \{0, 1, \dots, 99\}$? Wie viele davon sind Funktionen?

Lösung: Relation bedeutet $F \subseteq X \times Y$, also $F \in \mathfrak{P}(X \times Y)$:

$$\sharp\mathfrak{P}(X \times Y) = 2^{3 \cdot 100} = 1024^{30} \approx 10^{90}$$

Funktion bedeutet zudem linkstotal und rechtseindeutig:

$$\sharp \operatorname{Abb}(X, Y) = 100^3 = 10^6$$

☺ Relationen gibt es hier bereits astronomisch viele.
Funktionen sind etwas besonderes und deutlich rarer.

Rechenregeln für Mengen, konkret und vertraut

Die Rechenregeln für Mengen sind wunderbar konkret und praktisch:

$$\begin{aligned} X \sqcup \emptyset = X = \emptyset \sqcup X, &\qquad X \cup \emptyset = X = \emptyset \cup X, \\ X \sqcup Y = Y \sqcup X, &\qquad X \cup Y = Y \cup X, \\ (X \sqcup Y) \sqcup Z = X \sqcup (Y \sqcup Z), &\qquad (X \cup Y) \cup Z = X \cup (Y \cup Z). \end{aligned}$$

Das kartesische Produkt ist distributiv über die (disjunkte) Vereinigung:

$$\begin{aligned} X \times (Y \sqcup Z) = (X \times Y) \sqcup (X \times Z) &\qquad \text{ebenso für } \cup \text{ und } \cap \\ (X \sqcup Y) \times Z = (X \times Z) \sqcup (Y \times Z) &\qquad \text{ebenso für } \cup \text{ und } \cap \end{aligned}$$

Für kartesische Produkte haben wir folgende kanonische Bijektionen:

$$\begin{aligned} X \times \{a\} \cong X \cong \{a\} \times X, &\qquad (x, a) \leftrightarrow x \leftrightarrow (a, x) \\ X \times Y \cong Y \times X, &\qquad (x, y) \leftrightarrow (y, x) \\ (X \times Y) \times Z \cong X \times (Y \times Z), &\qquad ((x, y), z) \leftrightarrow (x, (y, z)) \end{aligned}$$

Schließlich gelten die vertrauten Potenzgesetze:

$$\begin{aligned} Z^{(X \sqcup Y)} \cong Z^X \times Z^Y, &\quad f \mapsto (\, f|_X,\, f|_Y \,) \\ (X \times Y)^Z \cong X^Z \times Y^Z, &\quad f \mapsto (\, \mathrm{pr}_1 \circ f,\, \mathrm{pr}_2 \circ f \,) \end{aligned}$$

Rechenregeln für Mengen, konkret und vertraut

☺ Die ersten acht Rechenregeln sind sofort klar, explizit und konkret.

Daraus folgen (erneut) die entsprechenden Rechenregeln für die natürlichen Zahlen. Der Nachweis per vollständiger Induktion ist länglich, die geometrische Realisierung ist dagegen anschaulich und konkret. Das nährt die Einsicht: Mengen sind konkret, Zahlen sind abstrakt.

Genauso wurde es Ihnen vermutlich in der Grundschule erklärt, ohne Bijektionen und Beweise. Jetzt verstehen Sie den Zusammenhang, Sie können nun Definitionen und Argumente präzise formulieren. So gesehen ist dies Schulmathematik vom höheren Stanndpunkt.

Die Bijektion $Z^{(X \sqcup Y)} \cong Z^X \times Z^Y$ entsteht aus $f \mapsto (f|_X, f|_Y)$ und umgekehrt $(g, h) \mapsto f = g \sqcup h$, also ausgeschrieben wie in Satz D2E:

$$f = g \sqcup h \,:\, X \sqcup Y \to Z \,:\, f(u) = \begin{cases} g(u) & \text{falls } u \in X, \\ h(u) & \text{falls } u \in Y. \end{cases}$$

Die Bijektion $(X \times Y)^Z \cong X^Z \times Y^Z$ entsteht aus $f \mapsto (\mathrm{pr}_1 \circ f, \mathrm{pr}_2 \circ f)$ und umgekehrt $(g, h) \mapsto f$ mit $f : Z \to X \times Y : f(x) = (g(x), h(x))$.

Anzahl der Abbildungen, Injektionen und Bijektionen

Satz E2H: Anzahl der Abbildungen, Injektionen und Bijektionen

Für je zwei Mengen X, Y mit $\sharp X = k$ und $\sharp Y = n$ gilt:

$$\boxed{\sharp\,\mathrm{Abb}(X,Y) = n^k}$$

Die Anzahl der injektiven Abbildungen ist (dank Satz E1F):

$$\boxed{\sharp\,\mathrm{Inj}(X,Y) = n\cdot(n-1)\cdots(n-k+1) \quad =: n^{\underline{k}}}$$

Im Spezialfall $k = n$ erhalten wir demnach

$$\boxed{\sharp\,\mathrm{Abb}(X,Y) = n^n}$$

sowie die Anzahl der Bijektionen:

$$\boxed{\sharp\,\mathrm{Bij}(X,Y) = n\cdot(n-1)\cdots 3\cdot 2\cdot 1 \quad = n^{\underline{n}} =: n!}$$

Die symmetrische Gruppe $\mathrm{S}_n = \mathrm{Aut}(\{1,\ldots,n\})$ hat $n!$ Elemente.

Anzahl der Abbildungen, Injektionen und Bijektionen

Anschaulich ist das plausibel. Die formale Abzählung gelingt mit E1F:

Beweis: Dank Sortierung zur Stufenform (E1F) haben wir die Bijektion $\{1,\ldots,n\}\times\{2,\ldots,n\}\times\cdots\times\{k,\ldots,n\} \xrightarrow{\sim} \mathrm{Inj}(\{1,\ldots,k\},\{1,\ldots,n\})$ mit der Zuordnung $(i_1,i_2,\ldots,i_k) \mapsto f = (1,i_1)\circ(2,i_2)\circ\cdots\circ(k,i_k)\circ\iota$. Daraus erhalten wie wunderbar direkt und explizit die Anzahl! QED

Es ist oft lehrreich, neu definierte Objekte zu zählen. Dies zwingt dazu, die Definition genau zu verstehen und klärt so Missverständnisse auf.
Defendit numerus. [Die Zahl gibt Schutz.] Juvenal (58–138 n.Chr.), *Satiren*

🙂 Nochmal zur Betonung: Abzählung E1D verlangt eine Bijektion, also sollten wir eine möglichst konkrete Bijektion vorweisen können. Die Mengen $\{1,\ldots,n\}$ sind das Urmeter, der universelle Maßstab, mit dem wir die Größe einer beliebigen endlichen Menge messen.

🙂 Die Nummerierung erlaubt direkten Zugriff auf alle Elemente. Sie wissen, wie viele es gibt, und sie können jedes adressieren. So generieren Sie eine gleichverteilt zufällige Injektion / Bijektion.

Illustration zu Permutationen

Ich schreibe Permutationen kurz und bequem in Listennotation:

$$\left[\begin{smallmatrix}1 & 2 & \ldots & n\\ a_1 & a_2 & \ldots & a_n\end{smallmatrix}\right] = [a_1, a_2, \ldots, a_n]$$

Permutationen der Menge $\{1,2\}$:

$$[1,2],\ [2,1]$$

Permutationen der Menge $\{1,2,3\}$:

$$[1,2,3],\ [1,3,2],\ [2,1,3],\ [2,3,1],\ [3,1,2],\ [3,2,1]$$

Permutationen der Menge $\{1,2,3,4\}$:

$$[1,2,3,4],\ [1,2,4,3],\ [1,3,2,4],\ [1,3,4,2],\ [1,4,2,3],\ [1,4,3,2],$$
$$[2,1,3,4],\ [2,1,4,3],\ [2,3,1,4],\ [2,3,4,1],\ [2,4,1,3],\ [2,4,3,1],$$
$$[3,1,2,4],\ [3,1,4,2],\ [3,2,1,4],\ [3,2,4,1],\ [3,4,1,2],\ [3,4,2,1],$$
$$[4,1,2,3],\ [4,1,3,2],\ [4,2,1,3],\ [4,2,3,1],\ [4,3,1,2],\ [4,3,2,1]$$

Illustration zur Fakultät

Rekursionsformel: $0! = 1$ und $(n+1)! = n!\cdot(n+1)$.
Ausgeschrieben: $n! = 1\cdot 2\cdot 3\cdots n$. Die ersten Werte sind:

$0! = 1$	$7! = 5\,040$	$14! = 87\,178\,291\,200$
$1! = 1$	$8! = 40\,320$	$15! = 1\,307\,674\,368\,000$
$2! = 2$	$9! = 362\,880$	$16! = 20\,922\,789\,888\,000$
$3! = 6$	$10! = 3\,628\,800$	$17! = 355\,687\,428\,096\,000$
$4! = 24$	$11! = 39\,916\,800$	$18! = 6\,402\,373\,705\,728\,000$
$5! = 120$	$12! = 479\,001\,600$	$19! = 121\,645\,100\,408\,832\,000$
$6! = 720$	$13! = 6\,227\,020\,800$	$20! = 2\,432\,902\,008\,176\,640\,000$

Die **Stirling–Formel** bietet eine gute Näherung für große n:

$$\boxed{n! \sim \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n}$$

Diese Näherung werden Sie in der Analysis ausführlich behandeln, sowie viele weitere nützliche Approximationen und Grenzwerte.

Binomialkoeffizienten: Definition

Für $z \in \mathbb{C}$ und $k \in \mathbb{N}$ definieren wir den **Binomialkoeffizienten**

$$\binom{z}{k} := \frac{z(z-1)\cdots(z-k+1)}{k\cdot(k-1)\cdots 1} = \prod_{j=0}^{k-1} \frac{z-j}{k-j} = \frac{z^{\underline{k}}}{k!}$$

Speziell für natürliche Zahlen $n \in \mathbb{N}$ und $0 \le k \le n$ gilt:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$$

Aus der Definition folgt sofort:

$$\binom{z+1}{k+1} = \binom{z}{k}\frac{z+1}{k+1} \qquad \text{und} \qquad \binom{z}{k+1} = \binom{z}{k}\frac{z-k}{k+1}$$

Daraus erhalten wir **Pascals Rekursionsformel**:

$$\binom{z+1}{k+1} = \binom{z}{k} + \binom{z}{k+1}$$

Binomialkoeffizienten: Rekursion

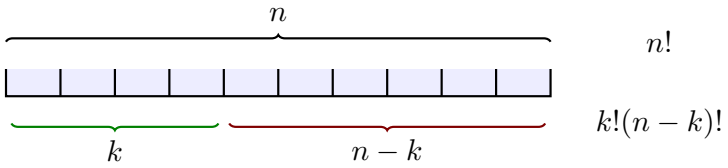
Hieraus erhalten wir das **Pascal–Dreieck für Binomialkoeffizienten**:

$\binom{n}{k}$	k=0	1	2	3	4	5	6	7	8	9	10
n=0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

Binomialkoeffizienten: Interpretation

Auf wie viele Arten können wir aus n Objekten genau k auswählen?



$n!$

$k!(n-k)!$

Die Gesamtzahl der Möglichkeiten ist

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Kombinatorische Herleitung: Wir können alle n Elemente auf $n!$ Arten anordnen. Bei jeder Anordnung wählen wir die ersten k Elemente aus. Die ersten k Elemente dürfen wir dabei auf $k!$ Arten beliebig umordnen. Die letzten $n-k$ Elemente dürfen wir auf $(n-k)!$ Arten umordnen. Die Auswahl ändert sich hierdurch nicht. Dies liefert die obige Formel.

Aufgabe: Zeigen Sie diese Aussage durch Induktion über n.
Der folgende Beweis führt dies sorgsam aus.

Binomialkoeffizienten: Interpretation

Satz E2ı: Teilmengen und Binomialkoeffizient

Wir betrachten eine Menge X und ihre k–elementigen Teilmengen:

$$\binom{X}{k} = \mathfrak{P}_k(X) := \{\, A \subseteq X \mid \sharp A = k \,\}$$

Ist X endlich, so auch $\binom{X}{k}$, und es gilt:

$$\sharp\binom{X}{k} = \binom{\sharp X}{k}$$

Beweis: Wir führen Induktion über die Anzahl $n = \sharp X$ der Elemente. Der Induktionsanfang $n = 0$ ist klar; sei also $n \ge 1$. Hier ist $k = 0$ klar; sei also auch $k \ge 1$. Wir wählen $z \in X$. Für $U = X \smallsetminus \{z\}$ gilt dann:

$$\tbinom{X}{k} = \tbinom{U}{k} \sqcup \{\, A \cup \{z\} \mid A \in \tbinom{U}{k-1} \,\} \cong \tbinom{U}{k} \sqcup \tbinom{U}{k-1}$$

Dank $\sharp U = n-1$ können wir die Induktionsvoraussetzung anwenden:

$$\sharp\tbinom{X}{k} = \tbinom{n-1}{k} + \tbinom{n-1}{k-1} = \tbinom{n}{k}$$

Der binomische Lehrsatz

Beispiele: Für je zwei reelle Zahlen $a, b \in \mathbb{R}$ gilt:

$$(a+b)^0 = \mathbf{1}$$
$$(a+b)^1 = \mathbf{1}\cdot a + \mathbf{1}\cdot b$$
$$(a+b)^2 = \mathbf{1}\cdot a^2 + \mathbf{2}\cdot ab + \mathbf{1}\cdot b^2$$
$$(a+b)^3 = \mathbf{1}\cdot a^3 + \mathbf{3}\cdot a^2b + \mathbf{3}\cdot ab^2 + \mathbf{1}\cdot b^3$$
$$(a+b)^4 = \mathbf{1}\cdot a^4 + \mathbf{4}\cdot a^3b + \mathbf{6}\cdot a^2b^2 + \mathbf{4}\cdot ab^3 + \mathbf{1}\cdot b^4$$
$$(a+b)^5 = \mathbf{1}\cdot a^5 + \mathbf{5}\cdot a^4b + \mathbf{10}\cdot a^3b^2 + \mathbf{10}\cdot a^2b^3 + \mathbf{5}\cdot a^1b^4 + \mathbf{1}\cdot b^5$$

☺ Der Koeffizient vor $a^k b^{n-k}$ ist genau der Binomialkoeffizient $\binom{n}{k}$.

Den ersten interessanten Fall $n = 2$ kennen Sie als „erste binomische Formel“ aus der Schule. Diese nützliche Rechenregel gilt für alle $n \in \mathbb{N}$: Das ist die Aussage des binomischen Lehrsatzes. Er gilt in jedem Ring, sogar Halbring, solange die beiden Elemente kommutieren: $ab = ba$.

Übung: Beweisen Sie diesen Satz per Induktion über n. Dabei wird das Induktionsargument des vorigen Beweises auf Summen angewendet.

Der binomische Lehrsatz

Satz E2J: der binomische Lehrsatz

Sei $(R, +, \cdot)$ ein Halbring und $a, b \in R$ mit $ab = ba$. Für alle $n \in \mathbb{N}$ gilt:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j$$

Beweis: Wir sammeln alle Terme $a^k b^{n-k}$ des n–fachen Produkts

$$(a+b)(a+b)\cdots(a+b).$$

Der Koeffizient vor dem Term $a^k b^{n-k}$ ist die Anzahl $\binom{n}{k}$. QED

☺ Speziell für $a = b = 1$ in $\mathbb{N}$ erhalten wir:

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \quad \text{entsprechend} \quad \mathfrak{P}(\{1,\dots,n\}) = \bigsqcup_{k=0}^{n} \mathfrak{P}_k(\{1,\dots,n\})$$

Speziell für $(a, b) = (p, 1-p)$ in $\mathbb{R}_{\geq 0}$ erhalten wir die Binomialverteilung

$$B(n,p)(k) = \binom{n}{k} p^k (1-p)^{n-k} \quad \text{mit} \quad \sum_{k=0}^{n} B(n,p)(k) = 1.$$

Nützliche Gleichungen für Binomialkoeffizienten

Der binomische Lehrsatz E2J liefert uns algebraisch die Gleichung $2^n = \sum_{k=0}^{n} \binom{n}{k}$ für alle $n \in \mathbb{N}$. Diese können wir konkret für Mengen realisieren und ablesen: $\mathfrak{P}(\{1,\dots,n\}) = \bigsqcup_{k=0}^{n} \mathfrak{P}_k(\{1,\dots,n\})$.

Aufgabe: (0) Erklären Sie die Symmetrie $\binom{n}{k} = \binom{n}{n-k}$ der Binomialkoeffizienten durch eine geeignete Bijektion.

(1) Zeigen Sie die folgende **Vandermonde–Identität**, indem Sie sie durch geeignete Mengen konkret darstellen:

$$\sum_{k=0}^{\ell} \binom{m}{k}\binom{n}{\ell-k} = \binom{m+n}{\ell}, \qquad \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

Lösung: (0) Sei X eine n–elementige Menge. Das Komplement $\complement : \mathfrak{P}(X) \to \mathfrak{P}(X) : A \mapsto X \smallsetminus A$ bildet k–elementige Teilmengen auf $(n-k)$–elementige Teilmengen ab. Dank $\complement \circ \complement = \mathrm{id}$ erhalten wir:

$$(\complement, \complement) \,:\, \binom{X}{k} \cong \binom{X}{n-k}$$

Nützliche Gleichungen für Binomialkoeffizienten

(1) Wir betrachten $X = \{1,\dots,m\}$ und $Y = \{m+1,\dots,m+n\}$.
Für die ℓ–elementigen Teilmengen von $Z = X \sqcup Y$ gilt dann:

$$\binom{Z}{\ell} = \bigsqcup_{k=0}^{\ell} \left\{ A \sqcup B \;\middle|\; A \in \binom{X}{k}, B \in \binom{Y}{\ell-k} \right\} \cong \bigsqcup_{k=0}^{\ell} \binom{X}{k} \times \binom{Y}{\ell-k}$$

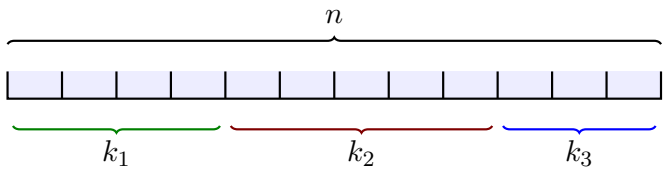
Die Bijektion „$\cong$“ schickt $C \in \binom{Z}{\ell}$ auf $(C \cap X, C \cap Y) \in \binom{X}{k} \times \binom{Y}{\ell-k}$ und umgekehrt $(A, B) \in \binom{X}{k} \times \binom{Y}{\ell-k}$ zurück auf $A \sqcup B \in \binom{Z}{\ell}$.

(2) Die zweite Gleichung folgt als Spezialfall für $n = m = \ell$.
Hierbei nutzen wir $\binom{n}{n-k} = \binom{n}{k}$, siehe (0).

☺ In manchen Fällen sind Zahlen einfacher: Wir begnügen uns dann mit der Anzahl der Elemente und vernachlässigen die Menge selbst. In anderen Fällen ist die dahinterliegende Menge einfacher oder informativer, dann lohnt es sich, die reichere Struktur zu nutzen.

Multinomialkoeffizienten

Auf wie viele Arten können wir n Objekte in ℓ Mengen zu $k_1, \ldots, k_\ell$ Elementen aufteilen? Hierbei sei $k_1, \ldots, k_\ell \geq 0$ und $k_1 + \cdots + k_\ell = n$.



Die Gesamtzahl der Möglichkeiten ist

$$\binom{n}{k_1, k_2, \ldots, k_\ell} := \frac{n!}{k_1! \cdot k_2! \cdots k_\ell!}.$$

Kombinatorische Herleitung: Wir können alle n Elemente auf $n!$ Arten anordnen. Die ersten k_1 bilden die erste Menge, die nächsten k_2 bilden die zweite Menge, usw. Innerhalb der $i$ten Menge können wir jeweils auf $k_i!$ Arten beliebig umordnen. Dies liefert die obige Formel.

Anwendungsbeispiele

Aufgabe: Wie viele Kartenverteilungen gibt es beim Skat?

Lösung: Von 32 Karten bekommt jeder der drei Spieler 10 Karten:

$$\binom{32}{10, 10, 10, 2} = \frac{32!}{10!\,10!\,10!\,2!} \approx 2.75 \cdot 10^{15}$$

Aufgabe: Auf wie viele Weisen lassen sich 12 (verschiedenfarbige) Bonbons gerecht unter zwei / drei / vier / zwölf Kindern aufteilen?

Lösung: Die Anzahl der möglichen Aufteilungen berechnen wir zu:

$$\begin{aligned}
\binom{12}{6,6} &= \frac{12!}{6!\,6!} &&= 924\\
\binom{12}{4,4,4} &= \frac{12!}{4!\,4!\,4!} &&= 34650\\
\binom{12}{3,3,3,3} &= \frac{12!}{3!\,3!\,3!\,3!} &&= 369600\\
\binom{12}{1,1,1,1,1,1,1,1,1,1,1,1} &= 12! &&= 479001600
\end{aligned}$$

Anwendungsbeispiele: Laplace–Experimente

Aufgabe: Wie wahrscheinlich ist es, bei 10 Münzwürfen genau 7 mal Kopf und 3 mal Zahl zu erhalten?

$$\begin{aligned}
\Omega &= \{0,1\}^{10}, & |\Omega| &= 2^{10} &&= 1024\\
A &= \left\{\begin{matrix}\text{Ergebnisse } \omega \in \Omega \text{ mit}\\ \omega_1 + \cdots + \omega_{10} = 3\end{matrix}\right\}, & |A| &= \binom{10}{7,3} &&= 120\\
& & \mathbf{P}(A) &= |A|/|\Omega| &&\approx 0.117
\end{aligned}$$

Aufgabe: Wie wahrscheinlich ist es, bei 10maligem Würfeln, die Augenzahlen $1, 2, 3, 4, 5, 6$ mit Häufigkeit $1, 2, 3, 3, 0, 1$ zu erhalten?

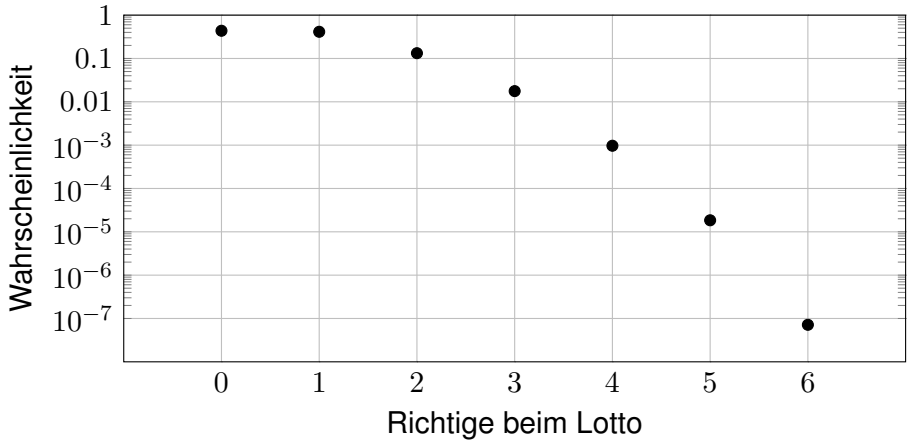
$$\begin{aligned}
\Omega &= \{1,2,3,4,5,6\}^{10}, & |\Omega| &= 6^{10} &&= 60\,466\,176\\
A &= \left\{\begin{matrix}\text{Ergebnisse } \omega \in \Omega \text{ mit}\\ \text{diesen Häufigkeiten}\end{matrix}\right\}, & |A| &= \binom{10}{1,2,3,3,0,1} &&= 50\,400\\
& & \mathbf{P}(A) &= |A|/|\Omega| &&\approx 0.00083
\end{aligned}$$

Anwendungsbeispiele: Lotto und zufällige Stichprobe

Aufgabe: Mit welcher Wkt haben Sie k Richtige beim Lotto „6 aus 49“?

Lösung: Von $N = 49$ Zahlen sind $K = 6$ Treffer. Ein Tipp wählt $n = 6$ der 49 Zahlen aus. Die Wkt für genau k Treffer ist demnach:

$$p(k) = H(N, K, n)(p) = \binom{K}{k}\binom{N-K}{n-k} \Big/ \binom{N}{n}.$$



Zerlegungen aka Partitionen

E241

Eine **Zerlegung** von X ist ein Mengensystem $Q \subseteq \mathfrak{P}(X)^*$ mit $X = \bigsqcup Q$.

Beispiele: Die Menge $\{1\}$ erlaubt nur eine Zerlegung, nämlich $\{\{1\}\}$.
Die Menge $\{1,2\}$ erlaubt zwei Zerlegungen: $\{\{1,2\}\}$ und $\{\{1\},\{2\}\}$.
Die Menge $\{1,2,3\}$ erlaubt die folgenden fünf Zerlegungen:

$$\{\{1,2,3\}\},\ \{\{1\},\{2,3\}\},\ \{\{1,2\},\{3\}\},\ \{\{1,3\},\{2\}\},\ \{\{1\},\{2\},\{3\}\}.$$

Die Menge $\{1,2,3,4\}$ erlaubt die folgenden fünfzehn Zerlegungen:

$$\{\{1,2,3,4\}\},$$
$$\{\{1,2\},\{3,4\}\},\ \{\{1,3\},\{2,4\}\},\ \{\{1,4\},\{2,3\}\},$$
$$\{\{1\},\{2,3,4\}\},\ \{\{2\},\{1,3,4\}\},\ \{\{3\},\{1,2,4\}\},\ \{\{4\},\{1,2,3\}\},$$
$$\{\{1,2\},\{3\},\{4\}\},\ \{\{1,3\},\{2\},\{4\}\},\ \{\{1,4\},\{2\},\{3\}\},$$
$$\{\{2,3\},\{1\},\{4\}\},\ \{\{2,4\},\{1\},\{3\}\},\ \{\{3,4\},\{1\},\{2\}\},$$
$$\{\{1\},\{2\},\{3\},\{4\}\}.$$

Zerlegungen: rekursiv aufbauen

E242
Erläuterung

Für Zerlegungen gibt es ein raffiniert rekursives Konstruktionsverfahren!
Jede k–Zerlegung von $\{1,\dots,n\}$ erhalten wir auf eine von zwei Arten:

- Wir nehmen eine $(k-1)$–Zerlegung P von $\{1,\dots,n-1\}$ und fügen ihr die neue Klasse $\{n\}$ hinzu: So erhalten wir $Q = P \cup \{\{n\}\}$.
- Wir nehmen eine k–Zerlegung P von $\{1,\dots,n-1\}$ und fügen einer Klasse $C \in P$ das Element n hinzu: $Q = (P \setminus \{C\}) \cup \{C \cup \{n\}\}$.

Übung: Führen Sie dies für die 3–Zerlegungen von $\{1,\dots,4\}$ aus, zur Illustration ebenso für alle weiteren Zerlegungen von $\{1,\dots,4\}$.

Wenn Sie Freude an dieser Rekursion haben, dann können Sie so systematisch alle Zerlegungen von $\{1,\dots,5\}$ konstruieren.
Zur Kontrolle haben Sie die folgende Tabelle der Stirling–Zahlen.

Wenn Sie Freude an der Programmierung haben, dann können Sie diese Rekursion auch direkt in ein Computerprogramm umsetzen.

Zerlegungen: rekursiv aufbauen

E243

Satz E2K: Zerlegungen und Stirling–Zahlen

Wir betrachten eine Menge X und ihre k–elementigen Zerlegungen:

$$\left\{ X \atop k \right\} := \left\{ Q \subseteq \mathfrak{P}(X)^* \;\middle|\; X = \bigsqcup Q \text{ Zerlegung mit } \sharp Q = k \right\}$$

Ist X endlich mit $\sharp X = n$, so definieren wir die **Stirling–Zahl**

$$\left\{ n \atop k \right\} := \sharp \left\{ X \atop k \right\}.$$

Für $n \geq 1$ gilt $\left\{ n \atop 1 \right\} = \left\{ n \atop n \right\} = 1$ sowie $\left\{ n \atop 0 \right\} = \left\{ n \atop k \right\} = 0$ für alle $k > n$.
Die weiteren Werte erhalten wir dank folgender Rekursionsformel:

$$\boxed{\left\{ n \atop k \right\} = \left\{ n-1 \atop k-1 \right\} + k \left\{ n-1 \atop k \right\}}$$

Beweis: Für $\sharp X = n \geq 1$ wählen wir $z \in X$ und setzen $U = X \setminus \{z\}$:

$$\left\{ X \atop k \right\} = \left\{ Q \in \left\{ X \atop k \right\} \;\middle|\; \{z\} \in Q \right\} \sqcup \left\{ Q \in \left\{ X \atop k \right\} \;\middle|\; \{z\} \notin Q \right\} \cong \left\{ U \atop k-1 \right\} \sqcup k \left\{ U \atop k \right\}$$

Zerlegungen: rekursiv aufbauen

E244
Erläuterung

Die abkürzende Schreibweise dieser Bijektion bedarf der Erläuterung.

Die Bezeichnung „$k\left\{ U \atop k \right\}$“ ist leider etwas verwickelt: Wir nehmen eine k–Zerlegung P von U, fügen einer Klasse $C \in P$ das Element z hinzu und erhalten $Q = (P \setminus \{C\}) \cup \{C \cup \{z\}\}$. Hierbei haben wir k mögliche Wahlen von C. Die hierzu benötigten Daten sind daher:

$$k \left\{ U \atop k \right\} := \left\{ (P, C) \;\middle|\; C \in P \in \left\{ U \atop k \right\} \right\}$$

Wir betrachten also Zerlegungen P mit einer markierten Klasse $C \in P$. Jede k–Zerlegung P erlaubt k Markierungen $C \in P$. Hierzu gehört die Abbildung $k\left\{ U \atop k \right\} \to \left\{ U \atop k \right\} : (P, C) \mapsto P$. Über jeder Zerlegung P liegen die k möglichen Wahlen (P, C) als Elemente der Faser. Wir erhalten somit

$$\left\{ X \atop k \right\} \cong \left\{ U \atop k-1 \right\} \sqcup k \left\{ U \atop k \right\}$$

wie gewünscht mit der Elementezahl $\sharp k\left\{ U \atop k \right\} = k \cdot \sharp \left\{ U \atop k \right\}$.

Übung: Schreiben Sie diese Bijektion nun explizit aus.

Zerlegungszahlen nach Stirling

Hieraus erhalten wir das **Stirling–Dreieck für Zerlegungszahlen**:

$\left\{{n \atop k}\right\}$	$k{=}1$	2	3	4	5	6	7	8	9	10
$n{=}1$	1									
2	1	1								
3	1	3	1							
4	1	7	6	1						
5	1	15	25	10	1					
6	1	31	90	65	15	1				
7	1	63	301	350	140	21	1			
8	1	127	966	1701	1050	266	28	1		
9	1	255	3025	7770	6951	2646	462	36	1	
10	1	511	9330	34105	42525	22827	5880	750	45	1

$$\left\{{n \atop k}\right\} = \left\{{n-1 \atop k-1}\right\} + k\left\{{n-1 \atop k}\right\}$$

Diese Werte heißen **Stirling–Zahlen zweiter Art**. Es gibt daneben auch die Stirling–Zahlen erster Art, die wir hier nicht betrachten.

Zerlegungszahlen nach Stirling

☺ Die ersten vier Zeilen entsprechen den Anzahlen der Zerlegungen, die wir eingangs auf Seite E241 explizit ausgeschrieben haben. Wenn Sie nun alle Zerlegungen von $\{1,2,3,4,5\}$ auflisten möchten, dann können Sie zumindest deren Anzahl mit der Tabelle prüfen.

☺ Die erste Spalte $\left\{{n \atop 1}\right\} = 1$ und die Diagonale $\left\{{n \atop n}\right\} = 1$ sind klar: Für jede n–elementige Menge $X = \{x_1, \ldots, x_n\}$ haben wir genau eine 1–Zerlegung, nämlich $\{\{x_1, \ldots, x_n\}\}$, und genau eine n–Zerlegung, nämlich $\{\{x_1\}, \ldots, \{x_n\}\}$. Das ist bei der Rekursion hilfreich.

☺ Die erste Nebendiagonale $\left\{{n \atop n-1}\right\} = \binom{n}{2}$ ist leicht zu verstehen: Wir zerlegen X in $n-1$ Klassen, gemäß $\{\{x_1, x_2\}, \{x_3\}, \ldots, \{x_n\}\}$. Das bedeutet, genau zwei Elemente liegen in einer gemeinsamen Klasse, alle anderen Elemente sind jeweils allein in ihrer Klasse.

☺ In der zweiten Spalte gilt $\left\{{n \atop 2}\right\} = (2^n - 2)/2 = 2^{n-1} - 1$: Jede Zerlegung $\{A, B\}$ entspricht $A \in \mathfrak{P}(X) \setminus \{\emptyset, X\}$ und $B = X \setminus A$. Die weiteren Zerlegungszahlen sind nicht so einfach zu erklären. Zum Glück haben wir die obige Rekursion, damit gelingt es!

Zerlegungszahlen nach Stirling

☺ Für die Binomialkoeffizienten haben wir eine geschlossene Formel:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Daraus haben wir Pascals Rekursionsformel abgeleitet und Pascals Dreieck erhalten. Sie nützt ebenso in zahlreichen weiteren Rechnungen und wird Ihnen auch in den Übungen immer wieder begegnen.

Für die Stirling–Zahlen $\left\{{n \atop k}\right\}$ hingegen haben wir keine ebenso schöne, geschlossene Formel, sondern nur die Rekursionsformel aus Satz E2K. Das genügt immerhin für unsere ersten Rechnungen und Beispiele. Die kleinen Werte haben wir im Stirling–Dreieck tabelliert.

Binomialkoeffizienten und Stirling–Zahlen und weitere kombinatorische Koeffizienten kommen in vielen, sehr unterschiedlichen Kontexten vor. Daher gibt es eine ausgedehnte Literatur zu nützlichen Formeln, Identitäten und Näherungen. Das ist beruhigend zu wissen.

Zerlegungszahlen nach Stirling

☺ Die Rekursion gilt nicht nur für die Anzahlen, auch für die Mengen!

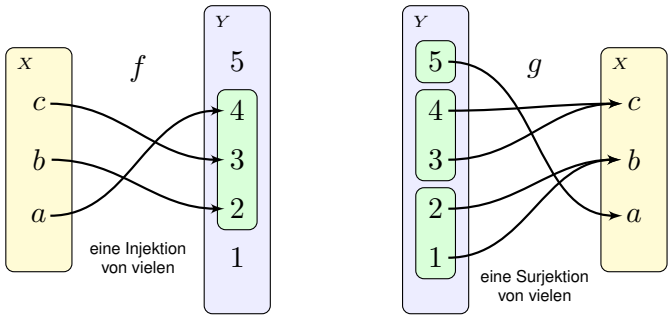
Sie können so alle Zerlegungen explizit generieren. Solche konkreten Konstruktionen sind eine wunderbare Programmierübung. Mehr dazu finden Sie im monumentalen Werk von Donald E. Knuth: *The Art of Computer Programming*, vol. 4A, §7.2.1.5 Generating all set partitions.

Wenn Sie sich ernsthaft für die Programmierung und langfristig auch für effiziente Algorithmen interessieren, dann sollten Sie unbedingt diese Bibel der Programmierkunst konsultieren. Keine leichte Kost, sondern ein nie versiegender Quell nahrhafter Erkenntnis.

Fun fact: Für seine TAOCP-Bücher erschuf Knuth das Textsatzsystem TEX, mit dem heute alle Welt (natur)wissenschaftliche Texte schreibt, und mit dem auch dieses Dokument für Sie erstellt wurde.

Injektionen und Surjektionen: Zusammenfassung

Als kleines Beispiel zur Illustration betrachten wir eine 3–elementige Menge $X = \{a, b, c\}$ und eine 5–elementige Menge $Y = \{1, 2, 3, 4, 5\}$.



Aufgabe:
(1) Wie viele Injektionen $f : \{a, b, c\} \hookrightarrow \{1, 2, 3, 4, 5\}$ gibt es?
(2) Wie viele Surjektionen $g : \{1, 2, 3, 4, 5\} \twoheadrightarrow \{a, b, c\}$ gibt es?

Lösung:
(1) Es gibt genau $\binom{5}{3} \cdot 3! = 10 \cdot 6 = 60$ Injektionen.
(2) Es gibt genau $\left\{ {5 \atop 3} \right\} \cdot 3! = 25 \cdot 6 = 150$ Surjektionen.

Injektionen und Surjektionen: Zusammenfassung

☺ Das ist eine erste Anwendung der **kanonischen Faktorisierung**.
Die Aufteilung in kleinere, leichtere Teilprobleme ist allgemein nützlich.

Satz E2L: Anzahl der Injektionen und der Surjektionen

Für alle endlichen Mengen X, Y mit $\sharp X = k$ und $\sharp Y = n$ gilt:

$$\sharp \operatorname{Inj}(X, Y) = \sharp \{\, f : X \hookrightarrow Y \,\} = \binom{n}{k} \cdot k!$$

$$\sharp \operatorname{Sur}(Y, X) = \sharp \{\, f : Y \twoheadrightarrow X \,\} = \left\{ {n \atop k} \right\} \cdot k!$$

Im Spezialfall $k = n$ erhalten wir erneut $\sharp \operatorname{Bij}(X, Y) = \sharp \operatorname{Bij}(Y, X) = k!$.

Beweis: (1) Wir haben $\binom{n}{k}$ Wahlen der Bildmenge $B \in \binom{Y}{k}$.
Zu gegebenem B haben wir dann $k!$ Zuordnungen $X \xrightarrow{\sim} B$.

(2) Wir haben $\left\{ {n \atop k} \right\}$ Wahlen der Zerlegung $Q \in \left\{ {Y \atop k} \right\}$ in Fasern.
Zu gegebenem Q haben wir dann $k!$ Zuordnungen $Q \xrightarrow{\sim} X$. QED

Injektionen und Surjektionen: Zusammenfassung

Ich führe hier die zweite Konstruktion (2) noch etwas genauer aus.
Die nachfolgende Aufgabe zeigt ein einfaches, konkretes Beispiel.

Jede surjektive Abbildung $f : Y \twoheadrightarrow X$ definiert eine Zerlegung in Fasern:

$$Q = \left\{\, f^{-1}(\{x\}) \subseteq Y \;\middle|\; x \in X \,\right\} \subseteq \mathfrak{P}(Y)^*, \quad \bigsqcup Q = Y.$$

Hat X genau k Elemente, so erhalten wir eine Zerlegung mit $\sharp Q = k$.

Umgekehrt können wir aus einer Zerlegung Q in $k = \sharp Q$ Klassen eine Surjektion $f : Y \to X$ konstruieren, indem wir jede Klasse $C \in Q$ auf ein Element $x \in X$ abbilden. Hierzu gibt es genau $k!$ Möglichkeiten.

Warum? Damit $f : Y \to X$ surjektiv wird, muss auch die Zuordnung $f' : Q \to X$ surjektiv sein. Wegen $\sharp Q = \sharp X = k$ ist f' somit auch injektiv, also insgesamt bijektiv, kurz $f' : Q \xrightarrow{\sim} X$ (siehe Satz E1H).

☺ Unsere Werkzeuge ermöglichen das strukturierte Abzählen!
Ohne die abstrakte Methode sind die konkreten Zahlenbeispiele kaum zu lösen; mit dem passenden Satz an Werkzeugen ist es jedoch leicht.

Anwendungsbeispiel zu Surjektionen

Aufgabe: Als konkretes Beispiel sei $Y = \{1, 2, 3, 4\}$ und $X = \{a, b\}$.
(1) Nennen Sie alle Zerlegungen Q von Y in zwei Klassen.
(2) Nennen Sie alle Surjektionen $Y \twoheadrightarrow X$.
Bestimmen Sie zuerst (a) die Anzahlen und dann (b) die Objekte selbst.

Lösung: (1a) Dank Stirling–Dreieck finden wir die Anzahl $\left\{ {4 \atop 2} \right\} = 7$.

(1b) Die sieben Zerlegungen der Menge Y in zwei Klassen sind:

$$\{\{1,2\},\{3,4\}\},\ \{\{1,3\},\{2,4\}\},\ \{\{1,4\},\{2,3\}\},$$
$$\{\{1\},\{2,3,4\}\},\ \{\{2\},\{1,3,4\}\},\ \{\{3\},\{1,2,4\}\},\ \{\{4\},\{1,2,3\}\},$$

(2a) Wir erhalten $2! \left\{ {4 \atop 2} \right\} = 2 \cdot 7 = 14$ Surjektionen $Y \twoheadrightarrow X$.

(2b) Zu jeder Zerlegung $Q = \{A, B\}$ der Startmenge Y gehören genau zwei Surjektionen $f, g : Y \twoheadrightarrow X$ auf die Zielmenge X:

- eine erste mit $f^{-1}(\{a\}) = A$ und $f^{-1}(\{b\}) = B$,
- eine zweite mit $g^{-1}(\{a\}) = B$ und $g^{-1}(\{b\}) = A$.

☺ Damit können wir alle vierzehn Surjektionen explizit ausschreiben.

Anwendungsbeispiel: Schokokekse

Aufgabe: (Aus dem Mathekalender 2012) Sie backen $k = 100$ Kekse. Sie geben n Chocolate Chips zum Teig, verteilen diese gründlich zufällig und teilen dann den Teig in 100 Kekse. Wieviele Chips brauchen Sie, damit mit 90% Sicherheit jeder Keks mindestens einen Chip enthält?

Lösung: Die Wkt, dass kein Chip im $i$ten Keks landet, ist $(99/100)^n$. Das Gegenereignis $A_i = \{\text{In Keks } i \text{ ist mindestens ein Chip.}\}$ hat demnach die komplementäre Wahrscheinlichkeit $\mathbf{P}(A_i) = 1 - 0.99^n$.

(1) Näherung: Zur Vereinfachung rechnen wir zunächst, als wären die Ereignisse A_i unabhängig. (Das ist genau genommen nicht richtig, erweist sich anschließend aber als erstaunlich gute Näherung.)

Die gewünschte Bedingung vereinfacht sich dann zu:

$$f(n) := (1 - 0.99^n)^{100} \quad \overset{!}{\geq} \quad 0.9$$

Wir erhalten somit (mit Hilfe eines Taschenrechners):

$$n \geq \frac{\ln(1 - 0.9^{1/100})}{\ln 0.99} \approx 682.17$$

Anwendungsbeispiel: Schokokekse

(2) Exakt gibt es $k^n = 100^n$ Verteilungen der n Chips auf $k = 100$ Kekse. Darunter sind genau $k!\left\{ {n \atop k} \right\}$ mit mindestens einem Chip in jedem Keks.

Anders gesagt: Es gibt k^n Abbildungen $f : \{1, \ldots, n\} \to \{1, \ldots, k\}$, davon sind genau $k!\left\{ {n \atop k} \right\}$ surjektiv. Ein Hoch auf Satz E2L!

Die gewünschte Bedingung ist demnach:

$$g(n) := \frac{k!}{k^n} \left\{ {n \atop k} \right\} \quad \overset{!}{\geq} \quad 0.9$$

Ausrechnen für $n = 100, 101, 102, \ldots$ mit Hilfe eines Computers liefert:

$$g(682) = 0.899499\ldots, \qquad g(683) = 0.900455\ldots$$

🙂 Sie brauchen also tatsächlich 683 Chocolate Chips! Das rechtfertigt nachträglich die naive Näherung in der vereinfachten Rechnung (1).

Das erklärt noch nicht, warum diese Näherung so gut funktioniert, oder in welchen anderen Situationen Sie diesen Trick anwenden können. Hierzu ist zudem eine allgemeine Fehlerabschätzung notwendig.

Abbildungen mit vorgegebenem Rang

Aufgabe: (1) Wie viele Abbildungen $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3\}$ treffen genau zwei Bildpunkte, erfüllen also $\sharp\,\mathrm{im}(f) = 2$?

(2) Was gilt allgemein? Bestimmen Sie die Anzahl der Abbildungen $f : X = \{1, \ldots, k\} \to Y = \{1, \ldots, n\}$ vom Rang $r = \sharp\,\mathrm{im}(f)$.

Lösung: (2) Seien X, Y endliche Mengen mit $\sharp X = k$ und $\sharp Y = n$ sowie

$$\begin{aligned} \mathrm{Abb}(X,Y)_r &:= \{\, f : X \to Y \mid \sharp\,\mathrm{im}(f) = r \,\} \\ &\cong \{\, (Q, \bar{f}, B) \mid Q \in \left\{ {X \atop r} \right\},\ B \in \binom{Y}{r},\ \bar{f} : Q \xrightarrow{\sim} B \,\}. \end{aligned}$$

Jede Abbildung $f : X \to Y$ mit $\sharp\,\mathrm{im}(f) = r$ ist eindeutig bestimmt durch ihre Zerlegung $Q \in \left\{ {X \atop r} \right\}$ in Fasern und ihre Bildmenge $B \in \binom{Y}{r}$ sowie die induzierte Bijektion $\bar{f} : Q \xrightarrow{\sim} B$ zwischen beiden. Wir haben also:

$$\sharp\,\mathrm{Abb}(X,Y)_r = \sum_{Q \in \left\{ {X \atop r} \right\}} \sum_{B \in \binom{Y}{r}} \sharp\,\mathrm{Bij}(Q,B) = \left\{ {k \atop r} \right\} \cdot \binom{n}{r} \cdot r!$$

(1) Für $(k, n, r) = (5, 3, 2)$ finden wir $\left\{ {5 \atop 2} \right\} = 15$ und $\binom{3}{2} = 3$ und $2! = 2$, also insgesamt $\sharp\,\mathrm{Abb}(\{1,2,3,4,5\}, \{1,2,3\})_2 = 15 \cdot 3 \cdot 2 = 90$.

Abbildungen mit vorgegebenem Rang

Zusammenfassend erhalten wir den folgenden schönen Satz:

Satz E2M: Anzahl der Abbildungen mit vorgegebenem Rang

Seien X, Y endliche Mengen mit $\sharp X = k$ und $\sharp Y = n$ Elementen sowie

$$\mathrm{Abb}(X,Y)_r := \{\, f : X \to Y \mid \sharp\,\mathrm{im}(f) = r \,\}.$$

Für jeden Rang $r \in \mathbb{N}$ haben wir:

$$\sharp\,\mathrm{Abb}(X,Y)_r = \left\{ {k \atop r} \right\} \cdot \binom{n}{r} \cdot r!$$

Im Spezialfall $r = k$ erhalten wir $\sharp\,\mathrm{Inj}(X,Y) = \binom{n}{r} \cdot r!$.
Im Spezialfall $r = n$ erhalten wir $\sharp\,\mathrm{Sur}(X,Y) = \left\{ {k \atop r} \right\} \cdot r!$.
Im Spezialfall $r = k = n$ erhalten wir $\sharp\,\mathrm{Bij}(X,Y) = r!$.

Beweis: Wir strukturieren die Menge $\mathrm{Abb}(X,Y)_r$ wie in der vorigen Aufgabe ausgeführt und gewinnen daraus die ersehnte Abzählung. QED

🙂 Diese allgemeine Technik perfektionieren wir durch die kanonische Faktorisierung E3I in Quotient-Bijektion-Inklusion $X \twoheadrightarrow Q \xrightarrow{\sim} B \hookrightarrow Y$.

Zerlegung und Quotient

E301

Beispiel: Sei $X = \{1,2,3,4,5,6,7\}$ und $Q = \{\{1,4\},\{2,3,6,7\},\{5\}\}$.

Definition E3A: Zerlegung und Quotient

Sei X eine Menge. Eine **Zerlegung** Q von X ist ein Mengensystem $Q \subseteq \mathfrak{P}(X)^*$ mit $X = \bigsqcup Q$. Explizit ausgeschrieben bedeutet das:

$$\bigcup Q = X \quad \wedge \quad \forall A, B \in Q : A = B \;\dot\vee\; A \cap B = \emptyset$$

Jedes Element $C \in Q$ nennen wir eine **Klasse** von Q, oft auch **Äquivalenzklasse**, je nach Kontext auch **Bahn** oder **Orbit**.

Jedes Element $x \in X$ liegt demnach in genau einer Klasse $C \in Q$.
Jedem Element $x \in X$ ordnen wir seine Klasse $C \in Q$ zu:

$$q : X \twoheadrightarrow Q : x \mapsto C \quad \text{mit} \quad x \in C \in Q$$

Übliche Schreibweisen sind $q(x) = \mathfrak{cl}_Q(x) = [x]_Q = [x] = \overline{x} = \dots$.

Die Zerlegung Q nennen wir auch eine **Quotientenmenge** von X und $q : X \to Q$ die zugehörige **Quotientenabbildung**, kurz **Quotient**.

Zerlegung und Quotient

E302
Erläuterung

Jedes Element $C \in Q$ nennen wir eine **Klasse** von Q, je nach Kontext auch **Äquivalenzklasse**, speziell bei Gruppenoperation auch **Bahn** oder **Orbit**; das sind alles schöne Namen für immer dieselbe Idee: eine Zerlegung von X in nicht-leere disjunkte Teilmengen.

Jedes Element $x \in X$ liegt demnach in genau einer Klasse $C \in Q$.
Dies definiert die Zuordnung $q : X \twoheadrightarrow Q : x \mapsto C$ mit $x \in C \in Q$.
Die Faser über dem Punkt C ist die Menge C, denn $q^{-1}(\{C\}) = C$.
Man nennt die Abbildung q daher auch die **kanonische Surjektion**.

Die Quotientenmenge Q und die Quotientenabbildung $q : X \to Q$ nennt man beide auch kurz **Quotient**, wenn dabei klar wird, was gemeint ist.
Diese ach so „abstrakte“ Konstruktion ist im Grunde konkret und explizit, einfach und elegant. Sie hat zahllose Anwendungen und Auswirkungen.

Daher ist es für Sie ganz sicher hilfreich, sich frühzeitig und gründlich damit vertraut zu machen. Ergreifen Sie also diese gute Gelegenheit.
Mit etwas Gewöhnung verliert auch dieser neue Begriff schnell seinen Schrecken und wird auch für Sie zu einem vielseitigen Werkzeug.

Repräsentanten: die Qual der Wahl

E303

Beispiel: Sei $X = \{1,2,3,4,5,6,7\}$ und $Q = \{\{1,4\},\{2,3,6,7\},\{5\}\}$.
Zu Q ist $R = \{4,3,5\}$ ein Repräsentantensystem, ebenso $\{1,2,5\}, \dots$

Definition E3B: Repräsentantensystem

Eine Teilmenge $R \subseteq X$ heißt **Repräsentantensystem** zu Q, falls gilt:

$$\forall C \in Q \;\; \exists! x \in R : x \in C$$

Somit wählt R aus jeder Klasse $C \in Q$ genau einen Repräsentanten.
Die Einschränkung $q|_R : R \to Q : x \mapsto [x]$ ist bijektiv. Die Umkehrung

$$r = q|_R^{-1} : Q \to X : C \mapsto r(C) \in C$$

ordnet jeder Klasse $C \in Q$ ein Element $r(C) \in C$ als Repräsentant zu.

Beispiel: Die Surjektion $f : \mathbb{R} \twoheadrightarrow \mathbb{R}_{\geq 0} : x \mapsto y = x^2$ zerlegt $\mathbb{R}$ in Fasern:

$$\mathbb{R} = \bigsqcup_{y \in \mathbb{R}_{\geq 0}} f^{-1}(\{y\})$$

Zur Klasse $C = \{-x, x\}$ wählen wir den nicht-negativen Repräsentanten $|x| \in C$; diese Wahlen definieren die Wurzelfunktion $\sqrt{} : \mathbb{R}_{\geq 0} \to \mathbb{R}$.

Repräsentanten: die Qual der Wahl

E304
Erläuterung

Beispiel: Die Menge $M = \bigsqcup\{A_1, \dots, A_n\}$ der SchülerInnen teilt sich in Klassen auf und $R = \{a_1, \dots, a_n\}$ enthält die KlassensprecherInnen.
Die Abbildung $r : A_i \mapsto a_i$ weist jeder Klasse ihren Repräsentanten zu.
Die Wahl ist willkürlich; aus mathematischer Sicht sind alle gleich gut.

Beispiel: In $(\mathbb{N}, \leq)$ hat jede nicht-leere Teilmenge $A \subseteq \mathbb{N}$ ein kleinstes Element; wir können daher $a = \min A$ als Repräsentanten wählen.
Das ist zwar ebenso willkürlich, aber immerhin kanonisch, einheitlich.
Oft sind wir froh, wenn uns die Qual der Wahl abgenommen wird.

☹ Meist ist die Wahl eines Repräsentantensystems ein Akt der Willkür.
Zur Frage der Existenz siehe das Auswahlaxiom auf Seite D123.

☺ In günstigen Fällen kommen wir ohne willkürliche Wahlen aus.
Man spricht dann auch von einer „natürlichen“ Konstruktion.

Meist liegt das daran, dass es nur eine Wahlmöglichkeit gibt, oder unter den vielen nur eine im Kontext „vernünftige“ und „richtige“ Wahl, zum Beispiel die kanonische, natürliche Bijektion in Satz D3D

Die Klassengleichung: doppeltes Abzählen

E305

Beispiel: Für $X = \{1,2,3,4,5,6,7\}$ und $Q = \{\{1,4\},\{2,3,6,7\},\{5\}\}$ ist die Elementezahl $\sharp X = 7$ gleich $\sum_{C\in Q} \sharp C = 2+4+1$ gemäß Q.

Lemma E3c: die Klassengleichung

Sei Q eine Zerlegung von X. Ist X endlich, so auch Q und

$$Q_n = \{\, C \in Q \mid \sharp C = n \,\} \quad \text{für jedes } n \in \mathbb{N}.$$

Damit gilt $Q = \bigsqcup_{n\in\mathbb{N}} Q_n$. Daraus folgt die **Klassengleichung**:

$$\boxed{\sharp X = \textstyle\sum_{C\in Q} \sharp C = \sum_{n\in\mathbb{N}} n \cdot \sharp Q_n,}$$

also $\sharp X = 1\cdot\sharp Q_1 + 2\cdot\sharp Q_2 + \cdots + N\cdot\sharp Q_N$, falls $\sharp C \le N$ für alle $C \in Q$.
Spezialfall: Haben alle Klassen $C \in Q$ dieselbe Größe $c = \sharp C$, so gilt

$$\sharp X = c\cdot\sharp Q, \quad \text{also} \quad \sharp Q = (\sharp X)/c.$$

Der Tourist fragt den Schäfer: „Wie zählen Sie so schnell Ihre Schafe?“ — „Das ist ganz einfach: Ich zähle die Beine und teile durch vier.“

Die Klassengleichung: doppeltes Abzählen

E306
Erläuterung

Wir haben $Q = \bigsqcup_{n\in\mathbb{N}} Q_n$. Doppeltes Abzählen ergibt demnach:

$$\sharp X = \sum_{C\in Q} \sharp C = \sum_{n\in\mathbb{N}} \sum_{C\in Q_n} \sharp C = \sum_{n\in\mathbb{N}} \sum_{C\in Q_n} n = \sum_{n\in\mathbb{N}} n\cdot\sharp Q_n$$

Haben alle Klassen $C \in Q$ dieselbe Größe $c = \sharp C$, so gilt

$$\sharp X = c\cdot\sharp Q, \quad \text{also} \quad \sharp Q = (\sharp X)/c.$$

Die rechte Gleichung motiviert für Q den Namen **Quotientenmenge** von X. Manche schauen lieber auf die linke Gleichung und nennen Q dann konsequenterweise eine **Faktormenge** von X. Das ist dieselbe Sache, von zwei verschiedenen Seiten betrachten.

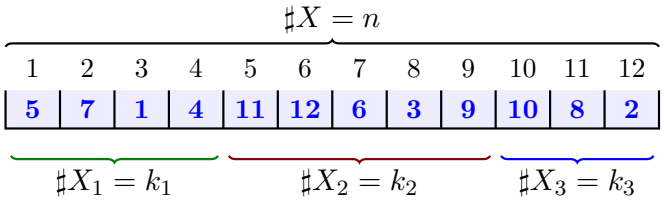
Beispiel: Die Menge X der Schüler einer Schule können Sie alle einzeln abzählen, oder erst klassenweise zählen und dann addieren. Das wird besonders einfach, wenn alle Klassen dieselbe Größe haben!

Beispiel: Einen Haufen Münzgeld können Sie unsortiert zählen, oder zuerst die 1-Cent-Münzen zusammenfassen, dann die 2-Cent-Münzen, die 5-Cent-Münzen, usw. Genau dasselbe tut die Klassengleichung

Erstes Beispiel zur Klassengleichung

E307

Kontakt-Los-Generator: Auf wie viele Arten können wir n Studierende aufteilen in genau ℓ Gruppen mit fester Größe $k_1, \ldots, k_\ell$?



Wir fixieren $X = \{1,\ldots,n\} = X_1 \sqcup \cdots \sqcup X_\ell$ mit $\sharp X_i = k_i$ und nutzen

$$f \;:\; \mathrm{S}_n \to \mathfrak{P}(X)^\ell \;:\; \sigma \mapsto \big(\sigma(X_1), \ldots, \sigma(X_\ell)\big).$$

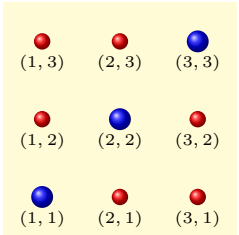
Jede Permutation $\sigma \in \mathrm{S}_n$ definiert eine Aufteilung $f(\sigma)$, wie gewünscht.
Alle Elemente ihrer Faser $[\sigma] = f^{-1}(\{f(\sigma)\})$ liefern genau dasselbe.
Es gilt $[\mathrm{id}] = \{\, \sigma_1\cdots\sigma_\ell \mid \sigma_i \in \mathrm{S}_{X_i} \,\} \cong \mathrm{S}_{X_1} \times \cdots \times \mathrm{S}_{X_\ell}$ und $\sigma : [\mathrm{id}] \cong [\sigma]$.
Jede solche Klasse $[\sigma]$ hat die Mächtigkeit $c = \sharp[\sigma] = k_1!\,k_2!\cdots k_\ell!$.
Wie viele Klassen gibt es? Klassengleichung $\sharp\,\mathrm{S}_n = n! = c\cdot\sharp Q$.

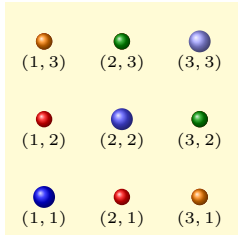
☺ Demnach gibt es $\sharp Q = n!/k_1!\,k_2!\cdots k_\ell!$ Klassen (E237).

Zweites Beispiel zur Klassengleichung

E308

Beispiel: Sei M eine Menge, $X = M^2$ und $\sigma : X \to X : (x,y) \mapsto (y,x)$.





Dies definiert die grobe Zerlegung $X = \mathrm{fix}(\sigma) \sqcup \mathrm{supp}(\sigma)$ und die feinere Bahnenzerlegung $Q = \{\, \{(x,y),(y,x)\} \mid (x,y) \in M^2 \,\}$ bezüglich σ.

Es gilt $\sigma \circ \sigma = \mathrm{id}_X$, daher hat jede Bahn die Länge entweder 1 oder 2:

$$\mathrm{fix}(\sigma) = \bigsqcup Q_1 \quad \text{mit} \quad Q_1 = \{\, \{(x,x)\} \mid x \in M \,\},$$
$$\mathrm{supp}(\sigma) = \bigsqcup Q_2 \quad \text{mit} \quad Q_2 = \{\, \{(x,y),(y,x)\} \mid x \neq y \text{ in } M \,\}.$$

Aus der Bahnengleichung folgt:

$$X = \mathrm{fix}(\sigma) \sqcup \mathrm{supp}(\sigma) \quad\Longrightarrow\quad \sharp X = \sharp\,\mathrm{fix}(\sigma) + 2\cdot\sharp Q_2$$

Involutionen und Parität

E309

Satz E3D: Involutionen und Parität

Wir nennen $\sigma : X \to X$ eine **Involution auf** X, wenn $\sigma \circ \sigma = \mathrm{id}_X$ gilt.
Somit ist $\sigma \in \mathrm{S}_X$ eine Permutation, und jeder Zykel hat Länge 1 oder 2.
Zum Beispiel ist id_X eine Involution, und jeder Punkt ist ein Fixpunkt.

Wir haben $X = \mathrm{fix}(\sigma) \sqcup \mathrm{supp}(\sigma)$. Ist X zudem endlich, so gilt

$$\sharp X = \sharp\,\mathrm{fix}(\sigma) + 2t$$

und $t \in \mathbb{N}$ ist die Anzahl der 2–Zykel. Demnach sind äquivalent:

1. Mindestens eine Involution $\sigma : X \to X$ hat ungerade Fixpunktzahl.
2. Die Menge X hat ungerade Elementezahl, kurz $\sharp X \in 2\mathbb{N} + 1$.
3. Jede Involution $\sigma : X \to X$ hat ungerade Fixpunktzahl.

Beispiel: Die Spiegelung $\sigma : M^2 \to M^2 : (x, y) \mapsto (y, x)$ ist involutiv mit $\mathrm{fix}(\sigma) = \Delta_M = \{\, (x, x) \mid x \in M \,\}$ und $\mathrm{supp}(\sigma) = \{\, (x, y) \mid x \neq y \,\}$.
Also ist $\sharp M^2$ ungerade genau dann, wenn $\sharp M$ ungerade ist.

Involutionen und Parität

E310
Erläuterung

Dieser Abzähltrick ist sehr einfach, geradezu banal, doch wirkungsvoll!
Abzählen ist gut, doppeltes Abzählen à la Klassengleichung ist besser.

Wir betrachten in Satz E3D nicht die genaue Elementezahl $\sharp S$,
sondern nur die Parität: $\sharp S$ ist entweder gerade oder ungerade.
Aus der Bahnengleichung $\sharp X = \sharp\,\mathrm{fix}(\sigma) + 2t$ mit $t \in \mathbb{N}$ lesen wir die Implikationen „(1) ⇒ (2) ⇒ (3)“ ab. Für „(3) ⇒ (1)“ nutzen wir $\sigma = \mathrm{id}_X$.

☺ Der Satz gilt genauso für jede Primzahl $p \in \mathbb{N}_{\geq 2}$ und $\sigma : X \to X$ mit $\sigma^p = \mathrm{id}_X$. Jede Bahn hat dann entweder Länge 1 oder Länge p.
Aus der Bahnengleichung erhalten wir dann $\sharp X = \sharp\,\mathrm{fix}(\sigma) + pt$.
Ich diskutiere hier zunächst nur den einfachsten Fall $p = 2$.

Ausblick: Existenzsätze für Fixpunkte sind ein wichtiges Werkzeug der Mathematik. Hierzu ist Satz E3D eine erste schöne Illustration.
In der Analysis lernen Sie Banachs Fixpunktsatz kennen und nutzen.
Die Topologie erklärt Ihnen Brouwers Fixpunktsatz, die Algebraische Topologie noch allgemeiner den Lefschetzschen Fixpunktsatz; dieser hat eine frappierende Ähnlichkeit zum Involutionssatz E3D.

Welche Zahlen sind Summe von zwei Quadraten?

E311

Erste experimentelle Daten:

$0 = 0^2 + 0^2$	$1 = 1^2 + 0^2$	$2 = 1^2 + 1^2$	$3 =$ ☹
$4 = 2^2 + 0^2$	$5 = 2^2 + 1^2$	$6 =$ ☹	$7 =$ ☹
$8 = 2^2 + 2^2$	$9 = 3^2 + 0^2$	$10 = 3^2 + 1^2$	$11 =$ ☹
$12 =$ ☹	$13 = 3^2 + 2^2$	$14 =$ ☹	$15 =$ ☹
$16 = 4^2 + 0^2$	$17 = 4^2 + 1^2$	$18 = 3^2 + 3^2$	$19 =$ ☹
$20 = 4^2 + 2^2$	$21 =$ ☹	$22 =$ ☹	$23 =$ ☹
$24 =$ ☹	$25 = 3^2 + 4^2$	$26 = 1^2 + 5^2$	$27 =$ ☹
$28 =$ ☹	$29 = 2^2 + 5^2$	$30 =$ ☹	$31 =$ ☹

Übung: Keine natürliche Zahl $4k + 3$ ist Summe von zwei Quadraten.
In $\mathbb{Z}_4$ gilt $\{\, a^2 \mid a \in \mathbb{Z}_4 \,\} = \{0, 1\}$ und $\{0, 1\} + \{0, 1\} = \{0, 1, 2\} \not\ni 3$.

Satz E3E: Fermats Zwei-Quadrate-Satz

Jede Primzahl p der Form $p = 4k + 1$ ist Summe von zwei Quadraten.

Welche Zahlen sind Summe von zwei Quadraten?

E312
Erläuterung

In dieser kleinen Tabelle springt sofort eine Beobachtung ins Auge:
In der rechten Spalte treten, soweit wir sehen, keine Treffer auf.
Wenn Sie möchten, können Sie dies nun allgemein beweisen.
Hierzu betrachten Sie Quadrate in $\mathbb{Z}_4$ ... Probieren Sie's!

Eine weitere Regelmäßigkeit dieser Tabelle ist etwas versteckt:
In der zweiten Spalte treten augenscheinlich sehr viele Treffer auf.
Nicht jede Zahl $4k + 1$ ist Summe zweier Quadrate, doch viele sind's.
Fermats berühmter Zwei-Quadrate-Satz besagt hierzu ganz allgemein:
Jede Primzahl p der Form $p = 4k + 1$ ist Summe von zwei Quadraten.

Kleine Beispiele probieren Sie leicht selbst oder mit einem Computer.
Doch wie beweisen wir dies allgemein? Es gibt unendlich viele Fälle!
Zu Fermats Zwei-Quadrate-Satz gibt es sehr viele schöne Beweise.
Ich zeige Ihnen hier ein besonders kurzes und geniales Argument.

Ich verlange nicht, dass Sie sofort alle Details nachrechnen,
vielmehr schlage ich vor, dass Sie zunächst die Beweisstruktur
verstehen lernen... und ihre Eleganz bewundern!

Involutionen und Parität

E313

Don Zagier: *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares.* Amer. Math. Monthly 77 (1990), p. 144.

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. ZAGIER
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x,y,z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$\sigma : (x,y,z) \mapsto \begin{cases} (x+2z,\ z,\ y-x-z) & \text{if } x < y-z \\ (2y-x,\ y,\ x-y+z) & \text{if } y-z < x < 2y \\ (x-2y,\ x-y+z,\ y) & \text{if } x > 2y \end{cases}$$

$\mathrm{fix}(\sigma) = \{(1,1,(p-1)/4)\}$ $\tau :$ has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x,y,z) \mapsto (x,z,y)$ also has a fixed point. □ $\mathrm{fix}(\tau) \ni (x,y,y) \Rightarrow p = x^2 + 4y^2 = x^2 + (2y)^2$

„The verifications of the implicitly made assertions. . .
are immediate and have been left to the reader.“

Involutionen und Parität

E314
Erläuterung

Aufgabe: Zeigen Sie die hier implizit gemachten Behauptungen:

(1) Die Menge $S := \{ (x,y,z) \in \mathbb{N}^3 \mid x^2 + 4yz = p \}$ ist endlich.

(2) Die Menge S wird zerlegt gemäß $S = S_1 \sqcup S_2 \sqcup S_3$ mit

$$S_1 = \{ (x,y,z) \in S \mid x < y - z \}, \qquad \sigma_1(x,y,z) = (x+2z, z, y-x-z),$$
$$S_2 = \{ (x,y,z) \in S \mid y - z < x < 2y \}, \qquad \sigma_2(x,y,z) = (2y-x, y, x-y+z),$$
$$S_3 = \{ (x,y,z) \in S \mid 2y < x \}, \qquad \sigma_3(x,y,z) = (x-2y, x-y+z, y).$$

(3) Die hier angegebenen Formeln für $\sigma_1, \sigma_2, \sigma_3 : \mathbb{Z}^3 \to \mathbb{Z}^3$ erfüllen $\sigma_3 \circ \sigma_1 = \mathrm{id}_{\mathbb{Z}^3}$ und $\sigma_1 \circ \sigma_3 = \mathrm{id}_{\mathbb{Z}^3}$ sowie $\sigma_2 \circ \sigma_2 = \mathrm{id}_{\mathbb{Z}^3}$.

(4) Es gilt $\sigma_1(S_1) \subseteq S_3$ und $\sigma_3(S_3) \subseteq S_3$ sowie $\sigma_2(S_2) \subseteq S_2$. Dies definiert die Involution $\sigma : S \to S$ mit $\sigma(u) = \sigma_i(u)$ für $u \in S_i$.

(5) Es gilt $\mathrm{fix}(\sigma) = \{(1,1,(p-1)/4)\}$. Somit ist $\sharp S$ ungerade.

(6) Die Involution $\tau : S \to S : (x,y,z) \mapsto (x,z,y)$ ist wohldefiniert.

(7) Da $\sharp S$ ungerade ist, ist auch $\sharp\,\mathrm{fix}(\tau)$ ungerade, also $\mathrm{fix}(\tau) \neq \emptyset$.

(8) Jeder Fixpunkt von τ hat die Form (x,y,y) mit $x^2 + (2y)^2 = p$.

Involutionen und Parität

E315
Erläuterung

Lösung: (1) Aus $(x,y,z) \in S$ folgt $x,y,z \geq 1$, da p prim ist.
Daraus wiederum folgt $x,y,z \in \{1,\ldots,p\}$, also grob $\sharp S \leq p^3$.

(2) Sei $(x,y,z) \in S$. Für $x = 2y$ wäre $p = 4y(y+z)$ nicht prim.
Für $x = y - z$ wäre $p = y^2 + 2yz + z^2 = (y+z)^2$ ebenfalls nicht prim.
Also gilt entweder $x < y - z$ oder $y - z < x < 2y$ oder $2y < x$.

(3,4) Definition einsetzen und sorgsam nachrechnen!

(5) Jeder Fixpunkt von σ liegt in S_2. Aus $(x,y,z) = (2y-x, y, x-y+z)$ folgt $x = y$, also $x(x+4z) = p$ und somit $x = y = 1$ und $z = (p-1)/4$.
Somit hat σ genau einen Fixpunkt: $\mathrm{fix}(\sigma) = \{(1,1,(p-1)/4)\}$.
Dank Bahnengleichung (Satz E3D) ist $\sharp S$ ungerade.

(6) Aus $(x,y,z) \in S$ folgt $(x,z,y) \in S$, also ist τ wohldefiniert.

(7) Dies folgt erneut aus der Bahnengleichung (Satz E3D).

(8) Tatatata! Augen reiben und alles nochmal durchgehen. . .

Die wunderschöne geometrische Interpretation dahinter erklären Ihnen
Edmund Weitz, *Was ist Mathematik eigentlich?*, `youtu.be/u7XZDniQEj4`,
Burkard Polster, *Fermats two square theorem*, `youtu.be/DjI1NICfjOk`.

Involutionen und Parität

E316
Erläuterung

Dieser Beweis-in-einem-Satz sagt uns nicht, wie man darauf kommt.
Das ist die genial-kreative Leistung des Autors. Don Zagier schreibt:

This proof is a simplification of one due to Heath-Brown [1] (inspired, in turn, by a proof given by Liouville). The verifications of the implicitly made assertions—that S is finite and that the map is well-defined and involutory (i.e., equal to its own inverse) and has exactly one fixed point—are immediate and have been left to the reader. Only the last requires that p be a prime of the form $4k+1$, the fixed point then being $(1,1,k)$.

Note that the proof is not constructive: it does not give a method to actually find the representation of p as a sum of two squares. A similar phenomenon occurs with results in topology and analysis that are proved using fixed-point theorems. Indeed, the basic principle we used: "The cardinalities of a finite set and of its fixed-point set under any involution have the same parity," is a combinatorial analogue and special case of the corresponding topological result: "The Euler characteristics of a topological space and of its fixed-point set under any continuous involution have the same parity."

For a discussion of constructive proofs of the two-squares theorem, see the Editor's Corner elsewhere in this issue.

REFERENCE

1. D. R. Heath-Brown, Fermat's two-squares theorem, *Invariant* (1984) 3–5.

Äquivalenzrelationen

Wir nennen $R_1 \subseteq X \times Y$ eine **Relation zwischen X und Y**.
Wir nennen $R_2 \subseteq X \times X$ eine **Relation auf der Menge X**.

Sei X eine Menge und $f : X \to Y$ eine Abbildung. Hierzu betrachten wir

$$(\sim) = R = R_f := \{\, (x,y) \in X \times X \mid f(x) = f(y) \,\} \subseteq X \times X.$$

Infix-Notation $x \sim y \Leftrightarrow f(x) = f(y)$, gesprochen „$x$ ist äquivalent zu y“.

Diese Relation erfreut sich folgender Eigenschaften für alle $x, y, z \in X$:

Reflexivität,	**Refl**(X,R):	$\Delta_X \subseteq R$,	$x\,R\,x$
Symmetrie,	**Sym**(X,R):	$R = R^\intercal$,	$x\,R\,y \Rightarrow y\,R\,x$
Transitivität,	**Tran**(X,R):	$R \bullet R \subseteq R$,	$x\,R\,y \wedge y\,R\,z \Rightarrow x\,R\,z$

Wir kehren nun die Sichtweise um und erheben dies zur Definition:

Definition E3F: Äquivalenzrelation

Eine Relation $R \subseteq X \times X$ auf der Menge X heißt **Äquivalenzrelation**, wenn R reflexiv, symmetrisch und transitiv ist.

Äquivalenzklassen und Quotientenmenge

Die **Äquivalenzklasse** von $x \in X$ bezüglich R ist die Menge

$$[x] = [x]_R := \{\, y \in X \mid x\,R\,y \,\}.$$

Jede Äquivalenzklasse ist nicht-leer, denn $x \in [x]_R$ dank Reflexivität.
Aus $y \in [x]_R$ folgt $[y]_R \subseteq [x]_R$ dank Transitivität, und dank Symmetrie $[y]_R \supseteq [x]_R$, insgesamt also $[y]_R = [x]_R$. Wir erhalten eine Zerlegung:
Je zwei Äquivalenzklassen sind entweder gleich oder disjunkt.

Der **Quotient** von X bezüglich R ist die Menge aller Äquivalenzklassen:

$$X/R := \{\, [x]_R \mid x \in X \,\}$$

Dies ist eine Zerlegung von X, also $X/R \subseteq \mathfrak{P}(X)^*$ und $X = \bigsqcup X/R$.
Jedes Element $x \in X$ gehört zu genau einer Klasse $c \in X/R$.

Die zugehörige **Quotientenabbildung** oder **kanonische Surjektion** ist

$$q = q_R : X \twoheadrightarrow X/R : x \mapsto [x]_R.$$

Genau dann gilt $q(x) = q(y)$, wenn $x\,R\,y$ gilt. Das bedeutet $R_q = R$.

Zerlegungen entsprechen Äquivalenzrelationen.

Proposition E3G: Zerlegungen entsprechen Äquivalenzrelationen.

Jede Äquivalenzrelation R auf X definiert eine Zerlegung Q von X:

$$Q = Z(R) = X/R := \{\, [x]_R \mid x \in X \,\}$$

Jede Zerlegung Q von X definiert eine Äquivalenzrelation R auf X:

$$R = A(Q) := \{\, (x,y) \in X \times X \mid \exists C \in Q : x \in C \wedge y \in C \,\}$$

Dabei gilt $A(Z(R)) = R$ und $Z(A(Q)) = Q$. Wir erhalten so die Bijektion

$$\begin{aligned}(A, Z) : \{\, Q \subseteq \mathfrak{P}(X)^* \mid X = \textstyle\bigsqcup Q \,\} \\ \cong \{\, R \subseteq X \times X \mid \Delta_X \subseteq R = R^\intercal = R \bullet R \,\}\end{aligned}$$

zwischen Zerlegungen von X und Äquivalenzrelationen auf X.

🙂 Es ist hilfreich und bequem, beide Sichtweise nutzen zu können.
Oft sind Äquivalenzrelationen bequemer, zum Beispiel in Satz E3H.
Die Zerlegung Q nutzen wir zur Definition des Quotienten $q : X \twoheadrightarrow Q$.

Wir betrachten Klassen statt Repräsentanten

Ist $C \in X/R$ eine Äquivalenzklasse, so nennen wir jedes Element $x \in C$ einen **Repräsentanten** der Klasse C. Die Wahl eines Repräsentanten ist im Allgemeinen vollkommen willkürlich, denn sie ist weder eindeutig noch irgendwie kanonisch, und im Allgemeinen auch nicht erforderlich:

🙂 Die Quotientenkonstruktion wurde gerade dazu erschaffen, um uns von Repräsentanten zu befreien! Es lebe die Klasse!

Das klingt revolutionär, und die mathematische Abstraktion ist es auch: Statt mit Elementen $x \in X$ arbeiten wir mit Äquivalenzklassen $C \in X/R$. Der Faktorisierungssatz E3J ist hierzu unser Universalwerkzeug.

🙂 Um diese Sichtweise zu betonen und didaktisch vorzubereiten, habe ich zunächst die Zerlegungen in den Vordergrund gestellt und möglichst ohne die Wahl von Repräsentanten gearbeitet.

Äquivalenzrelationen: Beispiele

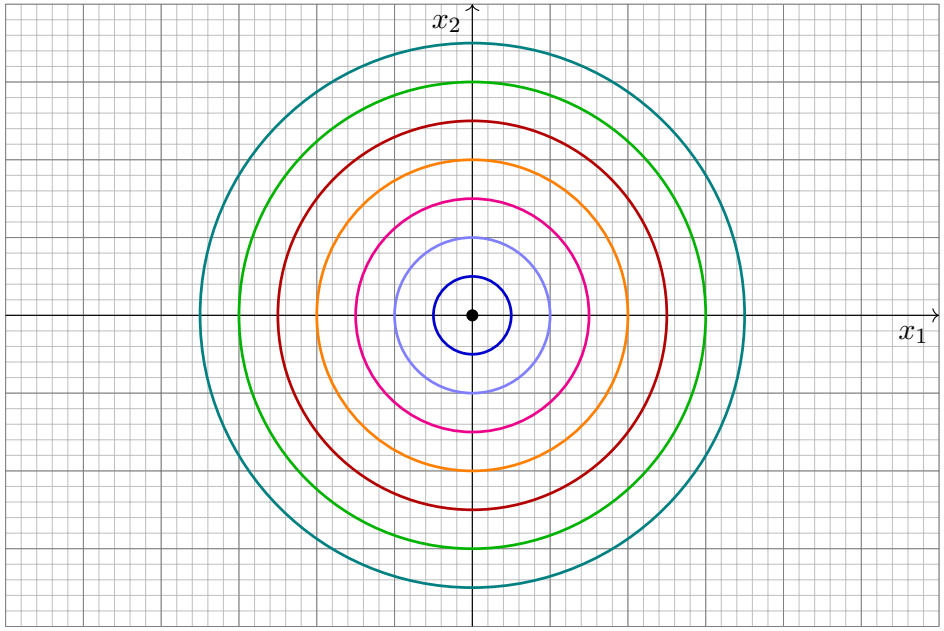
Beispiel: Die gröbste Äquivalenzrelation auf X ist $G = X \times X$.
Sie ist reflexiv, symmetrisch, transitiv. (Größer als $X \times X$ geht es nicht.)
Für jedes Element $a \in X$ gilt hier $[a] = X$, also $X/G = \{\, X \,\}$.
Die Quotientenabbildung $q : X \to X/G : a \mapsto X$ ist konstant.
Hier werden alle Elemente zu einer Klasse X zusammengefasst.

Beispiel: Die feinste Äquivalenzrelation ist $F = \Delta_X = \{\, (x,x) \mid x \in X \,\}$:
Sie ist reflexiv, symmetrisch, transitiv. (Kleiner als Δ_X geht es nicht.)
Für jedes Element $a \in X$ gilt $[a] = \{a\}$, also $X/F = \{\, \{a\} \mid a \in X \,\}$.
Die Quotientenabbildung $q : X \to X/F : a \mapsto \{a\}$ ist bijektiv.
Hier werden keine Elemente zusammengefasst, jedes bleibt einzeln.

Aufgabe: Im $\mathbb{R}^2$ betrachten wir $|x| = \sqrt{{x_1}^2 + {x_2}^2}$ und $u \sim v \Leftrightarrow |u| = |v|$.
Ist dies eine Äquivalenzrelation? Was sind hier die Äquivalenzklassen?

Lösung: (1) Ja, diese Relation $\sim$ ist reflexiv, symmetrisch, transitiv:
$|u| = |u|$, $\quad |u| = |v| \Rightarrow |v| = |u|$, $\quad |u| = |v| \wedge |v| = |w| \Rightarrow |u| = |w|$.
(2) Äq'klassen sind Kreislinien $S_r = \{\, (x_1, x_2) \in \mathbb{R}^2 \mid x_1^2 = x_2^2 = r^2 \,\}$.

Äquivalenzrelationen: Beispiele



Erzeugung von Äquivalenzrelationen

Satz E3H: die erzeugte Äquivalenzrelation

Jede Relation $P \subseteq X \times X$ erzeugt eine Äquivalenzrelation $T \subseteq X \times X$:

$$\begin{aligned} P &\mapsto R := P \cup \Delta_X \\ &\mapsto S := R \cup R^{\mathsf{T}} = P \cup \Delta_X \cup P^{\mathsf{T}} \\ &\mapsto T := \textstyle\bigcup_{n\in\mathbb{N}} S^{\bullet n} = \Delta_X \cup S \cup (S \bullet S) \cup (S \bullet S \bullet S) \cup \ldots \end{aligned}$$

Damit ist T die kleinste Äquivalenzrelation auf X, die P enthält.
Wir nennen T die von P auf X **erzeugte Äquivalenzrelation**.

Aufgabe: Auf $X = \mathbb{R}$ definieren wir P durch $a\,P\,b \Leftrightarrow b - a = 1$.
Ist P reflexiv? symmetrisch? transitiv? Bestimmen Sie R, S, T.

Lösung: P ist weder reflexiv noch symmetrisch noch transitiv.
Wir finden $a\,R\,b \Leftrightarrow b - a \in \{0, 1\}$: Diese Relation ist reflexiv.
Wir finden $a\,S\,b \Leftrightarrow b - a \in \{0, \pm 1\}$: reflexiv und symmetrisch.
Wir finden $a\,T\,b \Leftrightarrow b - a \in \mathbb{Z}$: reflexiv, symmetrisch und transitiv.

Erzeugung von Äquivalenzrelationen

Im ersten Schritt $P \mapsto R = P \cup \Delta_X$ machen wir R reflexiv, im zweiten $R \mapsto S = R \cup R^{\mathsf{T}}$ bilden wir die reflexiv-symmetrische Hülle S zu P, im dritten $S \mapsto T = \bigcup_{n\in\mathbb{N}} S^{\bullet n}$ bilden wir die transitive Hülle T von S.
☺ Ebenso genügt $S = P \cup P^{\mathsf{T}}$ und $T = \bigcup_{n\in\mathbb{N}} S^{\bullet n}$, denn $S^{\bullet 0} = \mathrm{id}_X$.

Übung: (1) Zeigen Sie, dass T eine Äquivalenzrelation auf X ist.
(2) Zudem ist T die kleinste Äquivalenzrelation, die P enthält.

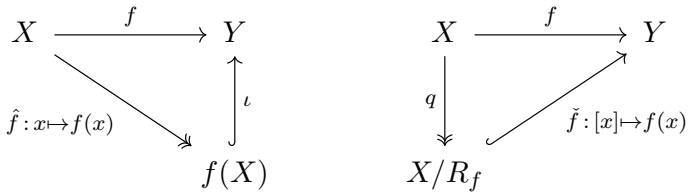
Lösung: (1) Die Relation S ist reflexiv und symmetrisch, also auch T.
Zudem ist T sogar transitiv: Wenn wir in endlich vielen S–Schritten von x nach y gelangen und von y nach z, dann auch von x nach z.

(2) Wir betrachten die Menge aller Äq'relationen auf X, die P enthalten:

$$\mathscr{A} = \{\, V \subseteq X \times X \mid V \text{ ist Äq'relation mit } V \supseteq P \,\}$$

Die größte solche Äq'relationen ist $X \times X \in \mathscr{A}$, die kleinste ist T:
Dank (1) gilt $T \in \mathscr{A}$. Für $V \in \mathscr{A}$ gilt $P \subseteq V$, also $S \subseteq V$ und $T \subseteq V$.
☺ Somit erhalten wir die alternative Konstruktion $T = \bigcap \mathscr{A}$.

Injektiv oder surjektiv machen: partielle Faktorisierung



Gegeben sei $f : X \to Y$, im Allgemeinen weder injektiv noch surjektiv.

Surjektiv machen: Wir gehen von $f : X \to Y$ zu $\hat{f} : X \twoheadrightarrow f(X)$ über.
Wir erhalten die Faktorisierung $f = \iota \circ \hat{f}$ in Surjektion und Inklusion.

Injektiv machen: Die Abbildung f definiert ihre Äquivalenzrelation

$$R_f := \{\, (x, x') \in X \times X \mid f(x) = f(x') \,\}.$$

Die Abbildung $\check{f} : X/R_f \to Y : [x] \mapsto f(x)$ ist wohldefiniert und injektiv.
Wir erhalten die Faktorisierung $f = \check{f} \circ q$ in Quotient und Injektion.

Injektiv oder surjektiv machen: partielle Faktorisierung

Hierbei ist $\hat{f}$ surjektiv, und zudem injektiv gdw f injektiv ist.
Ebenso ist $\check{f}$ injektiv, und zudem surjektiv gdw f surjektiv ist.

Die Konstruktion von $\hat{f} : X \twoheadrightarrow f(X)$ entsteht aus f durch Einschränkung der Zielmenge Y auf das Bild $f(X)$, siehe D306.

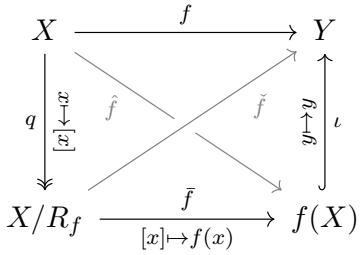
Dual hierzu: Die Konstruktion von $\check{f}$ nutzt den Quotienten X/R_f.

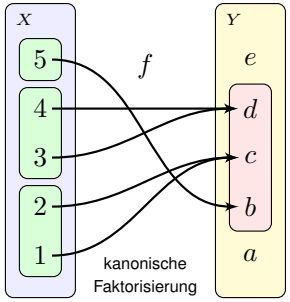
(1) Wohldefiniertheit: Aus $[x] = [x']$ folgt $f(x) = f(x')$.
Das ist ein einfacher Spezialfall des Faktorisierungssatzes E3J.

(2) Injektivität: Gleichheit $\check{f}(c) = \check{f}(c')$ bedeutet: Für Repräsentanten $x \in c$ und $x' \in c'$ gilt $f(x) = f(x')$, daraus folgt $(x, x') \in R_f$ also $c = c'$.

Der folgende Satz leistet beides zugleich: injektiv und surjektiv machen!
Dies nennt man die kanonische Faktorisierung.

Injektiv und surjektiv machen: die kanonische Faktorisierung





Satz E3I: die kanonische Faktorisierung

Jede Abbildung $f : X \to Y$ faktorisiert gemäß $f = \iota \circ \bar{f} \circ q$ in

1. die Quotientenabbildung $q : X \twoheadrightarrow X/R_f : x \mapsto [x]$,
2. die Bijektion $\bar{f} : X/R_f \xrightarrow{\sim} f(X) : [x] \mapsto f(x)$,
3. die Inklusion $\iota : f(X) \hookrightarrow Y : y \mapsto y$.

Im Beispiel oben gilt $X/R_f = \{\{1,2\},\{3,4\},\{5\}\}$ und $f(X) = \{b, c, d\}$
sowie $\bar{f} : X/R_f \to f(X) : \{1,2\} \mapsto c,\ \{3,4\} \mapsto d,\ \{5\} \mapsto b$.

Injektiv und surjektiv machen: die kanonische Faktorisierung

☺ So können wir jede beliebige Abbildung $f : X \to Y$
kanonisch zerlegen in die drei einfacheren Abbildungen $q, \bar{f}, \iota$.
Diese heißen daher **kanonische Surjektion / Bijektion / Injektion**.

Beweis: Die Abbildungen q und $\bar{f}$ und ι sind wohldefiniert.
Für Quotient q und Inklusion ι ist dies klar nach Konstruktion.
Für $\bar{f}$ folgt dies aus dem Faktorisierungssatz E3J oder hier direkt:

(0) Wohldefiniertheit: Aus $[x] = [x']$ folgt $f(x) = f(x')$.

(1) Injektivität: Gleichheit $\bar{f}(c) = \bar{f}(c')$ bedeutet: Für Repräsentanten $x \in c$ und $x' \in c'$ gilt $f(x) = f(x')$, daraus folgt $(x, x') \in R_f$ also $c = c'$.

(2) Surjektivität: Zu jedem Bildelement $y \in f(X)$ existiert mindestens ein Urbild $x \in X$ mit $f(x) = y$. Somit gilt auch $\bar{f}([x]) = y$. QED

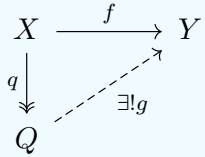
☺ Diese Zerlegung haben wir in Satz E2L erfolgreich genutzt, um Injektionen und Surjekionen zu zählen. Sie ist auch sonst oft nützlich und allgemein ein gutes Organisationsprinzip. Sie sehen im Verlauf Ihres Studiums immer wieder Anwendungen dieser Faktorisierung.

Faktorisierung über eine Surjektion

E329

Satz E3J: eindeutige Faktorisierung über eine Surjektion

Sei $q : X \twoheadrightarrow Q$ eine Surjektion, etwa ein Quotient.
Gegeben sei eine beliebige Abbildung $f : X \to Y$.



Zu (f, q) suchen wir eine **Faktorisierung** $g : Q \to Y$
mit $f = g \circ q$, also $f(x) = g(q(x))$ für alle $x \in X$.

Eindeutigkeit: Je zwei Faktorisierungen $g, g' : Q \to Y$ sind gleich.
Zu jedem Element $\overline{x} \in Q$ existiert ein Urbild $x \in X$ mit $q(x) = \overline{x}$:

$$g(\overline{x}) = g(q(x)) = (g \circ q)(x) = (g' \circ q)(x) = g'(q(x)) = g'(\overline{x})$$

Existenz: Genau dann existiert $g : Q \to Y$ mit $f = g \circ q$, wenn $R_q \subseteq R_f$:

$$\text{Kompatibilität:} \quad \forall x, x' \in X \,:\, q(x) = q(x') \Rightarrow f(x) = f(x')$$

In diesem Falle konstruieren wir g wie folgt: Zu jedem $\overline{x} \in Q$ wählen
wir willkürlich ein Urbild $x \in X$ mit $q(x) = \overline{x}$ und setzen $g(\overline{x}) := f(x)$.

$$g = f \circ q^{\mathsf{T}} = (Q, G, Y), \quad G = \left\{ (\overline{x}, y) \;\middle|\; \exists x \in X : q(x) = \overline{x} \wedge f(x) = y \right\}$$

Faktorisierung über eine Surjektion

E330
Erläuterung

Im Falle $f = g \circ q$ sagen wir f **faktorisiert über** q **zu** g oder auch
$f : X \to Y$ **induziert** $g : Q \to Y$ **über** $q : X \twoheadrightarrow Q$. Die Relation $g = f \circ q^{\mathsf{T}}$
ist linkstotal, da q surjektiv ist, und rechtseindeutig, da f kompatibel ist.

Die Bildmenge $f(X) = g(Q)$ in Y bleibt dabei unverändert.
Genau dann ist g injektiv, wenn $R_q = R_f$ gilt.

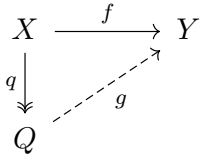
Beispiel: Speziell sei $q : X \to X/R$ ein Quotient. Genau dann
faktorisiert $f : X \to Y$ über q zu $g : X/R \to Y$, wenn $R \subseteq R_f$ gilt.
In diesem Fall ist g eindeutig und wohldefiniert durch $g([x]_R) = f(x)$.

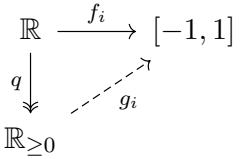
🙂 Der Faktorisierungssatz ist das Universalwerkzeug, um Abbildungen
$g : Q \to Y$ auf der Quotientenmenge Q zu konstruieren: Nahezu jede
Konstruktion verläuft genau so! Wie sollte es auch anders gehen?

Auf die Elemente die Quotientenmenge $Q = X/R$, also die Äq'klassen
$C = q(x)$, haben wir meist keinen direkten Zugriff, sondern nur über
Repräsentanten $x \in C$. Wir definieren daher $g : Q \to Y$ mit Hilfe von
Repräsentanten. Hier sagt uns Satz E3J genau, was zu tun ist.

Faktorisierung über eine Surjektion

E331





$$f_1 : \mathbb{R} \to [-1,1] : x \mapsto \sin(x)$$
$$f_2 : \mathbb{R} \to [-1,1] : x \mapsto \cos(x)$$
$$q : \mathbb{R} \to \mathbb{R}_{\geq 0} : x \mapsto x^2$$

Aufgabe: Finden Sie alle Faktorisierungen $g_1, g_2 : \mathbb{R}_{\geq 0} \to [-1, 1]$

1. mit $f_1 = g_1 \circ q$, also $\sin(x) = g_1(x^2)$ für alle $x \in \mathbb{R}$;
2. mit $f_2 = g_2 \circ q$, also $\cos(x) = g_2(x^2)$ für alle $x \in \mathbb{R}$.

Lösung: Wir wenden den Faktorisierungssatz E3J an:

1. Es gibt keine Faktorisierung g_1, denn f_1 ist nicht kompatibel mit q.
   Zum Beispiel gilt $q(-1) = q(+1)$, aber $\sin(-1) \neq \sin(+1)$.
2. Es gibt genau eine Faktorisierung g_2, denn f_2 ist kompatibel mit q.
   Explizit gilt $g_2(y) = \cos(\sqrt{y})$. Die Analysis zeigt Ihnen noch mehr:

$$\cos(x) = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{(2k)!} \quad \Longrightarrow \quad g_2(y) = \sum_{k=0}^{\infty} (-1)^k \frac{y^k}{(2k)!}$$

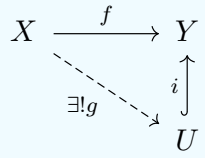
Faktorisierung über eine Injektion

E332
Erläuterung

Dual zur Faktorisierung über eine Surjektion wie in Satz E3J können wir
über eine Injektion faktorisieren. Das ist wesentlich einfacher:

Satz E3K: eindeutige Faktorisierung über eine Injektion

Sei $i : U \hookrightarrow Y$ eine Injektion, etwa eine Inklusion.
Gegeben sei eine beliebige Abbildung $f : X \to Y$.



Zu (f, i) suchen wir eine **Faktorisierung** $g : X \to U$
mit $f = i \circ g$, also $f(x) = i(g(x))$ für alle $x \in X$.

Eindeutigkeit: Je zwei Faktorisierungen $g, g' : X \to U$ sind gleich.
Aus $f(x) = i(g(x)) = i(g'(x))$ folgt $g(x) = g'(x)$ dank Injektivität von i.

Existenz: Genau dann existiert $g : X \to U$ mit $f = i \circ g$, wenn
$f(X) \subseteq i(U)$ gilt. In diesem Falle setzen wir $g(x) = i^{-1}(f(x))$, also:

$$g = i^{\mathsf{T}} \circ f = (X, G, U), \quad G = \left\{ (x, u) \;\middle|\; f(x) = i(u) \right\}$$

Wichtiger Spezialfall: Ist $\iota : U \subseteq Y$ eine Inklusion und $f(X) \subseteq U$, so ist
$g = f|_X^U$ die Einschränkung von f auf die Zielmenge U, siehe D306.

Aufbau des Zahlensystems $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

E333

Auf Grundlage der Mengenlehre bauen wir das Zahlensystem auf:

$$\begin{array}{ccccccccc} \mathbb{N} & \hookrightarrow & \mathbb{Z} & \hookrightarrow & \mathbb{Q} & \hookrightarrow & \mathbb{R} & \hookrightarrow & \mathbb{C} \\ & & \downarrow & & & & & & \\ & & \mathbb{Z}_n & & & & & & \end{array}$$

Die **natürlichen Zahlen** $(\mathbb{N}, +, 0, \cdot, 1)$ sind ein kommutativer Halbring; dabei erfüllt $(\mathbb{N}, 0, s)$ mit $s : n \mapsto n + 1$ die Dedekind–Peano–Axiome.

Die **ganzen Zahlen** $(\mathbb{Z}, +, 0, \cdot, 1)$ sind ein kommutativer Ring mit $\mathbb{N} \subset \mathbb{Z}$ als Teilhalbring und $\mathbb{Z} = \{\, z = a - b \mid a, b \in \mathbb{N} \,\}$.

Die **rationalen Zahlen** $(\mathbb{Q}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Z} \subset \mathbb{Q}$ als Teilring und $\mathbb{Q} = \{\, q = z/n \mid z, n \in \mathbb{Z},\ n \neq 0 \,\}$.

Die **reellen Zahlen** $(\mathbb{R}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Q} \subset \mathbb{R}$ und vollständig geordnet durch $x \leq y \ \Leftrightarrow\ \exists a \in \mathbb{R} : x + a^2 = y$.

Die **komplexen Zahlen** $(\mathbb{C}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{R} \subset \mathbb{C}$ dabei gilt $\mathbb{C} = \mathbb{R}[\mathrm{i}] = \{\, z = x + \mathrm{i}y \mid x, y \in \mathbb{R} \,\}$ mit $\mathrm{i}^2 = -1$.

Aufbau des Zahlensystems $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

E334
Erläuterung

Jede dieser Erweiterungen $\mathbb{N} \hookrightarrow \mathbb{Z}$ und $\mathbb{Z} \hookrightarrow \mathbb{Q}$ sowie $\mathbb{Q} \hookrightarrow \mathbb{R}$ erschafft einen neuen Zahlbereich durch eine geeignete Quotientenkonstruktion! Das ist weit raffinierter als man auf den ersten Blick erwarten würde. Wenn später einmal Zeit dazu ist, will ich dies gerne für Sie ausarbeiten; im Folgenden führe ich nur den Übergang von $\mathbb{Z}$ zu $\mathbb{Q}$ beispielhaft aus.

Die Erweiterung $\mathbb{R} \hookrightarrow \mathbb{C}$ ist im Vergleich dazu sehr viel einfacher: Hier genügen Paare $\mathbb{C} = \mathbb{R}^2$, denn jede komplexe Zahl $z \in \mathbb{Z}$ schreibt sich *eindeutig* als $z = x + y\mathrm{i}$. Auf diesen Paaren (x, y) reeller Zahlen definieren wir *unmittelbar* die Addition $(x, y) + (u, v) := (x + u, y + v)$ und die Multiplikation $(x, y) \cdot (u, v) := (xu - yv, xv + yu)$, ganz direkt.

Psychologisch wird Ihnen die Schwierigkeit umgekehrt erscheinen, da sie sich an die schwierigeren Konstruktionen $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R}$ bereits lange gewöhnt haben, aber die leichtere Konstruktion $\mathbb{R} \hookrightarrow \mathbb{C}$ für Sie noch ganz neu ist. Die mathematische Schwierigkeit jedoch, der Konstruktionsauswand, ist im letzten Schritt am geringsten.

Was ist der Nenner des Bruchs $c = a/b$?

E335

Aufgabe: Gegeben seien ganze Zahlen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Was ist der Nenner des Bruchs $c = a/b$ in $\mathbb{Q}$? Speziell für $c = 4/6$? Ist die Antwort wohldefiniert? Wo genau liegt das Problem?

Lösung: Naive Antwort: „Der Nenner von $c = a/b$ ist die Zahl b.“ Der Nenner von $c = 4/6$ wäre demnach die ganze Zahl 6. Ebenso gilt $c = 6/9$, der Nenner von c wäre also 9. Es gilt aber $6 \neq 9$. Die Antwort ist nicht wohldefiniert!

⚠ Der Versuch $N : \mathbb{Q} \to \mathbb{Z} : a/b \mapsto b$ scheitert. Dies ist keine Funktion! Der Faktorisierungssatz E3J benennt genau das Problem:

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z}^* & \xrightarrow{f = \mathrm{pr}_2} & \mathbb{Z}^* \\ {\scriptstyle q}\downarrow & \nearrow_{\nexists} & \\ \mathbb{Q} & & \end{array}$$

$$f : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Z}^* : (a, b) \mapsto b$$
$$q : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q} \ : (a, b) \mapsto a/b$$

Hier ist f nicht mit q kompatibel!

🙂 Jeder Bruch $c = a/b \in \mathbb{Q}$ erlaubt eine Darstellung $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\times$ als ein Paar (Zähler, Nenner). ☹ Diese Darstellung ist nicht eindeutig!

Was ist der Nenner des Bruchs $c = a/b$?

E336
Erläuterung

Niemand kann sagen, was „der“ Zähler und „der“ Nenner eines Bruchs sind: Diese Begriffe sind nicht wohldefiniert, wie wir gesehen haben. Wer es dennoch versucht, verwickelt sich in Widersprüche.

Wir können (mehr oder minder willkürliche) Wahlen treffen. Zum Beispiel könnten Sie hier vorschlagen, zu jedem Bruch $c \in \mathbb{Q}$ seine vollständig gekürzte Darstellung $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ zu betrachten, also $\mathrm{ggT}(a, b) = 1$ und $b > 0$. Dieser Repräsentant ist tatsächlich eindeutig. Wir könnten damit Zähler und Nenner von c definieren durch $Z(c) = a$ und $N(c) = b$. Im Beispiel wäre dann $Z(4/6) = Z(6/9) = 2$ und $N(4/6) = N(6/9) = 3$.

Auch diese gutgemeinte Antwort ist leider nur eine scheinbare Lösung. Versuchen Sie beispielsweise $1/2$ und $1/3$ zu addieren; dazu möchten Sie zuerst die beiden Brüche „auf einen gemeinsamen Nenner bringen.“ Sie merken sofort, auch diese Sprechweise gerät hier schnell in Not. Es ist zwar möglich, aber wir müssten uns extrem verrenken.

🙂 Diese Problematik erlaubt nur eine einzige vernünftige Lösung: Brüche sind Äquivalenzklassen!

Von den ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen $\mathbb{Q}$

Wir wollen den Ring $(\mathbb{Z}, +, \cdot)$ in einen Körper $(Q, +, \cdot)$ einbetten.
Idee: Wir rechnen mit Brüchen „a/b“. Das sind Äquivalenzklassen!

$$2/3 = 4/6 = 6/9 = 8/12 = \ldots \quad \text{allgemein:} \quad a/b = c/d \Leftrightarrow ad = cb$$

Brüche stellen wir dar durch Paare (Zähler, Nenner) bis auf Äquivalenz:

$$P = \mathbb{Z} \times \mathbb{Z}^* \quad \text{mit} \quad (a,b) \sim (c,d) \Leftrightarrow ad = cb.$$

Aufgabe: Ist diese Relation $\sim$ eine Äquivalenzrelation?

Lösung: Reflexiv: Es gilt $(a,b) \sim (a,b)$, denn $ab = ab$.

Symmetrisch: $(a,b) \sim (c,d) \Leftrightarrow ad = cb \Leftrightarrow cb = ad \Leftrightarrow (c,d) \sim (a,b)$.

Transitiv: Aus $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$ folgt $ad = cb$ und $cf = ed$, also $adf = cbf = cfb = edb$. Den Faktor $d \in \mathbb{Z}^*$ können wir kürzen! Daraus folgt $af = eb$, also $(a,b) \sim (e,f)$.

Wir definieren so die Quotientenmenge $Q := P/_\sim$ und die zugehörige Quotientenabbildung $q : P \twoheadrightarrow Q : (a,b) \mapsto [a,b]$, suggestiv $a/b := [a,b]$.

Von den ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen $\mathbb{Q}$

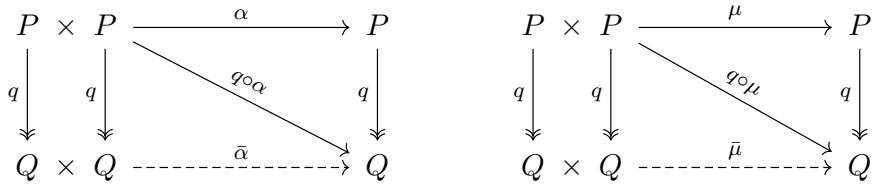
Brüche $a/b := [a,b]$ sind Äquivalenzklassen!

$$Q := P/_\sim \quad \text{mit} \quad P = \mathbb{Z} \times \mathbb{Z}^* \quad \text{und} \quad (a,b) \sim (c,d) \Leftrightarrow ad = cb$$

Addition und Multiplikation definieren wir zunächst für Paare:

$$+ = \alpha : P \times P \to P : ((a,b),(c,d)) \mapsto (ad + cb, bd)$$
$$\cdot = \mu : P \times P \to P : ((a,b),(c,d)) \mapsto (ac, bd)$$

Sind diese Verknüpfungen kompatibel mit der Quotientenabbildung q?



Für die Verknüpfungen $\bar\alpha$ und $\bar\mu$ wählen wir willkürlich Repräsentanten und verknüpfen diese in P. Ist das Ergebnis in Q wohldefiniert?

Von den ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen $\mathbb{Q}$

Beispiel: Führen willkürliche Wahlen zu verschiedenen Ergebnissen?

$$\frac{2}{3} + \frac{7}{8} = \frac{2 \cdot 8 + 7 \cdot 3}{3 \cdot 8} = \frac{37}{24}$$
$$\frac{4}{6} + \frac{-7}{-8} = \frac{4 \cdot (-8) + (-7) \cdot 6}{6 \cdot (-8)} = \frac{-74}{-48}$$

Gegeben seien jeweils äquivalente Darstellungen $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$, das heißt $ab' = a'b$ und $cd' = c'd$. Wir müssen zeigen:

$$(a,b) + (c,d) = (ad + cb, bd) \overset{!}{\sim} (a',b') + (c',d') = (a'd' + c'b', b'd')$$
$$(a,b) \cdot (c,d) = (ac, bd) \overset{!}{\sim} (a',b') \cdot (c',d') = (a'c', b'd')$$

Alle Definitionen liegen explizit vor. Prüfen wir es nach!

$$(ad + cb)(b'd') = adb'd' + cbb'd' = a'bdd' + c'dbb' = (a'd' + c'b')(bd)$$
$$acb'd' = a'c'bd$$

☺ Nun genügt geduldiges Nachrechnen der Körperaxiome für $(Q, +, \cdot)$.
Der folgende Satz fasst diese Konstruktion allgemein zusammen.

Einbettung eines Integritätsrings in seinen Bruchkörper

Satz E3L: Einbettung eines Integritätsrings in seinen Bruchkörper

Sei $(R, +, 0, \cdot, 1)$ ein Integritätsring, etwa die ganzen Zahlen $\mathbb{Z}$ oder ein Polynomring $K[X]$ über einem Körper K. Dann können wir R einbetten in einen Körper $(Q, +, 0, \cdot, 1)$, sodass $Q = \{\, a/b \mid (a,b) \in R \times R^* \,\}$ gilt.

Konstruktion: Wir nutzen Paare (Zähler, Nenner) bis auf Äquivalenz:

$$Q := P/_\sim \quad \text{mit} \quad P = R \times R^* \quad \text{und} \quad (a,b) \sim (c,d) \Leftrightarrow ad = cb$$

Dies ist eine Äquivalenzrelation, transitiv dank Kürzungsregel in R.
Sei $q : P \twoheadrightarrow Q : (a,b) \mapsto [a,b]$ die zugehörige Quotientenabbildung.
Wir haben die Einbettung $R \hookrightarrow Q : a \mapsto [a,1]$ und schreiben kurz $R \subseteq Q$.
Addition und Multiplikation definieren wir zunächst für Paare:

$$+ : P \times P \to P : ((a,b),(c,d)) \mapsto (ad + cb, bd)$$
$$\cdot : P \times P \to P : ((a,b),(c,d)) \mapsto (ac, bd)$$

Diese Verknüpfungen sind kompatibel mit der Quotientenabbildung $q : P \twoheadrightarrow Q$, daher definieren sie eine Addition und Multiplikation auf Q.
Damit ist $(Q, +, 0, \cdot, 1)$ ein Körper und $Q = \{\, a/b \mid (a,b) \in R \times R^* \,\}$.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Sei $n \in \mathbb{Z}$ eine ganze Zahl. Wir betrachten die Menge aller Vielfachen:

$$H = n\mathbb{Z} := \{\, nk \mid k \in \mathbb{Z} \,\}$$

Diese erfreut sich folgender Eigenschaften:

1. Es gilt $0 \in H$,
   denn $0 = n \cdot 0$.
2. Aus $a \in H$ folgt $-a \in H$,
   denn aus $a = nk$ folgt $-a = n \cdot (-k)$.
3. Aus $a, b \in H$ folgt $a + b \in H$,
   denn aus $a = nk$ und $b = n\ell$ folgt $a + b = n(k + \ell)$.

🙂 Zusammenfassend sagen wir hierzu: $(\mathbb{Z}, +, 0, -)$ ist eine kommutative Gruppe, und hierin ist $H \subseteq \mathbb{Z}$ eine Untergruppe.

Für die Multiplikation halten wir etwas allgemeiner fest:
Aus $a \in H$ folgt $ua \in H$ für alle $u \in \mathbb{Z}$, denn $u(nk) = n(uk)$.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Auf der Menge $\mathbb{Z}$ definieren wir die Relation „a kongruent b modulo n“:

$$a \equiv b \quad\Leftrightarrow\quad a \equiv_n b \quad :\Leftrightarrow\quad a - b \in n\mathbb{Z}$$

Dies ist eine Äquivalenzrelation:

1. Reflexivität: Es gilt $a \equiv a$, denn $a - a = 0 \in H$.
2. Symmetrie: $a \equiv b$ bedeutet $a - b \in H$, also $b - a \in H$, somit $b \equiv a$.
3. Transitivität: $a \equiv b$ und $b \equiv c$ bedeuten $a - b \in H$ und $b - c \in H$, daraus folgt $H \ni (a - b) + (b - c) = a - c$, somit $a \equiv c$.

🙂 Die drei definierenden Eigenschaften der Untergruppe $H \subseteq \mathbb{Z}$ übersetzen sich direkt in Reflexivität, Symmetrie und Transitivität.

Bemerkung: Wir nutzen den Rest $p : \mathbb{Z} \to \mathbb{Z}_n : a \mapsto a \operatorname{rem} n$.
Damit ist die Bedingung $a - b \in n\mathbb{Z}$ äquivalent zu $p(a) = p(b)$.
Auch daraus folgt sofort Reflexivität, Symmetrie und Transitivität.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Zu jeder ganzen Zahl $a \in \mathbb{Z}$ haben wir die zugehörige Äquivalenzklasse:

$$[a] = a + n\mathbb{Z} := \{\, a + nk \mid k \in \mathbb{Z} \,\}$$

Alle Äquivalenzklassen fassen wir zur Quotientenmenge zusammen:

$$\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z} := \left\{\, [a] = a + n\mathbb{Z} \;\middle|\; a \in \mathbb{Z} \,\right\}$$

Die zugehörige Quotientenabbildung ist demnach:

$$q \;:\; \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} \;:\; a \mapsto [a] = a + n\mathbb{Z}$$

Beispiel: Für $n = 0$ erhalten wir $\mathbb{Z}/0\mathbb{Z} = \{\, \{a\} \mid a \in \mathbb{Z} \,\}$.
Die Quotientenabbildung $q : \mathbb{Z} \to \mathbb{Z}/0\mathbb{Z} : a \mapsto \{a\}$ ist bijektiv.
Hier gibt es nur ein Repräsentantensystem, nämlich die Menge $\mathbb{Z}$.

Beispiel: Für $n = 1$ erhalten wir $\mathbb{Z}/1\mathbb{Z} = \{\, \mathbb{Z} \,\}$.
Die Quotientenabbildung $q : \mathbb{Z} \to \mathbb{Z}/1\mathbb{Z} : a \mapsto \mathbb{Z}$ ist konstant.
Für jedes Element $a \in \mathbb{Z}$ ist somit $\{a\}$ ein Repräsentantensystem.

Diese beiden Extremfälle kommen also natürlich vor, siehe E321.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Beispiel: Für $n = 2$ haben wir genau zwei Äquivalenzklassen:

$$\begin{aligned}\mathbb{Z}/2\mathbb{Z} = \{\; & 0 + 2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}, \\ & 1 + 2\mathbb{Z} = \{\ldots, -3, -1, 1, 3, 5, 7, \ldots\} \;\}\end{aligned}$$

Mögliche Repräsentantensysteme sind $\{0, 1\}$ oder $\{8, -5\}$ ….

Beispiel: Für $n = 3$ haben wir genau drei Äquivalenzklassen:

$$\begin{aligned}\mathbb{Z}/3\mathbb{Z} = \{\; & 0 + 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}, \\ & 1 + 3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}, \\ & 2 + 3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\} \;\}\end{aligned}$$

Mögliche Repräsentantensysteme sind $\{0, 1, 2\}$ oder $\{-1, 0, 1\}$ ….

Beispiel: Für jede ganze Zahl $n \in \mathbb{Z}_{\geq 1}$ erhalten wir die Zerlegung

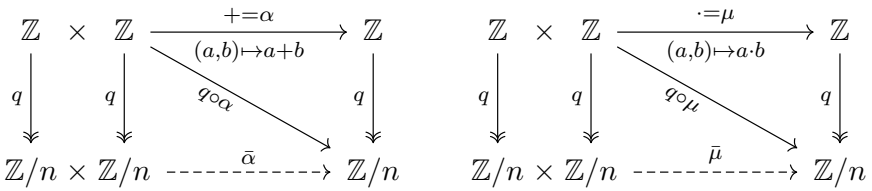
$$\mathbb{Z} = \bigsqcup \mathbb{Z}/n\mathbb{Z} = (n\mathbb{Z}) \sqcup (1 + n\mathbb{Z}) \sqcup \cdots \sqcup (n - 1 + n\mathbb{Z}).$$

Das kanonische Repräsentantensystem ist $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

E345

Übung: Sind Addition und Multiplikation in $\mathbb{Z}$ kompatibel mit q?



Für die Verknüpfungen $\bar{\alpha}$ und $\bar{\mu}$ wählen wir willkürlich Repräsentanten und verknüpfen diese in $\mathbb{Z}$. Ist das Ergebnis in $\mathbb{Z}/n$ wohldefiniert?

Erst mit dieser Garantie erhalten wir auf $\mathbb{Z}/n$ die Verknüpfungen

$$+ : \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n : [a] + [b] = [a+b],$$
$$\cdot : \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n : [a] \cdot [b] = [a \cdot b].$$

Alle Axiome eines kommutativen Rings gelten in $(\mathbb{Z}, +, 0, \cdot, 1)$, und $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$ überträgt diese auf $(\mathbb{Z}/n, +, [0], \cdot, [1])$. So wird $\mathbb{Z}/n$ zu einem kommutativen Ring und q zu einem Ringhomomorphismus.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

E346
Erläuterung

⚠ Der entscheidende Punkt der gesamten Konstruktion ist die Wohldefiniertheit der Addition und der Multiplikation auf $\mathbb{Z}/n$. Ab da liegen alle Daten explizit vor, und es genügt sorgsames Rechnen!

Wir nutzen die Surjektion $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$ und die Eigenschaften

$$q(a+b) = q(a) + q(b) \quad \text{und} \quad q(a \cdot b) = q(a) \cdot q(b).$$

Wir weisen für $(\mathbb{Z}/n, +, \cdot)$ die Axiome eines kommutativen Rings nach.

Wir zeigen zunächst **Ass**$(\mathbb{Z}/n, +)$. Vorgelegt seien $r_1, r_2, r_3 \in \mathbb{Z}/n$. Hierzu existieren Urbilder $a_1, a_2, a_3 \in \mathbb{Z}$ mit $q(a_i) = r_i$. Damit finden wir:

$$(r_1 + r_2) + r_3 = \big(q(a_1) + q(a_2)\big) + q(a_3) = q\big((a_1 + a_2) + a_3\big)$$
$$r_1 + (r_2 + r_3) = q(a_1) + \big(q(a_2) + q(a_3)\big) = q\big(a_1 + (a_2 + a_3)\big)$$

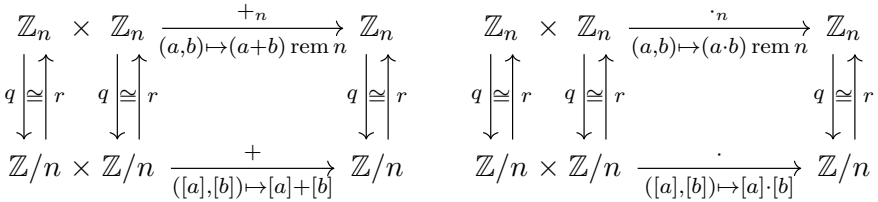
Aus **Ass**$(\mathbb{Z}, +)$ folgt **Ass**$(\mathbb{Z}/n, +)$. Ebenso alle anderen Ringaxiome A1E!

🙂 Jede Allaussage in $(\mathbb{Z}, +, \cdot)$ vererbt sich auf $(\mathbb{Z}/n, +, \cdot)$ dank des Homomorphismus $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$. Bitte führen Sie dies sorgsam aus!

Vergleich der Ringe $\mathbb{Z}_n$ und $\mathbb{Z}/n\mathbb{Z}$

E347

Sei $n \in \mathbb{N}_{\geq 1}$ und $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Wir haben das Bijektionspaar $(q, r) : \mathbb{Z}_n \cong \mathbb{Z}/n$ mit $q(a) = [a]$ und $r([a]) = a \operatorname{rem} n$. (Wohldefiniert!)



🙂 Beide Ringe leisten dasselbe, und (q, r) übersetzt alles verlustfrei. Somit ist $(q, r) : (\mathbb{Z}_n, +_n, \cdot_n) \cong (\mathbb{Z}/n, +, \cdot)$ ein Ringisomorphismus.

Sie können sich daher aussuchen, wie Sie rechnen möchten:
M mit Restklassen $[0], [1], \ldots, [n-1]$ im Restklassenring $\mathbb{Z}/n$ oder
I mit den kanonischen Repräsentanten $0, 1, \ldots, n-1$ im Ring $\mathbb{Z}_n$.

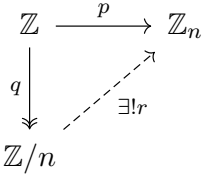
Restklassen sind die mathematische Sichtweise: elegant und abstrakt. Die Repräsentanten eignen sich besonders gut für die Programmierung, so können Sie alle Rechnungen direkt und effizient implementieren.

Vergleich der Ringe $\mathbb{Z}_n$ und $\mathbb{Z}/n\mathbb{Z}$

E348
Erläuterung

Aufgabe: Warum ist $r : \mathbb{Z}/n \to \mathbb{Z}_n : [a] \mapsto a \operatorname{rem} n$ wohldefiniert?

Lösung: Wir nutzen den Faktorisierungssatz E3J! Die Abbildung $p : \mathbb{Z} \to \mathbb{Z}_n : a \mapsto a \operatorname{rem} n$ ist kompatibel mit $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n : a \mapsto [a]$, denn $[a] = [b]$ bedeutet $a - b \in n\mathbb{Z}$, also $a \operatorname{rem} n = b \operatorname{rem} n$. Faktorisierung gibt $r : \mathbb{Z}/n \to \mathbb{Z}_n$ mit $p = r \circ q$, also $r([a]) = a \operatorname{rem} n$.



🙂 Der Faktorisierungssatz ist das Universalwerkzeug, um Abbildungen auf einer Quotientenmenge zu konstruieren. Nur so gelingt es!

Aufgabe: Warum ist $(q, r) : \mathbb{Z}_n \cong \mathbb{Z}/n$ ein Bijektionspaar?

Lösung: Für jedes $a \in \mathbb{Z}_n$ gilt $r(q(a)) = r([a]) = a \operatorname{rem} n = a$. Umgekehrt sei $x \in \mathbb{Z}/n$. Also gilt $x = [a]$ mit $a \in \mathbb{Z}$. Die euklidische Division ergibt $a = nk + a'$ mit $k = a \operatorname{quo} n \in \mathbb{Z}$ und $a' = a \operatorname{rem} n \in \mathbb{Z}_n$. Damit erhalten wir $q(r(x)) = q(r([a])) = q(a') = [a'] = [a] = x$.

🙂 Alle Daten liegen explizit vor, es genügt sorgsames Nachrechnen! Wir werden fortan $\mathbb{Z}_n$ und $\mathbb{Z}/n$ meist nicht mehr unterscheiden.

Beispiel einer Klausuraufgabe (2020)

Aufgabe: Wir betrachten den Restklassenring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.
(0) Schreiben Sie die Abbildung $f : \mathbb{Z}_9 \to \mathbb{Z}_9 : x \mapsto x^3$ explizit aus mit den kanonischen Repräsentanten $\overline{0}, \overline{1}, \ldots, \overline{8}$. (1) Ist f injektiv? (2) surjektiv?

Lösung: (0) Wir rechnen sorgsam modulo 9:

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$f(x)$	$\overline{0}$	$\overline{1}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{8}$

(1) In $\mathbb{Z}_9$ gilt $\overline{0} \neq \overline{3}$, aber $f(\overline{0}) = \overline{0} = f(\overline{3})$, daher ist f nicht injektiv.

(2) Zu $y = \overline{2}$ gibt es kein $x \in \mathbb{Z}_9$ mit $f(x) = y$. Somit ist f nicht surjektiv.

Aufgabe: (3) Dieselben Fragen für $g : \mathbb{Z}_{11} \to \mathbb{Z}_{11} : x \mapsto x^3$.
(4) Wie / Können Sie g als Produkt disjunkter Zykel schreiben?

Lösung: (3) Die Abbildung $g : \mathbb{Z}_{11} \to \mathbb{Z}_{11} : x \mapsto x^3$ ist bijektiv:

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$g(x)$	$\overline{0}$	$\overline{1}$	$\overline{8}$	$\overline{5}$	$\overline{9}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{3}$	$\overline{10}$

(4) Wir finden $g = (\overline{0})\,(\overline{1})\,(\overline{2}, \overline{8}, \overline{6}, \overline{7})\,(\overline{3}, \overline{5}, \overline{4}, \overline{9})\,(\overline{10})$.

Beispiel einer Klausuraufgabe (2020)

Aufgabe: Auf der Menge $\mathbb{R}$ definieren wir die Relation $\sim$ wie folgt:
Genau dann gilt $x \sim y$, wenn ein $\lambda \in \mathbb{R}_{\geq 1}$ existiert mit $\lambda x = y$.
(1) Welche der drei Axiome einer Äquivalenzrelation sind erfüllt?

Auf der Menge $\mathbb{R}$ sei $\approx$ die von $\sim$ erzeugte Äquivalenzrelation.
(2) Explizieren Sie $\approx$. (3) Nennen Sie alle Äquivalenzklassen.

Lösung: (1) Es gilt Reflexivität und Transitivität, aber nicht Symmetrie.

(1a) Reflexivität ist erfüllt: Für jedes $x \in \mathbb{R}$ gilt $x \sim x$, denn $\lambda x = x$ mit $\lambda = 1 \in \mathbb{R}_{\geq 1}$. (1b) Symmetrie ist nicht erfüllt: Zum Beispiel gilt $3 \sim 6$, denn $\lambda 3 = 6$ mit $\lambda = 2 \in \mathbb{R}_{\geq 1}$, aber nicht $6 \sim 3$, denn $1/2 \notin \mathbb{R}_{\geq 1}$.
(1c) Transitivität ist erfüllt: Aus $\lambda x = y$ und $\mu y = z$ mit $\lambda, \mu \in \mathbb{R}_{\geq 1}$ folgt $\kappa x = z$ mit $\kappa = \mu\lambda \in \mathbb{R}_{\geq 1}$.

(2) Genau dann gilt $x \approx y$, wenn ein $\lambda \in \mathbb{R}_{>0}$ existiert mit $\lambda x = y$.
(Ausführung als Übung: Beweisen Sie diese explizite Darstellung!)

(3) Die Zerlegung in Äquivalenzklassen ist $\mathbb{R}/_{\approx} = \{\mathbb{R}_{<0}, \{0\}, \mathbb{R}_{>0}\}$.

Beispiel einer Klausuraufgabe (2020)

Aufgabe: Auf der Menge $\mathbb{R}$ definieren wir die Relation $\sim$ wie folgt:
Genau dann gilt $x \sim y$, wenn ein $\lambda \in [\frac{1}{2}, 2]$ existiert mit $\lambda x = y$.
(1) Welche der drei Axiome einer Äquivalenzrelation sind erfüllt?

Auf der Menge $\mathbb{R}$ sei $\approx$ die von $\sim$ erzeugte Äquivalenzrelation.
(2) Explizieren Sie $\approx$. (3) Nennen Sie alle Äquivalenzklassen.

Lösung: (1) Es gilt Reflexivität und Symmetrie, aber nicht Transitivität.

(1a) Reflexivität ist erfüllt: Für jedes $x \in \mathbb{R}$ gilt $x \sim x$, denn $\lambda x = x$ mit $\lambda = 1 \in [\frac{1}{2}, 2]$. (1b) Symmetrie ist erfüllt: Ist $x \sim y$, dann ist $\lambda x = y$ mit $\lambda \in [\frac{1}{2}, 2]$, also $\lambda^{-1} y = x$. Dank $\lambda^{-1} \in [\frac{1}{2}, 2]$ folgt $y \sim x$. (1c) Transitivität ist nicht erfüllt: Zum Beispiel gilt $1 \sim 2$ und $2 \sim 4$, aber $1 \not\sim 4$.

(Zur Übung können Sie diese Aufgabe vielfältig variieren:
Beginnen Sie mit $\lambda \in S = \mathbb{R}_{\geq 1}, \mathbb{R}_{>1}, [\frac{1}{2}, 2], [1, 2], [2, 3], \ldots$.)

(2) Genau dann gilt $x \approx y$, wenn ein $\mu \in \mathbb{R}_{>0}$ existiert mit $\mu x = y$.
(Ausführung als Übung: Beweisen Sie diese explizite Darstellung!)

(3) Die Zerlegung in Äquivalenzklassen ist $\mathbb{R}/_{\approx} = \{\mathbb{R}_{<0}, \{0\}, \mathbb{R}_{>0}\}$.

Beispiel einer Klausuraufgabe (2020)

Ausführung: Auf der Menge $\mathbb{R}$ definieren wir die Relation $\simeq$ wie folgt:
Genau dann gilt $x \simeq y$, wenn ein wenn ein $\mu \in \mathbb{R}_{>0}$ existiert mit $\mu x = y$.

Diese Relation findet man anschaulich durch transitive Fortsetzung.
Wir zeigen nun, dass $\simeq$ gleich $\approx$ ist, wie oben in (2) behauptet.

(2a) Zunächst prüfen wir nach, dass $\simeq$ eine Äquivalenzrelation ist.
Wie oben in (1) ist dies leichte Routine. (1a) Reflexivität: Für jedes $x \in \mathbb{R}$ gilt $x \sim x$, denn $\lambda x = x$ mit $\lambda = 1 \in \mathbb{R}_{>0}$. (1b) Symmetrie: Ist $x \sim y$, dann ist $\lambda x = y$ mit $\lambda \in \mathbb{R}_{>0}$, also $\lambda^{-1} y = x$. Dank $\lambda^{-1} \in \mathbb{R}_{>0}$ folgt $y \sim x$.
(1c) Transitivität: Aus $\lambda x = y$ und $\mu y = z$ mit $\lambda, \mu \in \mathbb{R}_{>0}$
folgt $\kappa x = z$ mit $\kappa = \mu\lambda \in \mathbb{R}_{>0}$.

(2b) Offensichtlich gilt $x \sim y \Rightarrow x \simeq y$, das heißt $\simeq$ enthält $\sim$.
Dank (2a) enthält $\simeq$ die von $\sim$ erzeugte Äquivalenzrelation $\approx$.

(2c) Umgekehrt zeigen wir schließlich: $\approx$ enthält $\simeq$, also $x \simeq y \Rightarrow x \approx y$.
Angenommen, es gilt $x \simeq y$, also $\mu x = y$ mit $\mu \in \mathbb{R}_{>0}$. Wir können dann ein $n \in \mathbb{N}$ so wählen, dass $\kappa := \sqrt[n]{\mu} \in [\frac{1}{2}, 2]$. Für $i = 0, \ldots, n$ setzen wir $x_i = \kappa^i x$. Dann ist $x = x_0 \sim x_1 \sim \cdots \sim x_n = y$, also $x \approx y$.

Wie un/wahrscheinlich sind lange Zykel?

Aufgabe: (1) Vorgelegt seien $n, \ell \in \mathbb{N}$ mit $n/2 < \ell \leq n$.
Wie viele Permutationen $\sigma \in \mathrm{S}_n$ haben einen ℓ–Zykel?

Lösung: (1) Hat $\sigma \in \mathrm{S}_n$ einen ℓ–Zykel, so sind alle anderen Zykel strikt kürzer, denn $\ell > n/2$. Zur Konstruktion von σ wählen wir zunächst die Elemente des ℓ–Zykels: Dazu gibt es $\binom{n}{\ell}$ Möglichkeiten, diese könnnen wir auf $\ell!$ Weisen anordnen, je ℓ Anordnungen ergeben denselben Zykel.

Die verbleibenden $n - \ell$ Punkte können wir beliebig permutieren.

Die gesuchte Anzahl ist demnach

$$a_\ell = \binom{n}{\ell} \cdot \frac{\ell!}{\ell} \cdot (n-\ell)! = \frac{n!}{\ell}.$$

🙂 Das ist eine erfreulich einfache Formel!

Beispiel: Wir betrachten Permutationen von $n = 10$ Punkten. Der Anteil der Permutationen mit einem ℓ–Zykel ist genau $1/\ell$ für $\ell = 6, 7, \ldots, 10$.

Spezialfall: 10% dieser Permutationen bestehen aus einem 10–Zykel. Diesen Fall können Sie besonders leicht erklären. Versuchen Sie es!

Wie un/wahrscheinlich sind lange Zykel?

Aufgabe: (2) Sei $n = 2m$. Sie wählen zufällig eine Permutation $\sigma \in \mathrm{S}_n$.
Wie wahrscheinlich sind Permutationen mit einen Zykel der Länge $> m$?

Lösung: (2) Dank der vorigen Aufgabe ist die Wahrscheinlichkeit

$$p_n = \frac{1}{n!} \sum_{\ell=m+1}^{n} \frac{n!}{\ell} = \sum_{\ell=m+1}^{n} \frac{1}{\ell}.$$

Für $n = 2, 4, 6, 8, 10, \ldots$ erhalten wir folgende numerische Werte:

n	2	4	6	8	10	20	50	100	200	500
p_n	0.500	0.583	0.617	0.635	0.646	0.669	0.683	0.688	0.691	0.692
$1 - p_n$	0.500	0.417	0.383	0.365	0.354	0.331	0.317	0.312	0.309	0.308

🙂 Für große n nutzen wir geschickt den Vergleich mit dem Integral:

$$\ln\left(2 - \frac{1}{m+1}\right) = \int_{x=m}^{2m} \frac{1}{x+1}\,\mathrm{d}x \leq \sum_{\ell=m+1}^{2m} \frac{1}{\ell} \leq \int_{x=m}^{2m} \frac{1}{x}\,\mathrm{d}x = \ln 2$$

Somit gilt $p_n \nearrow \ln 2 \approx 0.693$ und $1 - p_n \searrow 1 - \ln 2 \approx 0.307$.

Das Erstirätsel (aka Gefangenenrätsel)

Zur Erstsemestereinführung veranstaltet die Fachschaft folgendes Spiel.

In einem Team von $n = 10$ Erstis trägt jeder eine Nummer $1, 2, \ldots, n$. Sie betreten nacheinander einen Raum mit n Boxen, diese enthalten zufällig verteilt die Zahlen $1, 2, \ldots, n$. Jeder Ersti muss seine Nummer finden und darf dazu in $n/2 = 5$ Boxen schauen; danach verlässt er den Raum durch eine andere Tür. Findet jeder Ersti seine eigene Nummer, so gewinnt das Team. Findet aber irgendein Ersti seine Nummer nicht, so verliert das Team. Vor dem Spiel darf das Team sich beraten, doch während des Spiels ist keine Kommunikation mehr möglich.

Aufgabe: (3) Angenommen, jeder Ersti öffnet seine Boxen zufällig.
Welche Gewinnwkt hat das Team mit dieser Zufallsstrategie?

(4) Gibt es eine Strategie mit Gewinnwkt über 30%?
Was ist für das Team die beste Strategie?

Lösung: (3) Bei zufälligem Öffnen hat jeder Ersti die Gewinnwkt $\frac{1}{2}$, das Team also die Gewinnwkt $\frac{1}{2^n}$. Für $n = 10$ ist dies $\frac{1}{1024} \approx 0.1\%$.

Das Erstirätsel (aka Gefangenenrätsel)

(4) Jeder Ersti $k = 1, 2, \ldots, n$ spielt die **Zykelverfolgungs-Strategie**: Er schaut zuerst in die Box mit seiner Nummer $i_1 = k$; liegt dort die Nummer k, so hat er gewonnen. Andernfalls sieht er dort die Nummer $i_2 \neq i_1$ und öffnet die Box Nummer i_2. Dies wiederholt er solange, bis er seine Nummer gefunden hat (oder aufhören muss).

Die Verteilung der Nummern auf die Boxen entspricht einer Permutation $\sigma \in \mathrm{S}_n$. Das Team verliert mit dieser Strategie, falls ein Zykel der Länge $> n/2$ vorliegt. Die Wkt hierfür ist $p_{10} = \sum_{\ell=6}^{10} \frac{1}{\ell} \approx 0.646$ wie oben in (2) berechnet. Das Team gewinnt also mit der Wkt $1 - p_{10} \approx 0.354$.

🙂 Für $n \to \infty$ konvergiert die Wkt $\frac{1}{2^n}$ in (1) sehr schnell gegen 0, während die Wkt $1 - p_n \searrow 1 - \ln 2 \approx 0.307$ immer über 30% bleibt.

🙂 Die Zykelverfolgungs-Strategie ist tatsächlich optimal, das heißt sie maximiert die Gewinnwkt. Dies bewiesen E. Curtin, M. Warshauer: *The locker puzzle.* Mathematical Intelligencer 28 (2006) 28–31.

Siehe `en.wikipedia.org/wiki/100_prisoners_problem`.

Kapitel F

Ordnungsrelationen und Mächtigkeit

Alles sollte so einfach wie möglich gemacht werden
— aber nicht noch einfacher.
Albert Einstein (1879–1955)

Inhalt dieses Kapitels F

Ordnungsrelationen

Ordnungsrelationen werden überall genutzt innerhalb der Mathematik sowie in ihren zahlreichen Anwendungen und nahezu überall im Alltag:

1. Mathematik und Physik:
   Anordnung der reellen Zahlen.
2. Informatik und Programmierung:
   Daten suchen und sortieren.
3. Optimierung und Spieltheorie:
   Ertrag maximieren, Kosten minimieren.
4. Wirtschafts- und Sozialwissenschaften:
   Präferenzen über mögliche Alternativen.

Überall wird mit „größer / kleiner / gleich“ oder „besser / schlechter / egal“ Ordnung geschaffen. Hierzu benötigen wir präzises Grundvokabular!

Im ersten Teil dieses Kapitels ist genau das unser Ziel: Wir diskutieren die nötigen Grundbegriffe zu Ordnungsrelationen, so dass Sie damit in Ihrem weiteren Studium gut und sicher arbeiten können.

Unendliche Mengen

Im zweiten Teil dieses Kapitels untersuchen wir unendliche Mengen. Die Grundlagen zu endlichen Mengen kennen Sie aus Kapitel E.

Der Invarianzsatz E1H garantiert: Für jede endliche Menge X und jede Selbstabbildung $h : X \to X$ sind die Eigenschaften *injektiv* und *surjektiv* und *bijektiv* äquivalent! Dies charakterisiert die endlichen Mengen (F2E). Für unendliche Mengen hingegen gilt diese Äquivalenz nicht mehr!

Auch für unendliche Mengen wollen wir die „Elementezahl“ vergleichen, und dies geschieht genau wie im endlichen Fall durch In/Sur/Bijektionen. Durch Bijektion definieren wir den Begriff der „Gleichmächtigkeit“, damit klären wir erste Beispiele und beweisen grundlegende Rechenregeln.

Dabei stellt sich heraus, dass die Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N}^n$, ... untereinander gleichmächtig sind, wir sagen dazu auch: sie sind *abzählbar unendlich*. Hingegen ist die Menge $\mathbb{R}$ der reellen Zahlen *überabzählbar unendlich*. Unendliche Mengen halten einige Überraschungen bereit!

Zum krönenden Abschluss erhalten wir Cantors ebenso eleganten wie sensationellen Beweis, dass fast alle reellen Zahlen transzendent sind.

Ordnungsrelationen: reelle Zahlen

In der Mathematik und der Physik, sowie generell in allen Natur- und Ingenieurwissenschaften, spielen die reellen Zahlen $(\mathbb{R}, +, \cdot, \leq)$ eine zentrale Rolle, insbesondere ihre charakterisierende Eigenschaft: Der Körper $(\mathbb{R}, +, \cdot, \leq)$ ist *geordnet* und zudem *(ordnungs)vollständig*.

Vollständigkeit bedeutet: Zu jeder Teilmenge $M \subseteq \mathbb{R}$, die nicht-leer und nach oben beschränkt ist, existiert in $\mathbb{R}$ eine kleinste obere Schranke. Diese Ordnungsbegriffe wollen wir in diesem Kapitel genauer erklären, und bereits die reellen Zahlen sind hierfür eine starke Motivation.

Auf dieser Vollständigkeit gründet die gesamte Analysis und somit all ihre wunderbaren Anwendungen: Grenzwerte von Folgen und Reihen, Ableitungen und Integrale, Fourier–Reihen und Differentialgleichungen, Wahrscheinlichkeitsrechnung und Optimierung, ... sowie darauf aufbauend ihre numerische Implementierung auf dem Computer.

Ordnungsrelationen: Suchen und Sortieren

In der Informatik und der Programmierung werden Ordnungsrelationen nahezu überall genutzt, um Daten effizient zu suchen und zu sortieren.

In fact, there were many installations in which the task of sorting was responsible for more than half of the computing time. From these statistics we may conclude that either (i) there are many important applications of sorting, or (ii) many people sort when they shouldn't, or (iii) inefficient sorting algorithms have been in common use. The real truth probably involves all three of these possibilities, but in any event we can see that sorting is worthy of serious study, as a practical matter.

Donald E. Knuth, *The Art of Computer Programming*

Der Erfolg von Computeranwendungen beruht nur zu einem Teil auf der Rechenleistung, zu einem weit größeren auf effizienten Algorithmen!

Ordnungsrelationen: Optimierung und Alltagsanwendungen

In der Optimierung und der Spieltheorie will man den Ertrag maximieren und/oder die Kosten minimieren. Das beginnt mit der Erklärung einer zu optimierenden „Zielfunktion“ und einer geeigneten Ordnungsrelation auf den Ergebnissen. Gesucht sind dann die besten Handlungsoptionen.

Die Wirtschafts- und Sozialwissenschaften nutzen diese Sichtweise: Hier beschreibt man komplexe Entscheidungssituationen durch die Präferenzen der Individuen über die möglichen Ergebnisse und sucht dann möglichst optimale Aktionen / Handlungsoptionen / Alternativen.

Auch im Alltag nutzen wir überall die Vergleiche wie „größer / kleiner / gleich“ oder „besser / schlechter / egal“. Das sind Ordnungsrelationen! Ihre sichere Beherrschung liegt nahezu allen rationalen Entscheidungen zu Grunde.

Zur mathematische Untersuchung solcher Probleme benötigen wir präzises Grundvokabular: Die zentrale Forderung ist die *Transitivität*. Häufig erwarten wir Transitivität und werden vom Gegenteil arg verblüfft. In solch Extremfällen sprechen wir von einem *Intransitivitäts-Paradox*.

Ordnungsrelationen in der Linearen Algebra

Ordnungsrelationen sind auch in der Linearen Algebra grundlegend. Als Ausblick nenne ich hier nur kurz folgende Beispiele:

Sei V ein Vektorraum über einem Körper K. Genau dann ist die Familie $(v_i)_{i\in I}$ eine Basis von V, wenn sie linear unabhängig ist und *maximal* mit dieser Eigenschaft, ebenso wenn sie V erzeugt und *minimal* ist mit dieser Eigenschaft. Wir benötigen hierzu präzise Begriffe!

Der Aufspann einer Teilmenge $X \subseteq V$ ist der *kleinste* Unterraum $U \leq V$, der die Menge X enthält. Dazu können wir U durch Ausschöpfung von innen konstruieren, aber ebenso durch Eingrenzung von außen, also als *Supremum*: Wir betrachten den Durchschnitt U aller Unterräume, die X enthalten, und zeigen dann, dass $U \leq V$ tatsächlich ein Unterraum ist. Somit ist U die kleinste obere Schranke von X, also das Supremum.

Auch die Summe von zwei Untervektorräumen sollte man so sehen: Es ist der kleinste Vektorraum, der beide enthält, als ein Supremum. Das Infimum ist als Durchschnitt besonders leicht zu konstruieren. Die Unterräume von V bilden damit einen Verband.

Ordnungsrelationen

F101

Beispiel: Für natürliche Zahlen $a, b \in \mathbb{N}$ definieren wir die Kleiner-Gleich-Relation $a \leq b$ durch die Bedingung $a + x = b$ für ein $x \in \mathbb{N}$:

$$(\leq) = R = \{\, (a,b) \in \mathbb{N} \times \mathbb{N} \mid \exists x \in \mathbb{N} : a + x = b \,\}$$

Diese Relation auf $X = \mathbb{N}$ erfreut sich folgender Eigenschaften:

Reflexivität,	**Refl**(X,R):	$\Delta_X \subseteq R$,	$a \leq a$
Transitivität,	**Tran**(X,R):	$R \bullet R \subseteq R$,	$a \leq b \wedge b \leq c \Rightarrow a \leq c$
Antisymmetrie,	**Asym**(X,R):	$R \cap R^\intercal \subseteq \Delta_X$,	$a \leq b \wedge b \leq a \Rightarrow a = b$
Totalität,	**Total**(X,R):	$R \cup R^\intercal = X \times X$,	$a \leq b \vee b \leq a$

Definition F1A: Ordnungsrelation

Eine Relation $R \subseteq X \times X$ auf der Menge X heißt… falls… gilt:

Name \ Eigenschaften	Refl	Tran	Asym	Total
totale Ordnung, lineare Ordnung, Toset	✓	✓	✓	✓
(partielle) **Ordnung**, Halbordnung, Poset	✓	✓	✓	
totale Präordnung, Präferenzordnung	✓	✓		✓
(partielle) **Präordnung**, Quasiordnung	✓	✓		

Ordnungsrelationen

F102
Erläuterung

Ist $R \subseteq X \times X$ eine totale / partielle Prä/Ordnung auf der Menge X, so nennen wir das Paar (X,R) eine total / partiell prä/geordnete Menge.

Die englischen Bezeichnungen Poset / Toset sind bequem und üblich. Für prägeordnete Mengen findet man auch die Bezeichnung Proset.

Manche der Axiome sind redundant: Aus Totalität folgt Reflexivität. Reflexivität und Antisymmetrie sind äquivalent zu $R \cap R^\intercal = \Delta_X$.

Beispiel: Jede Äquivalenzrelation ist eine symmetrische Präordnungen: Zusätzlich zu Reflexivität und Transitivität fordern wir noch Symmetrie.

Übliche Schreibweisen für Ordnungen sind $\leq, =, \geq$ oder $\sqsubseteq, =, \sqsupseteq$, für die Inklusion von Mengen passt dazu $\subseteq, =, \supseteq$ besonders gut.

Für Präordnungen eignen sich $\preccurlyeq, \approx, \succcurlyeq$ oder $\lesssim, \approx, \gtrsim$. Hier wird die Gleichheit $=$ gelockert zur Äquivalenz $\approx$ assoziierter Elemente.

Für die zugehörigen Striktordnungen schreiben wir dann entsprechend $<, =, >$ und $\sqsubset, =, \sqsupset$ und $\subseteq, =, \supseteq$ und $\prec, \approx, \succ$, etc.

Ordnungsrelationen: total vs partiell

F103

Beispiel: Auf $\mathbb{N}$ ist $\leq$ eine totale Ordnung, das Paar $(\mathbb{N}, \leq)$ ist ein Toset. Dasselbe gilt für $(\mathbb{Z}, \leq)$ und $(\mathbb{Q}, \leq)$ und $(\mathbb{R}, \leq)$ mit der üblichen Ordnung.

Beispiel: Sei Ω eine Menge und $\mathscr{A} = \mathfrak{P}(\Omega)$ die Potenzmenge. Die Inklusionsrelation $\subseteq$ erfreut sich folgender Eigenschaften:

Reflexivität,	**Refl**$(\mathscr{A}, \subseteq)$:	$A \subseteq A$
Transitivität,	**Tran**$(\mathscr{A}, \subseteq)$:	$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
Antisymmetrie,	**Asym**$(\mathscr{A}, \subseteq)$:	$A \subseteq B \wedge B \subseteq A \Rightarrow A = B$

Totalität gilt jedoch nicht: Es gilt weder $\{1\} \subseteq \{2\}$ noch $\{2\} \subseteq \{1\}$. Auf $\mathscr{A}$ ist $\subseteq$ eine partielle Ordnung, das Paar $(\mathscr{A}, \subseteq)$ ist ein Poset.

Definition F1B: vergleichbare Elemente

Sei $\preccurlyeq$ eine Prä/Ordnung auf X, also $(X, \preccurlyeq)$ eine prä/geordnete Menge.

Zwei Elemente $a, b \in X$ heißen **vergleichbar**, falls $a \preccurlyeq b$ oder $b \preccurlyeq a$ gilt. Die Prä/Ordnung $\preccurlyeq$ ist **total**, wenn je zwei Elemente vergleichbar sind.

Gilt weder $a \preccurlyeq b$ noch $b \preccurlyeq a$, so nennen wir a und b **unvergleichbar**. Dies kürzen wir mit $a \parallel b$ ab. Im obigen Beispiel gilt $\{1\} \parallel \{2\}$.

Ordnungsrelationen: assoziierte Elemente

F104

Beispiel: Auf der Menge $\mathbb{Z}$ definieren wir die Teilbarkeitsrelation $a \mid_{\mathbb{Z}} b$ durch $\exists a' \in \mathbb{Z} : aa' = b$. Diese erfreut sich folgender Eigenschaften:

Reflexivität,	**Refl**$(\mathbb{Z}, \mid_{\mathbb{Z}})$:	$a \mid_{\mathbb{Z}} a$
Transitivität,	**Tran**$(\mathbb{Z}, \mid_{\mathbb{Z}})$:	$a \mid_{\mathbb{Z}} b \wedge b \mid_{\mathbb{Z}} c \Rightarrow a \mid_{\mathbb{Z}} c$

Antisymmetrie gilt jedoch nicht: Aus $a \mid_{\mathbb{Z}} b$ und $b \mid_{\mathbb{Z}} a$ folgt nur $a = \pm b$. Auf der Menge $\mathbb{Z}$ ist die Teilbarkeit $\mid_{\mathbb{Z}}$ nur eine (partielle) Präordnung.

Definition F1C: assoziierte Elemente

Jede Präordnung $(\preccurlyeq) = R$ auf X definiert eine Äquivalenzrelation $(\approx) = R \cap R^\intercal$, **assoziierte Elemente** $a \approx b$ erfüllen $a \preccurlyeq b \wedge b \preccurlyeq a$.

Der Quotient $q : X \twoheadrightarrow Q = X/_\approx : a \mapsto [a]$ fasst assoziierte Elemente zusammen; auf Q erhalten wir die Ordnung $\leq$ mit $[a] \leq [b] \Leftrightarrow a \preccurlyeq b$.

Übung: Weisen Sie die impliziten Behauptungen sorgsam nach!

Beispiel: In der prägeordneten Menge $(\mathbb{Z}, \mid_{\mathbb{Z}})$ gilt $a \approx b \Leftrightarrow a = \pm b$, und $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/_\approx : a \mapsto \{\pm a\}$ entspricht $p : (\mathbb{Z}, \mid_{\mathbb{Z}}) \twoheadrightarrow (\mathbb{N}, \mid_{\mathbb{N}}) : a \mapsto |a|$. Die Präordnung $\mid_{\mathbb{Z}}$ auf $\mathbb{Z}$ wird zusammengefasst zur Ordnung $\mid_{\mathbb{N}}$ auf $\mathbb{N}$.

Ordnungsrelationen: Striktordnung

F105

Definition F1D: zugehörige Striktordnung

Sei $\preccurlyeq$ eine Prä/Ordnung auf X, also $(X, \preccurlyeq)$ eine prä/geordnete Menge.

Zu $(\preccurlyeq) = R$ ist $(\succcurlyeq) = R^\intercal$ die **umgekehrte Relation**: $a \succcurlyeq b \Leftrightarrow b \preccurlyeq a$.
Die Negation von $a \preccurlyeq b$ schreiben wir $a \not\preccurlyeq b$, also: $a \not\preccurlyeq b \Leftrightarrow \neg(a \preccurlyeq b)$.

Die **Striktordnung** $(\prec) = S$ zu $(\preccurlyeq) = R$ ist $a \prec b \Leftrightarrow a \preccurlyeq b \wedge b \not\preccurlyeq a$.
Die Striktordnung zu $\succcurlyeq$ schreiben wir entsprechend $\succ$.

Für je zwei Elemente a, b in $(X, \preccurlyeq)$ gilt genau eine der vier Relationen

$$a \prec b \;\dot\vee\; a \succ b \;\dot\vee\; a \approx b \;\dot\vee\; a \parallel b.$$

Ist die betrachtete Präordnung $(\preccurlyeq)$ total, so ist $a \parallel b$ ausgeschlossen.
Ist $(\preccurlyeq)$ eine Ordnung, also antisymmetrisch, so gilt $a \approx b \Leftrightarrow a = b$.

Ist $(\leq) = R$ eine totale Ordnung, so gilt für die Striktordnung $(<) = S$:
Trichotomie, **Tri**(X, S): $X \times X = S \sqcup \Delta_X \sqcup S^\intercal$, $x < y \;\dot\vee\; x = y \;\dot\vee\; y < x$
Transitivität, **Tran**(X, S): $S \bullet S \subseteq S$, $x < y \wedge y < z \Rightarrow x < z$
Wir nennen $(<) = S \subseteq X \times X$ dann eine **totale Striktordnung** auf X.
In diesem Falle ist $(\leq) = R = S \sqcup \Delta_X$ eine totale Ordnung auf X.

Ordnungsrelationen: Einschränkung

F106

Definition F1E: eingeschränkte Ordnungsrelation

Sei $U \subseteq X$. Ist (X, R) eine total / partiell prä/geordnete Menge, so auch ihre **Einschränkung** (U, R_U) auf die Menge U mit $R_U = R \cap (U \times U)$.
Wir nennen U in $(X, \leq)$ eine **Kette**, wenn $(U, \leq_U)$ total geordnet ist.

Beispiel: Wir schränken $(\mathbb{R}, \leq_\mathbb{R})$ ein zu $(\mathbb{Q}, \leq_\mathbb{Q})$ zu $(\mathbb{Z}, \leq_\mathbb{Z})$ zu $(\mathbb{N}, \leq_\mathbb{N})$.
Bequemer kürzen wir meist (U, R_U) zu (U, R) ab, also hier $(\mathbb{R}, \leq)$ zu $(\mathbb{Q}, \leq)$ zu $(\mathbb{Z}, \leq)$ zu $(\mathbb{N}, \leq)$. Alle vier sind total geordnet, also Ketten.

Beispiel: Die Teilbarkeits-Präordnung $|_\mathbb{Z}$ auf $\mathbb{Z}$ wird auf $\mathbb{N}$ eingeschränkt zur Teilbarkeits-Ordnung $|_\mathbb{N}$. Hier gilt Antisymmetrie, aber nicht Totalität.

Beispiel: In $(\mathfrak{P}(\mathbb{N}), \subseteq)$ haben wir die Kette

$$U = \{\, \emptyset \subset \{0\} \subset \{0,1\} \subset \{0,1,2\} \subset \{0,1,2,3\} \,\}.$$

Notation: Wir schreiben kurz und bequem $\{a_1 < a_2 < \cdots < a_n\}$ für die Menge $\{a_1, a_2, \ldots, a_n\}$ mit der Ordnung $a_1 < a_2 < \cdots < a_n$. (Satz F1F)
🙂 Jede endliche Kette lässt sich so sortieren und bequem darstellen.

Ordnungsrelationen: Zurückziehen

F107
Erläuterung

Beispiel: Auf $\mathbb{C} = \mathbb{R}^2$ definieren wir die Präordnung $a \preccurlyeq b \Leftrightarrow |a| \leq |b|$.
Eingeschränkt auf $\mathbb{N}$ oder $\mathbb{Q}_{\geq 0}$ oder $\mathbb{R}_{\geq 0}$ ist dies die übliche Ordnung.
In $\mathbb{R}$ hingegen sind $\pm a$ assoziiert, in $\mathbb{C}$ jeweils ganze Kreislinien (E322).

Allgemein haben wir die **Zurückziehung** bezüglich $f : X \to (Y, \sqsubseteq)$:

Sei $(Y, \sqsubseteq)$ eine prägeordnete Menge und $f : X \to Y$ eine Abbildung.
Auf X erhalten wir daraus die Präordnung $a \preccurlyeq b \Leftrightarrow f(a) \sqsubseteq f(b)$.

Ist f injektiv und $\sqsubseteq$ eine Ordnung, also antisymmetrisch, so auch $\preccurlyeq$.
Ist $\sqsubseteq$ total, so auch $\preccurlyeq$: Je zwei Elemente sind vergleichbar.

Beispiel: Für $f : \mathbb{C} \to (\mathbb{R}, \leq) : z \mapsto |z|$ erhalten wir das obige Beispiel.

Beispiel: Für die Inklusion $U \hookrightarrow X$ erhalten wir die Einschränkung.

Beispiel: Sei $(X, \preccurlyeq)$ eine geordnete Menge (Poset) und endlich, wir haben also eine Bijektion $\{1, \ldots, n\} \xrightarrow{\sim} X : i \mapsto x_i$. Diese können wir so sortieren, dass $x_{i-1} \preccurlyeq x_i$ gilt für alle $i = 2, \ldots, n$, eventuell mit $\approx$.
Dies zerlegt X in Äquivalenzklassen, und die Quotientenabbildung entspricht einer Surjektion $f : X \twoheadrightarrow \{1, \ldots, k\}$ mit $x \preccurlyeq y \Leftrightarrow f(x) \leq f(y)$.

Ordnungsrelationen: Erzeugung

F108

Satz F1F: die erzeugte Präordnung

Jede Relation $R \subseteq X \times X$ erzeugt eine Präordnung $P \subseteq X \times X$:

$$P = \bigcup_{n \in \mathbb{N}} R^{\bullet n} = \Delta_X \cup R \cup (R \bullet R) \cup (R \bullet R \bullet R) \cup \ldots$$

Damit ist P die kleinste Präordnung auf X, die R enthält.
Wir nennen P die von R auf X **erzeugte Präordnung**.

Übung: (1) Zeigen Sie, dass P tatsächlich eine Präordnung auf X ist.
(2) Zudem ist P die kleinste Präordnung, die P enthält (siehe Satz E3H).

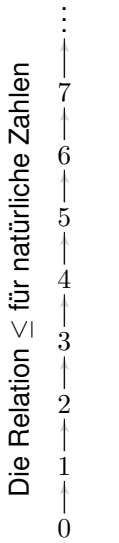
Beispiel: Für $X = \mathbb{N}$ und $R = \{\, (a, a+1) \mid a \in \mathbb{N} \,\}$ erhalten wir $P = \{\, (a, a+x) \mid a, x \in \mathbb{N} \,\} = (\leq)$, die übliche Ordnung auf $\mathbb{N}$.

Beispiel: Wir schreiben $\{a \approx b \prec c \approx d\}$ für die Menge $X = \{a, b, c, d\}$ mit der durch diese Angaben erzeugten Präordnung $P = (\preccurlyeq)$.

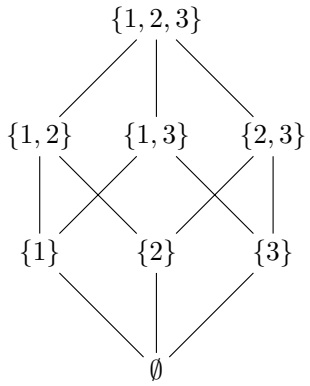
Beispiel: Ist R bereits transitiv, $R \bullet R = R$, so gilt $P = \Delta_X \cup R$.
Ist (X, R) eine geordnete Menge mit Striktordnung $S = R \setminus \Delta_X$, so ist S transitiv, also $S \bullet S = S$, und erzeugt $P = \Delta_X \cup S = R$.

Hasse–Diagramm als graphische Darstellung

Die Relation $a \leq b$ schreiben wir durch einen Pfeil $a \to b$ oder kurz eine Linie von a hoch zu b. Dies erzeugt eine Präordnung gemäß Satz F1F.



Inklusion von Mengen in $\mathfrak{P}(\{1,2,3\})$



Ordnungsrelationen: kleine Beispiele

Aufgabe: Für jede Menge X vereinbaren wir:

$$\mathbb{O}(X) := \{\, R \subseteq X \times X \mid R \text{ ist eine totale Ordnung auf } X \,\}$$
$$\mathbb{P}(X) := \{\, R \subseteq X \times X \mid R \text{ ist eine totale Präordnung auf } X \,\}$$

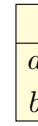
(1) Bestimmen Sie $\mathbb{O}(X)$ und $\mathbb{P}(X)$ für $X = \{a, b\}$. (2) für $X = \{a, b, c\}$.
(3) Bestimmen Sie $\sharp\mathbb{O}(X)$ und $\sharp\mathbb{P}(X)$ für X endlich mit n Elementen.

Lösung: (1) Es gibt genau drei totale Präordnungen auf $\{a, b\}$:

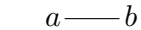
$$\mathbb{O} = \left\{ \begin{array}{ll} \{(a,a),(a,b),(b,b)\} & \text{kurz: } a \prec b \\ \{(a,a),(b,a),(b,b)\} & \text{kurz: } b \prec a \\ \{(a,a),(a,b),(b,a),(b,b)\} & \text{kurz: } a \approx b \end{array} \right\} = \mathbb{P}$$

	a	b
a	1	1
b	0	1

	a	b
a	1	0
b	1	1



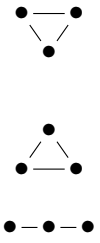
	a	b
a	1	1
b	1	1



Ordnungsrelationen: kleine Beispiele

(2) Es gibt genau 13 totale Präordnungen auf $X = \{a, b, c\}$:

$$\mathbb{O} = \left\{ \begin{array}{ll} a \prec b \prec c & a \prec b \approx c \\ a \prec c \prec b & b \prec a \approx c \\ b \prec a \prec c & c \prec a \approx b \\ b \prec c \prec a & a \approx b \prec c \\ c \prec a \prec b & a \approx c \prec b \\ c \prec b \prec a & b \approx c \prec a \\ & a \approx b \approx c \end{array} \right\} = \mathbb{P}$$



(3) Für $\sharp X = n$ finden wir $\sharp\mathbb{O}(X) = n!$ und $\sharp\mathbb{P}(X) = \sum_{k=0}^{n} k! \left\{ {n \atop k} \right\}$:

n	1	2	3	4	5	6	7	8	9	10
$\sharp\mathbb{O}$	1	2	6	24	120	720	5 040	40 320	362 880	3 628 800
$\sharp\mathbb{P}$	1	3	13	75	541	4 683	47 293	545 835	7 087 261	102 247 563

🙂 Die totalen Prä/Ordnungen auf X entsprechen den Bijektionen $f : X \xrightarrow{\sim} \{1, \ldots, n\}$ bzw. den Surjektionen $f : X \twoheadrightarrow \{1, \ldots, k\}$.

Ordnungsrelationen: kleine Beispiele

Die Anzahl $\sharp\mathbb{O}(X) = n!$ ist leicht zu sehen: Für jede Totalordnung auf X besteht das Hasse–Diagramm aus n übereinanderliegenden Punkten. Wir haben demnach $n!$ mögliche Beschriftungen mit Elementen aus X, und je zwei Beschriftungen ergeben verschiedene Totalordnungen.

Die Formel $\sharp\mathbb{P}(X) = \sum_{k=0}^{n} k! \left\{ {n \atop k} \right\}$ ist raffinierter, aber im Prinzip ähnlich: Das Hasse–Diagramm hat nun k Etagen, und $f : X \twoheadrightarrow \{1, \ldots, k\}$ ordnet die Elemente von X den Etagen zu. Untere Elemente sind kleiner als obere Elemente, Elemente auf derselben Etage sind assoziiert.

Die Anzahl $\sharp\mathbb{P}(A)$ heißt auch $n$te *Fubini–Zahl* (`oeis.org/A000670`) oder *Bell–Zahl* (`en.wikipedia.org/wiki/Ordered_Bell_number`).

Es ist oft lehrreich, neu definierte Objekte zu zählen. Dies zwingt dazu, die Definition genau zu verstehen und klärt so Missverständnisse auf.
Defendit numerus. [Die Zahl gibt Schutz.] Juvenal (58–138 n.Chr.), *Satiren*

Efrons intransitive Würfel: Welcher ist der beste?

Aufgabe: Der Statistiker Bradley Efron erfand folgende Würfel:

Alice

$$A : 5,5,5,1,1,1$$
$$B : 6,6,2,2,2,2$$
$$C : 3,3,3,3,3,3$$
$$D : 4,4,4,4,0,0$$

Bob

Je zwei Würfel treten gegeneinander an, z.B. A gegen B. Wie groß sind die Gewinnwkten $\mathbf{P}(A > B)$ etc.? Welcher Würfel ist dabei der beste?

Lösung: Abzählen aller Gewinnkombinationen ergibt:

$$\mathbf{P}(A > B) = 12/36 = 1/3, \qquad \mathbf{P}(B > C) = 12/36 = 1/3,$$
$$\mathbf{P}(C > D) = 12/36 = 1/3, \qquad \mathbf{P}(D > A) = 12/36 = 1/3,$$
$$\mathbf{P}(A > C) = 18/36 = 1/2, \qquad \mathbf{P}(B > D) = 20/36 = 5/9.$$

Es gibt keinen „besten“ Würfel: Jeder wird vom nächsten geschlagen!

🙂 Penney's Game: Intransitivität entsteht auch in zufälligen 0-1-Folgen beim Wettrennen von je zwei der acht Tripel: Wer schlägt hier wen?

Intransitive Gewinnwahrscheinlichkeiten

Aufgabe: Spieler A und B wählen je ein Muster der Länge n. Es gewinnt, wes Muster als erstes auftritt. Ab $n \geq 3$ sind die Wkten nicht transitiv!

B\A	00	01	10	11
00		1/2	3/4	1/2
01	1/2		1/2	1/4
10	1/4	1/2		1/2
11	1/2	3/4	1/2	

Wkt, dass Muster A vor Muster B eintritt.

B\A	000	001	010	011	100	101	110	111
000		1/2	3/5	3/5	7/8	7/12	7/10	1/2
001	1/2		1/3	1/3	3/4	3/8	1/2	3/10
010	2/5	2/3		1/2	1/2	1/2	5/8	5/12
011	2/5	2/3	1/2		1/2	1/2	1/4	1/8
100	1/8	1/4	1/2	1/2		1/2	2/3	2/5
101	5/12	5/8	1/2	1/2	1/2		2/3	2/5
110	3/10	1/2	3/8	3/4	1/3	1/3		1/2
111	1/2	7/10	7/12	7/8	3/5	3/5	1/2	

Es kommt noch verrückter: Die Muster 1010 und 0100 haben mittlere Wartezeit 20 bzw. 18, doch 1010 kommt vor 0100 mit Wkt $9/14 > 1/2$. Das seltenere Muster gewinnt gegen das häufigere Muster! Das zeigt, wie trügerisch unsere Intuition zu Wartezeiten und Gewinnwkten ist.
Martin Gardner: *The Colossal Book of Mathematics.* Norton & Co 2001

Warum gilt Intransitivität als paradox?

Häufig erwarten wir Transitivität und werden vom Gegenteil arg verblüfft. In solch Extremfällen sprechen wir von einem **Intransitivitäts-Paradox**.

Beispiel: Im Zeitalter digitaler Photographie kommt es vor, dass Sie von einem Motiv viele ähnliche Bilder / Schnappschüsse haben. Nun wollen Sie das schönste aussuchen und alle anderen löschen. Sie können je zwei vergleichen, aber nach dreien gefällt Ihnen doch das erste besser, sodass $x \prec y \prec z \prec x$. (Das liegt manchmal an wechselnden Kriterien.)

Beispiel: Lineare Ordnungen nutzen wir zum Suchen und Sortieren in Wörterbüchern, Datenbanken, Turnieren. Zirkulär wäre katastrophal. Für lineare Ordnungen haben wir phantastisch effiziente Algorithmen, ohne Transitivität versagen sie jedoch kläglich: Suchen und Sortieren kommt nicht zum Ende oder liefert fehlerhafte, widersinnige Resultate.

Beispiel: Bei Wahlen möchten wir demokratisch einen Sieger küren. Das ist unmöglich, falls das Ergebnis eine intransitive Relation ist. Sie kennen das von *Schere-Stein-Papier*. Das Wahlergebnis ist in diesem (und ähnlichen) Fällen nicht transitiv und daher unbrauchbar.

Warum gilt Intransitivität als irrational?

Wir untersuchen **rationale Entscheidungen** [*rational choice theory*]. Mit Transitivität verbieten wir zyklische Anordnungen wie $x \succ y \succ z \succ x$ oder allgemeiner $x \succcurlyeq y \succcurlyeq z \succ x$. Eine solche Präferenz würden wir als irrational betrachten. Warum ist Intransitivität eine logische Katastrophe?

Beispiel: In den Wirtschaftswissenschaften begründet man Transitivität dadurch, dass man einem Individuum mit intransitiver Präferenz alles Geld abknöpfen kann durch eine ewige **Geldpumpe** [*money pump*]:

Wegen $x \succcurlyeq y \succcurlyeq z$ kann man z zuerst in y und dann in x eintauschen; wegen $z \succ x$ kann man x gegen z und einen Geldbetrag tauschen, usw. Dieser närrische Kreislauf endet erst, wenn alles Geld verbraucht ist, oder wenn schließlich die Vernunft einsetzt: Intransitiv ist irrational.

🙂 Genau dieses Verhalten zeigt *Hans im Glück* der Brüder Grimm. Vordergründig illustriert dies Irrationalität, Planlosigkeit, Impulsivität, leichtfertiges Handeln ohne Erwägung naheliegender Konsequenzen, Unbeständigkeit durch Wechsel der Kriterien je nach Situation.

Untere und obere Schranken

Definition F1G: untere und obere Schranken

Sei $(X, \leq)$ eine geordnete Menge (Poset) sowie $U, V \subseteq X$ und $s \in X$.

s ist untere Schranke / Minorante von U: $\quad s \leq U \;:\Leftrightarrow\; \forall x \in U : s \leq x$

s ist obere Schranke / Majorante von U: $\quad U \leq s \;:\Leftrightarrow\; \forall x \in U : x \leq s$

Diese Eigenschaft definiert die Menge der unteren / oberen Schranken:

$$\mathrm{UnSch}(U) = \mathrm{UnSch}(U; X, \leq) := \{\, s \in X \mid s \leq U \,\}$$
$$\mathrm{ObSch}(U) = \mathrm{ObSch}(U; X, \leq) := \{\, s \in X \mid U \leq s \,\}$$

Wir nennen die Menge U in $(X, \leq)$ **nach unten / oben beschränkt**, falls $\mathrm{UnSch}(U) \neq \emptyset$ bzw. $\mathrm{ObSch}(U) \neq \emptyset$ gilt. Ebenso definieren wir:

$$U \leq V \quad :\Leftrightarrow \quad \forall x \in U \;\; \forall y \in V \;:\; x \leq y$$

Die Negation $s \not\leq U$ und $U \not\leq s$ und $U \not\leq V$ bedeutet, es gibt mindestens eine Ausnahme. Für die Striktordnung $<$ schreiben wir entsprechend $s < U$ und $U < s$ und $U < V$ und negiert $s \not< U$ und $U \not< s$ und $U \not< V$.

Untere und obere Schranken

Beispiele: In $(\mathbb{R}, \leq)$ gilt

$$\begin{array}{llll} 0 < [1,3], & 1 \not< [1,3], & 1 \leq [1,3], & 2 \not\leq [1,3], \\ [1,3] \not\leq 2, & [1,3] \leq 3, & [1,3] \not< 3, & [1,3] < 4, \\ [1,3] < [4,6], & [1,3] \not< [3,5], & [1,3] \leq [3,5], & [1,3] \not\leq [2,4]. \end{array}$$

Für alle $a \leq b$ in $\mathbb{R}$ haben wir

$$\begin{array}{ll|ll} \mathrm{UnSch}([a,b]) & = \mathbb{R}_{\leq a}, & \mathrm{ObSch}([a,b]) & = \mathbb{R}_{\geq b}, \\ \mathrm{UnSch}(\mathbb{R}_{\geq a}) & = \mathbb{R}_{\leq a}, & \mathrm{ObSch}(\mathbb{R}_{\geq a}) & = \emptyset, \\ \mathrm{UnSch}(\mathbb{R}_{\leq b}) & = \emptyset, & \mathrm{ObSch}(\mathbb{R}_{\leq b}) & = \mathbb{R}_{\geq b}, \\ \mathrm{UnSch}(\mathbb{R}) & = \emptyset, & \mathrm{ObSch}(\mathbb{R}) & = \emptyset, \\ \mathrm{UnSch}(\emptyset) & = \mathbb{R}, & \mathrm{ObSch}(\emptyset) & = \mathbb{R}. \end{array}$$

Beispiel: Die bequeme Schreibweise $1 \leq a, b \leq 5$ wird oft genutzt für $1 \leq \{a, b\} \leq 5$, also ausgeschrieben $1 \leq a \wedge a \leq 5 \wedge 1 \leq b \wedge b \leq 5$.

Notationskonflikt: Auch die Interpretation $1 \leq a \wedge b \leq 5$ ist möglich. Zur Sicherheit sollte man im Kontext erklären, was genau gemeint ist.

Kleinste und größte Elemente

Definition F1H: kleinste und größte Elemente

Sei $(X, \leq)$ eine geordnete Menge (Poset) sowie $U \subseteq X$ und $s \in X$.

s ist kleinstes Element von $U \quad :\Leftrightarrow \quad s \in U \wedge s \leq U$

s ist größtes Element von $U \quad :\Leftrightarrow \quad s \in U \wedge U \leq s$

Diese Eigenschaft definiert die Menge der kleinsten / größten Elemente:

$$\mathrm{Kl}(U) = \mathrm{Kl}(U, \leq) := \{\, s \in U \mid s \leq U \,\}$$
$$\mathrm{Gr}(U) = \mathrm{Gr}(U, \leq) := \{\, s \in U \mid U \leq s \,\}$$

Eindeutigkeit: U enthält höchstens ein kleinstes / größtes Element:

Für je zwei Elemente $s, t \in \mathrm{Kl}(U)$ gilt $s \leq t$ und $t \leq s$, also $s = t$.
Entweder gilt $\mathrm{Kl}(U) = \emptyset$ oder $\mathrm{Kl}(U) = \{s\}$, kurz $s =: \mathrm{kl}(U)$.

Für je zwei Elemente $s, t \in \mathrm{Gr}(U)$ gilt $s \leq t$ und $t \leq s$, also $s = t$.
Entweder gilt $\mathrm{Gr}(U) = \emptyset$ oder $\mathrm{Gr}(U) = \{t\}$, kurz $t =: \mathrm{gr}(U)$.

Kleinste und größte Elemente

Beispiele: In $(\mathbb{R}, \leq)$ gilt für alle $a < b$:

$$\begin{array}{ll|ll} \mathrm{Kl}([a,b]) & = \{a\}, & \mathrm{Gr}([a,b]) & = \{b\}, \\ \mathrm{Kl}(]a,b]) & = \emptyset, & \mathrm{Gr}(]a,b]) & = \{b\}, \\ \mathrm{Kl}([a,b[) & = \{a\}, & \mathrm{Gr}([a,b[) & = \emptyset, \\ \mathrm{Kl}(]a,b[) & = \emptyset, & \mathrm{Gr}(]a,b[) & = \emptyset. \end{array}$$

Beispiele: In $(\mathfrak{P}(\Omega), \subseteq)$ gilt:

$$\begin{array}{ll|ll} \mathrm{Kl}\,\mathfrak{P}(\Omega) & = \{\emptyset\}, & \mathrm{Gr}\,\mathfrak{P}(\Omega) & = \{\Omega\}, \\ \mathrm{kl}\,\mathfrak{P}(\Omega) & = \emptyset, & \mathrm{gr}\,\mathfrak{P}(\Omega) & = \Omega. \end{array}$$

Kleinste oder größte Elemente existieren auch hier nicht immer:

$$\begin{array}{ll|ll} \mathrm{Kl}\{\{1\},\{2\}\} & = \emptyset, & \mathrm{Gr}\{\{1\},\{2\}\} & = \emptyset, \\ \mathrm{Kl}\{\{1\},\{2\},\{1,2\}\} & = \emptyset, & \mathrm{Gr}\{\{1\},\{2\},\{1,2\}\} & = \{\{1,2\}\}, \\ \mathrm{Kl}\{\{1\},\{1,2\},\{1,3\}\} & = \{\{1\}\}, & \mathrm{Gr}\{\{1\},\{1,2\},\{1,3\}\} & = \emptyset, \\ \mathrm{Kl}\{\{1\},\{1,2\}\} & = \{\{1\}\}, & \mathrm{Gr}\{\{1\},\{1,2\}\} & = \{\{1,2\}\}. \end{array}$$

Definition F1I: minimale und maximale Elemente

Sei $(X, \leq)$ eine geordnete Menge (Poset) sowie $U \subseteq X$ und $s \in X$.

$$s \text{ ist minimal in } U \quad :\Leftrightarrow \quad s \in U \wedge \forall t \in U : t \leq s \Rightarrow t = s$$
$$s \text{ ist maximal in } U \quad :\Leftrightarrow \quad s \in U \wedge \forall t \in U : s \leq t \Rightarrow s = t$$

Diese Eigenschaft definiert die Menge der Minima / Maxima von U:

$$\operatorname{Min}(U) = \operatorname{Min}(U, \leq) := \{\, s \in U \mid \forall t \in U : t \leq s \Rightarrow t = s \,\}$$
$$\operatorname{Max}(U) = \operatorname{Max}(U, \leq) := \{\, s \in U \mid \forall t \in U : s \leq t \Rightarrow s = t \,\}$$

Bemerkung: In jedem Poset $(X, \leq)$ gelten die Inklusionen

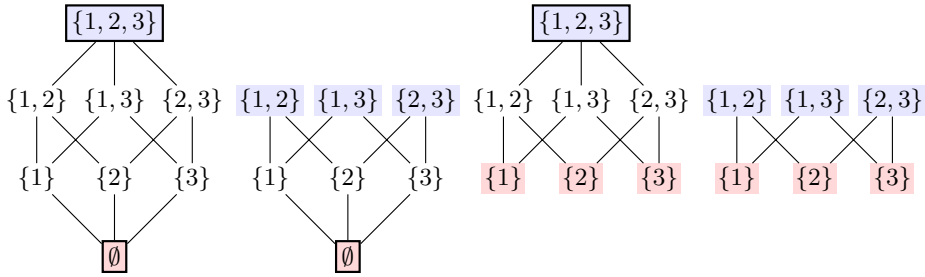
$$\operatorname{Min}(U) \supseteq \operatorname{Kl}(U) \quad \text{und} \quad \operatorname{Max}(U) \supseteq \operatorname{Gr}(U).$$

☺ Ist $(U, \leq)$ zudem total geordnet, also eine Kette in $(X, \leq)$, so gilt

$$\operatorname{Min}(U) = \operatorname{Kl}(U) \quad \text{und} \quad \operatorname{Max}(U) = \operatorname{Gr}(U).$$

Entweder gilt $\operatorname{Min}(U) = \emptyset$ oder $\operatorname{Min}(U) = \{s\}$, kurz $s =: \min(U)$.
Entweder gilt $\operatorname{Max}(U) = \emptyset$ oder $\operatorname{Max}(U) = \{t\}$, kurz $t =: \max(U)$.

Beispiele: Für U in $(\mathfrak{P}(\mathbb{N}), \subseteq)$ finden wir:



Minimale Elemente sind rot markiert, maximale Element blau.
Kleinste und größte Elemente sind zudem eingerahmt.

Beispiel: In $(\mathfrak{P}(\mathbb{Z}), \subseteq)$ betrachten wir

$$U = \{\, A \subseteq \mathbb{N} \mid \sharp A = \sharp(\mathbb{N} \setminus A) = \infty \,\} \quad \text{und} \quad V = U \cup \{\{-1\}\}.$$

Hier gilt $\operatorname{Min}(U) = \operatorname{Max}(U) = \emptyset$, also auch $\operatorname{Kl}(U) = \operatorname{Gr}(U) = \emptyset$,
hingegen $\operatorname{Min}(V) = \operatorname{Max}(V) = \{\{-1\}\}$ und $\operatorname{Kl}(V) = \operatorname{Gr}(V) = \emptyset$.

Definition F1J: Infimum und Supremum

Sei $(X, \leq)$ eine geordnete Menge (Poset) sowie $U \subseteq X$ und $s \in X$.

$$s \text{ ist Infimum von } U \quad :\Leftrightarrow \quad s \leq U \wedge \forall t \in X : t \leq U \Rightarrow t \leq s$$
$$s \text{ ist Supremum von } U \quad :\Leftrightarrow \quad U \leq s \wedge \forall t \in X : U \leq t \Rightarrow s \leq t$$

Das Infimum ist also **die größte untere Schranke** (untere Grenze),
und das Supremum ist **die kleinste obere Schranke** (obere Grenze).

$$\operatorname{Inf}(U) = \operatorname{Inf}(U; X, \leq) := \operatorname{Gr}(\operatorname{UnSch}(U; X, \leq))$$
$$\operatorname{Sup}(U) = \operatorname{Sup}(U; X, \leq) := \operatorname{Kl}(\operatorname{ObSch}(U; X, \leq))$$

Insbesondere sind beide somit eindeutig:
Entweder gilt $\operatorname{Inf}(U) = \emptyset$ oder $\operatorname{Inf}(U) = \{s\}$, kurz $s =: \inf(U)$.
Entweder gilt $\operatorname{Sup}(U) = \emptyset$ oder $\operatorname{Sup}(U) = \{t\}$, kurz $t =: \sup(U)$.

Wir nennen $(X, \leq)$ **ordnungsvollständig**, falls jede nicht-leere nach unten / oben beschränkte Teilmenge ein Infimum / Supremum besitzt.

Beispiel: In $(\mathbb{N}, |)$ gilt $\operatorname{UnSch}\{a, b\} = \operatorname{GT}(a, b)$ und $\inf\{a, b\} = \operatorname{ggT}(a, b)$
sowie entsprechend $\operatorname{ObSch}\{a, b\} = \operatorname{GV}(a, b)$ und $\sup\{a, b\} = \operatorname{kgV}(a, b)$.

Beispiel: In $(\mathfrak{P}(\Omega), \subseteq)$ gilt $\inf\{A, B\} = A \cap B$ und $\sup\{A, B\} = A \cup B$.
Für jedes Mengensystem $U \subseteq \mathfrak{P}(\Omega)$ gilt $\inf U = \bigcap U$ und $\sup U = \bigcup U$.

Beispiel: In $(\mathbb{Q}, \leq)$ sei $U = \{\, x \in \mathbb{Q} \mid x^2 \leq 2 \,\}$. Obere Schranken sind
1.5, 1.42, 1.415, 1.4143, ... Es gibt in $\mathbb{Q}$ keine kleinste obere Schranke!

Beispiel: In $(\mathbb{R}, \leq)$ gilt: Zu jeder Teilmenge $M \subseteq \mathbb{R}$, die nicht-leer und
nach oben beschränkt ist, existiert in $\mathbb{R}$ eine kleinste obere Schranke.
Im vorigen Beispiel gilt $\operatorname{Sup}(U; \mathbb{Q}, \leq) = \emptyset$, aber $\operatorname{Sup}(U; \mathbb{R}, \leq) = \{\sqrt{2}\}$.
Die rationalen Zahlen $(\mathbb{Q}, +, \cdot, \leq)$ sind ein geordneter Körper, doch die
zugrundeliegende geordnete Menge $(\mathbb{Q}, \leq)$ hat noch erhebliche Lücken!
Die reellen Zahlen $(\mathbb{R}, +, \cdot, \leq)$ sind ein vollständig geordneter Körper.
Erst damit lassen sich viele fundamentale und praktische Probleme
elegant und befriedigend lösen und eine tragfähige Grundlage finden.

Infimum und Supremum: erweiterte Zahlengerade $\bar{\mathbb{R}}$

Wir definieren die **erweiterte Zahlengerade** $\bar{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$.
Die Ordnung setzen wir fort durch $-\infty < a < +\infty$ für alle $a \in \mathbb{R}$.

Satz F1K: Supremum und Infimum in $\bar{\mathbb{R}}$

Jede Teilmenge $M \subseteq \bar{\mathbb{R}}$ hat ein Supremum und ein Infimum in $\bar{\mathbb{R}}$.
Dies definiert die beiden Abbildungen $\inf, \sup : \mathfrak{P}(\bar{\mathbb{R}}) \to \bar{\mathbb{R}}$.

Beispiele: Für alle $a < b$ in $\bar{\mathbb{R}}$ haben wir

$$\begin{aligned}
\mathrm{UnSch}(]a,b[) &= [-\infty, a], & \mathrm{ObSch}(]a,b[) &= [b, +\infty], \\
\inf(]a,b[) &= a, & \sup(]a,b[) &= b, \\
\mathrm{UnSch}(\mathbb{R}) &= \{-\infty\}, & \mathrm{ObSch}(\mathbb{R}) &= \{+\infty\}, \\
\inf(\mathbb{R}) &= -\infty, & \sup(\mathbb{R}) &= +\infty, \\
\mathrm{UnSch}(\emptyset) &= [-\infty, +\infty], & \mathrm{ObSch}(\emptyset) &= [-\infty, +\infty], \\
\inf(\emptyset) &= +\infty, & \sup(\emptyset) &= -\infty.
\end{aligned}$$

Infimum und Supremum: die Abbildungsmenge $\bar{\mathbb{R}}^\Omega$

Sei Ω eine Menge. Wir betrachten Funktionen $f, g : \Omega \to \bar{\mathbb{R}}$.
Die Ordnungsrelation $\leq$ auf $\bar{\mathbb{R}}^\Omega$ definieren wir punktweise:

$$f \leq g \quad :\Longleftrightarrow \quad \forall x \in \Omega : f(x) \leq g(x)$$

Das bedeutet, der Graph von f liegt unterhalb des Graphen von g.
Auch $\min(f, g)$ und $\max(f, g)$ definieren wir punktweise:

$$\begin{aligned}
\min(f,g) &: \Omega \to \bar{\mathbb{R}} : x \mapsto \min(f(x), g(x)) \\
\max(f,g) &: \Omega \to \bar{\mathbb{R}} : x \mapsto \max(f(x), g(x))
\end{aligned}$$

Ist $(f_i)_{i \in I}$ eine Familie von Funktionen $f_i : \Omega \to \bar{\mathbb{R}}$, so definieren wir:

$$\begin{aligned}
\inf_{i \in I} f_i &: \Omega \to \bar{\mathbb{R}} : x \mapsto \inf\{\, f_i(x) \mid i \in I \,\} \\
\sup_{i \in I} f_i &: \Omega \to \bar{\mathbb{R}} : x \mapsto \sup\{\, f_i(x) \mid i \in I \,\}
\end{aligned}$$

Dasselbe vereinbaren wir für Funktionen mit Werten in $\mathbb{R}$,
indem wir sie durch die Inklusionsabbildung $\mathbb{R} \hookrightarrow \bar{\mathbb{R}}$ verlängern.

Verbände und Vollständigkeit

Definition F1L: Verband und Vollständigkeit

Ein **Verband** $(X, \leq)$ ist eine geordnete Menge (Poset), in der je zwei Elemente $a, b \in X$ ein Infimum $a \wedge b = \inf\{a, b\}$ und ein Supremum $a \vee b = \sup\{a, b\}$ in X haben. Dies definiert die Verknüpfungen

$$\wedge, \vee : X \times X \to X : a \wedge b = \inf\{a, b\}, \quad a \vee b = \sup\{a, b\}.$$

Strenger nennen wir $(X, \leq)$ einen **vollständigen Verband**,
wenn jede Teilmenge $U \subseteq X$ ein Infimum $\bigwedge U = \inf U$ und ein Supremum $\bigvee U = \sup U$ in X hat. Dies definiert die Abbildungen

$$\bigwedge, \bigvee : \mathfrak{P}(X) \to X : \bigwedge U = \inf U, \quad \bigvee U = \sup U.$$

Beispiel: Die Logik nutzt den zweielementigen Verband $(\{0, 1\}, \leq)$.
Hierbei ist $a \wedge b$ das logische Und sowie $a \vee b$ das logische Oder.

Beispiel: Jede Menge Ω definiert den vollständigen Verband $(\mathfrak{P}(\Omega), \subseteq)$.
Hierbei ist $\inf U = \bigcap U$ der Schnitt und $\sup U = \bigcup U$ die Vereinigung.

Verbände und Vollständigkeit

Beispiel: Die natürlichen Zahlen sind ein Verband $(\mathbb{N}, |_{\mathbb{N}})$ mit der Teilbarkeitsrelation. Hier gilt $a \wedge b = \mathrm{ggT}(a, b)$ und $a \vee b = \mathrm{kgV}(a, b)$.
Dieser Verband ist vollständig, kleinstes Element ist 1, größtes ist 0.

Beispiel: Jede total geordnete Menge $(X, \leq)$ ist ein Verband dank $a \wedge b = \min\{a, b\} \in \{a, b\}$ und $a \vee b = \max\{a, b\} \in \{a, b\}$.
Demnach sind $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ Verbände. Diese sind nicht vollständig, insbesondere fehlen $\sup \emptyset = -\infty$ und $\inf \emptyset = +\infty$.

Beispiel: Die erweiterte Zahlengerade $(\bar{\mathbb{R}}, \leq)$ mit $\bar{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$ ist ein vollständiger Verband (Satz F1K), ebenso jedes Intervall $([a, b], \leq)$ mit $a \leq b$ in $\bar{\mathbb{R}}$ (siehe F1P). Auch $(\bar{\mathbb{N}}, \leq)$ mit $\bar{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$ und $(\bar{\mathbb{Z}}, \leq)$ mit $\bar{\mathbb{Z}} = \mathbb{Z} \cup \{\pm\infty\}$ sind vollständig, nicht jedoch $(\bar{\mathbb{Q}}, \leq)$ mit $\bar{\mathbb{Q}} = \mathbb{Q} \cup \{\pm\infty\}$.

Beispiel: Somit sind auch die Abbildungsmengen $(\bar{\mathbb{R}}^\Omega, \leq)$ und $([a, b]^\Omega, \leq)$ vollständige Verbände, wie oben erklärt. Der Vergleich $\leq$ wird hierbei punktweise definiert, ebenso Infimum und Supremum.

Übung: Ist $(X, \leq)$ ein (vollständiger) Verband, so auch $(X^\Omega, \leq)$ für jede Menge Ω. Beispiel: $(\mathfrak{P}(\Omega), \subseteq) \cong (\{0, 1\}^\Omega, \leq)$ gemäß D3D

Extremwerte einer Funktion

Sei Ω eine Menge, etwa $\Omega \subseteq \mathbb{R}^n$. Wir betrachten Funktionen $f : \Omega \to \bar{\mathbb{R}}$. Infimum und Supremum von f definieren wir durch

$$a = \inf f := \inf\{\, f(x) \mid x \in \Omega \,\},$$
$$b = \sup f := \sup\{\, f(x) \mid x \in \Omega \,\}.$$

Somit gilt $f(X) \subseteq [a, b]$. Gilt zudem $a \in f(X)$ bzw. $b \in f(X)$, so existieren $x_0, x_1 \in [a, b]$ mit $f(x_0) \leq f(x) \leq f(x_1)$ für alle $x \in [a, b]$.

Wir sagen dann, die Funktion f **nimmt ihr Infimum / Supremum** an. In diesem Fall existiert das **Minimum / Maximum** der Funktion f:

$$\min f := f(x_0) = \min\{\, f(x) \mid x \in \Omega \,\} = \inf f,$$
$$\max f := f(x_1) = \max\{\, f(x) \mid x \in \Omega \,\} = \sup f.$$

Die Menge aller Minimalstellen / Maximalstellen schreiben wir

$$\operatorname{Arg\,min}(f) := \{\, x \in \Omega \mid f(x) = \inf f \,\},$$
$$\operatorname{Arg\,max}(f) := \{\, x \in \Omega \mid f(x) = \sup f \,\}.$$

Extremwerte einer Funktion

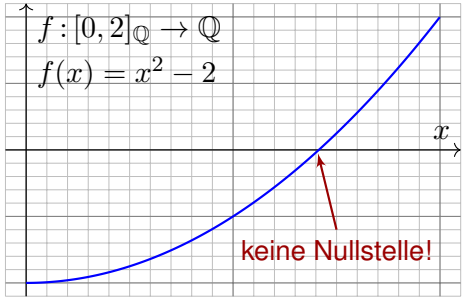
Somit nimmt die Funktion f genau dann ihr Infimum / Supremum an, wenn die Menge $\operatorname{Arg\,min}(f)$ bzw. $\operatorname{Arg\,max}(f)$ nicht-leer ist.

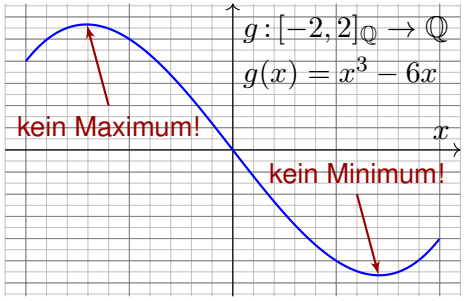
Darum geht es in der Optimierung: Den Minimalwert / Maximalwert einer Funktion $f : \Omega \to R$ bestimmen, und zudem einen oder alle Minimalstellen / Maximalstellen finden. Sie kennen erste Beispiele bereits aus der Schule unter dem Stichwort *Kurvendiskussion*.

Bemerkenswerterweise stellt sich selbst bei dieser einfachen Aufgabe bald heraus, dass die rationalen Zahlen $\mathbb{Q}$ hierfür ungenügend sind und wir zu ihrer Vervollständigung übergehen sollten: den reellen Zahlen $\mathbb{R}$. Erst damit lassen sich viele fundamentale und praktische Probleme elegant und befriedigend lösen und eine tragfähige Grundlage finden.

🙂 Die folgende Seite zeigt zwei einfache, eindrückliche Beispiele und zudem zwei grundlegend wichtige Sätze der Analysis.
Sie sind intuitiv plausibel, erschütternd falsch über $\mathbb{Q}$,
und glücklicherweise gültig über $\mathbb{R}$.

Extremwerte einer Funktion





Satz F1M: Zwischenwertsatz / Zusammenhang

Jede stetige Funktion $f : [a, b] \to \mathbb{R}$ hat die Zwischenwerteigenschaft: Zu jedem $y \in \mathbb{R}$ mit $f(a) \leq y \leq f(b)$ existiert $x \in [a, b]$ mit $f(x) = y$.

Satz F1N: Minimum und Maximum / Kompaktheit

Jede stetige Funktion $f : [a, b] \to \mathbb{R}$ nimmt Minimum und Maximum an: Es existieren $x_0, x_1 \in [a, b]$ mit $f(x_0) \leq f(x) \leq f(x_1)$ für alle $x \in [a, b]$.

Extrema in der Mathematik

Extreme Elemente (kleinstes / größtes Element bzw. Minima / Maxima) sind in der Mathematik und auch überall sonst besonders interessant. Viele ausgezeichnete Objekte entstehen als Lösung eines Problems der Minimierung bzw. der Maximierung. Erste sehr einfache Beispiele kennen Sie bereits aus dem Verlauf dieser Vorlesung:

Beispiel: Die von $P \subseteq X \times X$ erzeugte Äquivalenzrelation $T \subseteq X \times X$ ist die kleinste Äquivalenzrelation auf X, die P enthält (Satz E3H).

Beispiel: Die von $R \subseteq X \times X$ erzeugte eine Präordnung $P \subseteq X \times X$ ist die kleinste Präordnung auf X, die R enthält (Satz F1F).

Das ist ein recht allgemeines Prinzip zur Definition und zur Konstruktion mathematischer Objekte: Auf diese Weise konstruieren wir die erzeugte Untergruppe, den erzeugten Unterring, den erzeugten Untervektorraum, und vieles mehr. Später im Studium begegnet Ihnen auf gleiche Art die erzeugte Topologie und die erzeugte σ–Algebra in der Maßtheorie

Monotone Abbildungen

Definition F1O: isotone und antitone Abbildung

Sei $f : (X, \leq) \to (Y, \preccurlyeq)$ eine Abbildung geordneter Mengen.

$$\begin{aligned}
f \text{ ist isoton} &:\Leftrightarrow \forall a, b \in X : a \leq b \Rightarrow f(a) \preccurlyeq f(b) \\
f \text{ ist strikt isoton} &:\Leftrightarrow \forall a, b \in X : a < b \Rightarrow f(a) \prec f(b) \\
f \text{ ist antiton} &:\Leftrightarrow \forall a, b \in X : a \leq b \Rightarrow f(a) \succcurlyeq f(b) \\
f \text{ ist strikt antiton} &:\Leftrightarrow \forall a, b \in X : a < b \Rightarrow f(a) \succ f(b)
\end{aligned}$$

Isoton heißt auch **(monoton) wachsend** oder **ordnungserhaltend**, **antiton** heißt auch **(monoton) fallend** oder **ordnungsumkehrend**, beides heißt kurz **monoton**. Statt **strikt** sagt man auch **streng**.

Ein **(Ordnungs-)Isomorphismus** $(f, g) : (X, \leq) \cong (Y, \preccurlyeq)$ ist ein ordnungserhaltendes Bijektionspaar, $f : (X, \leq) \to (Y, \preccurlyeq)$ isoton und $g : (Y, \preccurlyeq) \to (X, \leq)$ isoton mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$.

Monotone Abbildungen

Beispiel: Eine monoton wachsende Folge in $\mathbb{R}$ ist eine isotone Abbildung $a : (\mathbb{N}, \leq) \to (\mathbb{R}, \leq) : n \mapsto a_n$, also $a_0 \leq a_1 \leq a_2 \leq a_3 \leq \ldots$; eine monoton fallende Folge entsprechend $a_0 \geq a_1 \geq a_2 \geq a_3 \geq \ldots$.

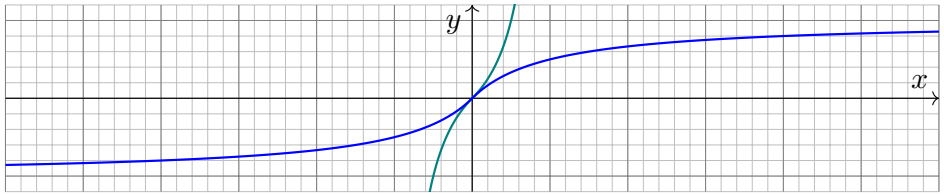
Beispiel: Die Abbildung $f : (\mathbb{R}, \leq) \to (\mathbb{R}, \leq) : x \mapsto x^2$ ist nicht monoton, weder fallend noch wachsend. Die Einschränkung $f|_{\mathbb{R}_{\leq 0}} : \mathbb{R}_{\leq 0} \to \mathbb{R}$ ist streng fallend, und $f|_{\mathbb{R}_{\geq 0}} : \mathbb{R}_{\geq 0} \to \mathbb{R}$ ist streng wachsend.

Beispiel: Die Abbildungen $f, g : (\mathbb{R}, \leq) \to (\mathbb{R}, \leq)$ mit $f(x) = x^3$ und $g(x) = \sqrt[3]{x}$ sind streng wachsend und erfüllen $g \circ f = \mathrm{id}_{\mathbb{R}}$ und $f \circ g = \mathrm{id}_{\mathbb{R}}$. Sie sind somit ein Ordnungsisomorphismus.

Beispiel: Zu jeder Abbildung $f : X \to Y$ zwischen Mengen X und Y sind $f_* : (\mathfrak{P}(X), \subseteq) \to (\mathfrak{P}(Y), \subseteq)$ und $f^* : (\mathfrak{P}(Y), \subseteq) \to (\mathfrak{P}(X), \subseteq)$ isoton, und strikt genau dann, wenn f injektiv bzw. surjektiv ist.

Beispiel: Das Komplement $\complement : (\mathfrak{P}(X), \subseteq) \to (\mathfrak{P}(X), \subseteq)$ ist strikt antiton. Somit ist $(\complement, \complement) : (\mathfrak{P}(X), \subseteq) \cong (\mathfrak{P}(X), \supseteq)$ ein Ordnungsisomorphismus.

Ordnungsisomorphismen



Beispiel F1P: erweiterte Zahlengerade und Intervall

Es gilt $\mathbb{R} \cong]-1, 1[$, genauer $(f, g) : \mathbb{R} \cong]-1, 1[$ vermöge

$$\begin{aligned}
f &: \mathbb{R} \to]-1, 1[: x \mapsto x/(1 + |x|), \\
g &:]-1, 1[\to \mathbb{R} : y \mapsto y/(1 - |y|).
\end{aligned}$$

Die beiden Abbildungen f und g sind isoton, also ordnungserhaltend. Dies setzen wir durch $\pm\infty \rightleftarrows \pm 1$ fort zu den Ordnungsisomorphismen

$$\begin{aligned}
(f_{\bar{\mathbb{R}}}, g_{\bar{\mathbb{R}}}) &: (\bar{\mathbb{R}}, \leq) \cong ([-1, 1]_{\mathbb{R}}, \leq), \\
(f_{\bar{\mathbb{Q}}}, g_{\bar{\mathbb{Q}}}) &: (\bar{\mathbb{Q}}, \leq) \cong ([-1, 1]_{\mathbb{Q}}, \leq).
\end{aligned}$$

Die erweiterte Zahlengerade $\bar{\mathbb{R}} \cong [-1, 1]$ ist somit sehr anschaulich!

Ordnungsisomorphismen

Übung: Was genau ist noch zu zeigen? Weisen Sie es sorgsam nach!

Satz F1Q: Streng monoton impliziert injektiv.

Sei $(X, \leq)$ total geordnet und $(Y, \preccurlyeq)$ geordnet.

(1) Ist $f : (X, \leq) \to (Y, \preccurlyeq)$ streng monoton, so ist f injektiv.

(2) Ist $f : (X, \leq) \to (Y, \preccurlyeq)$ streng isoton, so ist f ordnungsreflektierend:

$$\forall a, b \in X \ : \ f(a) \preccurlyeq f(b) \Rightarrow a \leq b$$

Ist f zudem bijektiv, so ist auch $f^{-1} : (Y, \preccurlyeq) \to (X, \leq)$ streng isoton.

Beweis: (1) Zu $a \neq b$ in X gilt entweder $a < b$ oder $a > b$.
Ohne Einschränkung sei $a < b$, notfalls tauschen wir a und b.

Ist f streng wachsend, so gilt $f(a) \prec f(b)$, also $f(a) \neq f(b)$.
Ist f streng fallend, so gilt $f(a) \succ f(b)$, also $f(a) \neq f(b)$.

In beiden Fällen ist f injektiv.

(2) Seien $a, b \in X$ und $f(a) \preccurlyeq f(b)$. Angenommen, es gälte nicht $a \leq b$.
Da $(X, \leq)$ total geordnet ist, bedeutet das $a > b$. Da f streng isoton ist,
folgt $f(a) \succ f(b)$, im Widerspruch zur Voraussetzung $f(a) \preccurlyeq f(b)$. QED

Aufgabe: Seien $(X, \leq)$ und $(Y, \preccurlyeq)$ geordnete Mengen (Posets).
Ist $f : (X, \leq) \to (Y, \preccurlyeq)$ bijektiv und strikt isoton ein Isomorphismus?

Lösung: Nein! Wir betrachten die Menge $\mathbb{Z}$ der ganzen Zahlen mit der partiellen Ordnung $(\preccurlyeq) = \{ (a, b) \in \mathbb{N} \times \mathbb{N} \mid \exists x \in \mathbb{N} : a + x = b \}$.
Die Funktion $f : (\mathbb{Z}, \preccurlyeq) \to (\mathbb{Z}, \preccurlyeq) : x \mapsto x + 1$ ist bijektiv und strikt isoton,
die Umkehrfunktion $f^{-1} : (\mathbb{Z}, \preccurlyeq) \to (\mathbb{Z}, \preccurlyeq) : x \mapsto x - 1$ ist nicht isoton!

Satz F1R: Fixpunktsatz von Knaster–Tarski

Sei $(X, \leq)$ eine geordnete Menge, in der jede Teilmenge $U \subseteq X$
ein Infimum und ein Supremum besitzt, etwa $([0, 1], \leq)$ oder $(\bar{\mathbb{R}}, \leq)$.

Ist $f : (X, \leq) \to (X, \leq)$ eine isotone Selbstabbildung,
so ist die Fixpunktmenge $F = \mathrm{fix}(f)$ nicht-leer.

Übung: Beweisen Sie dies, zunächst im Spezialfall $X = [0, 1]$.

Die natürlichen Zahlen sind wohlgeordnet.

F141

Satz F1S: Die natürlichen Zahlen sind wohlgeordnet.

In $(\mathbb{N}, \leq)$ hat jede nicht-leere Teilmenge $A \subseteq \mathbb{N}$ ein kleinstes Element m.

Beweis: (1) Es gibt ein Element $s \in A$, daher gilt $(s+1) \notin A$.

(2) Es gibt ein Element $m \in \mathbb{N}$ mit $m \leq A$ und $(m+1) \notin A$.
Andernfalls gälte $n \leq A \Rightarrow (n+1) \leq A$ für jedes $n \in \mathbb{N}$.
Dank $0 \leq A$ folgt per Induktion $\mathbb{N} \leq A$, im Widerspruch zu (1).

(3) Für dieses Element gilt $m \in A$.
Andernfalls wäre $(m+1) \leq A$, im Widerspruch zu (2). QED

🙂 Diese Aussage erweitert unser Repertoire an Induktionsbeweisen. Um zu beweisen, dass eine Aussage $A(n)$ für jedes $n \in \mathbb{N}$ gilt, nehmen wir das Gegenteil an und betrachten den „kleinsten Verbrecher“, also das kleinste Gegenbeispiel. Dies führen wir dann zum Widerspruch. Dieses Vorgehen ist für manche Beweise sehr effizient.

Wohlgeordnete Mengen

F142

Definition F1T: Wohlordnung

Eine geordnete Menge $(X, \leq)$ heißt **wohlgeordnet**, falls jede nicht-leere Teilmenge $A \subseteq X$ ein kleinstes Element besitzt.
In diesem Falle heißt $\leq$ eine **Wohlordnung** auf X.

Bemerkung: Jede Wohlordnung ist total, denn zu je zwei Elementen $a, b \in X$ besitzt $\{a, b\}$ ein kleinstes Element, also gilt $a \leq b$ oder $b \leq a$.

Beispiel: Die natürlichen Zahlen $(\mathbb{N}, \leq)$ sind wohlgeordnet (Satz F1S). Hingegen sind $(\mathbb{Z}, \leq)$ und $(\mathbb{Q}, \leq)$ und $(\mathbb{R}, \leq)$ nicht wohlgeordnet.

Beispiel: Ist $U \subseteq X$ und $(X, \leq)$ wohlgeordnet, so auch $(U, \leq_U)$. Insbesondere ist $\{\, 1 < 2 < \cdots < n \,\}$ wohlgeordnet für jedes $n \in \mathbb{N}$.

Beispiel: Ist $(X, \leq)$ endlich und total geordnet, so auch wohlgeordnet. Dank $\sharp X = n < \infty$ existiert eine Bijektion $\nu : \{1, \ldots, n\} \xrightarrow{\sim} X : i \mapsto x_i$. Diese können wir so sortieren, dass $x_1 < x_2 < \cdots < x_n$ gilt. Somit ist $\nu : \{1 < 2 < \cdots < n\} \xrightarrow{\sim} \{x_1 < x_2 < \cdots < x_n\}$ ein Isomorphismus.

Der Wohlordnungssatz

F143

Beispiel: Die ganzen Zahlen $\mathbb{Z}$ sind wohlgeordnet mit der Ordnung

$$(\mathbb{Z}, \preccurlyeq) = \{\, 0 \prec 1 \prec 2 \prec 3 \prec \ldots \prec -1 \prec -2 \prec -3 \prec \ldots \,\}.$$

Sprichwörtlich: *Chuck Norris hat bis unendlich gezählt. Zwei Mal.*

Beispiel: Für die reellen Zahlen $\mathbb{R}$ ist keine Wohlordnung elementar konstruierbar. Dennoch existieren solche Wohlordnungen:

Satz F1U: Wohlordnungssatz

Auf jeder Menge X existiert mindestens eine Wohlordnung $\leq$.

Bemerkung: Diesen Satz beweist man mit Hilfe des Auswahlaxioms. Umgekehrt folgt daraus das Auswahlaxiom, die beiden sind äquivalent:

Anwendungsbeispiel: Sei $(X, \leq)$ eine wohlgeordnete Menge. Zu jeder Zerlegung $Q \subseteq \mathfrak{P}(X)^*$ mit $X = \bigsqcup Q$ erhalten wir dann das Repräsentantensystem $R = \{\, \min C \mid C \in Q \,\}$, kanonisch bezüglich $\leq$.

🙂 Das ist oft bequem, um alle willkürlichen Wahlen in ein konkretes Eingabedatum $(X, \leq)$ abzukapseln. Die weitere Konstruktion kommt dann ohne Wahlen aus, sie ist eindeutig auf Grundlage von $(X, \leq)$.

Das Lemma von Zorn

F144

Satz F1V: Lemma von Zorn

Eine geordnete Menge, in der jede Kette eine obere Schranke hat, enthält mindestens ein maximales Element.

Oft konstruieren wir mathematische Objekte schrittweise, als eine Kette aufsteigender Größe. Ein maximales Element ist ein fertiges Resultat.

If you are building a mathematical object in stages and find that (i) you have not finished even after infinitely many stages, and (ii) there seems to be nothing to stop you continuing to build, then Zorn's lemma may well be able to help you.
Timothy Gowers: *How to use Zorn's lemma.* `gowers.wordpress.com/2008/08/12`

Für Konstruktionen mit unendlichen Mengen ist Zorns Lemma daher oft ein bequemes Hilfsmittel. Wie der Wohlordnungssatz ist Zorns Lemma äquivalent zum Auswahlaxiom: Auf Grundlage der Zermelo–Fraenkel–Axiome impliziert jede der drei Aussagen die beiden anderen. Dennoch provozieren sie unterschiedliche Gefühle:

> *The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?* (Jerry Bona)

Sind alle natürlichen Zahlen interessant?

Wir verfügen nun über recht mächtige mathematische Werkzeuge, und unvorsichtig verwendet kann man damit mächtig Quatsch erzeugen.

Quatz F1w: interessante Zahlen

Jede natürliche Zahl ist interessant.

Beweis: Angenommen, es gäbe uninteressante natürliche Zahlen. Unter diesen gäbe es dann eine kleinste – und die wäre interessant! Dies ist ein Widerspruch. Damit ist der Quatz bewiesen. QED

⚠ Warnung: Der folgende Quatz provoziert anhaltendes Nachdenken. Lesen Sie dies bitte nur, wenn Sie mathematisch gefestigt sind, Neugier und Grübelfreude verspüren und Zeit dafür haben.

Wir nutzen das lateinische Alphabet `a,b,c,...,z,A,B,C,...,Z`, mit Ziffern `0,1,...,9` usw. Insgesamt genügen uns 100 Zeichen.

Damit definieren wir natürliche Zahlen wie `20201206` oder `789!` oder `Die kleinste natürliche Zahl n, die ln(ln(n))>100 erfüllt.`

🙂 Auch große Zahlen lassen sich mit kurzen Zeichenketten definieren.

Sind die natürlichen Zahlen endlich?

Quatz F1x: Endlichkeit der natürlichen Zahlen

Jede natürliche Zahl lässt sich mit höchstens 200 Zeichen definieren.

Es gibt 100^{200} Zeichenketten der Länge 200 mit unseren 100 Zeichen, also höchstens 100^{200} natürliche Zahlen: Die Menge $\mathbb{N}$ ist endlich!

Beweis: Angenommen, es gäbe natürliche Zahlen die sich nur mit mehr als 200 Zeichen definieren lassen. Dann gäbe es darunter eine kleinste:

`Sei N die kleinste natürliche Zahl, die sich nur mit mehr als 200 Zeichen definieren lässt.`

Diese Zahl N haben wir soeben mit weniger als 200 Zeichen definiert. Dies ist ein Widerspruch. Damit ist der Quatz bewiesen. QED

Selbstverständlich ist die Behauptung falsch, und die Schlussfolgerung, dass $\mathbb{N}$ endlich sei, ist absurd. Doch der Beweis scheint überzeugend.

Übung: Wo genau liegt bei diesem Argument der Fehler?

Sind die natürlichen Zahlen endlich?

Hier wird später einmal eine Erklärung dieses Logikrätsels stehen. Viel fruchtbarer ist jedoch – wie immer – das eigene Nachdenken.

Die Behauptung, die Menge $\mathbb{N}$ sei endlich, ist offensichtlich falsch. Das Argument kann daher nicht richtig sein. Tatsächlich ist es falsch, doch auf eine subtile Weise, der Fehler ist keineswegs offensichtlich.

Dieser Quatz ist ein schaurig-schönes Beispiel für einen Denkfehler. Darf man als Lehrer/in überhaupt falsche Behauptungen zeigen? Ich denke, ja: Auch aus mahnenden Fehlern kann man lernen.

Es gibt drei Möglichkeiten, klug zu handeln:
1. Durch Nachahmen — Das ist die leichteste.
2. Durch Nachdenken — Das ist die edelste.
3. Durch Erfahrung — Das ist die bitterste.

Konfuzius (551–497 v.Chr.)

Sind die natürlichen Zahlen endlich?

Rekursion und ihre Folgen

F201

Beispiel: Wir betrachten die Menge $\mathbb{R}_{>0}$ und die Selbstabbildung

$$\varphi : \mathbb{R}_{>0} \to \mathbb{R}_{>0} : x \mapsto \tfrac{1}{2}(x + \tfrac{2}{x}).$$

Wir wählen den **Startwert** $x_0 := 1$ und definieren **rekursiv**

$$x_{n+1} := \varphi(x_n) \quad \text{für alle } n \in \mathbb{N}.$$

Dies **konstruiert** die Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}_{>0}$, also $f : \mathbb{N} \to \mathbb{R}_{>0} : n \mapsto x_n$.

$x_0 = 1$
$x_1 = 1.5$
$x_2 = 1.41666666\,66666666\,66666666\,66666666\,66666666\,66666666\,66666666\ldots$
$x_3 = 1.41421568\,62745098\,03921568\,62745098\,03921568\,62745098\,03921568\,627\ldots$
$x_4 = 1.41421356\,23746899\,10626295\,78899134\,91011655\,96221157\,44044584\,90\ldots$
$x_5 = 1.41421356\,23730950\,48801689\,62350253\,02436149\,81925776\,19742849\,828\ldots$
$x_6 = 1.41421356\,23730950\,48801688\,72420969\,80785696\,71875372\,34001561\,01\ldots$
$\ldots$

Wie garantieren wir Existenz und Eindeutigkeit der Folge $f : \mathbb{N} \to \mathbb{R}_{>0}$?

Rekursion und ihre Folgen

F202
Erläuterung

Die Konstruktion von Folgen per Rekursion ist ein sehr flexibles und praktisches Werkzeug, es wird daher in nahezu allen Bereichen der Mathematik gerne genutzt. Sie sehen hier eine Anwendung des **Newton–Verfahrens** zur iterativen Näherung einer Nullstelle.

🙂 Diese Folge konvergiert, wie hier zu erahnen, extrem schnell gegen einen Grenzwert. Dieser Wert ist der Fixpunkt der Abbildung φ, also $\sqrt{2}$. Mehr zum Newton–Verfahren und zu iterativen Methoden lernen Sie in der Analysis und der Numerik. Das ist ein sehr dynamisches Thema!

Wir wollen im Folgenden klären, dass die Angabe des Startpunkts x_0 und der Rekursionsvorschrift $x_{n+1} := \varphi(x_n)$ für alle $n \in \mathbb{N}$ tatsächlich genügen, um die gewünschte Folge $(x_n)_{n\in\mathbb{N}}$ eindeutig zu konstruieren. Es geht also um die **Existenz** und die **Eindeutigkeit** einer Funktion

$$f : \mathbb{N} \to \mathbb{R}_{>0} : n \mapsto x_n$$

mit den geforderten Eigenschaften. Endlich viele Rekursionsschritte sind kein Problem, doch wir wollen dies für alle $n \in \mathbb{N}$ bündeln.

Modelle der natürlichen Zahlen

F203

Beispiel: Endliche Zeichenketten über dem Alphabet $\{0, 1\}$ gemäß
$0 \mapsto 1 \mapsto 10 \mapsto 11 \mapsto 100 \mapsto 101 \mapsto 110 \mapsto 111 \mapsto 1000 \mapsto 1001 \mapsto \ldots$.

Beispiel: John von Neumanns Modell der natürlichen Zahlen
$0 = \emptyset \mapsto 1 = \{0\} \mapsto 2 = \{0, 1\} \mapsto 3 = \{0, 1, 2\} \mapsto 4 = \{0, 1, 2, 3\} \mapsto \ldots$.

Definition F2A: Modell der natürlichen Zahlen

Sei N eine Menge, $0 \in N$ ein Element und $\nu : N \to N$ eine Abbildung. Wir nennen 0 das Startelement und ν die Nachfolgerabbildung.

$$\{0\} \xrightarrow{\text{inc}} N \xrightarrow{\nu} N$$

Wir nennen das Tripel $(N, 0, \nu)$ ein **Modell der natürlichen Zahlen**, falls es die folgenden drei **Dedekind–Peano–Axiome** erfüllt:

- D0: Es gilt $0 \notin \nu(N)$: Für alle $p \in N$ gilt $\nu(p) \neq 0$.
- D1: Die Abbildung ν ist injektiv: Für alle $p \neq q$ in N gilt $\nu(p) \neq \nu(q)$.
- D2: Induktion: Für alle $E \subseteq N$ mit $0 \in E$ und $\nu(E) \subseteq E$ gilt $E = N$.

Modelle der natürlichen Zahlen

F204
Erläuterung

Die wesentliche Grundlage der Rekursion sind die natürlichen Zahlen. Zwei schön konkrete Modelle nenne ich hier, es gibt zahllose weitere. Genauso gelingt dies im vertrauten Dezimalsystem, zur Basis Zehn:

$$\begin{aligned}
&0 \mapsto 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 6 \mapsto 7 \mapsto 8 \mapsto 9 \mapsto \\
&10 \mapsto 11 \mapsto 12 \mapsto 13 \mapsto 14 \mapsto 15 \mapsto 16 \mapsto 17 \mapsto 18 \mapsto 19 \mapsto \\
&20 \mapsto 21 \mapsto 22 \mapsto 23 \mapsto \quad \ldots \quad \mapsto 97 \mapsto 98 \mapsto 99 \mapsto \\
&100 \mapsto 101 \mapsto 102 \mapsto 103 \mapsto \ldots
\end{aligned}$$

Wir müssen uns gar nicht festlegen, welche Menge N wir betrachten. Es zählt allein, dass $(N, 0, \nu)$ die Dedekind–Peano–Axiome erfüllt! Wir konzentrieren uns auf die charakteristischen Eigenschaften: Definition F2A macht unseren Blick frei auf das Wesentliche.

🙂 Die Mathematik, recht besehen, ist das Reich der Freiheit. Jede darf sich ihre natürlichen Zahlen vorstellen, wie sie mag. Wir finden anschließend eine eindeutige Übersetzung (F2C).

Dedekinds Rekursionssatz

Satz F2B: Rekursionssatz von Dedekind, 1888

Sei $(N, 0, \nu)$ ein Modell der natürlichen Zahlen (wie in F2A erklärt).

$$\begin{array}{ccccccccc} 0 & \xmapsto{\nu} & 1 & \xmapsto{\nu} & 2 & \xmapsto{\nu} & 3 & \xmapsto{\nu} & \dots \\ \downarrow f & & \downarrow f & & \downarrow f & & \downarrow f & & \\ a_0 & \xmapsto{\alpha} & a_1 & \xmapsto{\alpha} & a_2 & \xmapsto{\alpha} & a_3 & \xmapsto{\alpha} & \dots \end{array} \qquad \begin{array}{ccccc} \{0\} & \xhookrightarrow{\text{inc}} & N & \xrightarrow{\nu} & N \\ \downarrow f & & \downarrow f & & \downarrow f \\ \{a_0\} & \xhookrightarrow{\text{inc}} & A & \xrightarrow{\alpha} & A \end{array}$$

Das Tripel (A, a_0, α) bestehe aus einer Menge A, einem Element $a_0 \in A$ als Startpunkt und einer Abbildung $\alpha : A \to A$ als Rekursionsvorschrift.

Dann existiert genau eine Abbildung $f : N \to A$ als **rekursive Folge** mit Startwert $f(0) = a_0$ und der Rekursionsgleichung $f \circ \nu = \alpha \circ f$.

Eindeutigkeit: Angenommen die Abbildungen $f, g : N \to A$ erfüllen beide $f(0) = g(0) = a_0$ sowie $f \circ \nu = \alpha \circ f$ und $g \circ \nu = \alpha \circ g$.
Sei $E := \{\, n \in N \mid f(n) = g(n) \,\}$. Dann gilt $0 \in E$ und $\nu(E) \subseteq E$, denn aus $n \in E$ folgt $f(\nu(n)) = \alpha(f(n)) = \alpha(g(n)) = g(\nu(n))$, also $\nu(n) \in E$.
Dank Induktion (D2) folgt $E = N$. Das bedeutet $f = g$.

Dedekinds Rekursionssatz

Konstruktion von $f : N \to A$: Eine Teilmenge $R \subseteq N \times A$ nennen wir **rekursiv**, wenn $(0, a_0) \in R$ gilt und mit $(n, a) \in R$ auch $(\nu(n), \alpha(a)) \in R$.
Die größte rekursive Menge ist $N \times A$. Die kleinste ist der Durchschnitt

$$F := \bigcap \{\, R \subseteq N \times A \mid R \text{ ist rekursiv} \,\}.$$

Auch F ist rekursiv! Wir zeigen, dass $f = (N, F, A)$ eine Abbildung ist.

$$E := \{\, n \in N \mid \exists! a \in A : (n, a) \in F \,\}$$

Wir haben $E = N$ zu zeigen. Dies beweisen wir per Induktion.

Induktionsanfang $0 \in E$: Wir haben $(0, a_0) \in F$, denn F ist rekursiv. Gäbe es ein Paar $(0, b) \in F$ mit $b \neq a_0$, dann wäre $R = F \setminus \{(0, b)\}$ rekursiv dank (D0). Das steht im Widerspruch zur Definition von F.

Induktionsschritt $n \in E \Rightarrow n + 1 \in E$: Wegen $n \in E$ existiert genau ein $a \in A$ mit $(n, a) \in F$. Daher gilt $(\nu(n), \alpha(a)) \in F$, denn F ist rekursiv. Gäbe es ein Paar $(\nu(n), b) \in F$ mit $b \neq \alpha(a)$, dann wäre $F \setminus \{(\nu(n), b)\}$ rekursiv dank (D1). Das steht im Widerspruch zur Definition von F. QED

Dedekinds Rekursionssatz

☺ Rekursion nutzen wir überall! So definieren wir insbesondere die Addition, Multiplikation und Potenz auf den natürlichen Zahlen (A1A).

Bitte unterscheiden Sie die beiden Begriffe **Rekursion** und **Induktion**! Beide Werkzeuge werden oft gemeinsam genutzt, so wie hier zu sehen, sie sind jedoch verschieden und erfüllen unterschiedliche Aufgaben: Per Induktion beweisen wir, per Rekursion konstruieren wir.

☺ **Per Induktion beweisen wir** eine Aussage $p(n)$ für alle $n \in \mathbb{N}$.

$p(0)$	Induktionsanfang: Wir beweisen die Aussage $p(0)$.
$p(n) \Rightarrow p(n+1)$	Induktionsschritt: Wir beweisen $p(n) \Rightarrow p(n+1)$.
$\forall n \in \mathbb{N} : p(n)$	Induktionsschluss: die Allaussage $\forall n \in \mathbb{N} : p(n)$.

☺ **Per Rekursion konstruieren wir** eine Abbildung $f : \mathbb{N} \to A$.
Gegeben sei ein Element $a_0 \in A$ und eine Selbstabbildung $\alpha : A \to A$.
Rekursionsanfang: Wir legen den Startpunkt $f(0) = a_0$ fest.
Rekursionsschritt: Für jedes $n \in \mathbb{N}$ setzen wir $f(n + 1) = \alpha(f(n))$.
Dank Rekursionssatz F2B definiert dies genau eine Funktion $f : \mathbb{N} \to A$.

Dedekinds Rekursionssatz

Korollar F2C: Einzigkeit der natürlichen Zahlen

Zu je zwei Modellen $(N, 0, \nu)$ und $(N', 0', \nu')$ der natürlichen Zahlen existiert ein eindeutiger Isomorphismus $(f, f') : (N, 0, \nu) \cong (N', 0', \nu')$.

$$\begin{array}{ccccc} \{0\} & \xhookrightarrow{\text{inc}} & N & \xrightarrow{\nu} & N \\ f\downarrow\uparrow f' & & f\downarrow\uparrow f' & & f\downarrow\uparrow f' \\ \{0'\} & \xhookrightarrow{\text{inc}} & N' & \xrightarrow{\nu'} & N' \end{array}$$

Ausführlich: Es existiert genau ein Bijektionspaar $(f, f') : N \cong N'$ mit $f(0) = 0'$ und $f \circ \nu = \nu' \circ f$ sowie $f'(0') = 0$ und $f' \circ \nu' = \nu \circ f'$.

Beweis: Dank Existenz und Eindeutigkeit in Satz F2B existiert genau eine Abbildung $f : N \to N'$ mit $f(0) = 0'$ und $f \circ \nu = \nu' \circ f$ und genau eine Abbildung $f' : N' \to N$ mit $f'(0') = 0$ und $f' \circ \nu' = \nu \circ f'$.
Dank Eindeutigkeit in F2B gilt $f' \circ f = \mathrm{id}_N$ und $f \circ f' = \mathrm{id}_{N'}$. QED

☺ Jeder darf sich seine natürlichen Zahlen vorstellen, wie er mag. Zwischen je zwei Modellen übersetzt der eindeutige Isomorphismus.

Konstruktion einer Einbettung $\mathbb{N} \hookrightarrow X$

Satz F2D: Konstruktion einer Einbettung $\mathbb{N} \hookrightarrow X$

Sei X eine Menge und unendlich, das heißt, es gibt keine Bijektion $\nu : \{1, \ldots, n\} \xrightarrow{\sim} X$ mit $n \in \mathbb{N}$. Dann existiert eine Injektion $\nu : \mathbb{N} \hookrightarrow X$.

Beweis: Wir konstruieren $A_0 \subset A_1 \subset A_2 \subset \ldots \subset X$ mit $\sharp A_n = n$.

Wir beginnen mit $A_0 := \emptyset$. Sei $A_n \subseteq X$ mit $\sharp A_n = n$ bereits konstruiert.
Nach Voraussetzung gilt $A_n \neq X$, also gibt es ein Element $x_n \in X \setminus A_n$.
Wir wählen willkürlich und setzen $A_{n+1} := A_n \sqcup \{x_n\}$ mit $\sharp A_{n+1} = n + 1$.

Dies definiert die Abbildung $\nu : \mathbb{N} \to X : n \mapsto x_n$. Diese ist injektiv. QED

Formale Ausführung: Gegeben sei eine Wohlordnung auf X (F1U).
Wir starten mit der Menge $A_0 = \emptyset$ und nutzen die Rekursionsvorschrift

$$\varphi : \mathfrak{P}_{<\infty}(X) \to \mathfrak{P}_{<\infty}(X) : A \mapsto A' = A \sqcup \{\min(X \setminus A)\}.$$

Dank Rekursionssatz (F2B) erhalten wir so die Folge $(A_n)_{n \in \mathbb{N}}$.
Dies definiert eine Injektion $\nu : \mathbb{N} \hookrightarrow X : n \mapsto \min(X \setminus A_n)$. QED

Konstruktion einer Einbettung $\mathbb{N} \hookrightarrow X$

Die erste, anschauliche Konstruktion ist zunächst überzeugend, doch bei genauerer Betrachtung bin ich damit nicht recht glücklich:

In dieser Konstruktion müssen wir immer wieder willkürlich wählen! Für endlich viele (wenige) Schritte will ich das gerne übernehmen, doch für unendlich viele solcher Schritte fehlt mir schlicht die Zeit.

Wir wollen daher diese Wahlen auf ein Verfahren übertragen.
Genau solch ein Verfahren beschreibt die formale Ausführung.
Mit diesen Daten und dieser Methode läuft die Maschine von alleine.

Dedekinds Charakterisierung un/endlicher Mengen

Satz F2E: Dedekinds Charakterisierung un/endlicher Mengen

Für jede Menge X sind folgende Aussagen äquivalent:

(E0) X ist endlich, das heißt es existiert $\nu : \{1, \ldots, n\} \xrightarrow{\sim} X$.
(E1) Jede Surjektion $g : X \twoheadrightarrow X$ ist injektiv, somit bijektiv.
(E2) Jede Injektion $f : X \hookrightarrow X$ ist surjektiv, somit bijektiv.
(E3) Es gibt keine Bijektion $X \cong Y$ auf eine echte Teilmenge $Y \subsetneq X$.

Umgekehrt sind folgende Aussagen äquivalent:

(U0) X ist unendlich. (Dank F2D existiert also $\nu : \mathbb{N} \hookrightarrow X$.)
(U1) Es gibt Surjektionen $g : X \twoheadrightarrow X$, die nicht injektiv sind.
(U2) Es gibt Injektionen $f : X \hookrightarrow X$, die nicht surjektiv sind.
(U3) Es gibt eine Bijektion $X \cong Y$ auf eine echte Teilmenge $Y \subsetneq X$.

Dedekinds Charakterisierung un/endlicher Mengen

Beweis: Die Äquivalenzen „(E2) $\Leftrightarrow$ (E3)“ und „(U2) $\Leftrightarrow$ (U3)“ sind klar:
Zur Injektion $f : X \hookrightarrow X$ mit $Y = f(X)$ gehört die Bijektion $f|^Y : X \xrightarrow{\sim} Y$.
Zur Bijektion $h : X \xrightarrow{\sim} Y$ mit $Y \subseteq X$ gehört die Injektion $\iota_Y^X \circ h : X \hookrightarrow X$.

Der Invarianzsatz E1H garantiert „(E0) $\Rightarrow$ (E1)“ und „(E0) $\Rightarrow$ (E2)“.
Die Umkehrungen „(U0) $\Rightarrow$ (U1)“ und „(U0) $\Rightarrow$ (U2)“ gelten für $X = \mathbb{N}$:

Die Nachfolgerabbildung $f : \mathbb{N} \to \mathbb{N} : n \mapsto n + 1$ ist injektiv (D1), aber nicht surjektiv (D0). Die Linksinverse $g : \mathbb{N} \to \mathbb{N} : n \mapsto \max(0, n - 1)$ hingegen ist surjektiv, aber nicht injektiv, denn $g(0) = g(1) = 0$.

Allgemein: Zu X unendlich existiert eine Injektion $\nu : \mathbb{N} \hookrightarrow X$ (F2D).
Sei $B = \nu(\mathbb{N}) \subseteq X$ die Bildmenge. Wir haben dann $\mu = \nu|^B : \mathbb{N} \xrightarrow{\sim} B$.
Zu jeder Abbildung $h : \mathbb{N} \to \mathbb{N}$ definieren wir

$$h' : X \to X : x \mapsto \begin{cases} x & \text{falls } x \in X \setminus B, \\ (\mu \circ h \circ \mu^{-1})(x) & \text{falls } x \in B. \end{cases}$$

Genau dann ist h' injektiv bzw. surjektiv, wenn h dies ist. QED

Mächtigkeit von Mengen

Definition F2F: Mächtigkeit von Mengen

Seien X und Y Mengen. Wir vereinbaren folgende Schreibweisen:

1. $X \preccurlyeq Y$, falls eine Injektion $f : X \hookrightarrow Y$ existiert: reflexiv & transitiv!
   Interpretation: „Die Menge X ist höchstens so groß wie Y.“
2. $Y \succcurlyeq X$, falls eine Surjektion $g : Y \twoheadrightarrow X$ existiert oder $X = \emptyset$ gilt.
   Dies ist äquivalent zu $X \preccurlyeq Y$ (Links/Rechtsinverse, Satz D3A).
   Interpretation: „Die Menge Y ist mindestens so groß wie X.“
3. $X \cong Y$, falls eine Bijektion $(h, k) : X \cong Y$ existiert: Äquivalenz.
   Interpretation: „Die beiden Mengen X und Y sind gleich groß.“
   Traditionell sagen wir hierzu **gleichmächtig** oder **äquipotent**.

Existiert eine Zahl $n \in \mathbb{N}$ und eine Bijektion $\nu : \{1, \ldots, n\} \xrightarrow{\sim} X$,
so nennen wir die Menge X **endlich**, $\sharp X = n$, andernfalls **unendlich**.

Existiert eine Bijektion $\nu : \mathbb{N} \xrightarrow{\sim} X$, so heißt X **abzählbar unendlich**.

Abzählbar bedeutet endlich oder abzählbar unendlich, kurz $X \preccurlyeq \mathbb{N}$.
Andernfalls gilt $X \not\preccurlyeq \mathbb{N}$, und X heißt **überabzählbar (unendlich)**.

Mächtigkeit von Mengen

Die Relation $X \cong Y \Leftrightarrow \exists (h, k) : X \cong Y$ ist reflexiv dank $(\mathrm{id}, \mathrm{id}) : X \cong X$, symmetrisch dank Vertauschung und transitiv dank Komposition.

Die Relation $X \preccurlyeq Y \Leftrightarrow \exists f : X \hookrightarrow Y$ ist reflexiv dank $\mathrm{id}_X : X \hookrightarrow X$ und transitiv, denn die Komposition von Injektionen ergibt eine Injektion.

Satz von Cantor–Bernstein (F2N): Aus $X \preccurlyeq Y$ und $Y \preccurlyeq X$ folgt $X \cong Y$.
Aus $f : X \hookrightarrow Y$ und $g : Y \hookrightarrow X$ gewinnen wir $(h, k) : X \cong Y$.

Die Relation $Y \succcurlyeq X \Leftrightarrow (\exists g : Y \twoheadrightarrow X) \vee X = \emptyset$ ist äquivalent zu $X \preccurlyeq Y$:
Zu jeder Surjektion $g : Y \twoheadrightarrow X$ existiert $f : X \hookrightarrow Y$ mit $g \circ f = \mathrm{id}_X$ (D3A).

Wie üblich schreiben wir $X \prec Y$ für $X \preccurlyeq Y \wedge Y \not\preccurlyeq X$.
Interpretation: „Die Menge X ist strikt kleiner als Y.“

Wie üblich schreiben wir $Y \succ X$ für $Y \succcurlyeq X \wedge X \not\succcurlyeq Y$.
Interpretation: „Die Menge Y ist strikt größer als X.“

⚠ Die Begriffe „kleiner“ und „größer“ und „gleich groß“ sind hier immer im Sinne der Mächtigkeit gemeint, also auf In/Sur/Bijektionen bezogen.

Mächtigkeit von Teilmengen in $\mathbb{N}$

Aufgabe: Ist die Menge der natürlichen Zahlen $\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, \ldots \}$ größer als die Menge der Quadratzahlen $Q = \{ 0, 1, 4, 9, 16, 25, \ldots \}$?

Lösung: (0) Im Sinne der Inklusion haben wir $Q \subsetneq \mathbb{N}$.
Im Poset $(\mathfrak{P}(\mathbb{N}), \subseteq)$ ist demnach Q strikt kleiner als $\mathbb{N}$.

(1) Im Sinne der Mächtigkeit sind beide Mengen gleich groß!
Wir haben $(h, k) : \mathbb{N} \cong Q$ mit $h(x) = x^2$ und $k(y) = \sqrt{y}$.

⚠ Um mögliche Missverständnisse zu vermeiden, sagen wir statt *gleich groß* genauer *gleichmächtig* im Sinne der Definition F2F.

Die Mengen $\mathbb{N}$ und Q sind gleichmächtig, sie haben dieselbe **Mächtigkeit**, man sagt auch: sie haben dieselbe **Kardinalität**.

Mächtigkeit von Teilmengen in $\mathbb{N}$

Aufgabe: Vergleichen Sie die Mächtigkeit der Menge $\mathbb{N}$
mit der Menge $P = \{ 2, 3, 5, 7, 11, 13, \ldots \}$ der Primzahlen in $\mathbb{N}$.

Lösung: Beide sind gleichmächtig, wir haben eine Bijektion $\mathbb{N} \cong P$.

Ausführliche Konstruktion: Dank Satz C2C ist die Menge P unendlich.
Ihre Elemente können wir aufsteigend anordnen zu $p_0 < p_1 < p_2 < \ldots$.
Dies stiftet die (kanonische, isotone) Bijektion $h : \mathbb{N} \xrightarrow{\sim} P : n \mapsto p_n$.

🙂 Computer-Algebra-Systeme implementieren diese Abbildung $h : \mathbb{N} \xrightarrow{\sim} P$ als eine Funktion, etwa `Prime[n]` oder `ithprime(n)`.

Mächtigkeit der Potenzmenge

Satz F2G: Cantors (zweites) Diagonalargument

Zu jeder Menge X ist die Potenzmenge strikt größer: Es gibt Injektionen $X \hookrightarrow \mathfrak{P}(X)$, etwa $x \mapsto \{x\}$, aber keine Surjektionen $X \twoheadrightarrow \mathfrak{P}(X)$:

$$\text{Es gilt } \; X \prec \mathfrak{P}(X), \; \text{ das heißt } X \preccurlyeq \mathfrak{P}(X) \text{ und } X \not\approx \mathfrak{P}(X).$$

Insbesondere ist die Potenzmenge $\mathfrak{P}(\mathbb{N}) \cong \{0,1\}^{\mathbb{N}}$ überabzählbar.

Beweis: Vorgelegt sei eine beliebige Abbildung $f : X \to \mathfrak{P}(X)$.
Wir zeigen, dass f nicht surjektiv ist. Dazu betrachten wir die Menge

$$A = \{\, x \in X \mid x \notin f(x) \,\} \subseteq X.$$

Angenommen, es gäbe ein Element $x \in X$ mit $f(x) = A$.

- Gilt $x \in A$, so folgt $x \notin f(x) = A$, ein Widerspruch.
- Gilt $x \notin A$, so folgt $x \in f(x) = A$, ein Widerspruch.

Wir schließen: Es existiert kein Element $x \in X$ mit $f(x) = A$. QED

Mächtigkeit der Potenzmenge

☺ Dieser Beweis ist genial einfach und einfach genial!
Der Trick heißt auch *Cantors zweites Diagonalargument*.
Cantors erstes Diagonalargument beweist $\mathbb{N}^2 \cong \mathbb{N}$, siehe F2K.

Das Argument erinnert uns eindringlich an das Barbier-Paradoxon und die Russelsche Antinomie (D127). Dieses logische Problem der allzu naiven Mengenlehre beheben wir durch Beschränkung auf die streng reglementierten Mengenkonstruktionen nach Zermelo–Fraenkel und machen seither sehr gute Erfahrungen damit.

Im vorliegenden Beweis ist alles kristallklar, alles geht mit rechten Dingen zu: Wir widerlegen die Aussage $A \in \operatorname{im}(f)$, ganz einfach. Zudem ist dies ein wunderbares Beispiel für einen Beweis durch Widerspruch zusammen mit einer einfachen Fallunterscheidung.

☺ Ich hoffe, unsere soliden Vorbereitungen zahlen sich hier (und überall) für Sie aus, und Sie genießen die schönen Aha–Erlebnisse.

Illustration zu Cantors Diagonalverfahren

Angenommen, wir haben eine Folge von Mengen $A_0, A_1, A_2, \cdots \subseteq \mathbb{N}$,
zum Beispiel $A_0 = \emptyset$, $A_1 = \{0,1,3\}$, $A_2 = \mathbb{N}$, $A_3 = 2\mathbb{N}$, $A_4 = 2\mathbb{N}+1$, ...
Diese Mengen können wir übersichtlich in einer Tabelle anordnen:

	0	1	2	3	4	5	6	7	8	9	...
A_0	0	0	0	0	0	0	0	0	0	0	...
A_1	1	1	0	1	0	0	0	0	0	0	...
A_2	1	1	1	1	1	1	1	1	1	1	...
A_3	1	0	1	0	1	0	1	0	1	0	...
A_4	0	1	0	1	0	1	0	1	0	1	...
...	...										

Als Tabelle schreiben wir $a_{ij} = 1$, falls $j \in A_i$, und $a_{ij} = 0$, falls $j \notin A_i$.
Entlang der Diagonalen bilden wir die Menge $A = \{\, i \in \mathbb{N} \mid a_{ii} = 0 \,\}$.
Diese Menge kommt nicht in unserer Liste vor, denn $i \in A_i \Leftrightarrow i \notin A$.

☺ Es gibt keine Abzählung $A_0, A_1, A_2, \ldots$ der Potenzmenge $\mathfrak{P}(\mathbb{N})$.
Jede Folge $A_0, A_1, A_2, \cdots \subseteq \mathbb{N}$ lässt immer noch Mengen aus.

Illustration zu Cantors Diagonalverfahren

Mächtigkeit der ganzen Zahlen $\mathbb{Z}$

F221

Satz F2H: Mächtigkeit von $\mathbb{Z}$

Die Mengen $\mathbb{Z}$ und $\mathbb{N}$ sind gleichmächtig, kurz $\mathbb{Z} \cong \mathbb{N}$.

a	0	1	2	3	4	5	6	7	8	9	10	...
b	0	-1	1	-2	2	-3	3	-4	4	-5	5	...

Aufgabe: Formulieren Sie explizit dieses Bijektionspaar $(f, g) : \mathbb{N} \cong \mathbb{Z}$.

Lösung: Wir fassen diese Idee in explizite Formeln:

$$f : \mathbb{N} \to \mathbb{Z} : a \mapsto \begin{cases} a/2 & \text{falls } a \in 2\mathbb{N}, \\ -(a+1)/2 & \text{falls } a \in 2\mathbb{N}+1, \end{cases}$$

$$g : \mathbb{Z} \to \mathbb{N} : b \mapsto \begin{cases} 2b & \text{falls } b \geq 0, \\ -2b-1 & \text{falls } b < 0. \end{cases}$$

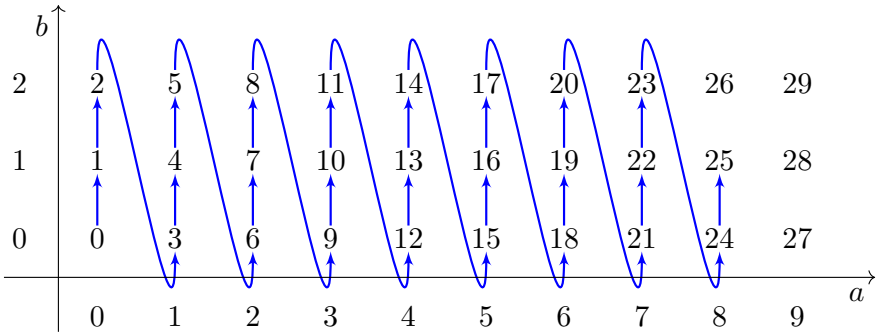
☺ Diese Abbildungen sind wohldefiniert und zueinander invers:
Es gilt $g \circ f = \mathrm{id}_{\mathbb{N}}$ und $f \circ g = \mathrm{id}_{\mathbb{Z}}$. Nachrechnen! QED

Mächtigkeit des Produkts $\mathbb{N} \times \{1, \dots, n\}$

F222

Satz F2I: Mächtigkeit von $\mathbb{N} \times \{1, \dots, n\}$

Die Mengen $\mathbb{N} \times \{1, \dots, n\}$ und $\mathbb{N}$ sind gleichmächtig.



Aufgabe: Formulieren Sie explizit dieses Bijektionspaar.

Lösung: Wir nutzen zunächst $\{1, \dots, n\} \cong \{0, \dots, n-1\} : k \leftrightarrows k-1$.
Zudem haben wir das Bijektionspaar $(f, g) : \mathbb{N} \times \{0, \dots, n-1\} \cong \mathbb{N}$
mit $f(a, b) = na + b$ und $g(c) = (c \operatorname{quo} n, c \operatorname{rem} n)$. QED

Grundrechenarten für Mächtigkeiten

F223
Erläuterung

Satz F2J: Grundrechenarten für Mächtigkeiten

Gegeben seien Bijektionen $(\alpha, \alpha') : A \cong A'$ und $(\beta, \beta') : B \cong B'$.
Daraus erhalten wir die Bijektionen

$$(\alpha \sqcup \beta, \alpha' \sqcup \beta') : A \sqcup B \cong A' \sqcup B',$$
$$(\alpha \times \beta, \alpha' \times \beta') : A \times B \cong A' \times B',$$
$$(\varphi, \varphi') : \mathrm{Abb}(A, B) \cong \mathrm{Abb}(A', B')$$

mit $\varphi(f) = \beta \circ f \circ \alpha'$ und $\varphi'(f') = \beta' \circ f' \circ \alpha$. Zudem haben wir

$$(\psi, \psi') : (Z^X)^Y \cong Z^{X \times Y} : f \leftrightarrows g$$

mit $g(x, y) = f(y)(x)$ für $f : Y \to \mathrm{Abb}(X, Z)$ und $g : X \times Y \to Z$.

Beweis: Diese Abbildungen sind wohldefiniert und zueinander invers:
Alles liegt explizit vor, es genügt sorgsames Nachrechnen! QED

Grundrechenarten für Mächtigkeiten

F224
Erläuterung

Für die erste Bijektion $A \sqcup B \cong A' \sqcup B'$ setzen wir Disjunktheit voraus, also $A \cap B = A' \cap B' = \emptyset$. Dies können wir immer erzwingen durch

$$(\{1\} \times A) \sqcup (\{2\} \times B) = (\{1\} \times A') \sqcup (\{2\} \times B')$$

Anschaulich gesagt, wir ersetzen die Menge A durch die Kopie $\{1\} \times A$; zwischen beiden übersetzen wir durch die kanonische Bijektion (ι_2, pr_2). Entsprechend verfahren wir für $\{2\} \times B$ sowie $\{1\} \times A'$ und $\{2\} \times B'$.

Beispiel: Es gilt $(\{1\} \times \mathbb{N}) \sqcup (\{2\} \times \mathbb{N}) = \{1, 2\} \times \mathbb{N} \cong \{0, 1\} \times \mathbb{N} \cong \mathbb{N}$.
Dies ist die Vereinigung von zwei disjunkten Kopien der Menge $\mathbb{N}$,
die Mächtigkeit bleibt dabei gleich (F2I).

Beispiel: Aus $\mathbb{Z} \cong \mathbb{N}$ folgt $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{N} \times \mathbb{N}$ dank F2J.
Wir werden im Folgenden sehen, dass $\mathbb{N}^2 \cong \mathbb{N}$ gilt (F2K).

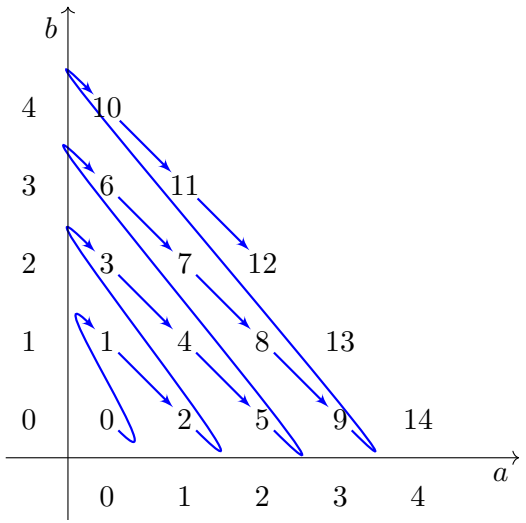
Beispiel: Aus $\mathbb{Z} \cong \mathbb{N}$ folgt $\mathbb{Z}^n \cong \mathbb{N}^n$ für alle $n \in \mathbb{N}$ dank F2J.
Wir zeigen im Folgenden $\mathbb{N}^n \cong \mathbb{N}$ für alle $n \in \mathbb{N}_{\geq 1}$ (F2M).

Mächtigkeit des Produkts $\mathbb{N} \times \mathbb{N}$

Satz F2K: Cantors erstes Diagonalargument

Die Menge $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ ist gleichmächtig zu $\mathbb{N}$, kurz $\mathbb{N}^2 \cong \mathbb{N}$.

Beweisidee:



Mächtigkeit des Produkts $\mathbb{N} \times \mathbb{N}$

Aufgabe: Formulieren Sie explizit dieses Bijektionspaar $(f, g) : \mathbb{N}^2 \cong \mathbb{N}$.

Lösung: Wir formulieren obige Skizze als Rekursion (Satz F2B):

$$g : \mathbb{N} \to \mathbb{N}^2 : \quad g(0) = (0,0) \text{ und } g(n+1) = \varphi(g(n)),$$

$$\varphi : \mathbb{N}^2 \to \mathbb{N}^2 : (a,b) \mapsto \begin{cases} (0, a+1) & \text{falls } b = 0, \\ (a+1, b-1) & \text{falls } b > 0. \end{cases}$$

Damit gilt etwas bequemer ausgeschrieben $g(c) = (s, r-s)$ mit

$$r = \max\{\, n \in \mathbb{N} \mid n(n+1)/2 \leq c \,\},$$
$$s = c - r(r+1)/2.$$

Die Umkehrfunktion ist erfreulich einfach (dank dem kleinen Gauß):

$$f : \mathbb{N}^2 \to \mathbb{N} : (a,b) \mapsto a + (a+b)(a+b+1)/2$$

☺ Diese Abbildungen sind wohldefiniert und zueinander invers:
Es gilt $g \circ f = \mathrm{id}_{\mathbb{N}^2}$ und $f \circ g = \mathrm{id}_{\mathbb{N}}$. Nachrechnen! QED

Abzählbare Vereinigung abzählbarer Mengen

Beispiel: Die Vereinigung $\bigsqcup_{i \in \mathbb{N}} \{i\} \times \mathbb{N} = \mathbb{N} \times \mathbb{N}$ ist abzählbar.
Für den allgemeinen Fall nutzen wir geschickt diesen Spezialfall:

Satz F2L: abzählbare Vereinigung abzählbarer Mengen

Jede abzählbare Vereinigung abzählbarer Mengen ist abzählbar:

Sei I eine abzählbare Indexmenge. Zu jedem Index $i \in I$ sei A_i eine abzählbare Menge. Dann ist auch $A = \bigcup_{i \in I} A_i$ abzählbar.

Beweis: Gegeben seien $f : I \hookrightarrow \mathbb{N}$ und $g_i : A_i \hookrightarrow \mathbb{N}$ für jedes $i \in I$.

$$\begin{array}{ccc} A = \bigcup_{i \in I} A_i & \xhookrightarrow{\quad h \quad} & \mathbb{N} \\ \mathrm{pr}_2 \uparrow\!\downarrow r & & \uparrow \text{F2K} \\ A' = \bigsqcup_{i \in I} \{i\} \times A_i & \xhookrightarrow{(i,a) \mapsto (f(i), g_i(a))} & \mathbb{N} \times \mathbb{N} \end{array}$$

Nach Indexwechsel dürfen wir $I \subseteq \mathbb{N}$ annehmen. Eine Rechtsinverse zu $\mathrm{pr}_2 : A' \twoheadrightarrow A$ ist $r : a \mapsto (j, a)$ mit $j = \min\{\, i \in I \mid a \in A_i \,\}$ dank F1S.

Somit gilt $A \preccurlyeq A' \preccurlyeq \mathbb{N} \times \mathbb{N} \preccurlyeq \mathbb{N}$. Dank Transitivität folgt $A \preccurlyeq \mathbb{N}$. QED

Abzählbare Vereinigung abzählbarer Mengen

Korollar F2M: Mächtigkeit von $\mathbb{N}^{(\mathbb{N})}$

(1) Es gilt $\mathbb{N}^n \cong \mathbb{N}$ für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$.

(2) Es gilt $\mathbb{N}^{(\mathbb{N})} \cong \mathbb{N}$ für die Menge alle Folgen mit endlichem Träger:

$$\mathbb{N}^{(\mathbb{N})} := \{\, f : \mathbb{N} \to \mathbb{N} \mid \sharp\,\mathrm{supp}(f) < \infty \,\}.$$

(3) Hingegen ist die Menge $\mathbb{N}^{\mathbb{N}} = \{\, f : \mathbb{N} \to \mathbb{N} \,\}$ überabzählbar.

Aufgabe: Beweisen Sie diese Aussagen als Wiederholung und Übung.

Lösung: (1) Induktion über $n \in \mathbb{N}_{\geq 1}$: Für $n = 1$ gilt $\mathbb{N}^1 \cong \mathbb{N}$.
Für $n \geq 2$ finden wir induktiv $\mathbb{N}^n = \mathbb{N}^{n-1} \times \mathbb{N} \cong \mathbb{N} \times \mathbb{N} \cong \mathbb{N}$ (F2K).

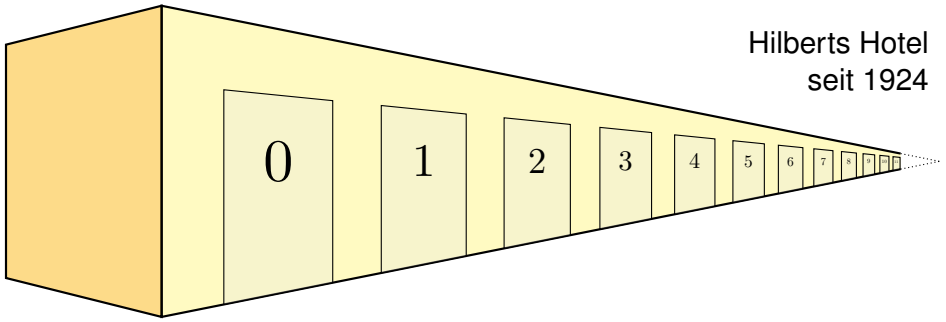
(2) Die Menge $\mathbb{N}^{(\mathbb{N})}$ ist eine abzählbare Vereinigung (F2L) gemäß

$$\mathbb{N}^{(\mathbb{N})} = \bigcup\nolimits_{n \in \mathbb{N}} \{\, f : \mathbb{N} \to \mathbb{N} \mid \mathrm{supp}(f) \subset \{0, \ldots, n\} \,\}$$

(3) Wir haben $\mathfrak{P}(\mathbb{N}) \cong \{0,1\}^{\mathbb{N}} \subseteq \mathbb{N}^{\mathbb{N}}$, und $\mathfrak{P}(\mathbb{N})$ ist überabzählbar (F2G).

Hilberts Hotel

Aus dem Paradies, das Cantor uns geschaffen,
soll uns niemand vertreiben können. (David Hilbert)



Hilberts Hotel hat die Zimmer $0, 1, 2, 3, \ldots$. Alle Zimmer sind belegt.
Ein weiterer Gast kommt noch unter dank $\mathbb{N} \hookrightarrow \mathbb{N} : n \mapsto n + 1$,
. . . auch abzählbar viele neue Gäste dank $\mathbb{N} \hookrightarrow \mathbb{N} : n \mapsto 2n$,
. . . sogar $\mathbb{N}^2 \hookrightarrow \mathbb{N} : (a, b) \mapsto a + (a + b)(a + b + 1)/2$.

Hilberts Hotel

Wenn in einem **endlichen Hotel** alle Zimmer belegt sind, dann kann kein Gast mehr aufgenommen werden, auch wenn die Managerin die Gäste neu auf die Zimmer verteilt. Es hilft alles nichts! (Invarianz E1H)

Anders in **Hilberts Hotel** mit unendlich vielen Zimmern $0, 1, 2, 3, \ldots$: Sind alle Zimmer belegt, so kann immer noch ein Gast aufgenommen werden: Der Gast von Zimmer 0 zieht nach 1, der von 1 nach 2, der von 2 nach 3, usw. Wir nutzen hierzu die Bijektion $\mathbb{N} \xrightarrow{\sim} \mathbb{N}_{\geq 1} : n \mapsto n + 1$.

Ebenso zwei Gäste, oder drei, oder vier. . . Nun kommt ein Hilbert–Bus mit unendlich vielen neuen Gästen. Die Managerin quartiert die alten Gäste um vermöge der Bijektion $\mathbb{N} \xrightarrow{\sim} 2\mathbb{N} : n \mapsto 2n$. Die neuen Gäste beziehen ihre Zimmer vermöge $\mathbb{N} \xrightarrow{\sim} 2\mathbb{N} + 1 : n \mapsto 2n + 1$. Zusammen erhalten wir so die Bijektion $\{0, 1\} \times \mathbb{N} \xrightarrow{\sim} \mathbb{N} : (i, n) \mapsto 2n + i$ (Satz F2I).

Schließlich kommen unendlich viele Busse, jeder mit unendlich vielen Gästen. Kein Problem, wir haben eine Bijektion $\mathbb{N} \times \mathbb{N} \xrightarrow{\sim} \mathbb{N}$ (Satz F2K).

Übung: Wie verteilen Sie die Zimmer jeweils neu? Schreiben Sie zur Wiederholung alle relevanten Bijektion möglichst schön und explizit aus!

Hilberts Hotel

HOTEL INFINITY, lyrics © 2000 by Lawrence Mark Lesser

On a dark desert highway — not much scenery
Except this long hotel stretchin' far as I could see.
Neon sign in front read "No Vacancy,"
But it was late and I was tired, so I went inside to plea.

The clerk said, "No problem. Here's what can be done —
We'll move those in a room to the next higher one.
That will free up the first room and that's where you can stay."
I tried understanding that as I heard him say:

[CHORUS] *"Welcome to the Hotel called Infinity —*
Where every room is full (every room is full)
Yet there's room for more.
Yeah, plenty of room at the Hotel called Infinity —
Move 'em down the floor (move 'em down the floor)
To make room for more."

Hilberts Hotel

I'd just gotten settled, I'd finally unpacked
When I saw 8 more cars pull into the back.
I had to move to room 9; others moved up 8 rooms as well.
Never more will I confuse a Hilton with a Hilbert Hotel!

My mind got more twisted when I saw a bus without end
With an infinite number of riders coming up to check in.
"Relax," said the nightman. "Here's what we'll do:
Move to the double of your room number:
that frees the odd-numbered rooms." [CHORUS]

Last thing I remember at the end of my stay —
It was time to pay the bill but I had no means to pay.
The man in 19 smiled, "Your bill is on me.
20 pays mine, and so on, so you get yours for free!"

(`www.math.utep.edu/Faculty/lesser/GreatestLESSERhits.html`)

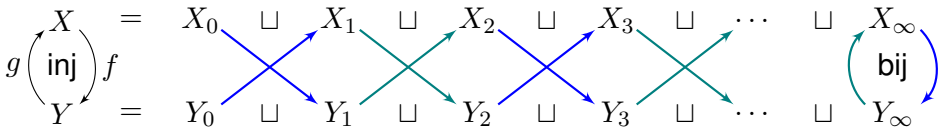
Der Äquivalenzsatz von Cantor–Bernstein

☺ Wir wollen nun zeigen: Aus $X \preccurlyeq Y$ und $Y \preccurlyeq X$ folgt $X \cong Y$:

Satz F2N: Äquivalenzsatz von Cantor–Bernstein

Aus gegebenen Injektionen $f : X \hookrightarrow Y$ und $g : Y \hookrightarrow X$
können wir eine Bijektion $(h, k) : X \cong Y$ konstruieren.

Wir bilden Urbildketten $x_0 \mapsfrom y_1 \mapsfrom x_2 \mapsfrom y_3 \mapsfrom \dots$ maximaler Länge.
Die Elemente der Länge n bilden die Menge $X_n \subseteq X$ bzw. $Y_n \subseteq Y$.



Cantors Reißverschluss: Jede Abbildung rechts von „=“ ist bijektiv!

Aus $f_n = f|_{X_n}^{Y_{n+1}} : X_n \xrightarrow{\sim} Y_{n+1}$ und $g_n = g|_{Y_n}^{X_{n+1}} : Y_n \xrightarrow{\sim} X_{n+1}$ erhalten wir
$h = f_0 \sqcup g_0^{-1} \sqcup f_2 \sqcup g_2^{-1} \sqcup \dots \sqcup f_\infty$ und $k = g_0 \sqcup f_0^{-1} \sqcup g_2 \sqcup f_2^{-1} \sqcup \dots \sqcup f_\infty^{-1}$.

☺ Der folgende Beweis formuliert diese Idee sorgfältig aus.

Der Äquivalenzsatz von Cantor–Bernstein

Wir lesen $X \preccurlyeq Y$ als „Die Menge X ist höchstens so groß wie Y.“
Wir lesen $Y \succcurlyeq X$ als „Die Menge Y ist mindestens so groß wie X.“
Wir lesen $X \cong Y$ als „Die Mengen X und Y sind gleich groß“,
hierzu sagen wir traditionell **gleichmächtig** oder **äquipotent**.

Der Satz garantiert, dass wir Mengen nach Mächtigkeit ordnen können.
Wir definieren die strikte Ordnung $X \prec Y$ durch $X \preccurlyeq Y$ und $Y \not\preccurlyeq X$ und
entsprechend $X \succ Y$ durch $X \succcurlyeq Y$ und $Y \not\succcurlyeq X$. Demnach gilt also
höchstens eine der drei Alternativen $X \prec Y$ oder $X \cong Y$ oder $X \succ Y$.

Der Äquivalenzsatz wurde 1887 von Georg Cantor formuliert, aber erst zehn Jahre später 1897 bewiesen. Dies gelang dem damals 19-jährigen Studenten Felix Bernstein in Cantors Seminar an der Universität Halle. Zeitgleich und unabhängig veröffentlichte Ernst Schröder einen Beweis, der sich jedoch später als fehlerhaft erwies. Bereits 1887 fand Richard Dedekind einen Beweis, den er nicht veröffentlichte. Daher trägt der Äquivalenzsatz oft eine Kombination dieser Namen. Wir präsentieren im Folgenden eine Konstruktion, die ohne das Auswahlaxiom auskommt.

Der Äquivalenzsatz von Cantor–Bernstein

Beweis: Gegeben sind $f : X \hookrightarrow Y$ und $g : Y \hookrightarrow X$. Die beiden Mengen

$$X_0 := X \setminus g(Y) \quad \text{und} \quad Y_0 := Y \setminus f(X)$$

enthalten alle Elemente ohne Urbild. Per Rekursion (F2B) enthalten

$$X_{n+1} := g(Y_n) \quad \text{und} \quad Y_{n+1} := f(X_n)$$

alle Elemente mit Urbildfolge der Länge $n+1$. Schließlich enthalten

$$X_\infty := \bigcap\nolimits_{\ell \in \mathbb{N}} (g \circ f)^\ell(X) \quad \text{und} \quad Y_\infty := \bigcap\nolimits_{\ell \in \mathbb{N}} (f \circ g)^\ell(Y)$$

alle Elemente mit unendlicher Urbildfolge. Wir definieren

$$h : X \to Y : x \mapsto \begin{cases} f(x) & \text{für } x \in \bigsqcup_{\ell \in \mathbb{N}} X_{2\ell} \sqcup X_\infty, \\ y & \text{für } x = g(y) \in \bigsqcup_{\ell \in \mathbb{N}} X_{2\ell+1}, \end{cases}$$

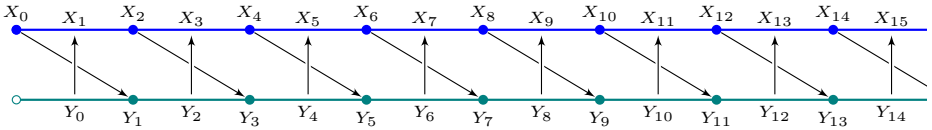
$$k : Y \to X : y \mapsto \begin{cases} x & \text{für } y = f(x) \in \bigsqcup_{\ell \in \mathbb{N}} Y_{2\ell+1} \sqcup Y_\infty, \\ g(y) & \text{für } y \in \bigsqcup_{\ell \in \mathbb{N}} Y_{2\ell}. \end{cases}$$

Damit gilt $k \circ h = \mathrm{id}_X$ und $h \circ k = \mathrm{id}_Y$. QED

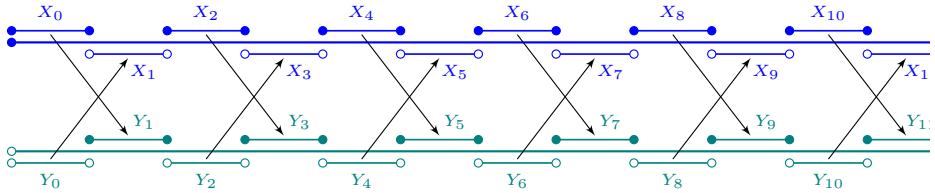
Der Äquivalenzsatz von Cantor–Bernstein

Beispiel: Die Intervalle $X = [0, \infty[$ und $Y =]0, \infty[$ sind gleichmächtig.

Beweis: Wir haben $f : X \hookrightarrow Y : x \mapsto x + 1$ und $g = \mathrm{inc} : Y \hookrightarrow X : y \mapsto y$.
Dank Cantor–Bernstein erhalten wir daraus $(h, k) : X \cong Y$. Skizze:



Alternative: Wir nutzen $f : x \mapsto x + 1$ und $g : y \mapsto y + 1$. Skizze:



Beispiel: Die Intervalle $X = [0, 3]$ und $Y = [0, 2[$ sind gleichmächtig.
Wir nutzen beispielsweise $f : X \hookrightarrow Y : x \mapsto x/2$ und $g : Y \hookrightarrow X : y \mapsto y$.

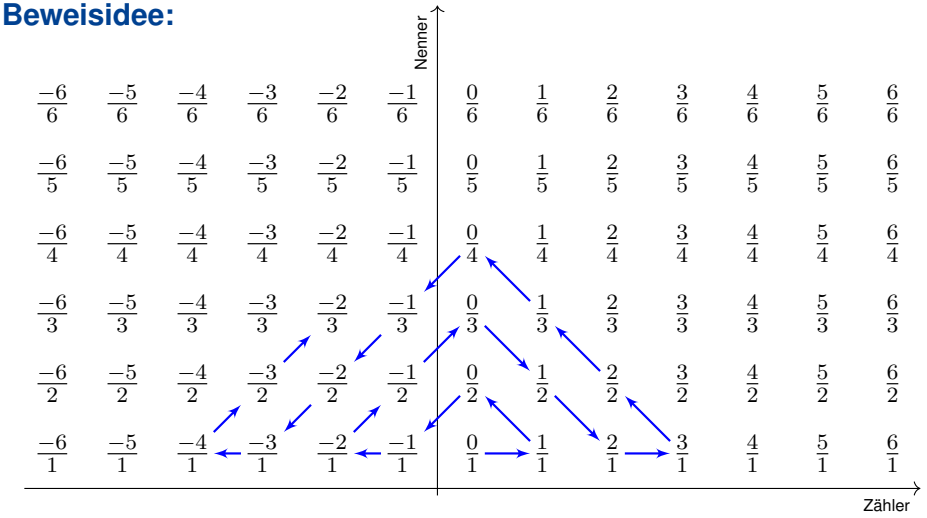
Übung: Führen Sie die Cantor–Bernstein–Konstruktion jeweils aus!

Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Satz F2O: Mächtigkeit von $\mathbb{Q}$

Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar unendlich, kurz $\mathbb{Q} \cong \mathbb{N}$.

Beweisidee:



Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Es gibt viele Möglichkeiten, eine solche Abzählung auszuführen.
Die Skizze zeigt eine anschauliche, graphische Vorgehensweise.

Wir wollen eine Bijektion $\mathbb{N} \xrightarrow{\sim} \mathbb{Q}$ konstruieren. Bei der oben skizzierten Abzählung werden tatsächlich alle rationalen Zahlen erreicht, jedoch müssen mehrfache Darstellungen derselben Zahl übergangen werden. Die Grundidee ist anschaulich anhand der Skizze vollkommen klar, doch eine vollständige Präzisierung scheint zunächst schwierig.

Um dies sorgfältig und explizit auszuformulieren, ist es geschickt, unsere bisherigen Konstruktionen gewinnbringend einzusetzen:

Wir haben einerseits $\mathbb{N} \subset \mathbb{Q}$, andererseits ist $\mathbb{Q} = \bigcup_{n \in \mathbb{N}^*} \{\, z/n \mid z \in \mathbb{Z} \,\}$ abzählbare Vereinigung abzählbarer Mengen, also abzählbar dank F2L.
Aus $f : \mathbb{N} \hookrightarrow \mathbb{Q}$ und $g : \mathbb{Q} \hookrightarrow \mathbb{N}$ erhalten wir $(h, k) : \mathbb{Q} \cong \mathbb{N}$ dank Satz F2N.

Damit gelingt eine ebenso präzise wie konkrete Konstruktion.
Wir müssen nur den Mut fassen, alles auszuschreiben!

🙂 *Beautiful is better than ugly. Explicit is better than implicit.*

Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Beweis: Wir haben einerseits die Inklusion $\mathbb{N} \subset \mathbb{Q}$, also $\mathbb{N} \preccurlyeq \mathbb{Q}$.
Die rationalen Zahlen sind also mindestens abzählbar unendlich.

Andererseits haben wir die Surjektion $q : \mathbb{Z} \times \mathbb{N}^* \twoheadrightarrow \mathbb{Q} : (a, b) \mapsto a/b$.

$$\begin{array}{ccc} \mathbb{Q} & \overset{h}{\dashrightarrow} & \mathbb{N} \\ {\scriptstyle q}\uparrow\downarrow{\scriptstyle r} & & \uparrow{\scriptstyle \text{F2K}} \\ \mathbb{Z} \times \mathbb{N}^* & \xrightarrow{\text{F2H}} & \mathbb{N} \times \mathbb{N} \end{array}$$

Somit gilt $\mathbb{Q} \preccurlyeq \mathbb{Z} \times \mathbb{N}^* \preccurlyeq \mathbb{N} \times \mathbb{N} \preccurlyeq \mathbb{N}$. Dank Transitivität folgt $\mathbb{Q} \preccurlyeq \mathbb{N}$.
Die rationalen Zahlen sind also höchstens abzählbar unendlich.

🙂 Dank Cantor–Bernstein F2N gilt $\mathbb{Q} \cong \mathbb{N}$. QED

Bemerkung: Die Quotientenabbildung $q : \mathbb{Z} \times \mathbb{N}^* \twoheadrightarrow \mathbb{Q} : (a, b) \mapsto a/b$ erlaubt eine schöne explizite Rechtsinverse $r : \mathbb{Q} \hookrightarrow \mathbb{Z} \times \mathbb{N}^* : c \mapsto (a, b)$ mit $c = a/b$ und $\operatorname{ggT}(a, b) = 1$: Dies ist die eindeutige Darstellung als vollständig gekürzter Bruch. Wir haben also $(r, q) : \mathbb{Q} \rightleftarrows \mathbb{Z} \times \mathbb{N}^*$.

Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Korollar F2P: Mächtigkeit von $\mathbb{Q}^{(\mathbb{N})}$

(1) Es gilt $\mathbb{Q}^n \cong \mathbb{N}$ für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$.
(2) Es gilt $\mathbb{Q}^{(\mathbb{N})} \cong \mathbb{N}$ für die Menge aller Folgen mit endlichem Träger:

$$\mathbb{Q}^{(\mathbb{N})} := \{\, f : \mathbb{N} \to \mathbb{Q} \mid \sharp\, \operatorname{supp}(f) < \infty \,\}.$$

(3) Hingegen ist die Menge $\mathbb{Q}^{\mathbb{N}} = \{\, f : \mathbb{N} \to \mathbb{Q} \,\}$ überabzählbar.

Aufgabe: Beweisen Sie diese Aussagen als Wiederholung und Übung.

Lösung: Dies beweisen wir wörtlich wie in F2M mit Hilfe von Satz F2J.
(1) Wir führen Induktion über $n \in \mathbb{N}_{\geq 1}$: Für $n = 1$ gilt $\mathbb{Q}^1 \cong \mathbb{N}$ (F2O).
Für $n \geq 2$ finden wir induktiv $\mathbb{Q}^n = \mathbb{Q}^{n-1} \times \mathbb{Q} \cong \mathbb{N} \times \mathbb{N} \cong \mathbb{N}$ (F2K).
(2) Die Menge $\mathbb{Q}^{(\mathbb{N})}$ ist eine abzählbare Vereinigung (F2L) gemäß

$$\mathbb{Q}^{(\mathbb{N})} = \bigcup\nolimits_{n \in \mathbb{N}} \{\, f : \mathbb{N} \to \mathbb{Q} \mid \operatorname{supp}(f) \subset \{0, \ldots, n\} \,\}$$

(3) Wir haben $\mathfrak{P}(\mathbb{N}) \cong \{0, 1\}^{\mathbb{N}} \subseteq \mathbb{Q}^{\mathbb{N}}$, und $\mathfrak{P}(\mathbb{N})$ ist überabzählbar (F2G).

Entwicklung reeller Zahlen in Basis B

F241

Sei $B \in \mathbb{N}_{\geq 2}$, etwa $B = 2$ binär, $B = 3$ ternär oder $B = 10$ dezimal:

$$\pi = 3.14159\,26535\,89793\,23846\,26433\,83279\,\ldots$$
$$0.1 = 0.09999\,99999\,99999\,99999\,99999\,99999\,\ldots$$

Satz F2Q: B–adische Entwicklung

Jede Ziffernfolge $a_1, a_2, a_3, \ldots \in \{0, \ldots, B-1\}$ definiert eine reelle Zahl

$$a = \sum_{k=1}^{\infty} a_k B^{-k} := \lim_{n\to\infty} \sum_{k=1}^{n} a_k B^{-k} \quad \in \quad [0,1].$$

Umgekehrt lässt sich jede reelle Zahl $a \in [0,1]$ so als eine B–adische Entwicklung schreiben (auf mindestens eine, höchstens zwei Weisen).

$$q \,:\, \{0,\ldots,B-1\}^{\mathbb{N}} \twoheadrightarrow [0,1] \,:\, (a_{n+1})_{n\in\mathbb{N}} \mapsto a$$

Zu jeder reellen Zahl $a \in \,]0,1]$ existiert genau eine solche B–adische Entwicklung, bei der unendlich viele Ziffern von 0 verschieden sind.

$$r \,:\, [0,1] \hookrightarrow \{0,\ldots,B-1\}^{\mathbb{N}} \,:\, a \mapsto (a_{n+1})_{n\in\mathbb{N}}$$

Entwicklung reeller Zahlen in Basis B

F242
Erläuterung

Für $s_n = \sum_{k=1}^{n} a_k B^{-k}$ gilt $0 = s_0 \leq s_1 \leq s_2 \leq s_3 \leq \ldots \leq 1$, also existiert der Grenzwert $a = \lim_{n\to\infty} s_n = \sup_{n\in\mathbb{N}} s_n$, denn $(\mathbb{R}, \leq)$ ist vollständig! Die B–adische Reihe definiert so die Abbildung $q : \mathbb{Z}_B^{\mathbb{N}} \twoheadrightarrow [0,1]$.

Umgekehrt konstruieren wir $r : [0,1] \to \mathbb{Z}_B^{\mathbb{N}} : a \mapsto (a_{n+1})_{n\in\mathbb{N}}$ rekursiv: Gegegen sei $a \in \,]0,1]$ und $(a_1, \ldots, a_n) \in \mathbb{Z}_B^n$ mit $s_n = \sum_{k=1}^{n} a_k B^{-k} < a$. Dazu definieren wir dann $a_{n+1} = \max\{\, z \in \mathbb{Z}_B \mid s_n + zB^{-n-1} < a \,\}$. Im Sonderfall $a = 0$ setzen wir $r(0) = (0,0,0,\ldots) \in \mathbb{Z}_B^{\mathbb{N}}$.

Somit ist r rechtsinvers zu q, das bedeutet, es gilt $q \circ r = \mathrm{id}_{[0,1]}$. Diese Konstruktion beweist, dass q surjektiv und r injektiv ist. Die Abbildung q ist zwar surjektiv, aber leider nicht injektiv: Manche Zahlen wie $a = 0.1$ haben zwei Darstellungen!

Es ist nicht ganz so einfach, eine Bijektion $\mathbb{Z}_B^{\mathbb{N}} \cong [0,1]$ zu konstruieren. Immerhin erhalten wir eine Bijektion $(q|_X^Y, r|_Y^X) : X \cong Y$ zwischen den Teilmengen $X = \{1,\ldots,B-1\}^{\mathbb{N}} \subsetneq \mathbb{Z}_B^{\mathbb{N}}$ und $Y = q(X) \subsetneq [0,1]$.

🙂 Der Satz von Cantor–Bernstein F2N löst das Problem sehr elegant! Der folgende Satz fügt nun alle Vorbereitungen sorgsam zusammen.

Mächtigkeit der reellen Zahlen $\mathbb{R}$

F243

Satz F2R: Mächtigkeit von $\mathbb{R}$

(1) Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar.
Genauer konstruieren wir eine Bijektion $\mathbb{R} \cong \{0,1\}^{\mathbb{N}} \cong \mathfrak{P}(\mathbb{N})$.

(2) Insbesondere ist die Menge $\mathbb{R}$ gleichmächtig zur Menge $\mathbb{R}^n$ aller n–Tupel für $n \geq 1$ sowie zur Menge $\mathbb{R}^{\mathbb{N}} = \{\, f : \mathbb{N} \to \mathbb{R} \,\}$ aller Folgen.

Beweis: (1a) Wir haben Bijektionen $f : \mathbb{R} \xrightarrow{\sim} \,]-1,+1[: x \mapsto x/(1+|x|)$ (D3C) sowie $g : \,]-1,+1[\xrightarrow{\sim} \,]0,1[: x \mapsto (x+1)/2$. Die Binärentwicklung stiftet die Injektion $r : \,]0,1[\hookrightarrow \{0,1\}^{\mathbb{N}}$ dank Satz F2Q für $B = 2$.

(1b) Umgekehrt haben wir $\{0,1\} \xrightarrow{\sim} \{1,2\}$ und somit $\{0,1\}^{\mathbb{N}} \xrightarrow{\sim} \{1,2\}^{\mathbb{N}}$. Satz F2Q für $B = 3$ stiftet eine Injektion $q : \{1,2\}^{\mathbb{N}} \hookrightarrow \,]0,1] \subset \mathbb{R}$.

Insgesamt haben wir also Injektionen $\{0,1\}^{\mathbb{N}} \hookrightarrow \mathbb{R}$ und $\mathbb{R} \hookrightarrow \{0,1\}^{\mathbb{N}}$. Dank Cantor–Bernstein F2N erhalten wir eine Bijektion $\mathbb{R} \cong \{0,1\}^{\mathbb{N}}$.

(2) Wir haben Bijektionen $\mathbb{N} \cong \mathbb{N} \times \{1,\ldots,p\} \cong \mathbb{N} \times \mathbb{N}$. Aus $\mathbb{R} \cong \{0,1\}^{\mathbb{N}}$ folgt $\mathbb{R}^p \cong \{0,1\}^{\mathbb{N}\times\{1,\ldots,p\}} \cong \{0,1\}^{\mathbb{N}}$ und $\mathbb{R}^{\mathbb{N}} \cong \{0,1\}^{\mathbb{N}\times\mathbb{N}} \cong \{0,1\}^{\mathbb{N}}$. QED

Übung: Führen Sie die letzten Rechnungen aus mit Hilfe von Satz F2J.

Mächtigkeit der reellen Zahlen $\mathbb{R}$

F244
Erläuterung

Schon das Ergebnis $\mathbb{N}^2 \cong \mathbb{N}$ ist erstaunlich, daraus abgeleitet $\mathbb{N}^n \cong \mathbb{N}$ und $\mathbb{N}^{(\mathbb{N})} \cong \mathbb{N}$ umso mehr (F2M). Zum Glück verfügen wir über effiziente Werkzeuge und können diese Behauptungen nun beweisen.

Naiv würde man vermuten, dass $\mathbb{N}^n$ „wesentlich mehr“ Punkte hat als $\mathbb{N}$. Das ist jedoch nicht der Fall, jedenfalls soweit es Bijektionen betrifft.

Ebenso möchte man glauben, dass $\mathbb{R}^n$ „wesentlich mehr“ Punkte hat als $\mathbb{R}$. Auch diese Intuition liegt falsch, wir finden Bijektionen $\mathbb{R}^n \cong \mathbb{R}$.

Das zeigt, wie sehr unsere naive Anschauung uns hier in die Irre leitet. Es betont auch den Wert präziser Definitionen und sorgsamer Beweise.

Dieses Thema wird Sie in Ihrem Studium immer wieder beschäftigen: Natürlich möchten Sie jedem Raum $\mathbb{R}^n$ seine Dimension „$\dim \mathbb{R}^n = n$“ zusprechen. Allein die Mächtigkeit macht jedoch keinen Unterschied: Alle Räume $\mathbb{R}^1, \mathbb{R}^2, \mathbb{R}^3, \ldots$ stehen paarweise in Bijektion. Die Dimension erhält erst durch zusätzliche Struktur ihren Sinn: bezüglich linearer Abbildungen von $\mathbb{R}$–Vektorräumen, oder Diffeomorphismen, oder Homöomorphismen, … Dazu später mehr im Studium.

Gibt es transzendente Zahlen?

Definition F2S: algebraisch vs transzendent

Eine reelle Zahl $\alpha \in \mathbb{R}$ heißt **algebraisch**, wenn sie Nullstelle eines rationalen Polynoms $P \in \mathbb{Q}[X]^*$ ist. Andernfalls heißt α **transzendent**.

Beispiele: Jede rationale Zahl $\alpha \in \mathbb{Q}$ ist algebraisch, als Nullstelle des Polynoms $X - \alpha \in \mathbb{Q}[X]^*$. Die reelle Zahl $\alpha = \sqrt{2}$ ist nicht rational (A1F), aber algebraisch, denn α ist Nullstelle von $X^2 - 2 \in \mathbb{Q}[X]^*$.

Es ist im Allgemeinen viel schwieriger, Transzendenz nachzuweisen!

Beispiel: Die Eulersche Zahl e ist transzendent. (C. Hermite, 1873)

$$\mathrm{e} = \exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} + \dots$$

Beispiel: Die Kreiszahl π ist transzendent. (F. Lindemann, 1882)

$$\frac{\pi}{4} = \arctan(1) = \sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \dots$$

☺ Die Quadratur des Kreises mit Zirkel und Lineal ist unmöglich!

Gibt es transzendente Zahlen?

Bereits im 18. Jahrhundert entwickelte sich langsam die Vorstellung von Transzendenz und die Vermutung, dass es transzendente Zahlen gibt, so etwa bei Gottfried Wilhelm Leibniz (1646–1716) und Leonhard Euler (1707–1783). Euler formulierte zwar keine klare Definition, war aber überzeugt, dass es solche „schwer fassbaren“ Zahlen geben müsse.

Ebenso wie „irrational“ für ‘unvernünftig’ ist auch „transzendent“ für ‘jenseits aller Vernunft’ zunächst ein negativer Begriff des Erstaunens, ja des Erschreckens. Diese Zahlen sind algebraisch nicht zugänglich.

Erste Konstruktionen und Nachweise transzendenter Zahlen gelangen 1844 Joseph Liouville (1809–1882), etwa für die Liouville-Konstante

$$L = \sum_{k=1}^{\infty} 10^{-k!} = 0.11000100000000000000000001000\dots$$

Georg Cantor bewies 1874 erneut die Existenz transzendenter Zahlen: Wie wir gleich sehen, sind sogar fast alle reellen Zahlen transzendent! Im Gegensatz zu Liouville ist Cantors Beweis jedoch nicht konstruktiv; er hilft nicht, einer fest gegebenen Zahl Transzendenz nachzuweisen.

Gibt es transzendente Zahlen?

Satz F2T: Die algebraischen Zahlen sind abzählbar.

Die Menge $\mathbb{A} \subseteq \mathbb{R}$ der algebraischen Zahlen ist abzählbar, kurz $\mathbb{A} \cong \mathbb{N}$. Somit ist das Komplement $\mathbb{T} = \mathbb{R} \setminus \mathbb{A}$ überabzählbar, genauer $\mathbb{T} \cong \mathbb{R}$.

Beweis: Die Menge der Polynome vom Grad $< n$ ist abzählbar:

$$\mathbb{Q}[X]_{<n} \underset{\text{Def}}{\cong} \mathbb{Q}^n \underset{\text{F2O}}{\cong} \mathbb{N}^n \underset{\text{F2M}}{\cong} \mathbb{N}$$

Also ist auch $\mathbb{Q}[X]$ abzählbar, als abzählbare Vereinigung (F2L):

$$\mathbb{Q}[X] \underset{\text{Def}}{=} \bigcup_{n\in\mathbb{N}} \mathbb{Q}[X]_{<n}$$

Zu jedem $P \in \mathbb{Q}[X]^*$ ist die Nullstellenmenge in $\mathbb{R}$ endlich (B3A, Übung). Somit ist die Menge $\mathbb{A}$ abzählbar, als abzählbare Vereinigung (F2L):

$$\mathbb{A} \underset{\text{Def}}{=} \bigcup_{P\in\mathbb{Q}[X]^*} \{\, \alpha \in \mathbb{R} \mid P(\alpha) = 0 \,\}$$

Wir haben also $\mathbb{A} \preccurlyeq \mathbb{N}$. Zusammen mit $\mathbb{N} \subseteq \mathbb{A}$ folgt $\mathbb{A} \cong \mathbb{N}$ (F2N). QED

Gibt es transzendente Zahlen?

Da $\mathbb{A}$ abzählbar ist, aber $\mathbb{R} = \mathbb{A} \sqcup \mathbb{T}$ überabzählbar, muss $\mathbb{T}$ überabzählbar sein, durch Kontraposition von Satz F2L.
Die genauere Bijektion $\mathbb{T} \cong \mathbb{R}$ führe ich hier nicht aus.

Diese grundlegende Elementezählung hat erstaunliche Konsequenzen:

☺ Wenn Sie zufällig gleichverteilt eine reelle Zahl $\alpha \in [0,1]$ wählen, dann ist das Ergebnis mit 100% Wahrscheinlichkeit transzendent.

☹ Sobald Sie jedoch eine konkrete Zahl α vorliegen haben, ist es meist extrem schwierig, ihr Transzendenz nachzuweisen.

Das ist Fluch und Segen von elegant-nicht-konstruktiven Beweisen. Ähnliche Situationen kennen wir von Dirichlets Schubfachprinzip E1I oder Zagiers Ein-Satz-Beweis für Fermats Zwei-Quadrate-Satz E3E.

Eine solche reine Existenzaussage ist zwar leider nicht konstruktiv, doch oft ist eine schwache Aussage besser als gar keine Aussage. Sie ist nicht das Ende der Problemlösung, sondern ein guter Anfang.

Kapitel G

Ringe und Körper

Be wise, generalize!
(mathematisches Sprichwort)

The commonly accepted attitudes toward the commutative law and the associative law are different. Many real life operations fail to commute; the mathematical community has learned to live with that fact and even to enjoy it. Violations of the associative law are usually considered by specialists only.

Paul Halmos (1916–2006), *Linear Algebra Problem Book* (1995)

Inhalt dieses Kapitels G

Motivation und Überblick

Das Ziel in diesem Kapitel sind Ringe und Körper,
insbesondere wollen wir Polynomringe behandeln.

Zur Vorbereitung ist es effizient, zunächst die Grundlagen
für Monoide und Gruppen zu legen; das ist der erste Teil.

Ich führe dazu die nötigen Vokabeln und ein
und erste einfache Rechnungen für Sie aus.

Der Weg ist lang, aus vielen kleinen Schritten,
aber er lohnt sich für eine solide Grundlage.

Motivation und Überblick

Verknüpfungen: allgemeine Definition

Definition G1A: Verknüpfung / Operation

Gegeben seien Mengen A, B, C. Jede Abbildung

$$* : A \times B \to C : (a,b) \mapsto c = *(a,b) = (a,b)* = a * b = ab$$

nennen wir **(zweistellige) Verknüpfung** oder **(binäre) Operation**.

Statt **Präfix** $*(a,b)$ oder **Postfix** $(a,b)*$ schreiben wir meist **Infix** $a * b$. Diese traditionelle **algebraische Schreibweise** ist kurz und bequem.

Statt $a * b$ schreiben wir auch kurz ab, falls die Verknüpfung $*$ aus dem Kontext hervorgeht und keine Missverständnisse zu befürchten sind.

Im Falle $B = C$ heißt $*: A \times B \to B$ **Linksoperation** von A auf B.
Im Falle $A = C$ heißt $*: A \times B \to A$ **Rechtsoperation** von B auf A.

Im Falle $A = B$ heißt $*: A \times A \to C$ eine **(äußere) Verknüpfung** auf A nach C. Sie heißt **kommutativ**, falls $a * b = b * a$ für alle $a, b \in A$ gilt.

Im Falle $A = B = C$ heißt $*: A \times A \to A$ **(innere) Verknüpfung** auf A. Sie heißt **assoziativ**, falls $(a * b) * c = a * (b * c)$ für alle $a, b, c \in A$ gilt.

Verknüpfungen: allgemeine Definition

Wir sagen **zweistellige Verknüpfung** oder **binäre Operation**, um zu betonen, dass genau zwei Elemente miteinander verknüpft werden.

Assoziativität $(a * b) * c = a * (b * c)$ erlaubt uns, Klammern wegzulassen, und Kommutativität erlaubt uns, Faktoren umzuordnen, siehe Satz G1C.

Eine n–stellige Verknüpfung für $n \in \mathbb{N}$ ist eine Abbildung der Form

$$f : A_1 \times \cdots \times A_n \to B : (a_1, \ldots, a_n) \mapsto b = f(a_1, \ldots, a_n).$$

Im Falle $A_1 = \cdots = A_n = B$ nennen wir f eine **innere Verknüpfung**; in allen anderen Fällen ist f einfach eine **(äußere) Verknüpfung**.

Im Falle $n = 0$ ist $f : \{0\} \to B : 0 \mapsto b$ einfach nur ein **Element** $b \in B$.
Im Falle $n = 1$ ist $f : A_1 \to B : a \mapsto b = f(a)$ einfach eine **Funktion**.
Im Falle $n = 2$ ist $f : A_1 \times A_2 \to B$ eine **zweistellige Verknüpfung**.
Im Falle $n = 3$ ist $f : A_1 \times A_2 \times A_3 \to B$ eine **ternäre Operation**.

Meist betrachten wir Verknüpfungen der Stelligkeit $n \leq 2$, aber auch Verknüpfungen von höherer Stelligkeit kommen vor und sind nützlich. Dies gilt besonders für **Multilinearformen**, die wir später untersuchen.

Verknüpfungen: erste Beispiele

Beispiel: Wir verknüpfen Zähler und Nenner zum Quotienten:

$$/ : \mathbb{Z} \times \mathbb{N}^* \to \mathbb{Q} : (z,n) \mapsto z/n$$

Beispiel: Die euklidische Division in $\mathbb{Z}$ definiert zwei Verknüpfungen

$$(\mathrm{quo}, \mathrm{rem}) : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{N} : (a,b) \mapsto (q,r)$$

als eindeutige Lösung der Gleichung $a = bq + r$ mit $0 \leq r < |b|$.

Allgemein zu je zwei reellen Zahlen $a, b \in \mathbb{R}$ mit $b \neq 0$ existiert genau ein Paar (q,r) mit $a = bq + r$ und $q \in \mathbb{Z}$ und $r \in [0, |b|[$. Dies definiert

$$(\mathrm{quo}, \mathrm{rem}) : \mathbb{R} \times \mathbb{R}^* \to \mathbb{Z} \times \mathbb{R}_{\geq 0} : (a,b) \mapsto (q,r).$$

Für $b = 1$ ist somit $a = q + r$ die Zerlegung in den ganzzahligen Teil $q = a \operatorname{quo} 1 = \lfloor a \rfloor \in \mathbb{Z}$ und den Nachkommateil $r = a \operatorname{rem} 1 \in [0, 1[$.

Verknüpfungen: erste Beispiele

Beispiele: Für jeden Ring $\mathbb{K} = \mathbb{Z}, \mathbb{Z}_n, \ldots$ haben wir die ersten drei, für jeden Körper $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, \ldots$ alle vier Grundrechenarten

Addition	$+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K} : (a,b) \mapsto a + b,$
Subtraktion	$- : \mathbb{K} \times \mathbb{K} \to \mathbb{K} : (a,b) \mapsto a - b,$
Multiplikation	$\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K} : (a,b) \mapsto a \cdot b,$
Division	$/ : \mathbb{K} \times \mathbb{K}^* \to \mathbb{K} : (a,b) \mapsto a/b.$

Addition und Multiplikation sind hier assoziativ und kommutativ, doch Subtraktion und Division sind i.A. weder assoziativ noch kommutativ:

$$3 - 5 \neq 5 - 3, \qquad (8 - 5) - 3 \neq 8 - (5 - 3),$$
$$3/5 \neq 5/3, \qquad (8/4)/2 \neq 8/(4/2).$$

Assoziativität und Kommutativität sind keineswegs selbstverständlich! Im Gegenteil sind dies seltene Glücksfälle, die wir wertschätzen sollten. Dank dieser besonderen Eigenschaften können wir effizient rechnen.

Verknüpfungen: erste Beispiele

Beispiel: Ist die Addition von Fließkommazahlen assoziativ?
Hier lohnt sich ein numerisches Experiment, einfach aber eindrücklich:

```
a = +1000000000  # +1e+9, eine Milliarde
b = -1000000000  # -1e+9, minus eine Milliarde
c = 0.000000001  # +1e-9, also ein Milliardstel
print( (a + b) + c )
print( a + (b + c) )
```

🙂 Die Rechnung `(a+b)+c` ergibt `1e-9`, das ist das korrekte Ergebnis.

☹ Die Rechnung `a+(b+c)` ergibt `0.0`, das ist ein (Rundungs-)Fehler.

⚠ Fließkommazahlen haben eine feste Zahl von (Nachkomma)Stellen, typischerweise 52 Bits (nach Standard IEEE 754), dazu 11 Bits für den Exponenten und noch eins für das Vorzeichen, also insgesamt 64 Bits. Die Menge dieser Zahlen ist endlich, sie hat höchstens 2^{64} Elemente.

⚠ Selbst mit mehr Bits und potentiell beliebig viel Speicher bleiben die darstellbaren Zahlen abzählbar. Die Menge $\mathbb{R}$ ist jedoch überabzählbar!

Verknüpfungen: erste Beispiele

⚠ Fließkomma-Arithmetik ist deutlich anders als exakte Arithmetik in $\mathbb{Q}$. Das muss man wissen, um böse Überraschungen zu vermeiden!

Aufgabe: Was liefert folgende Schleife? Wagen Sie eine Vorhersage!

```
x = 0.0
while x < 1.0: print(x); x += 0.1
```

Wie viele und welche Werte werden angezeigt? Wie erklären Sie das?

⚠ Insbesondere Analysis und Numerik nutzen die reellen Zahlen $\mathbb{R}$ als Grundlage. Alle Rechnungen (Operationen, Funktionen, etc.) sind exakt definiert, aber für praktische Belange meist zu aufwändig. Sie werden daher geeignet approximiert durch kostengünstigere Näherungen.

⚠ Die Numerik auf dem Computer ist nochmal komplizierter als in $\mathbb{R}$, denn nun sind selbst die grundlegenden Rechnungen (Operationen, Funktionen, etc.) nicht exakt, sondern nur genähert. Die Vermeidung bzw. Beschränkung von Rundungsfehlern ist daher eine eigene Kunst.

Verknüpfungen: erste Beispiele

Beispiele: Für Matrizen über $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}, \mathbb{Z}_n, \mathbb{H}, \ldots$ haben wir

$$\begin{aligned} \mathbf{+} &: \mathbb{K}^{m\times n} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n} \;:\; (A,B) \mapsto C = A \mathbf{+} B, \quad c_{ij} = a_{ij} + b_{ij}, \\ \mathbf{-} &: \mathbb{K}^{m\times n} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n} \;:\; (A,B) \mapsto D = A \mathbf{-} B, \quad d_{ij} = a_{ij} - b_{ij}. \end{aligned}$$

Diese Addition ist assoziativ und kommutativ, die Subtraktion i.A. nicht.
Zwei Matrizen passender Größe können wir multiplizieren vermöge

$$\bullet : \mathbb{K}^{p\times q} \times \mathbb{K}^{q\times r} \to \mathbb{K}^{p\times r} \;:\; (A,B) \mapsto C = A \bullet B, \quad c_{ik} = \textstyle\sum_{j=1}^{q} a_{ij} \cdot b_{jk}.$$

Für $p = q = r$ ist die Multiplikation assoziativ, aber i.A. nicht kommutativ.
Zudem operiert $\mathbb{K}$ auf $\mathbb{K}^{m\times n}$ von links und von rechts durch Skalierung:

$$\begin{aligned} \bullet &: \mathbb{K} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n} \;:\; (\lambda, A) \mapsto B = \lambda \bullet A, \quad b_{ij} = \lambda \cdot a_{ij} \\ \bullet &: \mathbb{K}^{m\times n} \times \mathbb{K} \to \mathbb{K}^{m\times n} \;:\; (A, \lambda) \mapsto C = A \bullet \lambda, \quad c_{ij} = a_{ij} \cdot \lambda \end{aligned}$$

Wir betrachten $\mathbb{K}^n \cong \mathbb{K}^{n\times 1} : (a_i) \leftrightarrows (a_{i1})$ meist als Spaltenvektoren,
je nach Bedarf $\mathbb{K}^n \cong \mathbb{K}^{1\times n} : (a_i) \leftrightarrows (a_{1i})$ auch als Zeilenvektoren.

Beispiel: $(\mathbb{K}^n, \mathbf{+}, \bullet)$, Addition von Vektoren, Mutiplikation mit Skalaren.

Verknüpfungen: erste Beispiele

Beispiele: Die quadratischen Matrizen bilden den Ring

$$(\mathbb{K}^{n\times n}, \mathbf{+}, 0_{n\times n}, \bullet, 1_{n\times n}).$$

Dieser operiert von links auf den Spaltenvektoren:

$$\bullet : \mathbb{K}^{n\times n} \times \mathbb{K}^n \to \mathbb{K}^n \;:\; (A,x) \mapsto Ax$$

So formulieren wir lineare Gleichungssysteme bequem als $Ax = y$.
Die invertierbaren Matrizen bilden die allgemeine lineare Gruppe

$$\begin{aligned} \mathrm{GL}_n(\mathbb{K}) &:= (\mathbb{K}^{n\times n}, \bullet, 1_{n\times n})^\times \\ &= \left\{ A \in \mathbb{K}^{n\times n} \;\middle|\; \exists B \in \mathbb{K}^{n\times n} : A \bullet B = B \bullet A = 1_{n\times n} \right\}. \end{aligned}$$

Diese Gruppe operiert auf Matrizen von links und von rechts:

$$\begin{aligned} \bullet &: \mathrm{GL}_m \mathbb{K} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n} \;:\; (S,A) \mapsto S \bullet A \\ \bullet &: \mathbb{K}^{m\times n} \times \mathrm{GL}_n \mathbb{K} \to \mathbb{K}^{m\times n} \;:\; (A,T) \mapsto A \bullet T \end{aligned}$$

Das entspricht den Zeilen/Spaltenoperationen im Gauß–Algorithmus.

Verknüpfungen: erste Beispiele

Jede Verknüpfung $* : A \times B \to C : (a,b) \mapsto a * b$ entspricht einer Tabelle: Jedem Paar $(a,b) \in A \times B$ wird sein Produkt $a * b$ in C zugeordnet.

🙂 Kleine Verknüpfungstabellen können wir explizit ausschreiben.

Beispiele: So definieren wir die logischen Verknüpfungen:

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\dot\vee$	0	1
0	0	1
1	1	0

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

Beispiel: Allgemein ist ein Junktor eine n–stellige Verknüpfung

$$J : \{0,1\}^n \to \{0,1\} : a \mapsto J(a).$$

Dies können wir als Wahrheitstabelle darstellen. Beliebig große Tabellen sind im Prinzip möglich, aber mit wachsenden Kosten. ($\mathrm{P} = \mathrm{NP}$? C1K)

Jede n–stellige Verknüpfung $J : \{0,1\}^n \to \{0,1\}$ können als eine Formel in den Verknüpfungen $\wedge, \vee, \neg$ darstellen (CNF / DNF, siehe Satz C1H).

Verknüpfungen: erste Beispiele

Beispiele: Verknüpfungstabellen für $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$:

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

Körper!

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Körper!

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

CRing!

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

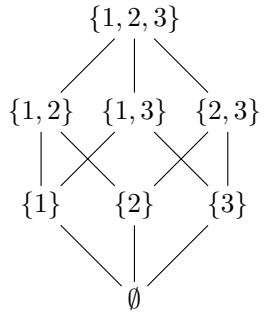
Körper!

Verknüpfungen: erste Beispiele

Beispiele: Wir kennen und nutzen ebenso Operationen auf Mengen:

Vereinigung	$\cup : \mathfrak{P}(X) \times \mathfrak{P}(X) \to \mathfrak{P}(X) : (A,B) \mapsto A \cup B$
Durchschnitt	$\cap : \mathfrak{P}(X) \times \mathfrak{P}(X) \to \mathfrak{P}(X) : (A,B) \mapsto A \cap B$
sym. Differenz	$\triangle : \mathfrak{P}(X) \times \mathfrak{P}(X) \to \mathfrak{P}(X) : (A,B) \mapsto A \triangle B$
Differenz	$\smallsetminus : \mathfrak{P}(X) \times \mathfrak{P}(X) \to \mathfrak{P}(X) : (A,B) \mapsto A \smallsetminus B$

Die ersten drei sind kommutativ und assoziativ, die vierte jedoch nicht.
Im Hasse-Diagramm gilt $A \cap B = \inf\{A,B\}$ und $A \cup B = \sup\{A,B\}$:



Verknüpfungen: erste Beispiele

Es gibt zahllose weitere Beispiele von Verknüpfungen, sowohl innere als auch äußere. In die große Vielfalt wollen wir etwas Ordnung bringen, wichtige Eigenschaften benennen und grundlegend untersuchen.
Wir wollen Werkzeuge bereitstellen, um damit effizient zu arbeiten.

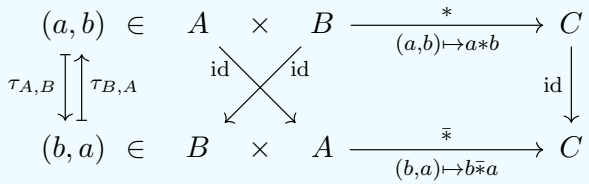
Vertauschung und Kommutativität

Definition G1B: Vertauschung und Kommutativität

Zu $* : A \times B \to C$ definieren wir die **entgegengesetzte Verknüpfung**

$$\bar{*} = *^{\mathrm{op}} \,:\, B \times A \to C \,:\, (b,a) \mapsto b \mathbin{\bar{*}} a = a * b.$$

Beide fassen wir übersichtlich als Diagramm zusammen:



Die Verknüpfung $*$ heißt **kommutativ** oder **symmetrisch**, falls $\bar{*} = *$.
Ausführlich bedeutet das: Es gilt $A = B$ und $a * b = b * a$ für alle $a, b \in A$.

Anschaulich gesagt: Es gilt $A = B$, und die Verknüpfungstabelle von $* : A \times A \to C$ ist spiegelsymmetrisch bezüglich der Hauptdiagonalen.

Vertauschung und Kommutativität

Zu jeder Verknüpfung $* : A \times B \to C$ haben wir die entgegengesetzte Verknüpfung $\bar{*} : B \times A \to C$ (G1B), diese ist definiert durch $b \mathbin{\bar{*}} a = a * b$ für alle $b \in B$ und $a \in A$. Die beiden Argumente werden also vertauscht; dies definiert zu $*$ eine neue Verknüpfung $\bar{*}$ mit demselben Ergebnis.

Die Vertauschung von (a, b) zu (b, a) entspricht dem Bijektionspaar

$$\tau_{A,B} \,:\, A \times B \xrightarrow{\sim} B \times A \,:\, (a,b) \mapsto (b,a),$$
$$\tau_{B,A} \,:\, B \times A \xrightarrow{\sim} A \times B \,:\, (b,a) \mapsto (a,b).$$

Somit gilt $\bar{*} = * \circ \tau_{B,A}$ und umgekehrt $* = \bar{*} \circ \tau_{A,B}$, wie im obigen Diagramm dargestellt. Insbesondere gilt $\bar{\bar{*}} = *$, also $(*^{\mathrm{op}})^{\mathrm{op}} = *$.

Anschaulich stellen wir uns die kartesischen Produktmengen $A \times B$ und $B \times A$ als Rechtecke vor. Die Vertauschung $(\tau_{A,B}, \tau_{B,A}) : A \times B \cong B \times A$ entspricht der Spiegelung an der Hauptdiagonalen. Der Übergang von $*$ zu $\bar{*}$ entspricht demnach der Spiegelung der Verknüpfungstabelle.

Beispiel: Komposition von Abbildungen

Beispiel: Zu je drei Mengen X, Y, Z haben wir die Komposition

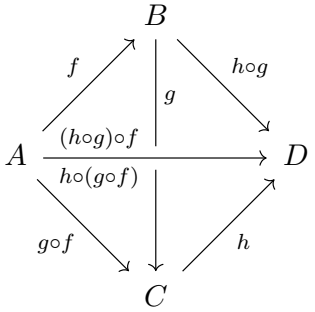
$$\bullet \,:\, \mathrm{Abb}(X,Y) \times \mathrm{Abb}(Y,Z) \to \mathrm{Abb}(X,Z) \,:\, (f,g) \mapsto f \bullet g,$$
$$\circ \,:\, \mathrm{Abb}(Y,Z) \times \mathrm{Abb}(X,Y) \to \mathrm{Abb}(X,Z) \,:\, (g,f) \mapsto g \circ f.$$

Diese beiden Verknüpfungen sind entgegengesetzt: $f \bullet g = g \circ f$.
Je nach Kontext sind beide Schreibweisen bequem und nützlich.

Erinnerung (D2A): Zu je zwei Abbildungen $f : X \to Y$ und $g : Y \to Z$ ist die **Komposition** $h = f \bullet g = g \circ f$ die Abbildung $h : X \to Z$ durch Hintereinanderausführung $h(x) = g(f(x))$, also $f \bullet g$ als „f vor g“ und $g \circ f$ als „g nach f“. Demnach gilt $\bar{\circ} = \bullet$ und entsprechend $\bar{\bullet} = \circ$.

Beispiel: Komposition von Abbildungen

Die Komposition von Abbildungen ist assoziativ:
Für je drei komponierbare Abbildungen $f : A \to B$ und $g : B \to C$ und $h : C \to D$ gilt die Gleichheit der Kompositionen $h \circ (g \circ f) = (h \circ g) \circ f$.



Verknüpfungen: Umklammern und Umordnen

Zu $*: A \times A \to A$ definieren wir die n–fache Verknüpfung für $n \in \mathbb{N}_{\geq 1}$:

$$
\begin{aligned}
* &: A^1 \to A : (a_1) && \mapsto a_1 \\
* &: A^2 \to A : (a_1, a_2) && \mapsto a_1 * a_2 \\
* &: A^3 \to A : (a_1, a_2, a_3) && \mapsto (a_1 * a_2) * a_3 \\
* &: A^4 \to A : (a_1, a_2, a_3, a_4) && \mapsto ((a_1 * a_2) * a_3) * a_4 \\
&\dots \\
* &: A^n \to A : (a_1, a_2, \dots, a_n) && \mapsto \ast_{i=1}^{n} a_i = (\dots((a_1 * a_2) * a_3)\dots) * a_n
\end{aligned}
$$

Diese Abbildungen definieren wir rekursiv für alle $n \in \mathbb{N}_{\geq 1}$ durch

$$\ast_{i=1}^{1} a_i := a_1, \qquad \ast_{i=1}^{n+1} a_i := \left(\ast_{i=1}^{n} a_i\right) * a_{n+1}$$

Satz G1C: Umklammern und Umordnen

(1) Ist $*: A \times A \to A$ assoziativ, so ist das Produkt $a_1 * a_2 * \dots * a_n$ klammer-unabhängig: Jede Klammerung führt zum selben Ergebnis.

(2) Ist $*$ zudem kommutativ, so können wir Faktoren beliebig umordnen.

Verknüpfungen: Umklammern und Umordnen

⚠ Im Allgemeinen sind dabei Reihenfolge und Klammerung wichtig!
Hier sind Assoziativität und Kommutativität höchst willkommene Hilfen:
Diesen unscheinbaren Satz verwenden wir nahezu in jeder Rechnung!

⚠ Kommutativität allein genügt noch nicht zur Umordnung.
Wir benötigen zunächst Assoziativität als Voraussetzung,
um die Klammern beliebig setzen zu können.

Beispiel: (siehe C405) Wir suchen eine geschlossene Formel für

$$S(n) \;:=\; \textstyle\sum_{k=1}^{n} k \;=\; 1 + 2 + \dots + n.$$

Dank Assoziativität und Kommutativität erhalten wir

$$
\begin{aligned}
2S(n) &= (1 + 2 + \dots + n{-}1 + n) + (1 + 2 + \dots + n{-}1 + n) \\
&= (1 + 2 + \dots + n{-}1 + n) + (n + n{-}1 + \dots + 2 + 1) \\
&= (1 + n) + (2 + n{-}1) + \dots + (n{-}1 + 2) + (n + 1) \\
&= n(n + 1)
\end{aligned}
$$

Daraus folgt die ersehnte geschlossene Formel $S(n) = n(n+1)/2$.

Verknüpfungen: Umklammern und Umordnen

Beweis: (1) Ist $*$ assoziativ, so ist das Produkt $a_1 * a_2 * \dots * a_n$ klammer-unabhängig: Jede Klammerung führt zum selben Ergebnis.

Wir präzisieren dies wie folgt: Für alle $2 \leq k \leq n$ in $\mathbb{N}$ gilt

$$\boxed{\ast_{i=1}^{n} a_i = \left(\ast_{i=1}^{k-1} a_i\right) * \left(\ast_{i=k}^{n} a_i\right).}$$

Für $n = 3$ verdanken wir dies der Definition bzw. der Assoziativität:

$$\ast_{i=1}^{3} a_i \overset{\text{Def}}{=} (a_1 * a_2) * a_3 \overset{\text{Ass}}{=} a_1 * (a_2 * a_3)$$

Allgemein für $n \geq 3$ beweisen wir die Aussage per Induktion über n.
Für $k = n$ ist dies die Definition, und für alle k mit $2 \leq k < n$ gilt:

$$
\begin{aligned}
\ast_{i=1}^{n} a_i &\overset{\text{Def}}{=} \left(\ast_{i=1}^{n-1} a_i\right) * a_n \overset{\text{Ind}}{=} \left[\left(\ast_{i=1}^{k-1} a_i\right) * \left(\ast_{i=k}^{n-1} a_i\right)\right] * a_n \\
&\overset{\text{Ass}}{=} \left(\ast_{i=1}^{k-1} a_i\right) * \left[\left(\ast_{i=k}^{n-1} a_i\right) * a_n\right] \overset{\text{Def}}{=} \left(\ast_{i=1}^{k-1} a_i\right) * \left(\ast_{i=k}^{n} a_i\right)
\end{aligned}
$$

🙂 Per Induktion über n schließen wir: Für jedes Produkt der Länge n in $(A, *)$ ist das Ergebnis unabhängig von der Klammerung.

Verknüpfungen: Umklammern und Umordnen

(2) Ist $*: A \times A \to A$ assoziativ und kommutativ, so können wir Produkte beliebig umordnen: Für jede Umordnung $\{i_1, \dots, i_n\} = \{1, \dots, n\}$ gilt

$$\boxed{a_{i_1} * a_{i_2} * \dots * a_{i_n} = a_1 * a_2 * \dots * a_n.}$$

Für $n = 2$ ist dies die Definition der Kommutativität. Allgemein für $n \geq 2$ führen wir Induktion über n. Es gibt genau ein k mit $i_k = n$, also gilt:

$$
\begin{aligned}
a_{i_1} * a_{i_2} * \dots * a_{i_n} &\overset{(1)}{=} (a_{i_1} * \dots * a_{i_{k-1}}) * (a_{i_k} * a_{i_{k+1}} * \dots * a_{i_n}) \\
&\overset{(1)}{=} (a_{i_1} * \dots * a_{i_{k-1}}) * [a_{i_k} * (a_{i_{k+1}} * \dots * a_{i_n})] \\
&\overset{\text{Com}}{=} (a_{i_1} * \dots * a_{i_{k-1}}) * [(a_{i_{k+1}} * \dots * a_{i_n}) * a_n] \\
&\overset{\text{Ass}}{=} [(a_{i_1} * \dots * a_{i_{k-1}}) * (a_{i_{k+1}} * \dots * a_{i_n})] * a_n \\
&\overset{(1)}{=} (a_{i_1} * \dots * a_{i_{k-1}} * a_{i_{k+1}} * \dots * a_{i_n}) * a_n \\
&\overset{\text{Ind}}{=} (a_1 * \dots * a_{n-1}) * a_n \\
&\overset{\text{Def}}{=} a_1 * a_2 * \dots * a_n
\end{aligned}
$$

🙂 Damit ist auch die Invarianz unter Umordnung bewiesen. QED

Komplexoperation: elementweise Verknüpfung von Mengen

G121

Zur Verknüpfung von Mengen nutzen wir die bequeme Schreibweise

$$2\mathbb{N} \quad = 2\cdot\mathbb{N} \quad = \{\, 2\cdot n \mid n\in\mathbb{N}\,\} \quad = \{\, 0,2,4,6,8,\dots\,\},$$
$$2\mathbb{N}+1 = 2\cdot\mathbb{N}+1 = \{\, 2\cdot n+1 \mid n\in\mathbb{N}\,\} = \{\, 1,3,5,7,9,\dots\,\}.$$

Hier werden Mengen elementweise verknüpft. Ausführlich bedeutet das:

Definition G1D: Komplexoperation

Jede Verknüpfung setzen wir fort von Elementen auf Teilmengen:

$$\begin{aligned}
* &: A \times B \to C : (a,b) \mapsto a*b \\
* &: A \times \mathfrak{P}(B) \to \mathfrak{P}(C) : (a,T) \mapsto a*T := \{\, a*b \mid b\in T\,\} \\
* &: \mathfrak{P}(A)\times B \to \mathfrak{P}(C) : (S,b) \mapsto S*b := \{\, a*b \mid a\in S\,\} \\
* &: \mathfrak{P}(A)\times \mathfrak{P}(B) \to \mathfrak{P}(C) : (S,T) \mapsto S*T := \{\, a*b \mid a\in S,\ b\in T\,\} \\
&\qquad\qquad = \textstyle\bigcup_{a\in S} a*T \quad = \bigcup_{b\in T} S*b
\end{aligned}$$

Als Spezialfälle erhalten wir $\{a\}*T = a*T$ und $S*\{b\} = S*b$.

Beispiel: In dieser Schreibweise gilt $\mathbb{N}+\mathbb{N}=\mathbb{N}$ und $\mathbb{N}-\mathbb{N}=\mathbb{Z}$.

Komplexoperation: elementweise Verknüpfung von Mengen

G122 Erläuterung

Formal handelt es sich hier um vier verschiedene Verknüpfungen, denn die Definitionsmengen sind offensichtlich verschieden: Verknüpft werden einmal Elemente, andermal Teilmengen! Zur Betonung und besseren Unterscheidung nutzen manche Autoren zwei verschiedene Symbole:

$$\begin{aligned}
* &: A \times B \to C : (a,b) \mapsto a*b \\
\circledast &: \mathfrak{P}(A)\times\mathfrak{P}(B) \to \mathfrak{P}(C) : (S,T) \mapsto S\circledast T := \{\, a*b \mid a\in S,\ b\in T\,\}
\end{aligned}$$

Ich verzichte auf die Betonung und schreibe viermal dasselbe Symbol. aus dem Kontext geht jeweils eindeutig hervor, was genau gemeint ist. Das ist zwar etwas schludrig, aber ein gängiger Kompromiss zwischen Kürze und Klarheit, solange es zu keinen Missverständnissen führt.

Dieses **Überladen** mathematischer Operatoren ist üblich und bequem: Wir hätten gar nicht genug Symbole für all die unzähligen Operationen, schon die Grundrechenarten in $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ müssten verschieden heißen!

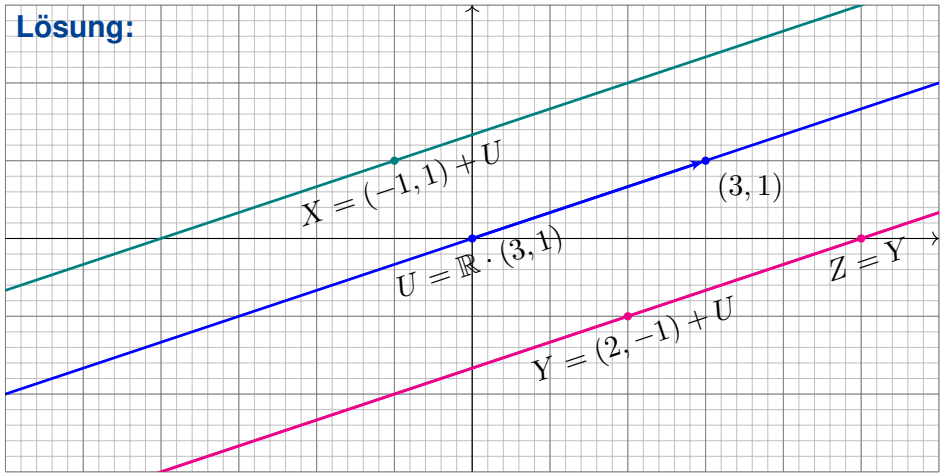
Programmiersprachen wie Python und C++ nutzen Überladen ebenfalls: Derselbe Operator erfüllt verschiedene Rollen, der Kontext bestimmt die Bedeutung: Diese wird syntaktisch am **Typ der Operanden** erkannt.

Komplexoperation: elementweise Verknüpfung von Mengen

G123

Aufgabe: Zeichnen Sie in der Ebene $\mathbb{R}^2$ die Mengen $U=\mathbb{R}\cdot(3,1)$ sowie $X=(-1,1)+U$ und $Y=(2,-1)+U$ und $Z=(5,0)+U$.

Lösung:



Komplexoperation: elementweise Verknüpfung von Mengen

G124 Erläuterung

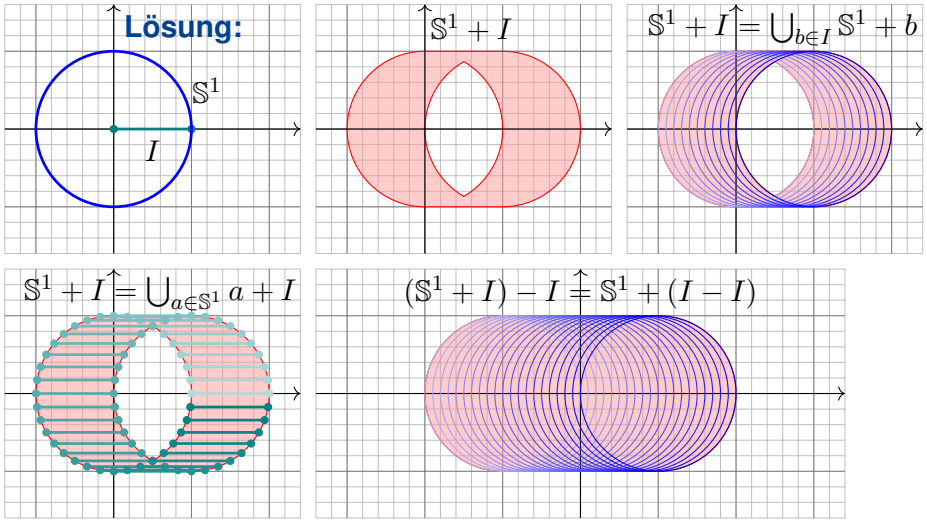
Hier ist $U=\mathbb{R}\cdot(3,1)=\{\, t\cdot(3,1) \mid t\in\mathbb{R}\,\}$ eine Ursprungsgerade und X,Y,X sind Verschiebungen. Man beachte $(2,-1)+U=(5,0)+U$.

Diese Notation und speziell die Anwendung auf Geraden, Ebenen, usw. ist typisch für die Lineare Algebra. Die folgenden Beispiele zeigen dazu analoge Konstruktionen, die nicht von Geraden handeln, sondern von anderen Mengen wie Intervallen, Kreisen, usw.

Komplexoperation: elementweise Verknüpfung von Mengen

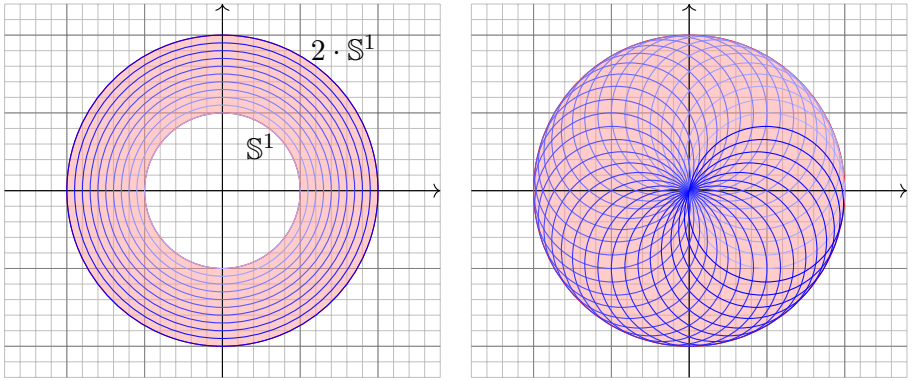
Aufgabe: Zeichnen Sie in der Ebene $\mathbb{R}^2$ die Mengen $I = [0,1] \times \{0\}$ und $\mathbb{S}^1 = \{\, (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \,\}$ sowie $\mathbb{S}^1 + I$ und $(\mathbb{S}^1 + I) - I$.

Lösung:



Komplexoperation: elementweise Verknüpfung von Mengen

Aufgabe: Zeichnen Sie $[1,2] \cdot \mathbb{S}^1$ und $\mathbb{S}^1 + \mathbb{S}^1$. **Lösung:**



⚠ Beachten Sie $2 \cdot \mathbb{S}^1 \neq \mathbb{S}^1 + \mathbb{S}^1$! Lesen Sie nochmals Definition G1D.

🙂 Mathematische Notation ist extrem knapp, präzise und elegant. In nur wenigen Zeichen können Sie damit viel zusammenfassen.

Komplexoperation: elementweise Verknüpfung von Mengen

Bemerkung G1E

(1) Ist $* : A \times A \to C$ kommutativ, so auch $* : \mathfrak{P}(A) \times \mathfrak{P}(A) \to \mathfrak{P}(C)$.

(2) Ist $* : A \times A \to A$ assoziativ, so auch $* : \mathfrak{P}(A) \times \mathfrak{P}(A) \to \mathfrak{P}(A)$.

Aufgabe: Schreiben Sie diese Rechnungen sorgfältig aus

Lösung: (1) Wir schreiben die Definition aus und vergleichen:

$$S * T = \{\, a * b \mid a \in S,\ b \in T \,\}$$
$$T * S = \{\, b * a \mid b \in T,\ a \in S \,\}$$

Ist $* : A \times A \to C$ kommutativ, so sind die rechten Mengen gleich.

(2) Wir schreiben die Definition aus und vergleichen:

$$\begin{aligned}(S * T) * U &= \{\, a * b \mid a \in S,\ b \in T \,\} * U \\ &= \{\, (a * b) * c \mid a \in S,\ b \in T,\ c \in U \,\} \\ S * (T * U) &= S * \{\, b * c \mid b \in T,\ c \in U \,\} \\ &= \{\, a * (b * c) \mid a \in S,\ b \in T,\ c \in U \,\}\end{aligned}$$

Ist $* : A \times A \to A$ assoziativ, so sind die rechten Mengen gleich.

Komplexoperation: elementweise Verknüpfung von Mengen

Anwendungen der Komplexoperation:

- Rechnen mit Restklassen in $\mathbb{Z}/n\mathbb{Z}$, allgemein Quotienten.
- Minkowski-Summe $A + B$ im $\mathbb{R}^n$ wie in obigen Beispielen.
- Fehlerrechnung und Intervallarithmetik

Beispiel: Sie wollen das Volumen eines Quaders schätzen. Sie kennen die Seitenlängen a, b, c nicht exakt, sondern können nur Intervalle angeben, etwa $A = [4.2, 4.4]$, $B = [5.9, 6.2]$, $C = [6.1, 6.2]$. Dann liegt das gesucht Volumen im Intervall $A \cdot B \cdot C = [151.158, 169.136]$.

🙂 Algebra rechnet exakt. „Aber in der Wirklichkeit ist nichts exakt. Das kann die Algebra nicht abbilden.“ Ja, in der Wirklichkeit ist kaum etwas exakt. Doch, wir können Ungenauigkeit algebraisch fassen!

Beispiel: In der Physik werden Messfehler bzw. Vertrauensintervalle in der Schreibweise $m \pm \Delta m$ angegeben. Das entspricht dem Intervall $[m - \Delta m, m + \Delta m]$. Die Verknüpfungen von fehlerbehafteten Werten geschieht dann wie oben gesehen.

Monoide und Gruppen: explizite Definition

Definition G1F: Monoid und Gruppe, explizite Formulierung

Ein **Magma** $(G, *)$ besteht aus einer Menge G mit innerer Verknüpfung

$$* : G \times G \to G : (a, b) \mapsto a * b.$$

Die Anzahl $\sharp G = |G|$ der Elemente heißt auch die **Ordnung** von G.

(G0) Eine **Halbgruppe** $(G, *)$ erfüllt zudem die Assoziativität:

$$\mathbf{Ass}(G, *) \quad :\Leftrightarrow \quad \forall a, b, c \in G : (a * b) * c = a * (b * c)$$

(G1) Ein **Monoid** $(G, *, e)$ besitzt zudem ein neutrales Element $e \in G$:

$$\mathbf{Ntr}(G, *, e) \quad :\Leftrightarrow \quad \forall a \in G : e * a = a = a * e$$

$$\mathbf{Mon}(G, *, e) \quad :\Leftrightarrow \quad \mathbf{Ass}(G, *) \wedge \mathbf{Ntr}(G, *, e)$$

(G2) Eine **Gruppe** $(G, *, e, \iota)$ besitzt zudem eine Inversion $\iota : G \to G$:

$$\mathbf{Inv}(G, *, e, \iota) \quad :\Leftrightarrow \quad \forall a \in G : a * \iota(a) = e = \iota(a) * a$$

$$\mathbf{Grp}(G, *, e, \iota) \quad :\Leftrightarrow \quad \mathbf{Ass}(G, *) \wedge \mathbf{Ntr}(G, *, e) \wedge \mathbf{Inv}(G, *, e, \iota)$$

(GA) Wir nennen $(G, *)$ **kommutativ** oder **abelsch**, falls gilt:

$$\mathbf{Com}(G, *) \quad :\Leftrightarrow \quad \forall a, b \in G : a * b = b * a$$

Monoide und Gruppen: explizite Definition

Wir betrachten hier eine grundlegende **algebraische Struktur** $(G, *)$ bestehend aus einer Menge G und einer Verknüpfung $* : G \times G \to G$.

Eigenschaften wie Assoziativität **Ass** und Kommutativität **Com** usw. sind **Aussageformen**: Für eine vorgelegte Struktur $(G, *)$ können die Aussagen $\mathbf{Ass}(G, *)$ und $\mathbf{Com}(G, *)$ wahr oder falsch sein.

🙂 Die obige Definition verlangt explizit alle vier Gruppendaten:

$$\mathbf{Grp}(G, *, e, \iota) \quad \Longleftrightarrow \quad \mathbf{Ass}(G, *) \wedge \mathbf{Ntr}(G, *, e) \wedge \mathbf{Inv}(G, *, e, \iota)$$

Die geforderten Eigenschaften sind dann Allaussagen. Das ist gut zu prüfen, alle Daten liegen vor, wir müssen nichts erfinden oder suchen.

Wir wandeln die explizite Definition G1F in eine implizite Definition G1I.

M Beide Sichtweisen sind bequem und nützlich, je nach Situation.

I Für die Programmierung benötige wir explizite Funktionen.

L *Beautiful is better than ugly. Explicit is better than implicit.*

Monoide und Gruppen: Schreibweisen

Die meisten der algebraischen Strukturen, die uns in der Linearen Algebra begegnen, sind assoziativ, viele davon zudem kommutativ. Nicht-assoziative kommen ebenfalls vor, ein besonders wichtiges Beispiel sind Lie–Algebren, doch insgesamt sind dies eher seltene Ausnahmen. Diese Einschätzung gründet teilweise auf mathematischer Notwendigkeit, vor allem aber auf Tradition und langer Erfahrung.

The commonly accepted attitudes toward the commutative law and the associative law are different. Many real life operations fail to commute; the mathematical community has learned to live with that fact and even to enjoy it. Violations of the associative law are usually considered by specialists only.
Paul Halmos, *Linear Algebra Problem Book* (1995)

Monoide und Gruppen: Schreibweisen

Neben der obigen Schreibweise $(G, *, e, \iota)$ sind weitere üblich:
Additive Schreibweise $(G, +, 0, -)$ mit „Plus“, „Null“, „Negation“.
Multiplikative Schreibweise $(G, \cdot, 1, ^{-1})$ mit „Mal“, „Eins“, „Inversion“.
Ebenso Verknüpfungen $*, \circ, \bullet, \ldots$, neutrale Elemente $e, \mathrm{id}, E, I, \ldots$

Eine gute Notation vermeidet Fehler und Missverständnisse. Das ist nicht nur eine mathematische Frage, sondern vor allem eine der Klarheit, der Bequemlichkeit und der jeweiligen Tradition. Die wahre Kraft der Begriffe steckt nicht in ihrer *Schreibung*, sondern in ihrer *Bedeutung*! Das können wir nun klar und präzise formulieren.

Beispiele mit 0, 1 und 2 Elementen

Ein Magma $(M, *)$ oder eine Halbgruppe kann leer sein:
Auf $M = \emptyset$ gilt es genau eine Verknüpfung $* : \emptyset \times \emptyset \to \emptyset$.
Dieses Beispiel ist zwar traurig, aber nicht ausgeschlossen.

Ein Monoid $(M, *, e)$ oder eine Gruppe hingegen ist niemals leer.
Wegen $e \in M$ enthält die Menge M mindestens ein Element.
Auf $M = \{e\}$ gilt es genau eine Verknüpfung $* : \{e\} \times \{e\} \to \{e\}$.
Damit ist $(M, *, e)$ ein Monoid, sogar eine Gruppe dank $\iota : e \mapsto e$.

Aufgabe: Wie viele Verknüpfungen $* : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ gibt es auf der Trägermenge $\mathbb{Z}_2 = \{0, 1\}$? Wie viele davon sind assoziativ? Wie viele Monoide $(G, *, e)$ gibt es? Wie viele Gruppen $(G, *, e, \iota)$?

Welche kennen Sie bereits aus anderem Kontext? als Junktoren?
Geben Sie diesen Verknüpfungen möglichst sprechende Namen.

Lösung: Die folgende Seite zeigt alle $2^{2\times 2} = 16$ Möglichkeiten.
Genau zwei davon sind Gruppen (grün), zwei weitere Monoide (gelb), und vier weitere immerhin noch assoziativ, also Halbgruppen (blau).
Die verbleibenden acht (grau) sind nicht assoziativ. Übung!

Beispiele mit 0, 1 und 2 Elementen

c_0	0	1
0	0	0
1	0	0

$\overline{\vee}$	0	1
0	1	0
1	0	0

$<$	0	1
0	0	1
1	0	0

$\overline{\mathrm{pr}_1}$	0	1
0	1	1
1	0	0

$>$	0	1
0	0	0
1	1	0

$\overline{\mathrm{pr}_2}$	0	1
0	1	0
1	1	0

$\dot{\vee}$	0	1
0	0	1
1	1	0

$\overline{\wedge}$	0	1
0	1	1
1	1	0

$\wedge$	0	1
0	0	0
1	0	1

$=$	0	1
0	1	0
1	0	1

pr_2	0	1
0	0	1
1	0	1

$\leq$	0	1
0	1	1
1	0	1

pr_1	0	1
0	0	0
1	1	1

$\geq$	0	1
0	1	0
1	1	1

$\vee$	0	1
0	0	1
1	1	1

c_1	0	1
0	1	1
1	1	1

Beispiele mit 0, 1 und 2 Elementen

Die Mathematik lebt vom Wechselspiel zwischen konkret und abstrakt!
Ein möglichst vielfältiger Beispielfundus ist wichtig zur Konkretisierung, um eindrücklich zu illustrieren und gegen naiven Irrglauben zu impfen.

Ich möchte Sie nachdrücklich zu guten Angewohnheiten ermutigen.
Dazu gehört, auch einfache Fragen zu stellen und zu beantworten.

Bei jeder neuen Definition sollten Sie sich routinemäßig fragen:
Wie sehen mögliche Beispiele und Gegenbeispiele aus?
Wie hängen die Eigenschaften untereinander zusammen?
Impliziert eine die andere? Oder sind sie unabhängig?

Aufgabe: Gibt es Verknüpfungen, die kommutativ sind, aber nicht assoziativ? Wie sehen (kleinste) Beispiele aus?

Lösung: Schon mit unserem kleinen Beispielfundus ist dies leicht zu beantworten: Die kleinsten Beispiele gibt es bereits mit zwei Elementen, und hier finden wir genau zwei: $\overline{\vee}$ und $\overline{\wedge}$.

Assoziativität und Kommutativität

🙂 In jeder Verknüpfungstabelle $* : M \times M \to M$ ist die Kommutativität leicht zu sehen als Spiegelsymmetrie entlang der Hauptdiagonalen.

☹ Die Assoziativität hingegen ist nicht offensichtlich, selbst in kleinen Beispielen wie diesen, und muss sorgsam nachgerechnet werden.

Führen Sie dies zur Übung an obigen Beispielen aus!

Neutrale Elemente: Eindeutigkeit

Beispiele: Gruppen: $(\mathbb{Z},+,0,-)$, $(\mathbb{Q}^*,\cdot,1,^{-1})$, $(\mathrm{GL}_n\,\mathbb{R},\cdot,1_{n\times n},^{-1})$, $(\mathrm{S}_n,\circ,\mathrm{id},^{-1})$, ... Monoide: $(\mathbb{N},+,0)$, $(\mathbb{Z},\cdot,1)$, $(\mathbb{R}^{n\times n},\cdot,1_{n\times n})$, $(\mathrm{E}_n,\circ,\mathrm{id})$, ... Halbgruppen: $(\mathbb{N}_{\geq 1},+)$, $(2\mathbb{Z},\cdot)$, ... Magmen: $(\mathbb{Z},-)$, $(\mathfrak{P}(N),\setminus)$, ...

Lemma G1G: Links-/Rechts-/Neutrale und Eindeutigkeit

Sei $(M,*)$ ein Magma. Ein Element $e\in M$ heißt

- **linksneutral**, falls $e*a=a$ für alle $a\in M$ gilt,
- **rechtsneutral**, falls $a*e=a$ für alle $a\in M$ gilt,
- **(beidseitig) neutral**, falls beides gilt.

Ist $e\in G$ linksneutral und $e'\in G$ rechtsneutral, so folgt ihre Gleichheit:

$$e \overset{\text{rNtr}}{=} e*e' \overset{\text{lNtr}}{=} e'$$

In jedem Magma $(M,*)$ existiert höchstens ein neutrales Element!

Beispiele: In $(\mathbb{N},+)$ ist 0 neutral. In $(\mathbb{N}_{\geq 1},+)$ ist kein Element neutral. In $(\mathbb{Z},-)$ ist das Nullelement 0 rechtsneutral, aber nicht linksneutral

Neutrale Elemente: Eindeutigkeit

☺ Gibt es Linksneutrale *und* Rechtsneutrale, so folgt Gleichheit.
Das die Aussage von Lemma G1G, einfach aber bemerkenswert.

⚠ Ohne Linksneutrales kann es mehrere Rechtsneutrale geben, und ohne Rechtsneutrales kann es mehrere Linksneutrale geben.

Beispiel: Wir betrachten nochmal die Verknüpfungen auf $\mathbb{Z}_2=\{0,1\}$, insbesondere die vier assoziativen, die kein neutrales Element haben:

c_0	0	1
0	0	0
1	0	0

c_1	0	1
0	1	1
1	1	1

pr_1	0	1
0	0	0
1	1	1

pr_2	0	1
0	0	1
1	0	1

Hier haben c_0 und c_1 weder Linksneutrales noch Rechtsneutrales, hingegen hat pr_1 zwei Rechtsneutrale, aber kein Linksneutrales, ebenso hat pr_2 zwei Linksneutrale, aber kein Rechtsneutrales.

☺ Diese Beispiele sind einfach doch konkret und hoffentlich hilfreich; Sie bezeugen, dass es in Lemma G1G wirklich etwas zu beweisen gibt! Diese Fragen und Bemerkungen illustrieren, wie wir umsichtig vorgehen und grundlegende Aussagen klären: durch Beweis oder Gegenbeispiel!

Inverse Elemente: Eindeutigkeit

Lemma G1H: Links-/Rechts-/Inverse und Eindeutigkeit

Sei $(M,*,e)$ ein Monoid und $a,b,c\in M$.

Wir nennen b **linksinvers** zu a, falls $b*a=e$ gilt.
Wir nennen c **rechtsinvers** zu a, falls $a*c=e$ gilt.

Ist b linksinvers zu a und c rechtsinvers zu a, so folgt $b=c$, denn

$$b \overset{\text{rNtr}}{=} b*e \overset{\text{rInv}}{=} b*(a*c) \overset{\text{Ass}}{=} (b*a)*c \overset{\text{lInv}}{=} e*c \overset{\text{lNtr}}{=} c.$$

Wir nennen b **invers** zu a, falls sowohl $b*a=e$ als auch $a*b=e$ gilt.
Damit ist b eindeutig durch a bestimmt, und wir schreiben $a^{-1}:=b$.

Die Menge aller invertierbaren Elemente in $(M,*,e)$ bezeichnen wir mit

$$M^\times=(M,*)^\times=(M,*,e)^\times:=\{\,a\in M\mid \exists b\in M: a*b=e=b*a\,\}.$$

Eindeutigkeit des Inversen zu a gilt immer, in jedem Monoid $(M,*,e)$;
Existenz muss gesondert gefordert werden: Das ist Axiom (G2).

Inverse Elemente: Eindeutigkeit

☺ Gibt es Linksinverse *und* Rechtsinverse, so folgt Gleichheit.
Das die Aussage von Lemma G1H und durchaus bemerkenswert.

⚠ Ohne Linksinverses kann es mehrere Rechtsinverse geben, und ohne Rechtsinverses kann es mehrere Linksinverse geben.

Beispiel: Wir betrachten das Monoid $(M,\circ,\mathrm{id})$ aller Abbildungen $M=\{\,f:\mathbb{N}\to\mathbb{N}\,\}$ mit Komposition $\circ$ und neutralem Element $\mathrm{id}=\mathrm{id}_{\mathbb{N}}$.

Die Abbildung $a:\mathbb{N}\to\mathbb{N}:n\mapsto n+1$ ist injektiv und hat unendlich viele Linksinverse b_k für $k\in\mathbb{N}$, nämlich $b_k(0)=k$ und $b(n)=n-1$ für $n\geq 1$.

Jede Abbildung b_k ist surjektiv und hat zwei Rechtsinverse, nämlich neben a noch a_k mit $a_k(k)=0$ und $a_k(n)=n+1$ für alle $n\neq k$.

Tatsächlich gilt $b_k\circ a=b_k\circ a_k=\mathrm{id}_{\mathbb{N}}$, wie Sie sofort nachprüfen.

☺ Diese Beispiele sind einfach doch konkret und hoffentlich hilfreich; Sie bezeugen, dass es in Lemma G1H wirklich etwas zu beweisen gibt! Diese Fragen und Bemerkungen illustrieren, wie wir umsichtig vorgehen und grundlegende Aussagen klären: durch Beweis oder Gegenbeispiel!

Monoide und Gruppen: implizite Definition

Definition G1ı: Monoid und Gruppe, implizite Formulierung

Ein **Magma** $(G, *)$ ist eine Menge G mit Verknüpfung $*: G \times G \to G$.

(G0) Eine **Halbgruppe** $(G, *)$ erfüllt zudem die Assoziativität:

$$\mathbf{Ass}(G,*) \quad :\Leftrightarrow \quad \forall a,b,c \in G : (a*b)*c = a*(b*c)$$

(G1) Ein **Monoid** $(G, *)$ besitzt zudem ein neutrales Element:

$$\mathbf{Mon}(G,*) \quad :\Leftrightarrow \quad \exists e \in G : \mathbf{Mon}(G,*,e)$$

$$\Leftrightarrow \begin{cases} \forall a,b,c \in G : (a*b)*c = a*(b*c) \\ \exists e \in G \ \forall a \in G : e*a = a = a*e \end{cases}$$

(G2) Eine **Gruppe** $(G, *, e)$ bzw. $(G, *)$ besitzt zudem eine Inversion:

$$\mathbf{Grp}(G,*,e) \quad :\Leftrightarrow \quad \exists(\iota: G \to G) : \mathbf{Grp}(G,*,e,\iota)$$

$$\mathbf{Grp}(G,*) \quad :\Leftrightarrow \quad \exists e \in G \ \exists(\iota: G \to G) : \mathbf{Grp}(G,*,e,\iota)$$

$$\Leftrightarrow \begin{cases} \forall a,b,c \in G : (a*b)*c = a*(b*c) \\ \exists e \in G \ \forall a \in G : \big[\, e*a = a = a*e \\ \qquad \wedge \exists b \in G : \quad a*b = e = b*a \,\big] \end{cases}$$

Monoide und Gruppen: implizite Definition

Formal korrekt besteht jede Gruppe $\underline{G} = (G, *, e, \iota)$ aus vier Daten: eine Trägermenge G und hierauf eine Verknüpfung $*: G \times G \to G$, hierzu ein neutrales Element $e \in G$ und eine Inversion $\iota: G \to G$.

🙂 Die längliche Notation gelingt auch kürzer und bequemer:
Aus den drei Gruppendaten $(G, *, e)$ lässt sich ι rekonstruieren.
Aus den zwei Gruppendaten $(G, *)$ lassen sich e und ι rekonstruieren.

Die fehlenden Daten werden dabei nicht mehr explizit mitgeliefert, sondern implizit nur ihre Existenz gefordert. (Eindeutigkeit gilt ohnehin.)

Alle drei Schreibweisen haben ihren Nutzen und ihre Berechtigung. Selbst wenn ich mich auf eine festlegen wollte, in der Literatur werden Ihnen auch die anderen begegnen. Ich stelle Ihnen daher alle drei vor und nutze die für die jeweilige Situation am besten geeignete Variante.

⚠ Allein aus der Menge G hingegen lässt sich $*$ nicht rekonstruieren!
Die zugrundeliegende Menge G nennen wir auch **Trägermenge**.
Die Verknüpfung $*: G \times G \to G$ ist eine **zusätzliche Struktur**!

Monoide und Gruppen: explizite vs implizite Definition

explizit $(G, *, e, \iota)$:	implizit $(G, *, e)$ bzw. $(G, *)$:
$(\mathbb{Z}, +, 0, -)$, $(\mathbb{Q}^*, \cdot, 1, ^{-1})$, $(\mathrm{GL}_n\,\mathbb{R}, \cdot, 1_{n\times n}, ^{-1})$, $(\mathrm{S}_n, \circ, \mathrm{id}, ^{-1})$	$(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathrm{GL}_n\,\mathbb{R}, \cdot)$, $(\mathrm{S}_n, \circ)$
🙂 Alle vier Gruppendaten werden explizit genannt. ☹ Die Notation ist leider etwas länglich.	☹ Manche Gruppendaten müssen implizit ergänzt werden. 🙂 Die Notation ist kurz und bequem.
🙂 Die explizite Definition nutzt nur Allquantoren. 🙂 Sie ist meist leicht und routiniert nachzuprüfen.	☹ Die implizite Definition mischt All- und Existenzquantoren. ☹ Die Mischung verkompliziert manche Nachweise.

Pars pro toto: Oft sagt man „die Gruppe G“, meint aber $\underline{G} = (G, *, e, \iota)$.

⚠ Allein die Menge G genügt i.A. nicht zur Definition der Gruppe $\underline{G}$!
Sender und Empfänger treffen also eine wohlwollende Übereinkunft:
Alle fehlenden Daten müssen aus dem Kontext erschlossen werden.

Monoide und Gruppen: implizite Definition

Aufgabe: Manche Autoren formulieren die Gruppenaxiome wie folgt:

$$\mathbf{Grp}(G,*) \quad :\Longleftrightarrow \quad \begin{cases} (0)\ \forall a,b,c \in G : (a*b)*c = a*(b*c) \\ (1)\ \exists e \in G \ \forall a \in G : e*a = a*e = a \\ (2)\ \forall a \in G \ \exists b \in G : a*b = b*a = e \end{cases}$$

Ist das „sinngemäß irgendwie richtig“? Wo sehen Sie Probleme?
Vergleichen Sie dies mit der obigen Formulierung in Definition G1ı.

Lösung: Die Bedingungen (0) und (1) sind unkritisch. Zur Formulierung von (2) benötigen wir ein zusätzliches Element $e \in G$. Dessen Existenz wurde zwar in (1) gefordert, aber es könnte mehrere geben, dann würde die Richtigkeit der Aussage (2) von einer willkürlichen Wahl abhängen.

In der hier gezeigten Formulierung muss man daher nach (1) zunächst die Eindeutigkeit klären. Dieser logisch nötige Einschub wird oft ausgelassen oder nachgereicht. Beides ist nicht ideal.

Linksgruppen und Rechtsgruppen sind Gruppen.

☺ Die linke oder rechte Hälfte der Gruppenaxiome genügt bereits:

Satz G1J: Linksgruppen und Rechtsgruppen sind Gruppen.

Eine **Linksgruppe** $(G, *, e, ')$ erfüllt:

(G0) Die Verknüpfung $*: G \times G \to G$ ist assoziativ:

$$\forall a, b, c \in G \,:\, (a * b) * c = a * (b * c)$$

(G1L) Das Element $e \in G$ ist linksneutral:

$$\forall a \in G \,:\, e * a = a$$

(G2L) Zu jedem Element $a \in G$ ist das Element $a' \in G$ linksinvers:

$$\forall a \in G \,:\, a' * a = e$$

Erfreulicherweise ist jede Linksgruppe $(G, *, e, ')$ bereits eine Gruppe:
Das Element a' ist rechtsinvers zu a, und e ist rechtsneutral.

Alles gilt sinngemäß genauso für jede **Rechtsgruppe** dank G1B.

Linksgruppen und Rechtsgruppen sind Gruppen.

MathematikerInnen pflegen **Denkökonomie**, soweit dies möglich ist:
Definitionen sollten keine unnötigen / redundanten Axiome fordern.
Sätze sollten keine unnötigen Voraussetzungen verlangen.

☹ Für den Beweiser / Hersteller ist der Satz dann im Allgemeinen schwieriger zu beweisen. Bestenfalls genügt kritische Durchsicht: Guter Stil verlangt, nicht verwendete Voraussetzungen zu löschen.

☺ Schwächere Voraussetzungen bedeuten einen stärkeren Satz!
Für den Anwender / Abnehmer ist der stärkere Satz allgemeiner und leichter anzuwenden, da weniger Voraussetzungen zu prüfen sind.

Unsere Definition G1I des Gruppenbegriffs ist noch etwas redundant:
Die geforderten Axiome können weiter gekürzt werden (auf 3 von 5).

☺ Der obige Satz G1J ist der erste und letzte Satz über Linksgruppen:
Wir führen diesen Begriff hier nur lokal als praktische Bezeichnung ein.
Der Satz garantiert, dass es keinen Unterschied gibt zwischen Gruppen und Linksgruppen und Rechtsgruppen. Das ist nützlich zu wissen.
Wir sprechen daher im Folgenden nur von Gruppen.

Linksgruppen und Rechtsgruppen sind Gruppen.

Beweis: Vorgelegt sei $a \in G$. Dank (G2L) gilt

$$a' * a = e \quad \text{und} \quad a'' * a' = e.$$

(G2R) Wir zeigen, dass a' rechtsinvers zu a ist:

$$a * a' \overset{(G1L)}{=} e * (a * a') \overset{(G2L)}{=} (a'' * a') * (a * a') \overset{(G0)}{=} a'' * (a' * (a * a'))$$

$$\overset{(G0)}{=} a'' * ((a' * a) * a') \overset{(G2L)}{=} a'' * (e * a') \overset{(G1L)}{=} a'' * a' \overset{(G2L)}{=} e$$

(G1R) Wir zeigen, dass e rechtsneutral zu a ist:

$$a * e \overset{(G2L)}{=} a * (a' * a) \overset{(G0)}{=} (a * a') * a \overset{(G2R)}{=} e * a \overset{(G1L)}{=} a$$

Somit ist $(G, *, e, ')$ eine Gruppe, wie behauptet. QED

☺ Der Beweis ist raffiniert, dabei sehr kurz und vollkommen elementar.

Als leichte Übung können Sie jeden Rechenschritt sorgsam nachprüfen:
Allein aus (G0) sowie (G1L) und (G2L) folgern wir (G2R) und (G1R).
Somit erfüllt $(G, *, e, ')$ die Definition G1I einer Gruppe. Das war's.

Linksgruppen und Rechtsgruppen sind Gruppen.

☺ Einen solchen Beweis selbst auszutüfteln ist anfangs schwierig, aber durchaus möglich: Machen Sie mit Stift und Papier ein paar Versuche!
Nur so gewinnen Sie eigene Erfahrung, können die Schwierigkeiten des Beweisens erahnen und lernen gut formulierte Beweise zu schätzen!

Das illustriert verschiedene Stufen mathematischen Könnens:

1. Sätze genau lesen, richtig verstehen und korrekt anwenden.
2. Beweise kritisch lesen, alle Argumente verstehen und prüfen.
3. Beweise zu gegebenen Aussagen selbst finden und ausführen.
4. Sätze und Beweise eigenständig formulieren und erarbeiten.

Übung zur Illustration: Beweisen Sie die folgende Äquivalenz.

Korollar G1K: ein Linksinverses zum Linksinversen

Sei $(M, *, e)$ ein Monoid. Angenommen, zum Element $a \in M$ existiert ein Linksinverses $a' \in M$, also $a' * a = e$. Dann sind äquivalent:

(1) Das Linksinverse a' zu a ist auch rechtsinvers, also $a * a' = e$.
(2) Auch zu a' existiert ein Linksinverses $a'' \in M$, also $a'' * a' = e$.

In diesem Falle ist a' eindeutig durch a bestimmt und $a'' = a$.

Lösung von Gleichungen in Gruppen

In $(\mathbb{R}, +, 0, -)$ lösen Sie Gleichungen wie in der Schule gelernt.

$$x + 5 = 3 \xrightarrow{\text{addiere } -5} x = 3 + (-5)$$

In jeder Gruppe $(G, *, e, ')$ können Sie Gleichungen ebenso lösen!

$$x * a = b \xrightarrow{\text{multipliziere } a' \text{ von rechts}} x = b * a'$$
$$a * y = b \xrightarrow{\text{multipliziere } a' \text{ von links}} y = a' * b$$

Satz G1L: Lösung von Gleichungen in Gruppen

Gegeben sei eine nicht-leere Halbgruppe $(G, *)$, also eine Menge $G \neq \emptyset$ mit assoziativer Verknüpfung $* : G \times G \to G$. Dann sind äquivalent:

(1) **Neutrales und Inverse:** Es existiert ein neutrales Element $e \in G$ und eine Inversion $' : G \to G$, die $(G, *, e, ')$ zu einer Gruppe machen.

(2) **Lösbarkeit von Gleichungen:** Zu je zwei Elementen $a, b \in G$ existieren Lösungen $x, y \in G$ der Gleichungen $x * a = b$ und $a * y = b$.

Zusatz: Die Lösungen x, y sind dann eindeutig durch a, b bestimmt und dank Inversion explizit gegeben durch $x = b * a'$ und $y = a' * b$.

Lösung von Gleichungen in Gruppen

☺ Die Implikation „(1) ⇒ (2)“ betrifft das Lösen von Gleichungen: Dies werden Sie häufig für Rechnungen in Gruppen nutzen können. Sie ist sehr leicht zu beweisen, versuchen Sie es zunächst selbst!

Die Implikation „(2) ⇒ (1)“ zeigt umgekehrt, dass die Lösbarkeit von Gleichungen die Gruppenaxiome impliziert. Das ist bemerkenswert! Wir müssen dazu lediglich $G \neq \emptyset$ und Assoziativität voraussetzen.

Assoziativität wollen wir aus diversen Gründen immer voraussetzen. Die hier sorgsam ausformulierte Äquivalenz „(1) ⇔ (2)“ besagt also:

☺ Allgemeine Gleichungen der Form $a * x = b$ und $y * a = b$ können wir in Gruppen lösen – und nur in Gruppen!

Hier sehen wir eine weitere, hilfreiche Charakterisierung von Gruppen. Für das Lösen von Gleichungen benötigen wir genau diese Struktur!

☺ Bereits diese ersten einfachen Rechnungen und Ergebnisse deuten an, dass Gruppen eine grundlegende Struktur der Mathematik sind.

Lösung von Gleichungen in Gruppen

Beweis: „(1) ⇒ (2)“: $x = b * a'$ und $y = a' * b$ lösen die Gleichungen:

$$x * a = (b * a') * a \overset{(G0)}{=} b * (a' * a) \overset{(G2)}{=} b * e \overset{(G1)}{=} b$$
$$a * y = a * (a' * b) \overset{(G0)}{=} (a * a') * b \overset{(G2)}{=} e * b \overset{(G1)}{=} b$$

Umgekehrt: Aus $x * a = b$ bzw. $a * y = b$ folgt:

$$x \overset{(G1)}{=} x * e \overset{(G2)}{=} x * (a * a') \overset{(G0)}{=} (x * a) * a' \overset{!}{=} b * a'$$
$$y \overset{(G1)}{=} e * y \overset{(G2)}{=} (a' * a) * y \overset{(G0)}{=} a' * (a * y) \overset{!}{=} a' * b$$

„(2) ⇒ (1)“: Wir zeigen die Eigenschaften (G1L) und (G2L).

(G1L) Wir wählen $a \in G$. Hierzu existiert ein Element $e \in G$ mit $e * a = a$. Zu jedem Element $b \in G$ existiert ein $y \in G$ mit $a * y = b$. Daraus folgt:

$$e * b = e * (a * y) \overset{(G0)}{=} (e * a) * y \overset{(G1)}{=} a * y = b$$

Also ist e linksneutral. (G2L) Zu $a \in G$ existiert $a' \in G$ mit $a' * a = e$. Somit ist $(G, *, e, ')$ eine Linksgruppe, dank G1J also eine Gruppe. QED

Lösung von Gleichungen in Gruppen

☺ Auch dieser Beweis ist recht raffiniert, dabei kurz und elementar. Ich führe dies exemplarisch aus, damit Sie an diesem Vorbild lernen.

Zur besseren Übersicht haben wir die Argumente geschickt aufgebaut: Zunächst beweisen wir, dass Linksgruppen stets Gruppen sind (G1J).

Dies nutzen wir dankend im obigen Beweis von Satz G1L, da wir nun nur noch die Hälfte der Gruppenaxiome prüfen müssen. Ich betone:

MathematikerInnen pflegen Denkökonomie, soweit dies möglich ist: Definitionen sollten keine unnötigen / redundanten Axiome fordern.

☺ Hier sehen Sie recht eindrücklich die beiden Seiten der Medaille. Für den Beweiser / Hersteller ist der stärkere Satz meist schwieriger zu beweisen. Für den Anwender / Abnehmer jedoch ist der stärkere Satz leichter anzuwenden. Oft stehen Sie (abwechselnd) auf beiden Seiten.

Als Anwender mathematischer Ergebnisse schätzen Sie die Garantie.
Als Hersteller mathematischer Ergebnisse spüren Sie die Pflicht.
Wie bereits in Kapitel C zur Induktion gilt das Grundprinzip:
Ihre Vorbereitung von heute ist Ihr Nutzen von morgen!

Sudoku als Verknüpfungstabelle

2	5			3		9		1
	1				4			
4		7				2		8
		5	2					
				9	8	1		
	4				3			
			3	6			7	2
	7							3
9		3				6		4

Lösung →

2	5	8	7	3	6	9	4	1
6	1	9	8	2	4	3	5	7
4	3	7	9	1	5	2	6	8
3	9	5	2	7	1	4	8	6
7	6	2	4	9	8	1	3	5
8	4	1	6	5	3	7	2	9
1	8	4	3	6	9	5	7	2
5	7	6	1	4	2	8	9	3
9	2	3	5	8	7	6	1	4

	2			3		9		7
	1							
4		7				2		8
		5	2				9	
			1	8		7		
	4				3			
				6			7	1
	7							
9		3		2		6		5

Lösung →

6	2	8	5	3	4	9	1	7
5	1	9	8	7	2	4	3	6
4	3	7	9	1	6	2	5	8
8	6	5	2	4	7	1	9	3
3	9	2	1	8	5	7	6	4
7	4	1	6	9	3	5	8	2
2	5	4	3	6	9	8	7	1
1	7	6	4	5	8	3	2	9
9	8	3	7	2	1	6	4	5

Aufgabe: Ist jede Gleichung $a * x = b$ und $y * a = b$ eindeutig lösbar? Gibt es kommutative Sudokus? und assoziative Sudokus? Satz G1L!

Sudoku als Verknüpfungstabelle

Lösung: Die Sudoku-Regeln verlangen, dass in jeder vollständig gelösten Tabelle jede der Zahlen $1, \ldots, 9$ genau einmal vorkommt

1. in jeder der neun Zeilen und
2. in jeder der neun Spalten sowie
3. in jedem der neun Teilquadrate.

Wir betrachten die Menge $G = \{1, \ldots, 9\}$ mit Tabelle $* : G \times G \to G$.
Bedingung (1) bedeutet: Für alle $a, b \in G$ ist $a * x = b$ eindeutig lösbar.
Bedingung (2) bedeutet: Für alle $a, b \in G$ ist $y * a = b$ eindeutig lösbar.

(a) Kommutativität verletzt Bedingung (3) und ist daher ausgeschlossen.

(b) Aus den Bedingungen (1) und (2) und Assoziativität folgt dank G1L, dass $(G, *)$ eine Gruppe ist. Insbesondere existiert dann ein neutrales Element $e \in G$. Ist $e = 1$, so haben wir $1 * 2 = 2 * 1$, was (3) widerspricht.

Allgemein sei $g \in G$ ein Nachbar von e in der selben Dreiergruppe.
Dann gilt $e * g = g * e$, also ist Bedingung (3) auch hier verletzt.
Wir schließen: Es gibt keine assoziativen Sudokus!

Quasigruppen und Sudoku

Eine **Quasigruppe** $(G, *)$ ist eine Menge G mit einer Verknüpfung $* : G \times G \to G$ und folgender Lösbarkeitseigenschaft:

Zu je zwei Elementen $a, b \in G$ existieren eindeutige Lösungen $x, y \in G$ der Gleichungen $x * a = b$ und $a * y = b$.

Zusammen mit Assoziativität erhalten wir eine Gruppe, siehe G1L: Jede assoziative Quasigruppe ist eine Gruppe.

Die obigen Sudokus zeigen weitere Beispiele von Quasigruppen. Zu einer Gruppe fehlt allein die Assoziativität.

Gruppen und Assoku

Viele Menschen weltweit lieben Sudokus und betreiben leidenschaftlich quasi Gruppentheorie als Hobby, als Zeitvertreib oder als Gehirnjogging. Ein besonderer Reiz an Quasigruppen ist, dass es davon sehr viele gibt und daher der Rätselspaß anscheinend niemals langweilig wird.

Gruppen sind besonders stark strukturiert und daher für dieses Rätsel zu einfach. Es gibt bis auf Isomorphie (also Umordnung der Elemente) genau zwei Gruppen mit neun Elementen, nämlich $\mathbb{Z}/9$ und $\mathbb{Z}/3 \times \mathbb{Z}/3$. Mit diesem Wissen ist jedes Gruppen-Sudoko viel leichter zu lösen.

Dennoch wäre dies eine bemerkenswerte Variante. Probieren Sie es! Ich schlage hierzu den Namen „Assoku“ vor: assoziatives Sudoku, die Regel der neun Teilquadrate wird durch Assoziativität ersetzt. Das Spielvergnügen kann man nur experimentell ermitteln.

Linkststranslationen

Sei $(G, *)$ ein Magma, also eine Menge G mit $*: G \times G \to G$.
Zu jedem Element $a \in G$ betrachten wir seine Linkstranslation

$$\lambda_a \,:\, G \to G \,:\, x \mapsto a * x.$$

Dies klärt die Lösungen von Gleichungen der Form $a * x = b$:

- Ist λ_a surjektiv, so nennen wir a **linkslösbar**:
  Zu jedem $b \in G$ existiert $x \in G$ mit $a * x = b$.
- Ist λ_a injektiv, so nennen wir a **linkskürzbar**:
  Für alle $x, y \in G$ gilt: Aus $a * x = a * y$ folgt $x = y$.
- Ist λ_a bijektiv, so nennen wir a **linksdividierbar**.
  Wir definieren die Linksdivision durch $a \backslash b = \lambda_a^{-1}(b)$.

Rechtstranslationen

Entsprechend für die Rechtstranslation

$$\rho_a \,:\, G \to G \,:\, x \mapsto x * a.$$

Dies klärt die Lösungen von Gleichungen der Form $x * a = b$:

- Ist ρ_a surjektiv, so nennen wir a **rechtslösbar**:
  Zu jedem $b \in G$ existiert $x \in G$ mit $x * a = b$.
- Ist ρ_a injektiv, so nennen wir a **rechtskürzbar**:
  Für alle $x, y \in G$ gilt: Aus $x * a = y * a$ folgt $x = y$.
- Ist ρ_a bijektiv, so nennen wir a **rechtsdividierbar**.
  Wir definieren die Rechtsdivision durch $b / a = \rho_a^{-1}(b)$.

Links- und Rechtstranslationen

Beispiel: Ist $(G, *, e, ^{-1})$ eine Gruppe, so ist jedes Element $a \in G$ sowohl linksdividierbar dank $a \backslash b = a^{-1} * b$ als auch rechtsdividierbar dank $b / a = b * a^{-1}$. Genau dies nutzen wir zur Lösung von Gleichungen!

Beispiel: Satz G1L besagt: Ist $(G, *)$ assoziativ und jedes Element $a \in G$ sowohl links- als auch rechtslösbar, so ist $(G, *)$ eine Gruppe.

Beispiel: In einer Quasigruppe $(Q, *)$ ist jedes Element linksdividierbar und rechtsdividierbar. Die obigen Sudokus illustrieren dies durch Beispiele ohne neutrales Element und ohne Assoziativität.

Lösbar und kürzbar impliziert invertierbar.

Aufgabe: Sei $(M, *, 1)$ ein Monoid und $a \in M$ ein Element.

(1) Ist a linkslösbar und linkskürzbar, so ist a invertierbar.

(2) Ist a rechtslösbar und rechtskürzbar, so ist a invertierbar.

Lösung: (1) Nach Voraussetzung ist $\lambda_a : M \to M : x \mapsto ax$ surjektiv.
Also existiert $b \in M$ mit $ab = 1$, das heißt, a ist rechtsinvertierbar.

Zudem ist $\lambda_a : M \to M : x \mapsto ax$ injektiv, also a linkskürzbar.
Wir haben $a1 = a = 1a = (ab)a = a(ba)$, nach Kürzen also $1 = ba$.

Demnach ist das Element a invertierbar durch b, denn $ab = 1 = ba$.

(2) Diese Aussage beweist man wörtlich genauso wie (1) durch Vertauschen von links und rechts, also Übergang zu $(M, *^{\mathrm{op}}, 1)$.

Unterstrukturen durch Einschränkung

Sei $(G, *)$ ein Magma, also eine Menge mit Verknüpfung $*: G \times G \to G$.
Für jede Teilmenge $U \subseteq G$ können wir die Verknüpfung einschränken zu

$$*|_{U\times G} : U \times G \to G : (u, a) \mapsto u * a \quad \text{Linksoperation von } U \text{ auf } G,$$
$$*|_{G\times U} : G \times U \to G : (a, u) \mapsto a * u \quad \text{Rechtsoperation von } U \text{ auf } G,$$
$$*|_{U\times U} : U \times U \to G : (u, v) \mapsto u * v \quad \text{äußere Verknüpfung auf } U.$$

Diese drei Einschränkungen gelingen immer und sind oft nützlich.
Für ganz besondere Teilmengen $U \subseteq G$ erhalten wir die Einschränkung

$$*_U = *|^U_{U\times U} : U \times U \to U : (u, v) \mapsto u * v.$$

Dies gelingt nicht immer, sondern erfordert die **Abgeschlossenheit** der Teilmenge $U \subseteq G$ unter der Verknüpfung $*: G \times G \to G$, also:

$$U * U \subseteq U \quad \Longleftrightarrow \quad \forall a, b \in U : a * b \in U$$

In Worten: Wenn wir zwei Elemente a, b aus U mit $*$ verknüpfen, dann erhalten wir immer ein Element $a * b$ in U (und nicht bloß irgendwo in G).

Unterstrukturen durch Einschränkung

Definition G1M: Unterstrukturen durch Einschränkung

Sei $(G, *)$ ein Magma, also $*: G \times G \to G$. Ein **Untermagma** $U \leq (G, *)$ ist eine Teilmenge $U \subseteq G$ mit $U * U \subseteq U$. Ausführlich: Für alle $a, b \in U$ gilt $a * b \in U$. Somit ist die Einschränkung $*_U = *|^U_{U\times U} : U \times U \to U$ von $*$ auf U wohldefiniert, und $(U, *_U)$ ist selbst ein Magma.

(G0) Ist $(G, *)$ assoziativ bzw. kommutativ, so auch $(U, *_U)$.

(G1) Für ein **Untermonoid** $U \leq (G, *, e)$ fordern wir zudem $e \in U$. Somit ist $(U, *_U, e)$ ein Monoid, denn $e * a = a * e = a$ für alle $a \in U$.

Ist $(U, *_U, e)$ zudem eine Gruppe, so nennen wir U eine **Untergruppe** im Monoid $(G, *, e)$. Ist $(G, *, e, \iota)$ selbst eine Gruppe, so bedeutet das:

(G2) Für eine **Untergruppe** $U \leq (G, *, e, \iota)$ fordern wir zudem $\iota(U) \subseteq U$. Ausführlich: Für alle $a \in U$ gilt $\iota(a) \in U$. Somit ist die Einschränkung $\iota_U = \iota|^U_U : U \to U$ wohldefiniert, und $(U, *_U, e, \iota_U)$ ist eine Gruppe.

Untergruppen

Beispiel: In jeder Gruppe $(G, *, e, \iota)$ sind $\{e\}$ und G Untergruppen.

Beispiele: In der Gruppe $(\mathbb{Z}, +, 0, -)$ gilt:

- Die Menge $2\mathbb{Z}$ ist eine Untergruppe, aber nicht $2\mathbb{Z} + 1$.
- Die Menge $U = n\mathbb{Z}$ mit $n \in \mathbb{N}$ ist eine Untergruppe. Umgekehrt:
- Jede Untergruppe $U < \mathbb{Z}$ hat die Form $U = n\mathbb{Z}$, siehe Satz G1v.
- Die Menge $\mathbb{N}$ ist ein Untermonoid, aber keine Untergruppe.
- Die Menge $\mathbb{N}_{\geq 5}$ ist eine Unterhalbgruppe, aber kein Untermonoid.

Beispiel: Im Monoid $(\mathbb{Z}, \cdot, 1)$ ist $\{0\}$ multiplikativ abgeschlossen, und $(\{0\}, \cdot, 0)$ ist ein Monoid, aber kein Untermonoid von $(\mathbb{Z}, \cdot, 1)$.

Übung: In der symmetrischen Gruppe S_3 gibt es genau 6 Untergruppen.

Untergruppen

Aufgabe: Die Untergruppenbedingung lässt sich wie folgt formulieren:

$$\begin{aligned} U \leq (G, *, e, \iota) \quad &:\Longleftrightarrow \quad e \in U \wedge \forall a, b \in U : [\, a * b \in U \wedge \iota(a) \in U \,] \\ &\Longleftrightarrow \quad U \neq \emptyset \wedge \forall a, b \in U : a * \iota(b) \in U \end{aligned}$$

Lösung: Die Implikation „⇒“ ist klar. Wir zeigen „⇐“:
(0) Wegen $U \neq \emptyset$ existiert $a \in U$, somit $e = a * \iota(a) \in U$.
(1) Für jedes $a \in U$ gilt dank (0) auch $\iota(a) = e * \iota(a) \in U$.
(2) Für alle $a, b \in U$ gilt $\iota(b) \in U$ dank (1), also $a * b = a * \iota(\iota(b)) \in U$.

Notation: Für eine Untergruppe $U \subseteq G$ in $(G, *)$ schreiben wir kurz $U \leq (G, *)$ oder noch kürzer $U \leq G$. Im Falle $U \subsetneq G$ ist U eine **echte Untergruppe**, geschrieben $U < G$. Dieselbe Notation nutzen wir für Untermonoide; der Kontext macht jeweils klar, was gemeint ist.

Die invertierbaren Elemente bilden eine Untergruppe.

Beispiele: Im Matrixring $K^{n\times n}$ gilt $(K^{n\times n},\cdot,1_{n\times n})^\times = \mathrm{GL}_n\, K$.
Im Monoid $(\mathrm{E}_X,\circ,\mathrm{id}_X)$ mit $\mathrm{E}_X = \mathrm{Abb}(X,X)$ gilt $\mathrm{E}_X^\times = \mathrm{S}_X$.
Im Ring $\mathbb{Z}_n$ gilt $\mathbb{Z}_n^\times = (\mathbb{Z}_n,\cdot,1)^\times = \{\, a\in\mathbb{Z}_n \mid \mathrm{ggT}(a,n)=1 \,\}$.
Ein Monoid $(M,*,e)$ ist genau dann eine Gruppe, wenn $M^\times = M$ gilt.

Satz G1N: Die invertierbaren Elemente bilden eine Gruppe.
In jedem Monoid $(M,*,e)$ ist $M^\times \leq (M,*,e)$ eine Untergruppe.
In $M^\times$ gilt $e^{-1}=e$ und $(a^{-1})^{-1}=a$ sowie $(a*b)^{-1}=b^{-1}*a^{-1}$.

Übung: Beweisen Sie dies zur Wiederholung (B1C).

Die invertierbaren Elemente bilden eine Untergruppe.

Beweis: Zunächst gilt $e*e=e$, also $e\in M^\times$ mit $e^{-1}=e$.
Für je zwei Elemente $a,b\in M^\times$ gilt $a*b\in M^\times$, denn wir haben:

$$(a*b)*(b^{-1}*a^{-1}) \overset{\text{Ass}}{=} (a*(b*b^{-1}))*a^{-1} \overset{\text{Inv}}{=} (a*1)*a^{-1} \overset{\text{Ntr}}{=} a*a^{-1} \overset{\text{Inv}}{=} e$$
$$(b^{-1}*a^{-1})*(a*b) \overset{\text{Ass}}{=} (b^{-1}*(a^{-1}*a))*b \overset{\text{Inv}}{=} (b^{-1}*1)*b \overset{\text{Ntr}}{=} b^{-1}*b \overset{\text{Inv}}{=} e$$

Also ist $a*b$ invertierbar mit dem Inversen $(a*b)^{-1}=b^{-1}*a^{-1}$.
Das heißt, $M^\times$ enthält e und ist abgeschlossen unter Multiplikation.

Für $a\in M^\times$ gilt $a*a^{-1}=a^{-1}*a=e$, also $a^{-1}\in M^\times$ mit $(a^{-1})^{-1}=a$.
Somit ist die Inversion $^{-1}\colon M^\times\to M^\times\colon a\mapsto a^{-1}$ auf $M^\times$ wohldefiniert.
Zusammengefasst bedeutet das: $(M^\times,*,e,^{-1})$ ist eine Gruppe. QED

Beispiele zu Untergruppen

Übung: (1) Ist $(U_i)_{i\in I}$ eine Familie von Untergruppen $U_i\leq(G,*,e,\iota)$, so ist auch die Schnittmenge $U=\bigcap_{i\in I}U_i$ eine Untergruppe in G.
(2) Geben Sie ein Beispiel für zwei Untergruppen $U,V\leq(G,*,e,\iota)$, sodass ihre Vereinigung $U\cup V$ keine Untergruppe in G ist.

Beispiele zu Untergruppen

Zu jedem Monoid $(G,\cdot,e)$ definieren wir das **Zentrum** als die Menge

$$Z(G)=Z(G,\cdot)=\left\{\, z\in G \;\middle|\; \forall a\in G\colon a\cdot z=z\cdot a \,\right\}$$

aller Elemente $z\in G$, die mit allen Elementen in G kommutieren.

Übung: (1) Das Zentrum $Z(G)$ ist ein Untermonoid von $(G,\cdot,e)$.
(2) Ist ein Element $z\in Z(G)$ invertierbar in G, so gilt $z^{-1}\in Z(G)$.
(3) Ist $(G,*,e)$ eine Gruppe, so ist $Z(G)$ eine Untergruppe.
(4) Allgemein gilt $Z(G)^\times = Z(G)\cap G^\times$.

Homomorphismen sind strukturerhaltende Abbildungen.

Die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}_{>0} : a \mapsto \mathrm{e}^a = \sum_{k=0}^{\infty} a^k/k!$ erfüllt $\exp(a+b) = \exp(a) \cdot \exp(b)$ sowie $\exp(0) = 1$ und $\exp(-x) = \exp(x)^{-1}$.

$$\begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \xrightarrow[(a,b)\mapsto a+b]{+} & \mathbb{R} \\ {\scriptstyle\exp}\downarrow\ {\scriptstyle\exp}\downarrow & & \downarrow{\scriptstyle\exp} \\ \mathbb{R}_{>0} \times \mathbb{R}_{>0} & \xrightarrow[(x,y)\mapsto x\cdot y]{\cdot} & \mathbb{R}_{>0} \end{array} \qquad \begin{array}{c} 0 \\ \downarrow{\scriptstyle\exp} \\ 1 \end{array} \qquad \begin{array}{ccc} \mathbb{R} & \xrightarrow[a\mapsto -a]{-} & \mathbb{R} \\ {\scriptstyle\exp}\downarrow & & \downarrow{\scriptstyle\exp} \\ \mathbb{R}_{>0} & \xrightarrow[x\mapsto x^{-1}]{-1} & \mathbb{R}_{>0} \end{array}$$

Die Logarithmusfunktion $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ erfüllt $\ln(x \cdot y) = \ln(x) + \ln(y)$ sowie $\ln(1) = 0$ und $\ln(x^{-1}) = -\ln(x)$. Übersichtlich als Diagramm:

$$\begin{array}{ccc} \mathbb{R}_{>0} \times \mathbb{R}_{>0} & \xrightarrow[(x,y)\mapsto x\cdot y]{\cdot} & \mathbb{R}_{>0} \\ {\scriptstyle\ln}\downarrow\ {\scriptstyle\ln}\downarrow & & \downarrow{\scriptstyle\ln} \\ \mathbb{R} \times \mathbb{R} & \xrightarrow[(a,b)\mapsto a+b]{+} & \mathbb{R} \end{array} \qquad \begin{array}{c} 1 \\ \downarrow{\scriptstyle\ln} \\ 0 \end{array} \qquad \begin{array}{ccc} \mathbb{R}_{>0} & \xrightarrow[x\mapsto x^{-1}]{-1} & \mathbb{R}_{>0} \\ {\scriptstyle\ln}\downarrow & & \downarrow{\scriptstyle\ln} \\ \mathbb{R} & \xrightarrow[a\mapsto -a]{-} & \mathbb{R} \end{array}$$

Homomorphismen sind strukturerhaltende Abbildungen.

Ein Homomorphismus ist eine strukturerhaltende Abbildung.
Wir erklären hier, was das genau bedeutet. Es lohnt sich, dies für jede mathematische Struktur zu definieren, zu untersuchen und zu nutzen.

Sie kennen und nutzen Homomorphismen bereits seit Schulzeiten, wenn auch nicht unter diesem Namen, meist unter gar keinem Namen.

Viele nützliche Rechenregeln, wie Potenzgesetze, Exponentialgesetze, Logarithmusgesetze und zahllose weitere, sind letztendlich nichts weiter als Homomorphismen (oder beruhen darauf). Wir wollen dies bündeln.

Die obigen Beispiele $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ und $\ln : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ sind Gruppenhomomorphismen, allgemein ist dies eine Abbildung $f : (G, *, e_G, \iota_G) \to (H, \bullet, e_H, \iota_H)$ mit folgenden Eigenschaften:

$$\begin{array}{ccc} G \times G & \xrightarrow[(a,b)\mapsto a*b]{*} & G \\ {\scriptstyle f}\downarrow\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ H \times H & \xrightarrow[(x,y)\mapsto x\bullet y]{\bullet} & H \end{array} \qquad \begin{array}{c} e_G \in G \\ {\scriptstyle f}\downarrow \\ e_H \in H \end{array} \qquad \begin{array}{ccc} G & \xrightarrow[a\mapsto \iota_G(a)]{\iota_G} & G \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ H & \xrightarrow[x\mapsto \iota_H(x)]{\iota_H} & H \end{array}$$

Homomorphismen sind strukturerhaltende Abbildungen.

Definition G1○: Homomorphismen

Ein **Homomorphismus** ist eine strukturerhaltende Abbildung.

(G0) Für Magmen und Halbgruppen verlangen wir Multiplikativität:

$$\left.\begin{array}{l} f : (G, *) \to (H, \bullet) \\ \text{Magmahomomorphismus} \end{array}\right\} :\Longleftrightarrow \begin{cases} f : G \to H \text{ Abbildung und} \\ \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \end{cases}$$

(G1) Für einen **Monoidhomomorphismus** fordern wir zudem $f(e) = e'$:

$$\left.\begin{array}{l} f : (G, *, e) \to (H, \bullet, e') \\ \text{Monoidhomomorphismus} \end{array}\right\} :\Longleftrightarrow \begin{cases} f : G \to H \text{ mit } f(e) = e' \text{ und} \\ \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \end{cases}$$

(G2) Für einen **Gruppenhomomorphismus** genügt Multiplikativität:

$$\left.\begin{array}{l} f : (G, *, e, \iota) \to (H, \bullet, e', \iota') \\ \text{Gruppenhomomorphismus} \end{array}\right\} :\Longleftrightarrow \begin{cases} f : G \to H \text{ Abbildung und} \\ \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \end{cases}$$

Daraus folgt bereits $f(e) = e'$ und $f \circ \iota = \iota' \circ f$, also $f(a^{-1}) = f(a)^{-1}$.

Homomorphismen sind strukturerhaltende Abbildungen.

Beispiel: Die Abbildung $f : (\mathbb{N}, \cdot, 1) \to (\mathbb{Z}, \cdot, 1) : a \mapsto 0$ ist multiplikativ, $f(a \cdot b) = f(a) \cdot f(b)$, aber kein Monoidhomomorphismus: $f(1) = 0 \neq 1$.

Schreibweise für Gruppenhomomorphismen:

$$\begin{aligned} \mathrm{Hom}(G, H) &= \mathrm{Hom}(G, *; H, \bullet) = \mathrm{Hom}(G, *, e, \iota; H, \bullet, e', \iota') \\ &:= \left\{ f : G \to H \;\middle|\; \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \right\} \end{aligned}$$

Aufgabe: Folgern Sie $f(e) = e'$ und $f(a^{-1}) = f(a)^{-1}$.

Lösung: (1) Wir betrachten

$$e' \bullet f(e) \overset{\text{Ntr}}{=} f(e) \overset{\text{Ntr}}{=} f(e * e) \overset{\text{Hom}}{=} f(e) \bullet f(e).$$

Multiplikation mit $f(e)^{-1}$ von rechts ergibt $e' = f(e)$.

(2) Für jedes Element $a \in G$ gilt

$$e' \overset{(1)}{=} f(e) \overset{\text{Inv}}{=} f(a * a^{-1}) \overset{\text{Hom}}{=} f(a) \bullet f(a^{-1}).$$

Wir folgern $f(a^{-1}) = f(a)^{-1}$ dank Eindeutigkeit des Inversen (G1H).

Isomorphismen sind strukturerhaltende Bijektionen.

Ist $\varphi : (G, *) \to (H, \bullet)$ ein Homomorphismus und zudem bijektiv, so nennen wir f einen **Isomorphismus** von $(G, *)$ nach $(H, \bullet)$.

Lemma G1P: Umkehrung eines Isomorphismus

In diesem Falle ist auch $\psi = \varphi^{-1} : (H, \bullet) \to (G, *)$ ein Isomorphismus.

Beweis: Zu $x, y \in H$ sei $a = \psi(x)$ und $b = \psi(y)$. Damit folgt:
$\psi(x \bullet y) = \psi(\varphi(a) \bullet \varphi(b)) = \psi(\varphi(a * b)) = a * b = \psi(x) * \psi(y)$. QED

Definition G1Q: Isomorphismus als Paar

Ein **Isomorphismus** $(\varphi, \psi) : (G, *) \cong (H, \bullet)$ zwischen zwei Gruppen ist ein Paar zueinander inverser Homomorphismen $\varphi : (G, *) \to (H, \bullet)$ und $\psi : (H, \bullet) \to (G, *)$ mit $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_H$.

Entsprechend für $(\varphi, \psi) : (G, *, e) \cong (H, \bullet, e')$ zwischen zwei Monoiden.

(Es genügt, einen anzugeben, der andere ist dann eindeutig bestimmt. Es ist jedoch oft bequem, das Paar vollständig und explizit anzugeben.)

Beispiel: Wir haben $(\exp, \ln) : (\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.

Isomorphismen sind strukturerhaltende Bijektionen.

Schreibweise für **Homomorphismen** und **Isomorphismen**:

$$\mathrm{Hom}(G, *; H, \bullet) = \{\, f : G \to H \mid \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \,\}$$
$$\mathrm{Iso}(G, *; H, \bullet) = \{\, f : G \xrightarrow{\sim} H \mid \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \,\}$$

Im Spezialfall $(G, *) = (H, \bullet)$ stimmen Start und Ziel überein, und wir sprechen dann von **Endomorphismen** und **Automorphismen**:

$$\mathrm{End}(G, *) = \mathrm{Hom}(G, *; G, *)$$
$$\mathrm{Aut}(G, *) = \mathrm{Iso}(G, *; G, *)$$

Beispiel: Für $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0} : x \mapsto x^n$ mit $n \in \mathbb{N}_{\geq 1}$ gilt $f \in \mathrm{Aut}(\mathbb{R}_{>0}, \cdot)$.
Es gilt $f(x \cdot y) = (x \cdot y)^n = x^n \cdot y^n = f(x) \cdot f(y)$, also $f \in \mathrm{End}(\mathbb{R}_{>0}, \cdot)$.
Zudem ist f invertierbar, durch $g(y) = \sqrt[n]{y}$, also gilt $f \in \mathrm{Aut}(\mathbb{R}_{>0}, \cdot)$.

Bemerkung: Dank G1P folgt daraus $\sqrt[n]{x \cdot y} = \sqrt[n]{x} \cdot \sqrt[n]{y}$.

L'algèbre est généreuse, elle donne souvent plus qu'on lui demande.
[Die Algebra ist großzügig, sie gibt oft mehr, als wir von ihr verlangen.]
Jean Le Rond d'Alembert (1717–1783)

Homomorphismen und Untergruppen

Satz G1R: Bild und Kern, surjektiv und injektiv

Sei $f : (G, *, e) \to (H, \bullet, e')$ ein Gruppenhomomorphismus.

(1) Ist $U \leq (G, *, e)$ eine Untergruppe, so auch $V = f(U) \leq (H, \bullet, e')$. Insbesondere ist das Bild $\mathrm{im}(f) = f(G) \leq (H, \bullet, e')$ eine Untergruppe.

(2) Genau dann ist f surjektiv, wenn $\mathrm{im}(f) = H$ gilt.

(3) Ist $V \leq (H, \bullet, e')$ eine Untergruppe, so auch $U = f^{-1}(V) \leq (G, *, e)$. Somit ist der Kern $\ker(f) := f^{-1}(\{e'\}) \leq (G, *)$ eine Untergruppe.

(4) Genau dann ist f injektiv, wenn $\ker(f) = \{e\}$ gilt. Allgemein:

(5) Für $a \in G$ gilt $b = f(a) \in \mathrm{im}(f)$ und $f^{-1}(\{b\}) = a \ker(f) = \ker(f)\, a$.

☺ Das unscheinbare Injektivitätskriterium (4) ist überaus praktisch und wird sich im Folgenden immer wieder als hilfreich erweisen.

Arbeitsersparnis: Für die Injektivität eines Gruppenhomomorphismus $f : (G, *, e) \to (H, \bullet, e')$ müssen wir nicht alle Fasern $f^{-1}(\{b\})$ prüfen, sondern nur eine einzige Faser, nämlich $\ker(f) = f^{-1}(\{e'\})$.

Homomorphismen und Untergruppen

Aufgabe: Rechnen Sie die Aussagen des Satzes sorgsam nach.

Lösung: (1) Es gilt $e' = f(e) \in V$. Zu $x, y \in V$ existieren $a, b \in U$ mit $f(a) = x$ und $f(b) = y$, also gilt $x \bullet y^{-1} = f(a) \bullet f(b)^{-1} = f(a * b^{-1}) \in V$.

(2) Die Aussage $\mathrm{im}(f) = H$ ist die Definition von Surjektivität.

(3) Wegen $f(e) = e' \in V$ gilt $e \in U$. Seien $a, b \in U$, also $f(a), f(b) \in V$. Dann gilt $a * b^{-1} \in U$, denn $f(a * b^{-1}) = f(a) \bullet f(b)^{-1} \in V$.

(4) Die Implikation „⇒“ ist klar. Die Umkehrung „⇐“ folgt aus (5):

(5) Gegeben seien $a, a' \in G$ mit $f(a) = f(a')$.

- Es gilt $e' = f(a)^{-1} f(a') = f(a^{-1} a')$, also $a^{-1} a' \in \ker(f)$, somit $a' \in a \ker(f)$.
- Es gilt $e' = f(a') f(a)^{-1} = f(a' a^{-1})$, also $a' a^{-1} \in \ker(f)$, somit $a' \in \ker(f)\, a$. QED

☺ Jede Faser ist entweder leer oder eine Translation des Kerns.

Der Satz von Cayley

Beispiel: Die Gruppe $G = (\mathbb{Z}_3, +, 0)$ bettet in $(\mathrm{S}_G, \circ, \mathrm{id}_G)$ ein vermöge

$$0 \mapsto \tau_0 = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} = \mathrm{id},$$

$$1 \mapsto \tau_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix} = (0,1,2),$$

$$2 \mapsto \tau_2 = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix} = (0,2,1).$$

🙂 Jede noch so abstrakte Gruppe lässt sich konkret darstellen:

Satz G1S: Darstellungssatz von Cayley

Jede Gruppe $(G, *, e)$ bettet in die symmetrische Gruppe $(\mathrm{S}_G, \circ, \mathrm{id})$ ein, ist also isomorph zu einer Untergruppe $U \leq \mathrm{S}_G$ von Permutationen.

Ist die Gruppe G endlich, von der Ordnung $n = \sharp G$, so gilt sogar:

Die Gruppe G bettet in die Gruppe S_n ein, ist also isomorph zu einer Untergruppe $U \leq \mathrm{S}_n$ von Permutationen auf der Menge $\{1, \ldots, n\}$.

Der Satz von Cayley

Beweis: Jedes Element $a \in G$ definiert seine Linkstranslation

$$\tau_a : G \to G : x \mapsto a * x.$$

Für $e \in G$ gilt $\tau_e = \mathrm{id}_G$. Dank Assoziativität haben wir $\tau_{a*b} = \tau_a \circ \tau_b$:

$$(\tau_a \circ \tau_b)(x) = \tau_a(\tau_b(x)) = a * (b * x) = (a * b) * x = \tau_{a*b}(x)$$

Wir erhalten somit den gewünschten Monoidhomomorphismus

$$\tau : (G, *, e) \to (\mathrm{E}_G, \circ, \mathrm{id}_G) : a \mapsto \tau_a.$$

Dieser ist injektiv: Für $a \neq b$ gilt $\tau_a \neq \tau_b$, denn $\tau_a(e) = a \neq b = \tau_b(e)$.

Aus $a * b = e = b * a$ folgt $\tau_a \circ \tau_b = \tau_{a*b} = \tau_e = \mathrm{id}_G$ und $\tau_b \circ \tau_a = \mathrm{id}_G$.
Für jedes Element $a \in G$ gilt demnach $\tau_{a^{-1}} = \tau_a^{-1}$. Wir erhalten so

$$\tau : (G, *, e) \hookrightarrow (\mathrm{S}_G, \circ, \mathrm{id}_G) : a \mapsto \tau_a.$$

Für die Untergruppe $U = \tau(G) \leq \mathrm{S}_G$ gilt somit $\tau : G \xrightarrow{\sim} U$. QED

Der Satz von Cayley

Ist die Gruppe G endlich, von der Ordnung $n = \sharp G$, so gilt sogar:

Die Gruppe G bettet in die Gruppe S_n ein, ist also isomorph zu einer Untergruppe $U \leq \mathrm{S}_n$ von Permutationen auf der Menge $\{1, \ldots, n\}$.

Hierzu nummerieren wir die Elemente von G durch $\nu : \{1, \ldots, n\} \xrightarrow{\sim} G$ und erhalten so einen Gruppenisomorphismus $\mathrm{S}_G \cong \mathrm{S}_n$. Genauer:

Aufgabe: Jede Bijektion $\nu : X \xrightarrow{\sim} Y$ definiert einen Isomorphismus von Monoiden $(\varphi, \psi) : \mathrm{E}_X \cong \mathrm{E}_Y$ und von Gruppen $(\varphi, \psi) : \mathrm{S}_X \cong \mathrm{S}_Y$ vermöge $\varphi(\tau) = \nu \circ \tau \circ \nu^{-1}$ und $\psi(\sigma) = \nu^{-1} \circ \sigma \circ \nu$.

Lösung: Für $\tau : X \to X$ gilt $\varphi(\tau) = \nu \circ \tau \circ \nu^{-1} : Y \to Y$, also ist φ wohldefiniert. Für $\tau = \mathrm{id}_X$ gilt $\varphi(\mathrm{id}_X) = \mathrm{id}_Y$. Für $\tau, \tau' : X \to X$ gilt

$$\begin{aligned} \varphi(\tau \circ \tau') &= \nu \circ (\tau \circ \tau') \circ \nu^{-1} \\ &= (\nu \circ \tau \circ \nu^{-1}) \circ (\nu \circ \tau' \circ \nu^{-1}) = \varphi(\tau) \circ \varphi(\tau'). \end{aligned}$$

Somit ist $\varphi : (\mathrm{E}_X, \circ, \mathrm{id}_X) \to (\mathrm{E}_Y, \circ, \mathrm{id}_Y)$ ein Monoidhomomorphismus. Umgekehrt gilt dasselbe für ψ. Schließlich finden wir $\psi \circ \varphi = \mathrm{id}$ und $\varphi \circ \psi = \mathrm{id}$, also $(\varphi, \psi) : \mathrm{E}_X \cong \mathrm{E}_Y$. Daraus folgt $(\varphi, \psi) : \mathrm{S}_X \cong \mathrm{S}_Y$.

Der Satz von Cayley

Der Satz von Cayley gilt wörtlich ebenso für Monoide:

Jedes Monoid $(G, *, e)$ bettet in das Abbildungsmonoid $(\mathrm{E}_G, \circ, \mathrm{id})$ ein, ist also isomorph zu einem Untermonoid $U \leq \mathrm{E}_G$ von Abbildungen.

Ist das Monoid G endlich, von der Ordnung $n = \sharp G$, so gilt sogar:
Das Monoid $(G, *, e)$ bettet in das Abbildungsmonoid $(\mathrm{E}_n, \circ, \mathrm{id})$ ein.

🙂 Solche Abbildungen und Permutationen sind wunderbar konkrete Objekte, mit denen wir bequem, explizit und effizient rechnen können. Die Grundlagen hierzu kennen Sie von Beginn des Kapitels E.

Übung: Wenn wir Rechtstranslationen $\tau_a : x \mapsto x * a$ betrachten, so erhalten wir eine Einbettung $\tau : (G, *, e) \hookrightarrow (\mathrm{E}_G, \bullet, \mathrm{id}_G)$.

Übung: Die entgegengesetzten Gruppen $(\mathrm{S}_X, \circ, \mathrm{id}_X)$ und $(\mathrm{S}_X, \bullet, \mathrm{id}_X)$ sind isomorph vermöge der Inversion $\varphi : \mathrm{S}_X \to \mathrm{S}_X : \sigma \mapsto \sigma^{-1}$.

Übung: Die entgegengesetzten Monoide $(\mathrm{E}_X, \circ, \mathrm{id}_X)$ und $(\mathrm{E}_X, \bullet, \mathrm{id}_X)$ sind nicht isomorph für $\sharp X \geq 2$: Sei $c : X \to X$ eine konstante Abbildung. In $(\mathrm{E}_X, \circ, \mathrm{id}_X)$ gilt dann $c \circ f = c$ für alle $f \in \mathrm{E}_X$. Hingegen gibt es in $(\mathrm{E}_X, \bullet, \mathrm{id}_X)$ kein Element c' mit $c' \bullet f = c'$ für alle $f \in \mathrm{E}_X$.

Summen und Produkte

Sei $(M,+,0)$ bzw. $(M,\cdot,1)$ ein Monoid, hier additiv oder multiplikativ geschrieben. Mehrfache Summen und Produkte definieren wir rekursiv:

$$\sum_{i=1}^{0} a_i := 0, \quad \sum_{i=1}^{n+1} a_i := \Big(\sum_{i=1}^{n} a_i\Big) + a_{n+1} = (\dots(a_1+a_2)+\dots)+a_{n+1}$$

$$\prod_{i=1}^{0} a_i := 1, \quad \prod_{i=1}^{n+1} a_i := \Big(\prod_{i=1}^{n} a_i\Big) \cdot a_{n+1} = (\dots(a_1\cdot a_2)\cdot\dots)\cdot a_{n+1}$$

Dank Assoziativität können wir beliebig umklammern,
bei kommutierenden Elementen auch beliebig umordnen:

Ist $I=\{i_1,i_2,\dots,i_n\}$ eine n–elementige Menge, so schreiben wir

$$\sum_{i\in I} a_i := \sum_{k=1}^{n} a_{i_k} \quad \text{und} \quad \prod_{i\in I} a_i := \prod_{k=1}^{n} a_{i_k}.$$

Eine Umnummerierung der Elemente ändert das Ergebnis nicht.

Sei J eine Menge und $I\subseteq J$ endlich, sodass $a_i=0$ für alle $i\in J\smallsetminus I$.
Dann definieren wir $\sum_{i\in J} a_i := \sum_{i\in I} a_i$ als endliche Summe wie oben.

Vielfache und Potenzen

Für $n\in\mathbb{N}$ definieren wir das $n$te Vielfache und die $n$te Potenz durch

$$a\bullet n := \textstyle\sum_{i=1}^{n} a \quad \text{und} \quad a^n := \prod_{i=1}^{n} a.$$

Ist $-a$ das Negative zu a in $(M,+,0)$, so setzen wir $a\bullet(-n) := (-a)\bullet n$.
Ist a^{-1} das Inverse zu a in $(M,\cdot,1)$, so setzen wir $a^{-n} := (a^{-1})^n$.

Auf dem Monoid M bzw. der Gruppe $M^\times$ definiert dies die Operationen

$$M\times\mathbb{N}\to M : (a,n)\mapsto a\bullet n, \qquad M^\times\times\mathbb{Z}\to M^\times : (a,n)\mapsto a\bullet n,$$
$$M\times\mathbb{N}\to M : (a,n)\mapsto a^n, \qquad M^\times\times\mathbb{Z}\to M^\times : (a,n)\mapsto a^n.$$

Wir schreiben $a\bullet n = n\bullet a$ von rechts oder von links, kurz $an=na$.

Satz G1T: Rechenregeln für Vielfache und Potenzen

Für alle $a\in M$ und $m,n\in\mathbb{N}$ bzw. $a\in M^\times$ und $m,n\in\mathbb{Z}$ gilt:

$$a\bullet 0=0,\ a\bullet 1=a,\ a\bullet(m+n)=a\bullet m+a\bullet n,\ a\bullet(m\cdot n)=(a\bullet m)\bullet n,$$
$$a^0=1,\quad a^1=a,\quad a^{m+n}=a^m\cdot a^n,\quad a^{m\cdot n}=(a^m)^n.$$

Kommutieren: Aus $a+b=b+a$ folgt $(a+b)\bullet n = a\bullet n+b\bullet n$.
Aus $a\cdot b=b\cdot a$ folgt entsprechend $(a\cdot b)^n=a^n\cdot b^n$.

Das erzeugte Untermonoid und die erzeugte Untergruppe

Satz G1U: erzeugtes Untermonoid und erzeugte Untergruppe

Sei $(M,\cdot,1)$ ein Monoid und $S\subseteq M$ eine Teilmenge.

(1) Das von $S\subseteq M$ in $(M,\cdot,1)$ **erzeugte Untermonoid** ist

$$[\,S\,] := \big\{\, s_1^{e_1}s_2^{e_2}\cdots s_n^{e_n} \;\big|\; n\in\mathbb{N},\ s_i\in S,\ e_i\in\mathbb{N} \,\big\}.$$

Dies ist ein Untermonoid in M und zudem das kleinste, das S enthält.

(2) Die von $S\subseteq M^\times$ in $(M,\cdot,1)$ **erzeugte Untergruppe** ist

$$\langle\, S\,\rangle := \big\{\, s_1^{e_1}s_2^{e_2}\cdots s_n^{e_n} \;\big|\; n\in\mathbb{N},\ s_i\in S,\ e_i\in\mathbb{Z} \,\big\}.$$

Dies ist eine Untergruppe in M und zudem die kleinste, die S enthält.
Die Inversion auf S ist dabei gegeben durch

$$\big(s_1^{e_1}s_2^{e_2}\cdots s_n^{e_n}\big)^{-1} = s_n^{-e_n}\dots s_2^{-e_2}s_1^{-e_1}.$$

Übung: Beweisen Sie die Behauptungen des Satzes. Was ist zu tun?

Beispiel: In der Gruppe $(\mathrm{S}_4,\circ,\mathrm{id})$ gilt $\langle\,(1,2),(2,3)\,\rangle = \mathrm{S}_3$.

Beispiele zu Homomorphismen und Untergruppen

Sei $(M,\cdot,1)$ ein Monoid, hier multiplikativ geschrieben.

(1) Zu jedem Element $a\in M$ haben wir den Monoidhomomorphismus

$$\psi : (\mathbb{N},+,0)\to(M,\cdot,1) : n\mapsto a^n.$$

Sein Bild ist das von a in $(M,\cdot,1)$ erzeugte Untermonoid:

$$\mathrm{im}(\psi) = \{\, a^n \mid n\in\mathbb{N}\,\} =: [\,a\,]$$

(2) Zu jedem $a\in M^\times$ haben wir den Gruppenhomomorphismus

$$\varphi : (\mathbb{Z},+,0)\to(M,\cdot,1) : n\mapsto a^n.$$

Sein Bild ist die von a in $(M,\cdot,1)$ erzeugte Untergruppe:

$$\mathrm{im}(\varphi) = \{\, a^n \mid n\in\mathbb{Z}\,\} =: \langle\,a\,\rangle$$

In additiver Schreibweise $(M,+,0)$ gilt entsprechend

$$[\,a\,] = a\mathbb{N} = a\bullet\mathbb{N} = \{\, a\bullet n \mid n\in\mathbb{N}\,\},$$
$$\langle\,a\,\rangle = a\mathbb{Z} = a\bullet\mathbb{Z} = \{\, a\bullet n \mid n\in\mathbb{Z}\,\}.$$

Wir nennen $\mathrm{ord}(a) := \sharp\langle\,a\,\rangle$ die Ordnung von a in der Gruppe $M^\times$.

Klassifikation der Untergruppen von $(\mathbb{Z},+)$

Beispiel: Für $n \in \mathbb{N}$ ist die Menge $n\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z},+)$.
Dabei ist $0\mathbb{Z} = \{0\}$ die triviale Gruppe und $1\mathbb{Z} = \mathbb{Z}$ die gesamte Gruppe.

Satz G1v: Klassifikation der Untergruppen von $(\mathbb{Z},+)$

Zu jeder Untergruppe $H \leq (\mathbb{Z},+)$ existiert $n \in \mathbb{N}$, sodass $H = n\mathbb{Z}$ gilt.

Beweis: Ist $H = \{0\}$, so haben wir $H = 0\mathbb{Z}$.
Andernfalls existiert ein Element $a \in H$ mit $a \neq 0$.
Wir können $a > 0$ annehmen, denn auch $-a$ liegt in H.
Somit existiert $n = \min\{\, a \in H \mid a > 0 \,\}$ dank Satz F1s.

Aus $n \in H \leq (\mathbb{Z},+)$ folgt zunächst $\langle\, n \,\rangle = n\mathbb{Z} \subseteq H$.
Wir zeigen nun die Umkehrung $H \subseteq n\mathbb{Z}$. Hierzu sei $a \in H$.
Euklidische Division ergibt $a = nq + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < n$.
Wegen $r = a - nq \in H$ folgt $r = 0$, denn n ist minimal.
Also gilt $a = nq \in n\mathbb{Z}$. Dies zeigt $H \subseteq n\mathbb{Z}$.

Damit ist $H = n\mathbb{Z}$ bewiesen. QED

Zyklische Untermonoide

Sei $(M,\cdot,1)$ ein Monoid und $a \in M$ ein Element. Wie sieht das erzeugte Monoid $[\, a \,]$ aus? Hierzu betrachten wir den Monoidhomomorphismus

$$\psi : (\mathbb{N},+,0) \to (M,\cdot,1) : k \mapsto a^k.$$

Sein Bild ist $[\, a \,] = \{\, a^k \mid k \in \mathbb{N} \,\}$. Ist ψ injektiv, so haben wir

$$\hat{\psi} : (\mathbb{N},+,0) \xrightarrow{\sim} ([\, a \,],\cdot,1) : k \mapsto a^k.$$

Andernfalls existieren $0 \leq m < n$ in $\mathbb{N}$, sodass ψ auf $\{0,\ldots,n-1\}$ injektiv ist und dann $a^n = a^m$ gilt. Graphisch bedeutet das folgendes:

$$a^0 \mapsto a^1 \mapsto a^2 \mapsto \ldots \mapsto a^m \mapsto a^{m+1} \mapsto \ldots \mapsto a^{n-1} \mapsto a^n$$

Demnach ist $n = \sharp[\, a \,]$ die Ordnung des erzeugten Untermonoids.
Im Falle $0 < m < n$ gilt zudem $a^{m-1} \neq a^{n-1}$, aber $a^{m-1} \cdot a = a^{n-1} \cdot a$.
Somit ist a nicht kürzbar, also insbesondere auch nicht invertierbar.

☺ Ist a in $(M,\cdot,1)$ invertierbar und $n = \sharp[\, a \,] < \infty$, so gilt $m = 0$. Somit ist $[\, a \,] = \langle\, a \,\rangle$ eine „zyklische Gruppe“. Der folgende Satz führt dies aus.

Zyklische Untergruppen

Beispiel: In der Gruppe $(\mathrm{S}_5,\circ,\mathrm{id})$ betrachten wir $\sigma = (1,2)(3,4,5)$:

$$\begin{aligned} &\sigma^0 = \mathrm{id}, && \sigma^1 = (1,2)(3,4,5), && \sigma^2 = (3,5,4),\\ &\sigma^3 = (1,2), && \sigma^4 = (3,4,5), && \sigma^5 = (1,2)(3,5,4),\\ &\sigma^6 = \mathrm{id}, && \sigma^7 = \sigma, && \ldots \quad \sigma^k = (1,2)^k(3,4,5)^k. \end{aligned}$$

In $(\mathrm{S}_5,\circ,\mathrm{id})$ erhalten wir so eine Untergruppe $\langle\, \sigma \,\rangle \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$.

Satz G1w: zyklische Untergruppe und Ordnung eines Elements

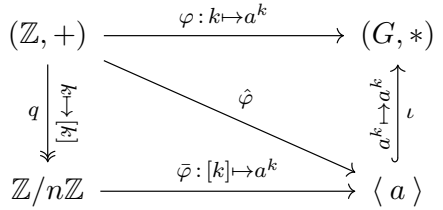
Sei $(G,*)$ eine Gruppe und $a \in G$ ein Element. Dazu betrachten wir den Gruppenhomomorphismus $\varphi : (\mathbb{Z},+) \to (G,*) : k \mapsto a^k$.

Sein Bild ist die Untergruppe $\langle\, a \,\rangle = \{\, a^k \mid k \in \mathbb{Z} \,\}$ in $(G,*)$.
Der Kern erfüllt $\ker(\varphi) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ dank Satz G1v.

0. Im Falle $n = 0$ hat a unendliche Ordnung, $\mathrm{ord}(a) = \sharp\langle\, a \,\rangle = \infty$, und wir erhalten den Gruppenisomorphismus $\hat{\varphi} : \mathbb{Z} \xrightarrow{\sim} \langle\, a \,\rangle : k \mapsto a^k$.
1. Im Falle $n \geq 1$ hat a endliche Ordnung, $\mathrm{ord}(a) = \sharp\langle\, a \,\rangle = n$, und wir erhalten den Isomorphismus $\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle\, a \,\rangle : [k] \mapsto a^k$.

Zyklische Untergruppen

Beweis: (1) Allein die Konstruktion von $\bar{\varphi}$ bedarf der Erläuterung.
Wir haben $\varphi : \mathbb{Z} \to G : k \mapsto a^k$ mit $\ker(\varphi) = n\mathbb{Z}$. Für alle $k, \ell \in \mathbb{Z}$ gilt demnach $\varphi(k) = \varphi(\ell)$ genau dann, wenn $k - \ell \in n\mathbb{Z}$ (G1R).
Aus φ erhalten wir $\bar{\varphi}$ durch die kanonische Faktorisierung E3I:



Dank dieser Konstruktion ist $\bar{\varphi}$ bijektiv. Zudem ist $\bar{\varphi}$ ein Homomorphismus, denn $[k] + [\ell] = [k+\ell] \mapsto a^{k+\ell} = a^k \cdot a^\ell$.

(0) Im Falle $n = 0$ ist $q : (\mathbb{Z},+) \twoheadrightarrow (\mathbb{Z}/0\mathbb{Z},+)$ ein Isomorphismus.
In diesem Falle ist $\hat{\varphi} : (\mathbb{Z},+) \xrightarrow{\sim} (\langle\, a \,\rangle,\cdot)$ ein Isomorphismus. QED

Übung: Ist $\sigma = \sigma_1 \circ \cdots \circ \sigma_m$ in $(\mathrm{S}_N,\circ,\mathrm{id})$ ein Produkt disjunkter Zykel der Länge $\ell_1,\ldots,\ell_m$, dann hat σ die Ordnung $\mathrm{ord}(\sigma) = \mathrm{kgV}(\ell_1,\ldots,\ell_m)$.

Kartesisches Produkt mit koordinatenweiser Verknüpfung

Beispiel: Mit koordinatenweiser Verknüpfung ist $(\mathbb{R}^n, +, 0, -)$ eine abelsche Gruppe. Gleiches gilt für $\mathbb{R}^{\mathbb{N}}$ und $\mathbb{R}^{(\mathbb{N})}$. Ausführlich:

Beispiel G1X: Produkt $G_1 \times \cdots \times G_n$ von Gruppen

Ist $(G_i, *_i, e_i, {}^{-1})$ eine Gruppe für $i = 1, \ldots, n$, so auch das Produkt

$$(G, *, e, {}^{-1}) \quad \text{mit} \quad G = G_1 \times \cdots \times G_n,$$
$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 *_1 b_1, \ldots, a_n *_n b_n),$$
$$e = (e_1, \ldots, e_n) \quad \text{und} \quad (a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1}).$$

Die Projektion $\mathrm{pr}_i : G \twoheadrightarrow G_i : a \mapsto a_i$ ist ein Gruppenhomomorphismus, ebenso die Einbettung $\iota_i : G_i \hookrightarrow G : a_i \mapsto (e_1, \ldots, a_i, \ldots, e_n)$.

Gleiches gilt sinngemäß für das Produkt von Monoiden $(G_i, *_i, e_i)$. Genau dann ist G kommutativ, wenn alle $G_1, \ldots, G_n$ dies sind.

Übung: Rechnen Sie dieses und das nächste Beispiel sorgsam nach. Diese Konstruktionen sind grundlegend und werden uns oft nützen.

Funktionen mit punktweiser Verknüpfung

Beispiel G1Y: Potenz G^Ω und $G^{(\Omega)}$ einer Gruppe

(1) Sei Ω eine Menge. Ist $(G, +, 0, -)$ eine Gruppe, so auch die Potenz

$$(G, +, 0, -)^\Omega = (G^\Omega, \mathbf{+}, \mathbf{0}, \mathbf{-}) \text{ mit } G^\Omega = \mathrm{Abb}(\Omega, G) = \{\, f : \Omega \to G \,\},$$
$$(f \mathbf{+} g)(x) = f(x) + g(x), \quad \mathbf{0} : \Omega \to G : x \mapsto 0 \text{ und } (\mathbf{-}f)(x) = -f(x).$$

Hierbei ist $\mathrm{pr}_x : G^\Omega \twoheadrightarrow G : f \mapsto f(x)$ ein Gruppenhomomorphismus, ebenso $\iota_x : G \hookrightarrow G^\Omega : a \mapsto f$ mit $f(x) = a$ und $f(y) = 0$ für $y \neq x$.

(2) Für den Träger $\mathrm{supp}(f) = \{\, x \in \Omega \mid f(x) \neq 0 \,\}$ gilt $\mathrm{supp}(\mathbf{0}) = \emptyset$ und $\mathrm{supp}(\mathbf{-}f) = \mathrm{supp}(f)$ sowie $\mathrm{supp}(f \mathbf{+} g) \subseteq \mathrm{supp}(f) \cup \mathrm{supp}(g)$. In G^Ω liegt somit die Untergruppe der Funktionen mit endlichem Träger:

$$G^{(\Omega)} = \{\, f : \Omega \to G \mid \sharp\,\mathrm{supp}(f) < \infty \,\}$$

Gleiches gilt sinngemäß für die Potenz eines Monoids $(G, +, 0)$. Genau dann sind G^Ω und $G^{(\Omega)}$ kommutativ, wenn G dies ist.

Fundamentalsatz der Arithmetik als Isomorphismus

Beispiel G1Z: Fundamentalsatz der Arithmetik

Sei $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ die Menge der Primzahlen in $(\mathbb{N}_{\geq 1}, \cdot)$.
Wir betrachten die Menge $\mathbb{N}^{(\mathbb{P})} = \{\, e : \mathbb{P} \to \mathbb{N} \mid \sharp\,\mathrm{supp}(e) < \infty \,\}$.

(1) Hierzu haben wir den Monoidhomomorphismus

$$\Phi \;:\; (\mathbb{N}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{N}_{\geq 1}, \cdot) \;:\; e \mapsto \textstyle\prod_{p \in \mathbb{P}} p^{e(p)}.$$

Ausgeschrieben ist dies das (endliche!) Produkt $2^{e(2)} \cdot 3^{e(3)} \cdot 5^{e(5)} \cdots$.
Dank Fundamentalsatz der Arithmetik A2J ist Φ ein Isomorphismus.

(2) Übergang zu Brüchen ergibt den Gruppenisomorphismus

$$\Phi \;:\; (\mathbb{Z}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{Q}_{>0}, \cdot) \;:\; e \mapsto \textstyle\prod_{p \in \mathbb{P}} p^{e(p)}.$$

(3) Hinzufügen des Vorzeichens $\pm$ ergibt die Isomorphismen

$$\Phi \;:\; (\mathbb{Z}/2, +) \times (\mathbb{N}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{Z}^*, \cdot) \;:\; (s, e) \mapsto (-1)^s \textstyle\prod_{p \in \mathbb{P}} p^{e(p)},$$
$$\Phi \;:\; (\mathbb{Z}/2, +) \times (\mathbb{Z}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{Q}^*, \cdot) \;:\; (s, e) \mapsto (-1)^s \textstyle\prod_{p \in \mathbb{P}} p^{e(p)}.$$

Fundamentalsatz der Arithmetik als Isomorphismus

☺ Abstrakte Theorie wirkt ganz konkret! Die Umkehrfunktion $\Phi^{-1} : (\mathbb{N}^*, \cdot) \to (\mathbb{N}^{(\mathbb{P})}, +)$ ist die Primfaktorzerlegung und notorisch schwer zu berechnen. Genau darauf beruhen Cryptosysteme wie RSA.

Aufgabe: Ist $\sqrt[3]{72/125}$ rational? Nutzen Sie den Isomorphismus Φ!

Lösung: Als Primfaktorzerlegung finden wir hier $72/125 = 2^3\, 3^2\, 5^{-3}$.
In $\mathbb{Z}^{(\mathbb{P})}$ können wir $\Phi^{-1}(72/125) = (3, 2, -3, 0, \ldots)$ nicht durch 3 teilen.
In $(\mathbb{Q}_{>0}, \cdot)$ können wir aus $72/125$ demnach nicht die 3te Wurzel ziehen.

Aufgabe: Wir kennen den Isomorphismus $(\exp, \ln) : (\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$. Existiert ebenso ein Isomorphismus $(\varphi, \psi) : (\mathbb{Q}, +) \cong (\mathbb{Q}_{>0}, \cdot)$?

Lösung: Nein! In $(\mathbb{Q}, +)$ können wir jedes Element durch 2 dividieren, aber in $(\mathbb{Q}_{>0}, \cdot)$ nicht aus jedem Element die Quadratwurzel ziehen, zum Beispiel ist $\sqrt{2}$ irrational, siehe Satz A1F.

Übung: Existiert ein Isomorphismus $(\varphi, \psi) : (\mathbb{C}, +) \cong (\mathbb{C}^\times, \cdot)$?

Betrag und Vorzeichen reeller Zahlen

Beispiel: Für reelle Zahlen haben wir den **Absolutbetrag**

$$|-| : \mathbb{R} \twoheadrightarrow \mathbb{R}_{\geq 0} : x \mapsto |x| = \begin{cases} +x & \text{falls } x \geq 0, \\ -x & \text{falls } x \leq 0, \end{cases}$$

und das **Vorzeichen**

$$\operatorname{sign} : \mathbb{R} \twoheadrightarrow \{\pm 1, 0\} : x \mapsto \begin{cases} +1 & \text{falls } x > 0, \\ -1 & \text{falls } x < 0, \\ 0 & \text{falls } x = 0. \end{cases}$$

Beide sind multiplikativ, genauer Monoidhomomorphismen,
denn es gilt $|1| = 1$ und $|x \cdot y| = |x| \cdot |y|$ für alle $x, y \in \mathbb{R}$,
sowie $\operatorname{sign}(1) = 1$ und $\operatorname{sign}(x \cdot y) = \operatorname{sign}(x) \cdot \operatorname{sign}(y)$.

Für jedes invertierbare Element $x \in \mathbb{R}^\times = \mathbb{R} \smallsetminus \{0\}$
sind auch $|x|$ und $\operatorname{sign}(x)$ invertierbar, und es gilt
$|x^{-1}| = |x|^{-1}$ und $\operatorname{sign}(x^{-1}) = \operatorname{sign}(x)^{-1} = \operatorname{sign}(x)$.

Betrag und Vorzeichen reeller Zahlen

Durch Einschränkung erhalten wir die Gruppenhomomorphismen

$$|-| : (\mathbb{R}^\times, \cdot, 1) \twoheadrightarrow (\mathbb{R}_{>0}, \cdot, 1),$$
$$\operatorname{sign} : (\mathbb{R}^\times, \cdot, 1) \twoheadrightarrow (\{\pm 1\}, \cdot, 1).$$

Zusammengesetzt erhalten wir den Gruppenisomorphismus:

$$(\varphi, \psi) : \mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}_{>0}$$

Hierbei ist $\varphi(x) = (\operatorname{sign}(x), |x|)$ und $\psi(s, r) = s \cdot r$.
Beide Abbildungen sind Gruppenhomomorphismen,
und nach Konstruktion gilt $\psi \circ \varphi = \mathrm{id}$ und $\varphi \circ \psi = \mathrm{id}$.

Der Absolutbetrag $|x|$ heißt auch **Norm** und misst den Abstand
von x zum Nullpunkt. Insbesondere erhalten wir so die Menge

$$\mathbb{S}^0 := \{\, x \in \mathbb{R} \mid |x| = 1 \,\} = \{-1, +1\}.$$

Dies ist der Kern von $x \mapsto |x|$. Ebenso gilt $\mathbb{R}_{>0} = \ker(\operatorname{sign})$.

Betrag und Richtung komplexer Zahlen

Beispiel: Auch für komplexe Zahlen haben wir den **Absolutbetrag**

$$|-| : \mathbb{C} \twoheadrightarrow \mathbb{R}_{\geq 0} : z = x + \mathrm{i}y \mapsto |z| = \sqrt{x^2 + y^2}.$$

Dies heißt auch **Norm** und misst den Abstand von z zum Nullpunkt.
Somit ist die Menge $\mathbb{S}^1 := \{\, z \in \mathbb{C} \mid |z| = 1 \,\}$ die Einheitskreislinie.

Analog zum Vorzeichen reeller Zahlen definieren wir die **Richtung**

$$\operatorname{sign} : \mathbb{C} \twoheadrightarrow \mathbb{S}^1 \sqcup \{0\} : z \mapsto \begin{cases} z/|z| & \text{falls } z \neq 0, \\ 0 & \text{falls } z = 0. \end{cases}$$

Beide sind multiplikativ, genauer Monoidhomomorphismen,
denn es gilt $|1| = 1$ und $|z \cdot w| = |z| \cdot |w|$ für alle $z, w \in \mathbb{C}$,
und somit $\operatorname{sign}(1) = 1$ und $\operatorname{sign}(z \cdot w) = \operatorname{sign}(z) \cdot \operatorname{sign}(w)$.

Für jedes invertierbare Element $z \in \mathbb{C}^\times = \mathbb{C} \smallsetminus \{0\}$
sind auch $|z|$ und $\operatorname{sign}(z)$ invertierbar, und es gilt
$|z^{-1}| = |z|^{-1}$ und $\operatorname{sign}(z^{-1}) = \operatorname{sign}(z)^{-1} = \overline{\operatorname{sign}(z)}$.

Betrag und Richtung komplexer Zahlen

Durch Einschränkung erhalten wir die Gruppenhomomorphismen

$$|-| : (\mathbb{C}^\times, \cdot, 1) \twoheadrightarrow (\mathbb{R}_{>0}, \cdot, 1),$$
$$\operatorname{sign} : (\mathbb{C}^\times, \cdot, 1) \twoheadrightarrow (\mathbb{S}^1, \cdot, 1).$$

Diese sind surjektiv mit $\ker(z \mapsto |z|) = \mathbb{S}^1$ und $\ker(\operatorname{sign}) = \mathbb{R}_{>0}$.

Zusammengesetzt erhalten wir den Gruppenisomorphismus:

$$(\varphi, \psi) : \mathbb{C}^\times \cong \mathbb{S}^1 \times \mathbb{R}_{>0}$$

Hierbei ist $\varphi(z) = (\operatorname{sign}(z), |z|)$ und $\psi(s, r) = s \cdot r$.
Beide Abbildungen sind Gruppenhomomorphismen,
und nach Konstruktion gilt $\psi \circ \varphi = \mathrm{id}$ und $\varphi \circ \psi = \mathrm{id}$.

Eingeschränkt auf $\mathbb{R}$ gilt $\mathbb{C}^\times \cap \mathbb{R} = \mathbb{R}^\times$ und $\mathbb{S}^1 \cap \mathbb{R} = \mathbb{S}^0$,
und wir erhalten erneut den obigen Gruppenisomorphismus

$$\mathbb{R}^\times \cong \mathbb{S}^0 \times \mathbb{R}_{>0}.$$

Ringe und Körper: Definition

Definition G2A: Ring und Körper

Ein [kommutativer] **Ring** $(R, +, 0, \cdot, 1)$ besteht aus einer Menge R mit Verknüpfungen $+, \cdot : R \times R \to R$ und Elementen $0, 1 \in R$, sodass gilt:

0. Für alle Elemente $a, b, c \in R$ gelten die Distributivgesetze $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.
1. $(R, +, 0)$ ist eine kommutative Gruppe.
2. $(R, \cdot, 1)$ ist ein [kommutatives] Monoid.

Wir setzen $R^* := R \setminus \{0\}$. Der Ring $(R, +, 0, \cdot, 1)$ heißt

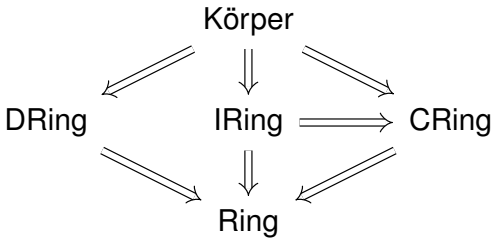
- **Divisionsring**, wenn $R^* < (R, \cdot, 1)$ eine Gruppe ist.
- **Körper**, wenn $R^* < (R, \cdot, 1)$ eine kommutative Gruppe ist.
- **Integritätsring**, wenn $R^* < (R, \cdot, 1)$ ein kommutatives Monoid ist.

Für den Ring $(R, +, 0, \cdot, 1)$ schreiben wir auch $(R, +, \cdot)$ oder kurz R.

Beispiele: Wir haben die Ringe $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ sowie $\mathbb{Z}/n\mathbb{Z}$.
Der Nullring $(\{0\}, +, 0, \cdot, 1)$ ist ein Ring, und zwar der einzige mit $1 = 0$.

Ringe und Körper: Definition

Überblick:



$(R, +, 0, \cdot, 1)$		$(R, +, 0)$				$(R, +, \cdot)$		$(R, \cdot, 1)$					
Name	Beispiele	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	$1 \neq 0$	Ntf	$\text{In}\mathring{\text{v}}$	Com
Körper	$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DRing	$\mathbb{H} \subset \mathbb{C}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
IRing	$\mathbb{Z}, \mathbb{Q}[X]$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
CRing	$\mathbb{Z}_n, \mathbb{R}^\Omega$	✓	✓	✓	✓	✓	✓	✓	✓				✓
Ring	$\mathbb{R}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓				

Statt explizit $(R, +, 0, \cdot, 1)$ schreiben wir auch kurz implizit $(R, +, \cdot)$;
die neutralen Elemente 0 und 1 sind daraus eindeutig rekonstruierbar.

Ringe und Körper: Definition

Hier steht „Ntf“ für Nullteilerfreiheit, also $a \neq 0 \wedge b \neq 0 \Rightarrow a \cdot b \neq 0$
bzw. äquivalent hierzu $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ für alle $a, b \in R$.

Ich nutze die bequemen Abkürzungen

- „DRing“ für Divisionsring (engl. *division ring*, *division algebra*),
- „IRing“ für Integritätsring (engl. *integral ring*, *integral domain*),
- „CRing“ für kommutativer Ring (engl. *commutative ring*).

Auch bei kommutativen Ringen möchte ich meist $1 \neq 0$ fordern,
ich scheue mich jedoch, dies in die Definition aufzunehmen.
Wir müssen es daher bei Bedarf jeweils explizit fordern.

Muss es wirklich so allgemein sein? Dazu gibt es sehr verschiedene Ansichten. Am liebsten wäre mir Lineare Algebra allein über Körpern.

Doch dieser Wunsch nach Einfachheit stößt sich schnell an der Realität: Eher früher als später benötigen wir Matrixringe und Polynomringe, etc.

Ich halte es daher für besser, Sie von Anfang an auf die nötige Vielfalt sanft vorzubereiten. Umso mehr schätzen wir die heile Welt der Körper.

Ringe und Körper: logische Spitzfindigkeit

In der Definition G2A eines Rings $(R, +, 0, \cdot, 1)$ muss die Kommutativität der Addition nicht gefordert werden, sie folgt aus den anderen Axiomen:

Aufgabe: Gegeben sei $(R, +, 0, \cdot, 1)$ mit $+, \cdot : R \times R \to R$ und $0, 1 \in R$, so dass beide Distributivgesetze gelten und zudem:

1. $(R, +, 0)$ ist eine Gruppe.
2. $(R, \cdot, 1)$ ist ein Monoid.

Dann ist $(R, +, 0)$ kommutativ und somit $(R, +, 0, \cdot, 1)$ ein Ring.

Lösung: Wir entwickeln $(1 + 1) \cdot (a + b)$ auf zwei Arten:

$$\begin{aligned}(1+1)\cdot(a+b) &\overset{\text{DR}}{=} 1\cdot(a+b)+1\cdot(a+b) &&\overset{\text{Ntr}}{=} a+b+a+b\\ (1+1)\cdot(a+b) &\overset{\text{DL}}{=} (1+1)\cdot a+(1+1)\cdot b\\ &\overset{\text{DR}}{=} 1\cdot a+1\cdot a+1\cdot b+1\cdot b &&\overset{\text{Ntr}}{=} a+a+b+b\end{aligned}$$

Wir addieren $-a$ von links, $-b$ von rechts und erhalten $a + b = b + a$.

Bemerkung: Hierzu genügt, dass $(R, +, 0)$ ein kürzbares Monoid ist.
Dasselbe Argument gilt also auch für Halbringe mit kürzbarer Addition.

Lemma G2B

In jedem Ring $(R, +, 0, \cdot, 1)$ gilt für alle $a, b \in R$:

1. $0 \cdot a = 0 = a \cdot 0$.
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$

Beweis: (1) Es gilt $0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$.
Addition von $-(0 \cdot a)$ ergibt $0 = 0 \cdot a$. Ebenso folgt $a \cdot 0 = 0$.

(2) Es gilt $(a \cdot b) + ((-a) \cdot b) = (a + (-a)) \cdot b = 0 \cdot b = 0$,
ebenso $(a \cdot b) + (a \cdot (-b)) = a \cdot (b + (-b)) = a \cdot 0 = 0$.

(3) Es folgt $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$. QED

Folgerung: Ist $(R, +, 0, \cdot, 1)$ ein Ring mit $1 = 0$, so folgt $R = \{0\}$,
denn für jedes Element $a \in R$ gilt dann $a = 1 \cdot a = 0 \cdot a = 0$.

Konvention: Wir sparen Klammern und schreiben $(a \cdot b) + c = a \cdot b + c$
(Punkt vor Strich). Für die Multiplikation schreiben wir statt $a \cdot b$ kurz ab.

Lemma G2C

In jedem Körper / Divisionsring / Integritätsring $(R, +, 0, \cdot, 1)$ gilt:

1. Die Menge R enthält mindestens zwei Elemente:
   $1 \neq 0$
2. Nullteilerfreiheit:
   $a \neq 0 \wedge b \neq 0 \;\Rightarrow\; a \cdot b \neq 0$
   $a \cdot b = 0 \;\Rightarrow\; a = 0 \vee b = 0$
3. Kürzbarkeit:
   $a \cdot x = a \cdot y \wedge a \neq 0 \;\Rightarrow\; x = y$
   $x \cdot a = y \cdot a \wedge a \neq 0 \;\Rightarrow\; x = y$

Beweis: (1) Das Untermonoid $R^* = R \setminus \{0\}$ enthält das Einselement 1.

(2) Abgeschlossenheit von $R^* < (R, \cdot, 1)$: Aus $a, b \in R^*$ folgt $a \cdot b \in R^*$.

(3) Aus $a \cdot x = a \cdot y$ folgt $0 = a \cdot x - a \cdot y = a \cdot (x - y)$.
Dank $a \neq 0$ und (2) folgt $x - y = 0$, somit $x = y$. QED

Satz G2D: allgemeine Distributivität und binomische Formeln

(1) In jedem Ring R gilt das allgemeine Distributivitätsgesetz:

$$\Big(\sum_{i\in I} a_i\Big) \cdot \Big(\sum_{j\in J} b_j\Big) = \sum_{(i,j)\in I\times J} a_i \cdot b_j = \sum_{i\in I}\sum_{j\in J} a_i b_j = \sum_{j\in J}\sum_{i\in I} a_i b_j$$

Seien $a, b \in R$ kommutierende Elemente, also $ab = ba$. Dann gilt

$$(a+b)^2 = a^2 + 2ab + b^2 \quad \text{und} \quad (a-b)(a+b) = a^2 - b^2.$$

Allgemein für alle $n \in \mathbb{N}$ gilt hierzu (2) der binomische Lehrsatz

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j$$

sowie (3) die geometrische Teleskopsumme

$$(a-b) \cdot \sum_{i=0}^{n} a^{n-i} b^i = a^{n+1} - b^{n+1}.$$

Beweis: (1) Induktion über die Elementezahl $\sharp I$ und $\sharp J$.

(2) Induktion über $n \in \mathbb{N}$ oder anschaulich wie in E2J.

(3) Induktion über $n \in \mathbb{N}$ oder anschaulich wie folgt:

$$\begin{aligned}(a-b) \cdot (a^n b^0 + a^{n-1} b^1 + \cdots + a^0 b^n) \\ = \quad a^{n+1} b^0 + a^n b^1 + \cdots + a^1 b^n \\ - a^n b^1 - \cdots - a^1 b^n - a^0 b^{n+1}\end{aligned}$$

In dieser Teleskopsumme löschen sich innere Terme paarweise aus.
Schließlich bleiben nur die beiden Randterme a^{n-1} und $-b^{n+1}$ stehen.

Beispiel: Für $q \in \mathbb{C}$ mit $q \neq 1$ gilt

$$1 + q + q^2 + \cdots + q^{n-1} = \frac{1 - q^n}{1 - q}.$$

Geometrische Reihe: Für $|q| < 1$ und $n \to \infty$ gilt $q^n \to 0$, und somit

$$\sum_{k=0}^{\infty} q^k \;=\; \lim_{n\to\infty} \sum_{k=0}^{n-1} q^k \;=\; \lim_{n\to\infty} \frac{1-q^n}{1-q} \;=\; \frac{1}{1-q}.$$

Homomorphismen von Ringen und Körpern

G209

Definition G2E: Homomorphismen von Ringen und Körpern

Seien $(R,+,0,\cdot,1)$ und $(S,+,0,\cdot,1)$ Ringe. Ein **Homomorphismus**

$$\varphi:(R,+,0,\cdot,1)\to(S,+,0,\cdot,1)$$

ist eine Abbildung $\varphi:R\to S$, sodass für alle $a,b\in R$ gilt:

$$\begin{aligned}\varphi(a+b)&=\varphi(a)+\varphi(b), & \varphi(0)&=0,\\ \varphi(a\cdot b)&=\varphi(a)\cdot\varphi(b), & \varphi(1)&=1.\end{aligned}$$

Ist φ zudem bijektiv, so nennen wir φ einen **Isomorphismus** (G1P).

Beispiele: Die Inklusionen $\mathbb{Z}\hookrightarrow\mathbb{Q}\hookrightarrow\mathbb{R}\hookrightarrow\mathbb{C}\hookrightarrow\mathbb{H}$ sind Ringhomomorphismen, ebenso die Quotientenabbildung $\mathbb{Z}\twoheadrightarrow\mathbb{Z}/n\mathbb{Z}$.

Beispiel: Die Konjugation $\overline{\ }:\mathbb{C}\to\mathbb{C}:x+\mathrm{i}y\mapsto x-\mathrm{i}y$ erfüllt $\overline{\overline{z}}=z$ sowie $\overline{z+w}=\overline{z}+\overline{w}$ und $\overline{z\cdot w}=\overline{z}\cdot\overline{w}$, ist also ein Automorphismus (A3B).

Beispiel: Die Abbildung $\varphi:\mathbb{Z}\to\mathbb{Z}:a\mapsto 0$ ist additiv und multiplikativ, erfüllt aber nicht $\varphi(1)=1$. Somit ist φ kein Ringhomomorphismus.

Homomorphismen von Ringen und Körpern

G210
Erläuterung

Lemma G2F: Komposition und Umkehrung

(0) Für jeden Ring $(R,+,0,\cdot,1)$ ist $\mathrm{id}_R:R\to R$ ein Homomorphismus.

(1) Ist $\varphi:(R,+,0,\cdot,1)\to(S,+,0,\cdot,1)$ und $\psi:(S,+,0,\cdot,1)\to(T,+,0,\cdot,1)$ ein Homomorphismus, so auch $\psi\circ\varphi:(R,+,0,\cdot,1)\to(T,+,0,\cdot,1)$.

(2) Ist $\varphi:(R,+,0,\cdot,1)\to(S,+,0,\cdot,1)$ ein bijektiver Homomorphismus, so auch $\psi=\varphi^{-1}:(S,+,0,\cdot,1)\to(R,+,0,\cdot,1)$.

Aufgabe: Beweisen Sie dies zur Wiederholung (G1P).

Unterringe und Unterkörper

G211

Definition G2G: Unterring und Unterkörper

Sei $(R,+,0,\cdot,1)$ ein Ring und darin $S\subseteq R$ eine Teilmenge.
Wir nennen S einen **Unterring** oder **Teilring**, kurz $S\leq R$, falls gilt:

1. $S\leq(R,+,0)$ ist eine Untergruppe, also $0\in S$ und $S-S\subseteq S$,
2. $S\leq(R,\cdot,1)$ ein Untermonoid, also $1\in S$ und $S\cdot S\subseteq S$.

In diesem Falle ist $(S,+_S,0,\cdot_S,1)$ selbst ein Ring, und die Inklusion $S\hookrightarrow R$ ist ein Ringhomomorphismus. Ist S zudem ein Körper, so nennen wir S einen **Unterkörper** oder **Teilkörper** in R.

Beispiele: $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}\subset\mathbb{H}$ sind Teilringe bzw. Teilkörper.
Die Menge $\mathbb{Q}[\sqrt{2}]=\{\,a+b\sqrt{2}\mid a,b\in\mathbb{Q}\,\}$ ist ein Teilkörper von $\mathbb{R}$.
Die Menge $\mathbb{Z}[\mathrm{i}]<\mathbb{C}$ ist ein Teilring, und $\mathbb{Q}[\mathrm{i}]<\mathbb{C}$ ist ein Teilkörper.

Beispiele: Im Matrixring $\mathbb{R}^{n\times n}$ ist $\mathbb{R}\cdot 1_{n\times n}$ ein Teilkörper.
Auch im Polynomring $\mathbb{R}[X]$ ist $\mathbb{R}\subseteq\mathbb{R}[X]$ ein Teilkörper.

Beispiel: Die Menge $2\mathbb{Z}\subset\mathbb{Z}$ ist kein Teilring, denn $1\notin 2\mathbb{Z}$.
Der Nullring $\{0\}\subset\mathbb{Z}$ ist kein Teilring von $\mathbb{Z}$, denn $1\notin\{0\}$.

Unterringe und Unterkörper

G212
Erläuterung

Wir betrachten hier Ringe mit Einselement. Daher verlangen wir von Homomorphismen und Unterringen, dass sie das Einselement erhalten.

Beispiel: Im Ring $(\mathbb{Z},+,0,\cdot,1)$ ist $\{0\}$ eine additive Untergruppe und multiplikativ abgeschlossen. Somit ist $(\{0\},+,0,\cdot,0)$ ein Ring, aber kein Unterring von $(\mathbb{Z},+,0,\cdot,1)$, da das Einselement nicht erhalten bleibt.

Bemerkung: Die Begriffe „Unterring“ und „Teilring“ sind synonym, geschrieben $S\leq R$, so wie „Untermenge“ und „Teilmenge“, $A\subseteq B$.

Im Falle $S\leq R$ nennen wir S einen **Unterring** von R und umgekehrt nennen wir R einen **Oberring** von S oder eine **Ringerweiterung**.

Im Falle $S\subsetneq R$ ist S ein **echter Unterring** von R, geschrieben $S<R$, oder umgekehrt gesagt, R ein **echter Oberring** von S, kurz $R>S$.

Beispiel: Der Körper $\mathbb{C}=\mathbb{R}[\mathrm{i}]\supset\mathbb{R}$ der komplexen Zahlen ist eine Körpererweiterung der reellen Zahlen. Gleiches gilt für $\mathbb{Q}[\sqrt{2}]\supset\mathbb{Q}$.

Die Begriffe „Unterkörper“ und „Oberkörper“ klingen zwar recht lustig, entsprechen aber ansonsten genau der Definition für Ringe.

Charakteristischer Unterring

G213

Satz G2H: charakteristscher Unterring und Charakteristik

Zu jedem Ring $(R,+,0,\cdot,1)$ existiert genau ein Ringhomomorphismus

$$\varphi : (\mathbb{Z},+,0,\cdot,1) \to (R,+,0,\cdot,1) : k \mapsto k\cdot 1_R = 1_R \cdot k$$

dank Satz G1T. Sein Bild in R ist der **charakteristische Unterring**

$$\mathrm{Char}(R) = \mathrm{Char}(R,+,\cdot) := \{\, k\cdot 1_R \mid k\in\mathbb{Z} \,\}.$$

Für den Kern gilt $\ker(\varphi) := \varphi^{-1}(\{0\}) = n\mathbb{Z}$ für ein $n\in\mathbb{N}$ dank G1V.
Daraus gewinnen wir den charakteristischen **Ringisomorphismus**

$$\bar\varphi : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{Char}(R) : [k] \mapsto k\cdot 1_R.$$

Wir nennen $\mathrm{char}(R) := n$ die **Charakteristik** des Rings R.
Ist R nullteilerfrei, so ist n prim, also $n\in\{0,2,3,5,7,11,13,\ldots\}$.

Beispiele: Für $\mathbb{K}=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{H}$ gilt $\mathrm{Char}(\mathbb{K})=\mathbb{Z}$ und $\mathrm{char}(\mathbb{K})=0$.
Für $R=\mathbb{Z}/n$, $(\mathbb{Z}/n)[X]$, $(\mathbb{Z}/n)^{s\times s}$ gilt $\mathrm{Char}(R)\cong\mathbb{Z}/n$ und $\mathrm{char}(R)=n$.

Charakteristischer Unterring

G214
Erläuterung

Anschaulich entsteht die Menge $\mathrm{Char}(R)$ aus dem Einselement 1 durch wiederholte Addition bzw. Subtraktion. Die elegantere Sichtweise ist der eindeutige Ringhomomorphismus $\varphi\colon\mathbb{Z}\to R$ mit Bild $\mathrm{im}(\varphi)=\mathrm{Char}(R)$.

Bemerkung: Somit ist $\mathrm{Char}(R)$ der kleinste Teilring von $(R,+,0,\cdot,1)$, denn jeder Teilring $S\le(R,+,0,\cdot,1)$ enthält 1 und somit $\mathrm{Char}(R)$.

🙂 In jedem noch so komplizierten Ring R finden wir einen sehr vertrauten Unterring $\mathbb{Z}/n\mathbb{Z}\cong\mathrm{Char}(R)$ dank des Isomorphismus $\bar\varphi$.

Freshman's dream: Frobenius–Endomorphismus

G215

Im Allgemeinen gilt $(a+b)^2 = a^2+2ab+b^2 \neq a^2+b^2$.
In Charakteristik 2 gilt $1+1=0$, also sind beide gleich!

Satz G2I: Frobenius–Endomorphismus in Charakteristik p

Sei $(R,+,\cdot)$ ein kommutativer Ring von Primcharakteristik $p>0$.
Dann ist die Abbildung

$$\mathfrak{f} = \mathfrak{f}_R : (R,+,\cdot) \to (R,+,\cdot) : a \mapsto a^p$$

ein Ringhomomorphismus, genannt **Frobenius–Endomorphismus**.

Beweis: Es gilt $\mathfrak{f}(a\cdot b) = (a\cdot b)^p = a^p\cdot b^p = \mathfrak{f}(a)\cdot\mathfrak{f}(b)$ sowie $\mathfrak{f}(1)=1$.
Die Addition ist interessant: Für alle $k\in\mathbb{N}$ mit $0<k<p$ gilt

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1} \in p\mathbb{Z},$$

denn die Primzahl p erscheint nur im Zähler, aber nicht im Nenner (A2J).
Dank G2D folgt $\mathfrak{f}(a+b) = \sum_{k=0}^{p}\binom{p}{k}a^k b^{p-k} = a^p+b^p = \mathfrak{f}(a)+\mathfrak{f}(b)$. QED

Freshman's dream: Frobenius–Endomorphismus

G216
Erläuterung

Beide Voraussetzungen des Satzes sind wesentlich: Primcharakteristik und Kommutativität. Hierzu ein einfaches, aber illustratives Beispiel:

Aufgabe: Sei $p\ge 2$ prim. In $\mathbb{Z}_p^{2\times 2}$ betrachten wir die Matrizen

$$E=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\quad A=\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right),\quad B=\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),\quad C=\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right).$$

Berechnen Sie A^n und B^n sowie $(E+A)^n$ und $(E+B)^n$ für $n\in\mathbb{N}$.
Für welche Exponenten $n\in\mathbb{N}$ gilt demnach $(E+A)^n = E^n+A^n$?
Vergleichen Sie $(A+B)^n$ mit A^n+B^n: Wann gilt hier Gleichheit?

Lösung: Es gilt $A^0=B^0=E$ und $A^n=B^n=0$ für $n\ge 2$.
Dank $EA=AE$ gilt $(E+A)^n=\sum_{k=0}^{n}\binom{n}{k}E^{n-k}A^k = E+nA$.
Für alle Exponenten $n\ge 2$ gilt andererseits $E^n+A^n=E$.
Also gilt $(E+A)^n = E^n+A^n$ genau dann, wenn $n\in\{1\}\cup p\mathbb{N}_{\ge 1}$.

Es gilt $A+B=C$ und $C^n=E$ für n gerade und $C^n=C$ für n ungerade.
Hingegen gilt $A^n+B^n=0$ für $n\ge 2$, also $(A+B)^n = A^n+B^n$ für $n=1$, aber nicht für $n\neq 1$. Selbst für $n=p$ gilt hier $(A+B)^p \neq A^p+B^p$.

Beispiel: Matrixringe

♦ Satz B1A: Matrixring über R

Sei $(R,+,0,\cdot,1)$ ein Ring und $n\in\mathbb{N}_{\geq 1}$ eine natürliche Zahl.
Die $n\times n$–Matrizen über R bilden den Ring $(R^{n\times n},\boldsymbol{+},0_{n\times n},\boldsymbol{\cdot},1_{n\times n})$:

$$\boldsymbol{+}: R^{n\times n}\times R^{n\times n}\to R^{n\times n} : (A,B)\mapsto C=A\boldsymbol{+}B,\ \ c_{ij}=a_{ij}+b_{ij},$$
$$\boldsymbol{\cdot}: R^{n\times n}\times R^{n\times n}\to R^{n\times n} : (A,B)\mapsto C=A\boldsymbol{\cdot}B,\ \ c_{ik}=\textstyle\sum_{j=1}^{n} a_{ij}\cdot b_{jk}.$$

Für $n\geq 2$ ist dieser Matrixring nicht kommutativ und hat Nullteiler:

$$\begin{bmatrix}1&0\\0&0\end{bmatrix}\boldsymbol{\cdot}\begin{bmatrix}0&1\\0&0\end{bmatrix}=\begin{bmatrix}0&1\\0&0\end{bmatrix}\quad\text{vs}\quad\begin{bmatrix}0&1\\0&0\end{bmatrix}\boldsymbol{\cdot}\begin{bmatrix}1&0\\0&0\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$$

In $R^{n\times n}$ liegt der Unterring $R\cdot 1_{n\times n}=\{\operatorname{diag}(a,\ldots,a)\mid a\in R\}$.
Dieser ist isomorph zum Koeffizientenring R dank der Einbettung

$$\varphi : R\xrightarrow{\sim} R\cdot 1_{n\times n} : a\mapsto a\cdot 1_{n\times n}.$$

Für die Charakteristik gilt demnach $\operatorname{char}(R^{n\times n})=\operatorname{char}(R)$.

Beispiel: Matrixringe

♦ Beispiel B1F: die komplexen Zahlen $\mathbb{C}$ als Matrizen über $\mathbb{R}$

Im Matrixring $(\mathbb{R}^{2\times 2},+,0_{2\times 2},\cdot,1_{2\times 2})$ ist die Teilmenge

$$C:=\left\{\,z=\left[\begin{smallmatrix}x&-y\\y&x\end{smallmatrix}\right]\;\middle|\;x,y\in\mathbb{R}\,\right\}$$

ein Unterkörper isomorph zu den komplexen Zahlen A3B:

$$(\mathbb{C},+,\cdot)\cong(C,+,\cdot)\ :\ x+\mathrm{i}y\rightleftarrows\left[\begin{smallmatrix}x&-y\\y&x\end{smallmatrix}\right]$$

♦ Beispiel B1G: die Quaternionen $\mathbb{H}$ als Matrizen über $\mathbb{C}$

Im Matrixring $(\mathbb{C}^{2\times 2},+,0_{2\times 2},\cdot,1_{2\times 2})$ ist die Teilmenge

$$H:=\left\{\,q=\left[\begin{smallmatrix}z&-w\\\overline{w}&\overline{z}\end{smallmatrix}\right]\;\middle|\;z,w\in\mathbb{C}\,\right\}=\mathbb{R}E+\mathbb{R}I+\mathbb{R}J+\mathbb{R}K$$
$$\text{mit}\quad E=\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right],\ I=\left[\begin{smallmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{smallmatrix}\right],\ J=\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right],\ K=\left[\begin{smallmatrix}0&-\mathrm{i}\\-\mathrm{i}&0\end{smallmatrix}\right]$$

ein Divisionsring isomorph zu Hamiltons Quaternionen A3D:

$$(\mathbb{H},+,\cdot)\cong(H,+,\cdot)\ :\ \alpha+\beta\mathrm{i}+\gamma\mathrm{j}+\delta\mathrm{k}\rightleftarrows\alpha E+\beta I+\gamma J+\delta K$$

Beispiel: Transposition

🙂 Die Konstruktion von $C<\mathbb{R}^{2\times 2}$ und $H<\mathbb{C}^{2\times 2}$ als Teilring ist eine enorme Arbeitsersparnis: Den Matrixring $K^{n\times n}$ über einem Ring K haben wir bereits allgemein konstruiert. Für C und H genügt dann die Prüfung der (wenigen!) Axiome eines Unterrings bzw. Unterkörpers!

Beispiel G2J: Transposition

Sei $(K,+,\cdot)$ ein kommutativer Ring. Dann ist die Transposition

$$^{\mathsf{T}} : K^{n\times n}\to K^{n\times n} : A\mapsto A^{\mathsf{T}}$$

ein Anti-Automorphismus: Statt Multiplikativität gilt entgegengesetzt

$$(A\boldsymbol{\cdot}B)^{\mathsf{T}}=B^{\mathsf{T}}\boldsymbol{\cdot}A^{\mathsf{T}}.$$

Beweis: Wir setzen die Definitionen ein und rechnen es nach:

$$\begin{aligned}(A\boldsymbol{\cdot}B)^{\mathsf{T}}_{ki}&=(A\boldsymbol{\cdot}B)_{ik}&&=\textstyle\sum_{j=1}^{n}a_{ij}\cdot b_{jk}\\(B^{\mathsf{T}}\boldsymbol{\cdot}A^{\mathsf{T}})_{ki}&=\textstyle\sum_{j=1}^{n}b^{\mathsf{T}}_{kj}\cdot a^{\mathsf{T}}_{ji}&&=\textstyle\sum_{j=1}^{n}b_{jk}\cdot a_{ij}\end{aligned}$$

Additivität $(A+B)^{\mathsf{T}}=A^{\mathsf{T}}+B^{\mathsf{T}}$ und Involution $(A^{\mathsf{T}})^{\mathsf{T}}=A$ sind klar. QED

Beispiel: Transposition-Konjugation

Beispiel G2K: Transposition-Konjugation

Sei $(R,+,\cdot)$ ein Ring und $^*: R\to R: a\mapsto a^*$ ein Anti-Automorphismus.
Zu $A=(a_{ij})_{ij}$ ist dann $A^\dagger=(a^*_{ij})_{ji}$ die transponiert-konjugierte Matrix.

Dies definiert einen Anti-Automorphismus $^\dagger: R^{n\times n}\to R^{n\times n}: A\mapsto A^\dagger$:
Statt Multiplikativität gilt entgegengesetzt $(A\boldsymbol{\cdot}B)^\dagger=B^\dagger\boldsymbol{\cdot}A^\dagger$.

Beweis: Wir setzen die Definitionen ein und rechnen es nach:

$$\begin{aligned}(A\boldsymbol{\cdot}B)^\dagger_{ki}&=(A\boldsymbol{\cdot}B)^*_{ik}&&=\textstyle\sum_{j=1}^{n}(a_{ij}\cdot b_{jk})^*\\(B^\dagger\boldsymbol{\cdot}A^\dagger)_{ki}&=\textstyle\sum_{j=1}^{n}(B^\dagger)_{kj}\cdot(A^\dagger)_{ji}&&=\textstyle\sum_{j=1}^{n}b^*_{jk}\cdot a^*_{ij}\end{aligned}$$

Additivität $(A+B)^\dagger=A^\dagger+B^\dagger$ und Involution $(A^\dagger)^\dagger=A$ sind klar. QED

Beispiele: Auf $\mathbb{K}=\mathbb{R},\mathbb{C},\mathbb{H}$ mit der Konjugation $a\mapsto a^*=\overline{a}$ erhalten wir den Anti-Automorphismus $^\dagger:\mathbb{K}^{n\times n}\to\mathbb{K}^{n\times n}: A\mapsto A^\dagger=\overline{A}^{\mathsf{T}}$. Speziell auf $C<\mathbb{R}^{2\times 2}$ ist $z=\left[\begin{smallmatrix}x&-y\\y&x\end{smallmatrix}\right]\mapsto z^{\mathsf{T}}=\left[\begin{smallmatrix}x&y\\-y&x\end{smallmatrix}\right]$ die komplexe Konjugation (B1F). Auf $H<\mathbb{C}^{2\times 2}$ ist $q\mapsto q^\dagger=\overline{q}^{\mathsf{T}}$ die quaternionische Konjugation (B1G).

Zentrum eines Rings

Zwei Elemente a, b im Ring R **kommutieren**, falls $ab = ba$ gilt.
Anders gesagt, ihr **Kommutator** $[a, b] := ab - ba$ ist gleich Null.

Das **Zentrum** des Rings $(R, +, 0, \cdot, 1)$ ist die Menge

$$Z(R) = Z(R, \cdot) = \{\, z \in R \mid \forall a \in R : az = za \,\}.$$

Anders gesagt, ein Element $z \in R$ ist **zentral** im Ring R,
falls z mit allen Elementen $a \in R$ kommutiert.

Satz G2L: Das Zentrum ist ein Unterring.

Das Zentrum $Z(R)$ ist ein kommutativer Unterring von $(R, +, 0, \cdot, 1)$.
Ist R zudem ein Divisionsring, so ist $Z(R)$ ein Unterkörper.

Beispiele: Genau dann gilt $Z(R) = R$, wenn R kommutativ ist.

Im Ring $\mathbb{H}$ der Quaternionen finden wir das Zentrum $Z(\mathbb{H}) = \mathbb{R}$.

Es gilt $Z(R^{n\times n}) = Z(R) \cdot 1_{n\times n} = \{\, \operatorname{diag}(a, \ldots, a) \mid a \in Z(R) \,\}$.

Zentrum eines Rings

Aufgabe: Rechnen Sie die Aussage des Satzes nach. Was ist zu tun?

Kartesisches Produkt mit koordinatenweiser Verknüpfung

Beispiel G2M: Produkt $R_1 \times \cdots \times R_n$ von Ringen

Ist $(R_i, +_i, 0_i, \cdot_i, 1_i)$ ein Ring für $i = 1, \ldots, n$, so auch

$$(R, +, 0, \cdot, 1) \quad \text{mit} \quad R = R_1 \times \cdots \times R_n \quad \text{und}$$
$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 +_1 b_1, \ldots, a_n +_n b_n),$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot_1 b_1, \ldots, a_n \cdot_n b_n),$$
$$\text{sowie} \quad 0 = (0_1, \ldots, 0_n) \quad \text{und} \quad 1 = (1_1, \ldots, 1_n).$$

Die Projektion $\operatorname{pr}_i : R \twoheadrightarrow R_i : a \mapsto a_i$ ist ein Ringhomomorphismus,
i.A. aber nicht die Einbettung $\iota_i : R_i \hookrightarrow R : a_i \mapsto (0_1, \ldots, a_i, \ldots, 0_n)$.

Für das Zentrum gilt $Z(R_1 \times \cdots \times R_n) = Z(R_1) \times \cdots \times Z(R_n)$.
Für $n \geq 2$ hat R Nullteiler, $(1, 0, 0, \ldots) \cdot (0, 1, 0, \ldots) = (0, 0, 0, \ldots)$.

Beweis: Geduldiges Nachrechnen (G1X). Übung! QED

Beispiel: Im Ring $R^{n\times n}$ ist $D = \{\, \operatorname{diag}(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in R \,\}$
ein Teilring isomorph zum Produktring $R^n = R \times \cdots \times R$.

Funktionen mit punktweiser Verknüpfung

Beispiel: Die reellen Funktionen $f : \mathbb{R}^n \supseteq \Omega \to \mathbb{R}$ bilden einen Ring
bezüglich punktweiser Addition und Multiplikation. Ausführlich:

Beispiel G2N: Potenz R^Ω eines Rings, Funktionenring

Sei Ω eine Menge. Ist $(R, +, \cdot)$ ein Ring, so auch die Potenz

$$(R, +, \cdot)^\Omega = (R^\Omega, \boldsymbol{+}, \boldsymbol{\cdot}) \text{ mit } R^\Omega = \operatorname{Abb}(\Omega, R) = \{\, f : \Omega \to R \,\},$$
$$(f \boldsymbol{+} g)(x) = f(x) + g(x) \text{ und } (f \boldsymbol{\cdot} g)(x) = f(x) \cdot g(x)$$

Hierbei ist $\operatorname{pr}_x : R^\Omega \twoheadrightarrow R : f \mapsto f(x)$ ein Ringhomomorphismus,
i.A. aber nicht $\iota_x : R \hookrightarrow R^\Omega : a \mapsto f$ mit $f(x) = a$ und $f(y) = 0$ für $y \neq x$.

Für das Zentrum gilt $Z(R^\Omega) = Z(R)^\Omega$. Für $\sharp\Omega \geq 2$ hat R^Ω Nullteiler.

In R^Ω liegen die Funktionen mit endlichem Träger, $R^{(\Omega)} \subseteq R^\Omega$.
Im Falle $\sharp\Omega = \infty$ ist $R^{(\Omega)}$ ein „Teilring ohne Eins“.

Beweis: Geduldiges Nachrechnen (G1Y). Übung! QED

Beispiel: Wir erhalten so den Funktionenring $\mathbb{R}^\mathbb{R} = \{\, f : \mathbb{R} \to \mathbb{R} \,\}$,
allgemein den Funktionenring R^R für jeden Ring $(R, +, 0, \cdot, 1)$.

Polynomringe: Definition

Definition G3A: Polynomring $K[X]$ über K in einer Variablen X

Sei $(R, +, 0, \cdot, 1)$ ein kommutativer Ring, $K \leq R$ ein Teilring und $X \in R$.

Wir nennen R einen **Polynomring** über dem Koeffizientenring $K \leq R$ in der Variablen $X \in R$, geschrieben $R = K[X]$, falls sich jedes Element $P \in R^*$ eindeutig schreiben lässt als eine Summe der Form

$$P = p_0 + p_1 X + p_2 X^2 + \cdots + p_n X^n$$

mit $n \in \mathbb{N}$ und $p_0, p_1, p_2, \ldots, p_n \in K$ sowie $p_n \neq 0$. Wir nennen P dann ein **Polynom** vom **Grad** $\deg(P) := n$ mit **Leitkoeffizient** $\mathrm{lc}(P) := p_n$.

Dabei heißt X^i das **$i$te Monom** in X und p_i der **$i$te Koeffizient** sowie $p_i X^i$ der **$i$te Term** des Polynoms P. Wir schreiben kurz

$$P = \sum_{i=0}^{n} p_i X^i = \sum_{i \in \mathbb{N}} p_i X^i = \sum_i p_i X^i$$

und vereinbaren dazu $p_i = 0$ für alle $i > n$.

Für das **Nullpolynom** $P = 0$ setzen wir $\deg(0) := -\infty$ und $\mathrm{lc}(0) := 0$.

Polynomringe: Addition und Multiplikation

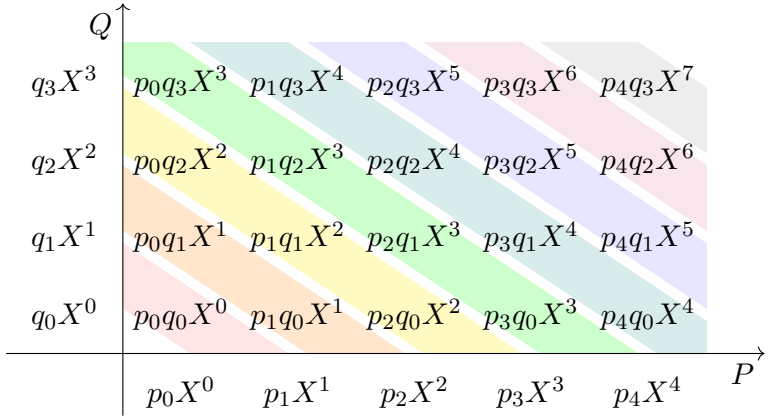
Die raffinierte Definition G3A impliziert sofort folgende Rechenregeln:

Vergleich: $\sum_i p_i X^i = \sum_i q_i X^i$ in $K[X] \;\Leftrightarrow\; p_i = q_i$ in K für alle i

Addition: $\left[\sum_i p_i X^i\right] + \left[\sum_i q_i X^i\right] = \sum_i (p_i + q_i) X^i$

Multiplikation: $\left[\sum_i p_i X^i\right] \cdot \left[\sum_j q_j X^j\right] = \sum_k r_k X^k,\; r_k = \sum_{i+j=k} p_i q_j$

Diese (endliche!) Summe durchläuft alle Paare $(i, j) \in \mathbb{N}^2$ mit $i + j = k$.



Rechenregeln für den Polynomgrad

Satz G3B: Rechenregeln für den Polynomgrad

(1) Für je zwei Polynome P und Q in $K[X]$ gilt:

$$\deg(P + Q) \leq \max\{\deg P, \deg Q\}$$

Gleichheit gilt genau dann, wenn $\deg P \neq \deg Q$ oder $\mathrm{lc}\, P + \mathrm{lc}\, Q \neq 0$.

(2) Für je zwei Polynome P und Q in $K[X]$ gilt:

$$\deg(P \cdot Q) \leq \deg P + \deg Q$$

Gleichheit gilt genau dann, wenn $P = 0$ oder $Q = 0$ oder $\mathrm{lc}\, P \cdot \mathrm{lc}\, Q \neq 0$. In diesem Fall gilt für die Leitkoeffizienten $\mathrm{lc}(P \cdot Q) = \mathrm{lc}\, P \cdot \mathrm{lc}\, Q$.

(3) Genau dann ist $K[X]$ ein Integritätsring, wenn K dies ist. Dann gilt:

$$\deg(P \cdot Q) = \deg(P) + \deg(Q)$$
$$\mathrm{lc}(P \cdot Q) = \mathrm{lc}(P) \cdot \mathrm{lc}(Q)$$

Rechenregeln für den Polynomgrad

Beweis: (1,2) Die beiden Ungleichungen sind klar. Die Bedingungen für Gleichheit folgen aus obigen Formeln für Addition und Multiplikation.

(3) „⇒“: Ist $K[X]$ nullteilerfrei, so auch der Unterring K.
„⇐“: Ist K nullteilerfrei, so auch $K[X]$ dank (2). QED

Beispiel: Wider Erwarten gilt nicht immer $\deg(PQ) = \deg P + \deg Q$.
In $\mathbb{Z}/6\mathbb{Z}[X]$ gilt $(\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{3}X) = \bar{1} + \bar{5}X + \bar{6}X^2 = \bar{1} + \bar{5}X$.
In $\mathbb{Z}/4\mathbb{Z}[X]$ gilt $(\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{2}X) = \bar{1} + \bar{4}X + \bar{4}X^2 = \bar{1}$.

☺ Über einem Integritätsring kann dieses Problem nicht auftreten!

Aufgabe: Für jeden Integritätsring K gilt $K[X]^\times = K^\times$.

Lösung: Die Inklusion $K[X]^\times \supseteq K^\times$ ist klar. Wir zeigen $K[X]^\times \subseteq K^\times$:
Für $P, Q \in K[X]$ mit $PQ = 1$ gilt $0 = \deg 1 = \deg(PQ) = \deg P + \deg Q$ dank (2), also $\deg P = \deg Q = 0$, somit $P, Q \in K^\times$.

Beispiele und Gegenbeispiele

Aufgabe: Für $S = \mathbb{Q}[\sqrt{2}] := \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$ gilt $\mathbb{Q} < S < \mathbb{R}$.
Ist S ein Polynomring über $\mathbb{Q} \leq S$ in der Variablen $x = \sqrt{2}$?

Lösung: Nein! Jedes Element $p \in S$ schreibt sich zwar als eine Summe $p = \sum_k p_k x^k$ mit $p_k \in \mathbb{Q}$, aber nicht eindeutig: $2x^0 - 1x^2 = 0$.

Aufgabe: Für $T = \mathbb{Q}[\mathrm{e}] := \{ \sum_k p_k \mathrm{e}^k \mid p_k \in \mathbb{Q} \}$ gilt $\mathbb{Q} < T < \mathbb{R}$.
Ist T ein Polynomring über $\mathbb{Q} \leq T$ in der Variablen $x = \mathrm{e}$?

Lösung: Ja! Jedes Element $p \in R$ schreibt sich als eine Summe $p = \sum_k p_k x^k$ mit $p_k \in \mathbb{Q}$, aber zwar eindeutig, denn e ist transzendent.

Aufgabe: Ist $\mathbb{R}$ ein Polynomring über $\mathbb{Q} \leq \mathbb{R}$ in einer Variablen $x \in \mathbb{R}$?

Lösung: Nein! Nicht jede reelle Zahl $r \in \mathbb{R}$ schreibt sich als Summe $r = \sum_k r_k x^k$ mit $r_k \in \mathbb{Q}$: Die Menge $\mathbb{Q}[x] = \bigcup_{n\in\mathbb{N}} \{ \sum_{k=0}^{n-1} p_k x^k \mid p_k \in \mathbb{Q} \}$ ist abzählbar (F2L), aber die gesamte Menge $\mathbb{R}$ ist überabzählbar (F2R).

🙂 Bitte lesen Sie noch einmal sorgfältig die raffinierte Definition G3A.
Diese Beispiele illustrieren eindrücklich ihre Flexibilität und Präzision.

Normierte Polynome

Ein Polynom $P \in K[X]$ heißt **normiert**, falls $\mathrm{lc}(P) = 1$ gilt.

$$\begin{aligned} K[X]^1_n &= \{ P \in K[X] \mid \deg P = n \wedge \mathrm{lc}\, P = 1 \} \\ K[X]_n &= \{ P \in K[X] \mid \deg P = n \} \\ K[X]_{\leq n} &= \{ P \in K[X] \mid \deg P \leq n \} \\ K[X]_{<n} &= \{ P \in K[X] \mid \deg P < n \} \end{aligned}$$

Durch Einschränkung erhalten wir folgende Verknüpfungen:

$$\begin{aligned} + &: K[X]_{\leq n} \times K[X]_{\leq n} \to K[X]_{\leq n} \\ \cdot &: K[X]_{\leq r} \times K[X]_{\leq s} \to K[X]_{\leq r+s} \end{aligned}$$

Normierung verhindert Auslöschung im höchsten Grad:

$$\begin{aligned} \cdot &: K[X]^1_r \times K[X]^1_s \to K[X]^1_{r+s} \\ \cdot &: K[X]^1_r \times K[X]_s \to K[X]_{r+s} \\ \cdot &: K[X]_r \times K[X]^1_s \to K[X]_{r+s} \end{aligned}$$

Polynom und Polynomfunktion

Definition G3C: Jedes Polynom definiert eine Polynomfunktion.

Jedes Polynom $P(X) = \sum_{i=0}^n p_i X^i$ in $K[X]$ definiert eine Funktion

$$f_P : K \to K : a \mapsto P(a) = \sum_{i=0}^n p_i a^i.$$

Wir nennen f_P die **Polynomfunktion** des Polynoms P.

Beispiel: Für $P = X^2 + X \in \mathbb{Z}_2[X]$ gilt $P(0) = P(1) = 0$, also $f_P = 0$.
⚠ Für das Polynom gilt $P \neq 0$, und dennoch $f_P = 0$. Wir unterscheiden sorgsam zwischen Polynom $P \in K[X]$ und Funktion $f_P : K \to K$.

Definition G3C: Polynomfunktion für Matrizen (Fortsetzung)

Ebenso können wir in $P(X)$ eine quadratische Matrix einsetzen:

$$F_P : K^{m\times m} \to K^{m\times m} : A \mapsto P(A) = \sum_{i=0}^n p_i A^i.$$

Beispiel: Für $A = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right] \in \mathbb{Z}_2^{2\times 2}$ gilt $P(A) = A^2 + A = 0 + A = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$.

Polynom und Polynomfunktion

Satz G3D: Polynom und Polynomfunktion

Weiterhin sei $(K, +, \cdot)$ ein kommutativer Ring. Die Zuordnung

$$f : K[X] \to \mathrm{Abb}(K, K) : P \mapsto f_P$$

ist ein Ringhomomorphismus (siehe G2N). Das heißt ausführlich:
Es gilt $f_0 = 0$ und $f_{P+Q} = f_P + f_Q$ sowie $f_1 = 1$ und $f_{P\cdot Q} = f_P \cdot f_Q$.

Dasselbe gilt entsprechend für Matrizen:

$$F : K[X] \to \mathrm{Abb}(K^{m\times m}, K^{m\times m}) : P \mapsto F_P$$

Übung: Rechnen Sie die Eigenschaften sorgsam nach:

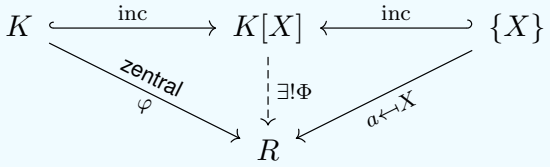
$$\begin{aligned} f_{P+Q}(a) &\overset{\text{Def}}{=} (P+Q)(a) \overset{!}{=} P(a) + Q(a) \overset{\text{Def}}{=} f_P(a) + f_Q(a) \\ f_{P\cdot Q}(a) &\overset{\text{Def}}{=} (P\cdot Q)(a) \overset{!}{=} P(a) \cdot Q(a) \overset{\text{Def}}{=} f_P(a) \cdot f_Q(a) \end{aligned}$$

🙂 Diese Beispiele sind Spezialfälle des folgenden Satzes.

Die universelle Abbildungseigenschaft des Polynomrings

Satz G3E: universelle Abbildungseigenschaft (UAE)

Sei $(K,+,\cdot)$ ein kommutativer Ring und $(R,+,\cdot)$ ein Ring sowie $\varphi\colon K\to R$ ein Ringhomomorphismus mit $\varphi(K)\subseteq Z(R)$.



Zu jedem Element $a\in R$ existiert genau einen Ringhomomorphismus $\Phi\colon K[X]\to R$ mit $\Phi|_K=\varphi$ und $\Phi(X)=a$. Dieser ist gegeben durch

$$\Phi(p_0+p_1X+\cdots+p_nX^n)=\varphi(p_0)+\varphi(p_1)a+\cdots+\varphi(p_n)a^n.$$

Wir nennen $\Phi=\Phi_a=\Phi_{X\mapsto a}$ den **Einsetzungshomomorphismus**.

Die universelle Abbildungseigenschaft des Polynomrings

Eindeutigkeit: Sind $\Phi,\Psi\colon K[X]\to R$ zwei Ringhomomorphismen mit $\Phi|_K=\Psi|_K=\varphi$ und $\Phi(X)=\Psi(X)=a$, so gilt $\Phi=\Psi$, denn:

$$\Phi(\textstyle\sum_i p_iX^i)\overset{\text{add}}{=}\sum_i\Phi(p_iX^i)\overset{\text{mult}}{=}\sum_i\Phi(p_i)\Phi(X)^i\underset{X\mapsto a}{\overset{\varphi}{=}}\sum_i\varphi(p_i)a^i$$

$$\Psi(\textstyle\sum_i p_iX^i)\overset{\text{add}}{=}\sum_i\Psi(p_iX^i)\overset{\text{mult}}{=}\sum_i\Psi(p_i)\Psi(X)^i\underset{X\mapsto a}{\overset{\varphi}{=}}\sum_i\varphi(p_i)a^i$$

Das beweist die Eindeutigkeit und gibt uns auch schon einen Hinweis, wie wir die ersehnte Abbildung $\Phi\colon K[X]\to R$ konstruieren müssen:

Existenz: Wir konstruieren $\Phi\colon K[X]\to R$ wie folgt: Jedes Element $P\in K[X]$ schreibt sich nach Definition G3A eindeutig als Summe $P=\sum_i p_iX^i$ mit $p_i\in K$. Wir setzen dann $\Phi(P):=\sum_i\varphi(p_i)a^i$.

Homomorphie: Damit ist die Eindeutigkeit gezeigt und die (einzig mögliche) Abbildung $\Phi\colon K[X]\to R$ konstruiert. Es bleibt nun noch nachzuweisen, dass Φ tatsächlich ein Ringhomomorphismus ist.

Die universelle Abbildungseigenschaft des Polynomrings

Es gilt $\Phi(0)=\varphi(0)=0$ und $\Phi(1)=\varphi(1)=1$.

Für die Addition finden wir:

$$\begin{aligned}\Phi\big([\textstyle\sum_i p_iX^i]+[\sum_i q_iX^i]\big)&=\Phi\big(\sum_i[p_i+q_i]X^i\big)\\&=\textstyle\sum_i\varphi(p_i+q_i)a^i\end{aligned}$$

$$\begin{aligned}\Phi\big(\textstyle\sum_i p_iX^i\big)+\Phi\big(\sum_i q_iX^i\big)&=\big[\textstyle\sum_i\varphi(p_i)a^i\big]+\big[\sum_i\varphi(q_i)a^i\big]\\&=\textstyle\sum_i\big[\varphi(p_i)+\varphi(q_i)\big]a^i\end{aligned}$$

Für die Multiplikation finden wir entsprechend:

$$\begin{aligned}\Phi\big([\textstyle\sum_i p_iX^i]\cdot[\sum_j q_jX^j]\big)&=\Phi\big(\sum_k\big[\sum_{i+j=k}p_iq_j\big]X^k\big)\\&=\textstyle\sum_k\big[\sum_{i+j=k}\varphi(p_iq_j)\big]a^k\big)\end{aligned}$$

$$\begin{aligned}\Phi\big(\textstyle\sum_i p_iX^i\big)\cdot\Phi\big(\sum_j q_jX^j\big)&=\big[\textstyle\sum_i\varphi(p_i)a^i\big]\cdot\big[\sum_j\varphi(q_j)a^j\big]\\&=\textstyle\sum_k\big[\sum_{i+j=k}\varphi(p_i)\varphi(q_j)\big]a^k\big)\end{aligned}$$

Hier nutzen wir, dass alle $b\in\varphi(K)$ mit $a\in R$ kommutieren. QED

Die universelle Abbildungseigenschaft des Polynomrings

Diese sorgsame Rechnung ist länglich, aber nicht wirklich schwer. So ist es oft bei grundlegenden Überprüfungen: Ihre Ausführung ist nahezu mechanisch, aber auch dies muss erledigt werden.

Wir sehen dabei kleinste Details, die sonst leicht übersehen werden, hier dass a mit allen Koeffizienten $b\in\varphi(K)$ kommutieren muss. Genau dazu dient die technische Voraussetzung $\varphi(K)\leq Z(R)$.

Auch dies ist ein allgemeines Phänomen: Durch die Ausführung des Beweises verstehen Sie den Satz wesentlich besser, Voraussetzung und Folgerung! Und Sie sehen, dass der Beweis gar nicht schwer ist.

Das Gegenstück hierzu sind gute Beispiele und Gegenbeispiele. Diesen wenden wir uns nun anschließend zu.

Erste Anwendungen der universellen Abbildungseigenschaft

Dank UAE (Satz G3E) haben wir die Ring-Endomorphismen

$$F_p : K[X] \to K[X] : X \mapsto X^p \quad \text{für } p \in \mathbb{N},$$

wobei stillschweigend $F_p|_K = \mathrm{id}_K$ gelte.

Aufgabe: Es gilt $F_1 = \mathrm{id}_{K[X]}$ und $F_p \circ F_q = F_{p\cdot q}$ für alle $p, q \in \mathbb{N}$.

Lösung: Dank Eindeutigkeit gilt $F_1 = \mathrm{id}_{K[X]}$ und $F_p \circ F_q = F_{pq}$:

$$(F_p \circ F_q)(X) = F_p(F_q(X)) = F_p(X^q) = (X^p)^q = X^{pq} = F_{pq}(X).$$

Ausführlich: Beide Abbildungen $F_p \circ F_q$ und F_{pq} sind Endomorphismen des Rings $K[X]$, eingeschränkt auf K sind beide die Identität, und beide bilden die Variable X gleich ab, denn $(F_p \circ F_q)(X) = F_{pq}(X)$.
Dank der Eindeutigkeitsaussage von Satz G3E folgt $F_p \circ F_q = F_{p\cdot q}$.

Erste Anwendungen der universellen Abbildungseigenschaft

Dank UAE (Satz G3E) haben wir die Ring-Endomorphismen

$$G_a : K[X] \to K[X] : X \mapsto X + a \quad \text{für } a \in K,$$

wobei stillschweigend $G_a|_K = \mathrm{id}_K$ gelte.

Aufgabe: Es gilt $G_0 = \mathrm{id}_{K[X]}$ und $G_a \circ G_b = G_{a+b}$ für alle $a, b \in K$.

Lösung: Dank Eindeutigkeit gilt $G_0 = \mathrm{id}_{K[X]}$ und $G_a \circ G_b = G_{a+b}$:

$$(G_a \circ G_b)(X) = G_a(G_b(X)) = G_a(X + b) = (X + a) + b$$
$$= X + (a + b) = G_{a+b}(X).$$

Beide Abbildungen $G_a \circ G_b$ und G_{a+b} sind Endomorphismen des Rings $K[X]$, eingeschränkt auf K sind beide die Identität, und beide bilden die Variable X auf dasselbe Element ab, denn $(G_a \circ G_b)(X) = G_{a+b}(X)$.
Dank der Eindeutigkeitsaussage von Satz G3E folgt $G_a \circ G_b = G_{a+b}$.

Insbesondere gilt demnach $G_a \circ G_{-a} = G_{a-a} = G_0 = \mathrm{id}_{K[X]}$.
Somit ist G_a ein Ringautomorphismus mit $G_a^{-1} = G_{-a}$.

Eindeutigkeit des Polynomrings bis auf Isomorphismus

Korollar G3F: Eindeutigkeit bis auf Isomorphismus

Je zwei Polynomringe $K[X]$ und $K[Y]$ sind kanonisch isomorph.
Es existiert genau ein Isomorphismus $(\varphi, \psi) : K[X] \cong K[Y]$
mit $\varphi|_K = \psi|_K = \mathrm{id}_K$ sowie $\varphi(X) = Y$ und $\psi(Y) = X$.

Beweis: Dank Satz G3E existiert je genau ein Ringhomomorphismus

$$\varphi : K[X] \to K[Y] : X \mapsto Y \quad \text{mit} \quad \varphi|_K = \mathrm{id}_K,$$
$$\psi : K[Y] \to K[X] : Y \mapsto X \quad \text{mit} \quad \psi|_K = \mathrm{id}_K\,.$$

Dank Eindeutigkeit in G3E gilt $\psi \circ \varphi = \mathrm{id}_{K[X]}$ und $\varphi \circ \psi = \mathrm{id}_{K[Y]}$. QED

Eindeutigkeit des Polynomrings bis auf Isomorphismus

Bemerkung: Erst die Präzisierung $\varphi|_K = \psi|_K = \mathrm{id}_K$ sowie die Wahl $\varphi(X) = Y$ und $\psi(Y) = X$ legen den Isomorphismus (φ, ψ) fest.

Auch $X \mapsto Y + 1$ und $Y \mapsto X - 1$ liefert einen Isomorphismus,
wie in der vorigen Aufgabe allgemein ausgeführt.

Auch $\varphi : \mathbb{C}[X] \to \mathbb{C}[Y] : X \mapsto Y$ mit $\varphi|_{\mathbb{C}} = \mathrm{conj}$ ist ein Isomorphismus;
hier werden die Koeffizienten nicht festgehalten, sondern konjugiert.

🙂 Satz G3E ist das Universalwerkzeug zur Konstruktion von Ringhomomorphismen $\Phi : K[X] \to R$ und trägt daher zurecht den klangvollen Namen „universelle Abbildungseigenschaft“, kurz UAE.

Konstruktion des Polynomrings

Satz G3G: Existenz des Polynomrings

Zu jedem kommutativen Ring $(K, +, 0, \cdot, 1)$
existiert ein Polynomring $(K[X], +, 0, \cdot, 1)$.

Beweis: Wir betrachten die Menge

$$R = K^{(\mathbb{N})} = \{\, a : \mathbb{N} \to K : i \mapsto a_i \mid \sharp\,\mathrm{supp}(a) < \infty \,\}$$

der Folgen $a = (a_0, a_1, a_2, \dots)$ mit Werten $a_i \in K$ und endlichem Träger.
Das bedeutet, es existiert ein $n \in \mathbb{N}$, sodass $a_i = 0$ für alle $i > n$ gilt.
Somit liegt $\deg(p) := \sup\{\, n \in \mathbb{N} \mid p_n \neq 0 \,\}$ in der Menge $\mathbb{N} \cup \{-\infty\}$.

Auf der Menge R definieren wir Summe und Produkt wie oben gesehen:

$$+_R \;:\; R \times R \to R \;:\; (a,b) \mapsto s = a +_R b, \quad s_i = a_i + b_i$$
$$\cdot_R \;:\; R \times R \to R \;:\; (a,b) \mapsto p = a \cdot_R b, \quad p_k = \textstyle\sum_{i+j=k} a_i \cdot b_j$$

Man rechnet nun geduldig nach, dass $(R, +_R, 0_R, \cdot_R, 1_R)$ tatsächlich
ein kommutativer Ring ist, mit $0_R = (0, 0, 0, \dots)$ und $1_R = (1, 0, 0, \dots)$.

Konstruktion des Polynomrings

☺ Genau so implementieren wir Polynome auf dem Computer.
Das so definierte Produkt von Folgen heißt das **Faltungsprodukt**.
Es entspricht genau dem Vorbild von Polynomen und tut, was es soll.
Die hierzu nötigen Rechnungen sind länglich, aber leicht: Übung!
Wir haben die analogen Überprüfungen für Matrizen ausgeführt.

Die Abbildung $\iota : K \to R : a \mapsto (a, 0, 0, \dots)$ ist ein Ringhomomorphismus
und injektiv. Mittels ι identifizieren wir nun den Koeffizientenring K mit
dem Teilring $\iota(K) < R$; fortan schreiben wir kurz $K < R$ als Teilring.
Statt $(R, +_R, 0_R, \cdot_R, 1_R)$ schreiben wir bequemer $(R, +, 0, \cdot, 1)$.

Speziell für das Element $X = (0, 1, 0, 0, \dots)$ gilt $X^0 = (1, 0, 0, 0, \dots)$,
$X^1 = (0, 1, 0, 0, \dots)$, $X^2 = (0, 0, 1, 0, \dots)$, usw. Jedes Element $p \in R$
schreibt sich somit eindeutig als eine (endliche) Summe der Form

$$p = \textstyle\sum_{i \in \mathbb{N}} p_i X^i.$$

Somit ist R ein Polynomring über $K < R$ in der Variablen X. QED

Was bedeutet identifizieren?

Es entsteht hier ein kleines, technisches Problem: Wir haben eine
Einbettung $\iota : K \hookrightarrow R$, wollen aber eine Teilmenge $K \subseteq R$. Dies tritt
immer wieder auf, daher erkläre ich exemplarisch, wie wir dies lösen.

Wir wollen identifizieren vermöge $\iota : K \xrightarrow{\sim} \iota(K) \subseteq R$.
Die einfachste Möglichkeit ist der **Austausch der Elemente**.
Wir nehmen K und R als disjunkt an, wie im obigen Beispiel.

Wir betrachten $R' = (R \setminus \iota(K)) \cup K$, das heißt, wir entfernen die
Elemente $\iota(K)$ und ersetzen sie durch K. Wir nutzen die Bijektion
$\varphi : R' \xrightarrow{\sim} R$ mit $\varphi(a) = \iota(a)$ für $a \in K$ und $\varphi(b) = b$ für $b \in R \setminus \iota(K)$.

Damit können wir die Ringstruktur von R auf R' verpflanzen,
sodass $\varphi : (R', +, \cdot) \xrightarrow{\sim} (R, +, \cdot)$ ein Ringisomorphismus wird:

$$a' + b' := \varphi^{-1}\big(\varphi(a') + \varphi(b')\big), \qquad a' \cdot b' := \varphi^{-1}\big(\varphi(a') \cdot \varphi(b')\big)$$

Die Ringe $(R, +, \cdot)$ und $(R', +, \cdot)$ sind im Wesentlichen gleich,
wir haben lediglich die Elemente $\iota(K)$ gegen K ausgetauscht.
Nun ist $K \leq R'$ tatsächlich ein Teilring.

Wozu führen wir diese Konstruktion aus?

Polynomringe sind eine grundlegende und allgegenwärtige Konstruktion
überall in der Mathematik. Wir üben uns daher in der gebotenen Sorgfalt
und erläutern das mathematische Vorgehen im Detail.

Die Definition G3A legt fest, was genau wir von Polynomen verlangen.
Die universelle Abbildungseigenschaft G3E garantiert anschließend
die Eindeutigkeit des Polynomrings bis auf Isomorphismus G3F.

Eine kritische Leserin muss jedoch befürchten, dass unsere
Forderungen gar nicht erfüllbar sind, zumindest nicht immer,
etwa weil wir zu viele und widersprüchliche Anforderungen stellen.

Der Satz G3G versichert uns, dass unser Wunsch erfüllbar ist. Wie
können wir das beweisen, nachvollziehbar und lückenlos begründen?
Die **Existenz** des gewünschten Rings $K[X]$ beweisen wir durch seine
Konstruktion. Nach Definition G3A ist jedes Polynom $P = \sum_i p_i X^i$
eindeutig durch seine Koeffizientenfolge $p = (p_0, p_1, p_2, \dots) \in K^{(\mathbb{N})}$
festgelegt. Wir können also einfach mit Folgen rechnen. Die Ausführung
dieser Idee ist nun leicht, und erfordert lediglich Sorgfalt und Geduld.

Polynome in mehreren Variablen

Genauso konstruiert man den Polynomring in zwei Variablen X, Y:

$$K[X,Y] = \left\{ \sum_{(i,j)\in\mathbb{N}^2} p_{i,j} X^i Y^j \;\middle|\; p_{i,j} \in K \right\}$$

Dabei gilt $K[X,Y] = K[X][Y] = K[Y][X]$, denn

$$\sum_{(i,j)\in\mathbb{N}^2} p_{i,j} X^i Y^j = \sum_{j\in\mathbb{N}} \Big[\sum_{i\in\mathbb{N}} p_{i,j} X^i\Big] Y^j = \sum_{i\in\mathbb{N}} \Big[\sum_{j\in\mathbb{N}} p_{i,j} Y^j\Big] X^i.$$

Auch Polynome in drei Variablen X, Y, Z gelingen ebenso:

$$K[X,Y,Z] = \left\{ \sum_{(i,j,k)\in\mathbb{N}^3} p_{i,j,k} X^i Y^j Z^k \;\middle|\; p_{i,j,k} \in K \right\}$$

Selbst Polynome in beliebig vielen Variablen $(X_i)_{i\in I}$ sind möglich.
Wir nutzen dann Multiindizes $\nu \in \mathbb{N}^{(I)}$ und Monome $X^\nu = \prod_{i\in I} X_i^{\nu_i}$:

$$K\big[(X_i)_{i\in I}\big] = \left\{ \sum_{\nu\in\mathbb{N}^{(I)}} p_\nu X^\nu \;\middle|\; p_\nu \in K \right\}.$$

☺ Grundlegend ist die eindeutige Darstellung als solch eine Summe.
Definition und Konstruktion übertragen sich wörtlich auf diesen Fall.
Statt des Modells $K^{(\mathbb{N})}$ betrachtet man entsprechend $K^{(\mathbb{N}^{(I)})}$.

Polynome in mehreren Variablen

Polynome in mehreren Variablen

Polynome in mehreren Variablen

Euklidische Division für Polynome

Aufgabe: Berechnen Sie im Polynomring $\mathbb{Z}[X]$ die euklidische Division von $S = 2X^4 - 5X^3 + 2X^2 - 9X + 8$ durch $P = X^2 - 3X$.

Lösung: Schriftliche Polynomdivision

$$
\begin{array}{rl}
2X^4 - 5X^3 + 2X^2 & -9X + 8 = \left(X^2 - 3X\right)\left(2X^2 + X + 5\right) + 6X + 8 \\
\underline{-2X^4 + 6X^3} & \\
X^3 + 2X^2 & \\
\underline{-X^3 + 3X^2} & \\
5X^2 & -9X \\
\underline{-5X^2 + 15X} & \\
6X + 8 &
\end{array}
$$

Wir erhalten den Quotienten $Q = 2X^2 + X + 5$ mit Rest $R = 6X + 8$.

Euklidische Division für Polynome

Aus der Grundschule kennen Sie die schriftliche Division von natürlichen Zahlen in Basis $B = 10$. Das Verfahren verläuft genauso, doch durch den Übertrag kommt es vor, dass man die nächste Ziffer überschätzt.

Die Polynomdivision in $K[X]$ ist wesentlich leichter als die Division in $\mathbb{N}$. Subjektiv mag es Ihnen umgekehrt erscheinen, weil Sie die Division in $\mathbb{N}$ schon seit Ihrer Kindheit kennen, die Polynomdivision erst kürzer. Objektiv gesehen ist die erste schwerer als die zweite.

Übung: Wenn Sie gerne programmieren, dann können Sie beide Divisionen als Übung implementieren: die Division von Polynomen $\sum_i a_i X^i$ und von natürlichen Zahlen $\sum_i a_i B^i$. Sie werden sehen: Polynome sind leichter als Zahlen!

Euklidische Division für Polynome

Hier noch ein berühmtes Beispiel, die sogenannte geometrische Teleskopsumme; für die allgemeinen Formel siehe Satz G2D:

$$
\begin{array}{rl}
\left(X^5 \right. & \left. - 1\right) : \left(X - 1\right) = X^4 + X^3 + X^2 + X + 1 \\
\underline{-X^5 + X^4} & \\
X^4 & \\
\underline{-X^4 + X^3} & \\
X^3 & \\
\underline{-X^3 + X^2} & \\
X^2 & \\
\underline{-X^2 + X} & \\
X - 1 & \\
\underline{-X + 1} & \\
0 &
\end{array}
$$

Euklidische Division für Polynome

Die Division von Polynomen gelingt über jedem kommutativen Ring K, wir benötigen lediglich, dass der Leitkoeffizient $\mathrm{lc}(P)$ in K invertierbar ist. In den obigen Beispielen war P normiert, also $\mathrm{lc}(P) = 1$.

Euklidische Division für Polynome

Satz G3H: euklidische Division für Polynome

Sei $P \in K[X]$ ein Polynom mit invertierbarem Leitkoeffizient $\operatorname{lc} P \in K^\times$.
Zu jedem $S \in K[X]$ existiert genau ein Paar $Q, R \in K[X]$, für das gilt

$$S = PQ + R \quad \text{und} \quad \deg R < \deg P.$$

Wir nennen $S \operatorname{quo} P := Q$ den **Quotienten** und $S \operatorname{rem} P := R$ den **Rest** der euklidischen Division von S durch P. Dies definiert die Operationen

$$(\operatorname{quo}, \operatorname{rem}) : K[X] \times K[X]_n^1 \to K[X] \times K[X]_{<n} : (S, P) \mapsto (Q, R).$$

Eindeutigkeit: Angenommen die Polynome $Q, Q', R, R' \in K[X]$ erfüllen $S = PQ + R = PQ' + R'$ und $\deg R, \deg R' < \deg P$.

Dann gilt $P(Q - Q') = R' - R$. Dank $\operatorname{lc} P \in K^\times$ und Satz G3B folgt:

$$\deg P + \deg(Q - Q') = \deg(R' - R) < \deg P.$$

Daraus folgt $\deg(Q - Q') < 0$, also $Q - Q' = 0$, und somit $R' - R = 0$.

Euklidische Division für Polynome

Die **Existenz** von (Q, R) beweisen wir durch Konstruktion wie folgt:

Algo G3H: Division mit Rest von zwei Polynomen

Eingabe: $S, P \in K[X]$ mit $\operatorname{lc} P \in K^\times$
Ausgabe: $Q, R \in K[X]$ mit $S = PQ + R$ und $\deg R < \deg P$

```
1: Q ← 0; R ← S                                  // Invariante S = PQ + R
2: while deg R ≥ deg P do                        // Solange noch etwas zu tun ist
3:     T ← lc(P)^{-1} lc(R) · X^{deg R − deg P}  // deg(PT) = deg R, lc(PT) = lc R
4:     R ← R − PT; Q ← Q + T                     // Invariante S = PQ + R
5: return (Q, R)                                 // S = PQ + R und deg R < deg P
```

Beweis: Dieser Algorithmus ist korrekt, erfüllt also seine Spezifikation:

1. Der Algorithmus terminiert, denn $\deg R$ sinkt in jeder Iteration.
2. Die Rückgabe (Q, R) erfüllt $S = PQ + R$ und $\deg R < \deg P$.

Aufgabe: Führen Sie die Argumente sorgfältig aus.
Wenn Sie den Algorithmus auf das obige Beispiel an.

Euklidische Division für Polynome

Lösung: (1) Der Term T ist so gewählt, dass R und PT gleichen Grad und gleichen Leitkoeffizienten haben. Also gilt $\deg(R - PT) < \deg R$.
Der Algorithmus endet nach höchstens $1 + \deg S - \deg P$ Iterationen.

(2) Die Initialisierung $Q \leftarrow 0$, $R \leftarrow S$ garantiert, dass $S = PQ + R$.
Jede Iteration $R \leftarrow R - PT$, $Q \leftarrow Q + T$ erhält diese Gleichung.
Zum Schluss gilt also $S = PQ + R$ mit $\deg R < \deg P$, wie gewünscht.

Aufgabe: Formulieren Sie alternativ einen Induktionsbeweis über $\deg S$.

Beide sind logisch äquivalent; die induktive Form ist in der Mathematik geläufiger, die iterative Form in der Informatik. Das ist sehr praktisch!

Lösung: Für $\deg S < \deg P$ genügt $(Q, R) = (0, S)$. Sei $\deg S \geq \deg P$ und die Aussage gelte für alle Polynome $\tilde{S} \in K[X]$ mit $\deg \tilde{S} < \deg S$.
Wir setzen $T = \operatorname{lc}(P)^{-1} \operatorname{lc}(S) \cdot X^{\deg S - \deg P} \in K[X]$ und $\tilde{S} = S - PT$.
Damit gilt $\deg(PT) = \deg S$ und $\operatorname{lc}(PT) = \operatorname{lc} S$, also $\deg \tilde{S} < \deg S$.
Nach Induktionsvoraussetzung gibt es $\tilde{Q}, R \in R[X]$ mit $\tilde{S} = P\tilde{Q} + R$ und $\deg R < \deg P$. Daher gilt $S = \tilde{S} + PT = PQ + R$ für $Q = \tilde{Q} + T$.

Euklidische Division für Polynome

Bemerkung: Für jedes Polynom P mit Grad $\deg P = n \in \mathbb{N}$ und invertierbarem Leitkoeffizienten $\operatorname{lc} P \in K^\times$ erhalten wir eine Bijektion

$$K[X] \times K[X]_{<n} \xrightarrow{\sim} K[X] : (Q, R) \mapsto S = PQ + R.$$

Die Voraussetzung $\operatorname{lc} P \in K^\times$ ist hierbei wesentlich. Gegenbeispiel:
Im Ring $K = \mathbb{Z}$ der ganzen Zahlen ist 2 nicht invertierbar, die Abbildung $\mathbb{Z}[X] \times \mathbb{Z}[X]_{<0} \to \mathbb{Z}[X] : (Q, 0) \mapsto 2Q + 0$ ist injektiv, aber nicht bijektiv.

Nullstellen von Polynomen

Sei K ein kommutativer Ring und $P \in K[X]$ ein Polynom über K.

Vorgelegt sei ein Element $a \in K$. Gilt $P(a) = 0$, so nennen wir a eine **Nullstelle** des Polynoms P, oder eine **Wurzel** der Gleichung $P(X) = 0$.

Lemma G3I: Nullstelle als Linearfaktor abspalten

Genau dann gilt $P(a) = 0$, wenn die Faktorisierung $P = (X - a)Q$ für ein $Q \in K[X]$ gilt. In diesem Fall ist Q eindeutig bestimmt.

Beweis: Die Implikation „$\Leftarrow$“ ist klar, wir zeigen nur noch „$\Rightarrow$“:

Dank Polynomdivision G3H existiert genau ein Paar $Q, R \in K[X]$ mit $P = (X - a)Q + R$ und $\deg R < \deg(X - a) = 1$, also $R \in K$.

Demnach verschwindet $P(a) = R$ genau dann, wenn $R = 0$ gilt. Dies ist gleichbedeutend mit $P = (X - a)Q$. QED

Nullstellen von Polynomen

Nullstellen von Polynomen

Weiterhin sei K ein kommutativer Ring.

Satz G3J: Nullstellen und Vielfachheiten

(1) Zu $P \in K[X]^*$ und $a \in K$ gibt es genau ein Paar (m, Q) mit $m \in \mathbb{N}$ und $Q \in K[X]$, so dass $P = (X - a)^m Q$ und $Q(a) \neq 0$ gilt.

Im Falle $m \geq 1$ nennen wir a eine Nullstelle von P der **Vielfachheit** m, bei $m = 1$ eine **einfache**, bei $m \geq 2$ eine **mehrfache Nullstelle**.

(2) Jedes Polynom $P \in K[X]^*$ schreibt sich als Produkt

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$$

mit paarweise verschiedenen $a_1, \ldots, a_k \in K$ und ihren Vielfachheiten $m_1, \ldots, m_k \in \mathbb{N}_{\geq 1}$, sodass $Q \in K[X]^*$ keine Nullstellen in K hat.

Beweis: Induktion über $\deg P$. QED

Nullstellen von Polynomen

Anzahl der Nullstellen eines Polynoms

G337

Jedes Polynom $P \in K[X]^*$ schreibt sich wie oben erklärt als Produkt

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q.$$

Somit hat P *mindestens* die Nullstellen $a_1, \ldots, a_k \in K$.

⚠ Im Allgemeinen ist diese Zerlegung nicht eindeutig!

⚠ Es kann noch weitere Nullstellen geben!

Beispiel: Über dem Ring $K = \mathbb{Z}/8$ erlaubt das Polynom $P = X^2 - \bar{1}$ vier verschiedene Nullstellen, nämlich $\pm\bar{1}$ und $\pm\bar{3}$. Hier gilt

$$P \;=\; (X - \bar{1})(X + \bar{1}) \;=\; (X - \bar{3})(X + \bar{3}).$$

Beispiel: Im Matrixring $\mathbb{C}^{2\times 2}$ hat das Polynom $P = X^2 + 1 \in \mathbb{R}[X]$ unendlich viele Nullstellen! Ausführliche Konstrukion: Die Matrix

$$M = \begin{pmatrix} \mathrm{i}x & -y - \mathrm{i}z \\ y - \mathrm{i}z & -\mathrm{i}x \end{pmatrix}$$

mit $x, y, z \in \mathbb{R}$ erfüllt $M^2 = -1$ genau dann, wenn $x^2 + y^2 + z^2 = 1$ gilt.

Anzahl der Nullstellen eines Polynoms

G338
Erläuterung

Optimistisch würde man vermuten, dass ein Polynom $P \in K[X]$ vom Grad n höchstens n Nullstellen haben kann. Das ist im Allgemeinen jedoch falsch! Um Sie vor naivem Irrglauben zu bewahren, nennen ich hier eindrückliche Gegenbeispiele.

Im zweiten Beispiel ist die Nicht-Kommutativität Ursache des Problems. Die hier angegebenen Matrizen sind übrigens genau die Quaternionen $q = xI + yJ + zK \in H < \mathbb{C}^{2\times 2}$ mit Norm $|q| = 1$, siehe Beispiel B1G. Selbst in Schiefkörpern schlägt die naive Vermutung also fehl!

Im ersten Beispiel sind offensichtlich die Nullteiler das Problem. Für Körper und Integritätsringe sieht es besser aus!

Anzahl der Nullstellen eines Polynoms

G339

Satz G3K: eindeutige Faktorisierung der Nullstellen

Sei $(K, +, 0, \cdot, 1)$ ein Integritätsring: $1 \neq 0$, kommutativ, nullteilerfrei.

(1) Jedes Polynom $P \in K[X]^*$ faktorisiert als ein Produkt

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$$

mit paarweise verschiedenen $a_1, \ldots, a_k \in K$ und ihren Vielfachheiten $m_1, \ldots, m_k \in \mathbb{N}_{\geq 1}$, sodass $Q \in K[X]^*$ keine Nullstellen in K hat.

(2) In diesem Falle sind $a_1, \ldots, a_k$ die einzigen Nullstellen von P. Die Faktorisierung ist eindeutig bis auf Umordnung der Faktoren.

(3) Ein Polynom $P \in K[X]$ vom Grad $n \in \mathbb{N}$ hat höchstens n Nullstellen in K (mit Vielfachheiten gezählt, das bedeutet $m_1 + \cdots + m_k \leq n$).

(4) Je zwei Polynome $P, Q \in K[X]_{\leq n}$ sind bereits dann gleich, wenn sie an $n + 1$ Stellen $x_0, x_1, \ldots, x_n \in K$ übereinstimmen.

Anzahl der Nullstellen eines Polynoms

G340
Erläuterung

Beweis: (2) Wir vergleichen zwei solche Zerlegungen

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q = (X - b_1)^{n_1} \cdots (X - b_\ell)^{n_\ell} R.$$

Wir zeigen $k = \ell$ sowie nach Umordnung $a_1 = b_1, \ldots, a_k = b_k$ und $m_1 = n_1, \ldots, m_k = n_k$. Wir führen Induktion über k. Für $k = 0$ hat $P = Q$ keine Nullstellen in K, daher gilt auch $\ell = 0$ und $P = R$.

Sei $k \geq 1$. Aus $P(a_k) = 0$ und der Nullteilerfreiheit von K folgt, dass einer der Faktoren $(a_k - b_1), \ldots, (a_k - b_\ell)$ gleich 0 sein muss. Durch Umordnung erreichen wir $a_k = b_\ell$. Dank G3J folgt $m_k = n_\ell$ und $(X - a_1)^{m_1} \cdots (X - a_{k-1})^{m_{k-1}} Q = (X - b_1)^{n_1} \cdots (X - b_{\ell-1})^{n_{\ell-1}} R$. Nach Induktionsannahme folgt dann $k - 1 = \ell - 1$ und $a_1 = b_1, \ldots, a_{k-1} = b_{k-1}$ und $m_1 = n_1, \ldots, m_{k-1} = n_{k-1}$.

(3) Das folgt aus (2) und (1) dank Additivität des Grades (G3B).

(4) Auch $P - Q$ ist vom Grad $\leq n$, hat aber $n + 1$ Nullstellen. Dank (3) gilt $P - Q = 0$, also $P = Q$. QED

Auswertung und Interpolation

Satz G3L: Auswertung und Interpolation

Sei $(K,+,\cdot)$ ein Körper und $x_0,x_1,\ldots,x_n \in K$ paarweise verschieden. Zu beliebigen Werten $y_0,y_1,\ldots,y_n \in K$ existiert genau ein Polynom $P \in K[X]_{\leq n}$ mit $P(x_0)=y_0, P(x_1)=y_1, \ldots, P(x_n)=y_n$. Wir haben

$$K[X]_{\leq n} \xrightarrow{\sim} K^{n+1} \;:\; P \mapsto (P(x_0),P(x_1),\ldots,P(x_n))$$

sowie den surjektiven Ringhomomorphismus

$$\varphi \;:\; K[X] \twoheadrightarrow K^{n+1} \;:\; P \mapsto (P(x_0),P(x_1),\ldots,P(x_n))$$

mit $\ker\varphi = (X-x_0)(X-x_1)\cdots(X-x_n)K[X]$ dank Satz G3K.

Existenz: Eine mögliche Lösung ist die Lagrange–Interpolation

$$L(X) := \sum_{j=0}^{n} y_j L_j(X) \in K[X]_{\leq n} \quad \text{mit} \quad L_j(X) := \prod_{i\neq j} \frac{X-x_i}{x_j-x_i} \in K[X]_n.$$

Eindeutigkeit folgt aus Satz G3K(4). QED

Auswertung und Interpolation

Vorgegeben seien $n+1$ verschiedene Stützstellen $x_0,x_1,\ldots,x_n \in \mathbb{K}$. Für alle $i \neq j$ ist demnach $x_j - x_i \neq 0$ im Körper K invertierbar. Zu jedem $j = 0,1,\ldots,n$ definieren wir das **Lagrange–Polynom**

$$L_j(X) := \prod_{i\neq j} \frac{X-x_i}{x_j-x_i} \quad \in \mathbb{K}[X]_n$$

Dieses Polynom erfüllt $L_j(x_j)=1$ und $L_j(x_i)=0$ für alle $i \neq j$. Zu den Werten $y_0,y_1,\ldots,y_n \in \mathbb{K}$ betrachten wir die Linearkombination

$$L(X) := \sum_{j=0}^{n} y_j L_j(X) \quad \in \mathbb{K}[X]_{\leq n}.$$

Diese erfüllt $L(x_j)=y_j$ für alle $j=0,1,\ldots,n$, wie gewünscht.

⚠ Dies konstruiert *eine* Lösung. Es könnte noch *weitere* geben!

🙂 Die Eindeutigkeit haben wir in Kapitel B mit dem Gauß–Algorithmus gezeigt (siehe Seite B309 zur Vandermonde–Matrix). Hier nun gelingt uns ein zweiter, unabhängiger Beweis dank euklidischer Division.

Polynom vs Polynomfunktion

Satz G3M: Polynom vs Polynomfunktion

Sei K ein Körper. Jedes Polynom $P = \sum_{i=0}^{n} p_i X^i \in K[X]$ definiert die zugehörige Polynomfunktion $f_P : K \to K : a \mapsto P(a) = \sum_{i=0}^{n} p_i a^i$.

Dies stiftet den Ringhomomorphismus $f : K[X] \to K^K : P \mapsto f_P$.

1. Ist K unendlich, dann ist f injektiv, aber nicht surjektiv.
2. Ist K endlich, dann ist f surjektiv, aber nicht injektiv.

Beweis: (1a) Je zwei Polynome $P,Q \in K[X]_{\leq n}$ sind gleich, wenn sie an $n+1$ Stellen $x_0,x_1,\ldots,x_n \in K$ übereinstimmen. Aus der Gleichheit $f_P = f_Q$ folgt demnach die Gleichheit $P = Q$.

(1b) Die Funktion $\delta_0 : K \to K$ mit $\delta_0(0)=1$ und $\delta_0(x)=0$ für $x \neq 0$ ist keine Polynomfunktion. Wäre $\delta_0 = f_P$ für ein $P \in K[X]_{\leq n}$, so folgt $f_P(x) = f_0(x)$ für alle $x \in K^*$, also $P = 0$. Es gilt jedoch $\delta_0 \neq f_0$.

(2a) Die Lagrange-Interpolation G3L garantiert die Surjektivität.

(2b) Dank G3K gilt $\ker(f) = F \cdot K[X]$ mit $F = \prod_{a\in K}(X-a)$. QED

Polynom vs Polynomfunktion

Wir haben anfangs gesehen, dass wir das Polynom $P \in K[X]$ und seine Polynomfunktion $f_P : K \to K : a \mapsto P(a)$ unterscheiden müssen:

Das Polynom P bestimmt die zugehörige Funktion f_P, aber umgekehrt können wir im Allgemeinen aus f_P nicht eindeutig P rekonstruieren.

Der obige Satz G3M klärt die Beziehung $f : K[X] \to K^K : P \mapsto f_P$ nun abschließend und umfassend auf:

1. Für jeden unendlichen Körper K besteht dieses Problem nicht, hier können wir Polynome und Polynomfunktionen identifizieren.
2. Für jeden endlichen Körper ist die Zuordnung f nicht injektiv, aber wir können immerhin ihren Kern präzise angeben.

🙂 Speziell für den Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ bestimmt der folgende Satz G3N das Polynom $F = \prod_{a\in\mathbb{F}_p}(X-a) = X^p - X$. Das ist explizit und elegant!

Satz G3N: der kleine Satz von Fermat

(1) Sei K ein Körper der Charakteristik $p > 0$ und $\mathfrak{f} : K \to K : a \mapsto a^p$ der Frobenius–Endomorphismus. Dann gilt $\mathrm{fix}(\mathfrak{f}) = \mathrm{Char}(K) \cong \mathbb{Z}/p\mathbb{Z}$.

(2) Über $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ gilt somit die Zerlegung $X^p - X = \prod_{a\in\mathbb{F}_p}(X - a)$.

(3) Für jede ganze Zahl $a \in \mathbb{Z}$ gilt $a^p \equiv a \mod p$, also $a^p - a \in p\mathbb{Z}$.

(4) Für jede ganze Zahl $a \in \mathbb{Z} \smallsetminus p\mathbb{Z}$ gilt $a^{p-1} \equiv 1 \mod p$.

Beweis: (1a) Wir zeigen „$\mathrm{fix}(\mathfrak{f}) \supseteq \mathrm{Char}(K)$“. Es gilt $\mathfrak{f}(0_K) = 0_K$ und $\mathfrak{f}(1_K) = 1_K$. Per Induktion gilt $\mathfrak{f}(1_K \cdot n) = 1_K \cdot n$ für alle $n \in \mathbb{N}$, denn

$$\begin{aligned}\mathfrak{f}(1_K \cdot (n+1)) &\overset{\text{Def}}{=} \mathfrak{f}(1_K \cdot n + 1_K) \overset{\text{Add}}{=} \mathfrak{f}(1_K \cdot n) + \mathfrak{f}(1_K)\\ &\overset{\text{Fix}}{=} 1_K \cdot n + 1_K \overset{\text{Def}}{=} 1_K \cdot (n+1).\end{aligned}$$

(1b) Wir zeigen die Umkehrung „$\mathrm{fix}(\mathfrak{f}) \subseteq \mathrm{Char}(K)$“. Jeder Fixpunkt von $\mathfrak{f}$ ist eine Nullstelle des Polynoms $F = X^p - X$. Dieses hat höchstens p Nullstellen in K, und dank (1a) gilt $F(a) = 0$ für alle $a \in \mathrm{Char}(K)$.

Die weiteren Aussagen (2–4) sind damit klar. QED

Übung: Sei $p \geq 2$ eine Primzahl und $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

1. Zu jeder beliebigen Abbildung $g : \mathbb{F}_p \to \mathbb{F}_p$ existiert genau ein Polynom $P \in \mathbb{F}_p[X]_{<p}$ mit $g = f_P$, also $g(a) = P(a)$ für alle $a \in \mathbb{F}_p$.
2. Für je zwei Polynome $P, Q \in \mathbb{F}_p[X]$ gilt $f_P = f_Q$ genau dann, wenn $P - Q \in (X^p - X)\mathbb{F}_p[X]$ gilt.

Beispiel: Für $P = X^2 - X \in \mathbb{F}_2[X]$ gilt $P(0) = P(1) = 0$, also $f_P = 0$. Für $P = X^p - X \in \mathbb{F}_p[X]$ und alle $a \in \mathbb{F}_p$ gilt $P(a) = 0$, also $f_P = 0$.

Beispiel: Spezialfall $p = 2$: Für alle $a \in \mathbb{Z}$ gilt $a^2 \equiv a \mod 2$.
Das können Sie auch ganz elementar beweisen, siehe C215.

Bemerkung: Ist $p \geq 3$ prim, so gilt $a^{p-1} - 1 \equiv 0$ modulo p. Dies ist ein erster Primzahltest für p, wenn auch noch recht grob. Etwas genauer gilt

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0, \quad \text{also } a^{\frac{p-1}{2}} \equiv \pm 1.$$

Eine weitere Verfeinerung führt zum extrem effizienten Primzahltest von Miller–Rabin, siehe `de.wikipedia.org/wiki/Miller-Rabin-Test`.

Zur Abrundung betrachten wir komplexe und reelle Polynome:

Satz G3O: Fundamentalsatz der Algebra

(1) Zu jedem komplexen Polynom $P = X^n + c_1X^{n-1} + \cdots + c_n \in \mathbb{C}[X]$ existieren komplexe Nullstellen $z_1, z_2, \ldots, z_n \in \mathbb{C}$, sodass

$$P = (X - z_1)(X - z_2)\cdots(X - z_n).$$

(2) Für jedes reelle Polynom $P = X^n + c_1X^{n-1} + \cdots + c_n \in \mathbb{R}[X]$ folgt

$$P = (X - a_1)\cdots(X - a_k)(X^2 - 2u_1X + w_1)\cdots(X^2 - 2u_\ell X + w_\ell)$$

mit $n = k + 2\ell$ und $a_i, u_j, w_j \in \mathbb{R}$ sowie der Diskriminante $u_j^2 - w_j < 0$.

Den Fundamentalsatz (1) kann ich Ihnen hier leider nicht beweisen. Aber Sie können immerhin die Äquivalenz „(1) ⇔ (2)“ erklären:

Übung: „(1) ⇒ (2)“: Zu $P \in \mathbb{R}[X] \subset \mathbb{C}[X]$ existieren dank (1) komplexe Nullstellen $z_1, \ldots, z_n \in \mathbb{C}$, sodass $P = (X - z_1)\cdots(X - z_n)$ gilt.
Wegen $P \in \mathbb{R}[X]$ gilt $P(\overline{z_j}) = \overline{P(z_j)} = \overline{0} = 0$. Nicht-reelle Nullstellen treten also immer als konjugierte Paare $u \pm \mathrm{i}v \in \mathbb{C} \smallsetminus \mathbb{R}$ auf. Dabei gilt:

$$\big(X - (u + \mathrm{i}v)\big)\big(X - (u - \mathrm{i}v)\big) = X^2 - 2uX + u^2 + v^2 \in \mathbb{R}[X].$$

Zusammenfassung konjugierter Paare ergibt die reelle Darstellung (2).

Übung: Die umgekehrte Implikation „(2) ⇒ (1)“ folgt aus der Mitternachtsformel zur Lösung quadratischer Gleichungen und der Existenz von Quadratwurzeln in $\mathbb{C}$ (siehe Polarkoordinaten A305).

Arithmetik in $\mathbb{Z}$ und in $K[X]$

Wir erkennen eine verblüffende, wichtige Gemeinsamkeit des Rings $\mathbb{Z}$ der ganzen Zahlen und des Polynomrings $K[X]$ über einem Körper K:

1. Beide sind Integritätsringe mit euklidischer Division (A2A, G3H).
2. Darauf beruht der Algorithmus von Eulid (A2H) und Bézout (A2I).
3. Daraus folgt das Lemma von Euklid (A2M): unzerlegbar vs prim.
4. Wir erhalten die eindeutige Zerlegung in Primfaktoren (A2J).

Aufgabe: Wiederholen Sie die genannten Ergebniss für den Ring $\mathbb{Z}$. Formulieren und beweisen Sie alles entsprechend für den Ring $K[X]$ und allgemein für jeden euklidischen Ring im Sinne von Punkt (1).

Arithmetik in $\mathbb{Z}$ und in $K[X]$

Assoziierte Elemente in einem Integritätsring

Definition G3P: assoziierte Elemente

Im Folgenden sei $(R, +, 0, \cdot, 1)$ ein Integritätsring. Dann ist $R^* = R \setminus \{0\}$ ein Untermonoid von $(R, \cdot, 1)$, da aus $a \neq 0$ und $b \neq 0$ stets $ab \neq 0$ folgt. In $(R, \cdot, 1)$ bezeichnet $R^\times$ die Untergruppe der invertierbaren Elemente.

(1) Zwei Elemente $a, b \in R$ unseres Rings heißen **assoziiert** in R, wenn es ein invertierbares Element $u \in R^\times$ gibt sodass $au = b$ gilt.

Dies ist eine Äquivalenzrelation, geschrieben $a \sim_R b$ oder kurz $a \sim b$.

Übung: Prüfen Sie nach, dass $\sim_R$ eine Äquivalenzrelation auf R ist.

Beispiele: Genau dann ist R ein Körper, wenn $R^\times = R^*$ gilt.
Für jedes Ringelement $a \in R$ gilt dann entweder $a = 0$ oder $a \sim 1$.

In $\mathbb{Z}$ gilt $\mathbb{Z}^\times = \{-1, +1\} \subsetneq \mathbb{Z}^*$. Assoziiert $a \sim b$ bedeutet hier $a = \pm b$.
In jeder Äq'klasse $\{\pm a\}$ wählen wir $|a|$ als kanonischen Repräsentanten.

In $K[X]$ gilt $K[X]^\times = K^\times$. Assoziiert $P \sim Q$ heißt $P = uQ$ mit $u \in K^\times$.
In jeder Äq'klasse $K^\times Q$ wählen wir den Repräsentanten P mit $\operatorname{lc} P = 1$.

Teilbarkeit in einem Integritätsring

Definition G3P: Teilbarkeit

(2) Seien $a, b \in R$. Wir sagen a **teilt** b, oder b ist ein **Vielfaches** von a, falls es $a' \in R$ gibt mit $aa' = b$. Dies schreiben wir $a \mid_R b$ oder kurz $a \mid b$. Andernfalls sagen wir a teilt nicht b, geschrieben $a \nmid_R b$ oder kurz $a \nmid b$.

Beispiel: Für jedes Element $a \in R$ gilt $1 \mid a$, und $a \mid 1$ gdw $a \in R^\times$.
Ebenso gilt $a \mid 0$, und $a \mid 0$ gdw $a = 0$. ⚠ Es gilt $0 \mid 0$, also „0 teilt 0".
Weiterhin können wir nicht durch 0 teilen, denn $0/0$ hat keinen Sinn!

Aufgabe: (a) Teilbarkeit ist eine Präordnung (im Sinne von F1A).
Kleinste Elemente sind 1 und alle $u \in K^\times$, das größte Element ist 0.
(b) Aus gegenseitiger Teilbarkeit $a \mid b$ und $b \mid a$ folgt Assoziertheit $a \sim b$.

Lösung: (a) Es gilt Reflexivität $a \mid a$, dank $a \cdot 1 = a$, und Transitivität: Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$, denn $aa' = b$ und $bb' = c$ impliziert $aa'b' = c$.

(b) Gilt $aa' = b$ und $bb' = a$, so folgt $aa'b' = a$. Im Integritätsring R können wir $a \neq 0$ kürzen und erhalten $a'b' = 1$, also $a', b' \in R^\times$.
Im Sonderfall $a = 0$ gilt $b = 0$, also ebenfalls $a \sim b$.

Größte gemeinsame Teiler

G353
Erläuterung

Definition G3P: größte gemeinsame Teiler

(3) Die Menge der **gemeinsamen Teiler** von $a_1, \dots, a_n \in R$ ist

$$\mathrm{GT} = \mathrm{GT}_R(a_1, \dots, a_n) := \{\, t \in R \mid t \mid_R a_1, \dots, t \mid_R a_n \,\}.$$

Die Menge der **größten gemeinsamen Teiler** definieren wir durch

$$\mathrm{GGT} = \mathrm{GGT}_R(a_1, \dots, a_n) := \{\, t \in \mathrm{GT} \mid \forall s \in \mathrm{GT} : s \mid_R t \,\}.$$

Hier verstehen wir „größer“ im Sinne der Präordnung $\mid_R$ auf R. (F1H)

Übung: Alle Elemente der Menge GGT sind zueinander assoziiert: Für jeden Repräsentanten $t \in \mathrm{GGT}$ gilt demnach $\mathrm{GGT} = K^\times t$.

Konvention: Wir betrachten insbesondere die Ringe $\mathbb{Z}$ und $K[X]$. Ist t unser kanonischer Repräsentant, so schreiben wir kurz $\mathrm{ggT} := t$.

Beispiel: In $\mathbb{Z}$ gilt $\mathrm{GT}(45, 60) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$ und $\mathrm{GGT} = \{\pm 15\}$. Wir nennen $\mathrm{ggT}(45, 60) = +15$ kurz *den* größten gemeinsamen Teiler.

⚠ Ohne diese Normierung nennen wir $t \in \mathrm{GGT}$ vorsichtig *einen* ggT.

Kleinste gemeinsame Vielfache

G354
Erläuterung

Definition G3P: kleinste gemeinsame Vielfache

(4) Die Menge der **gemeinsamen Vielfachen** von $a_1, \dots, a_n \in R$ ist

$$\mathrm{GV} = \mathrm{GV}_R(a_1, \dots, a_n) := \{\, v \in R \mid a_1 \mid_R v, \dots, a_n \mid_R v \,\}.$$

Die Menge der **kleinsten gemeinsamen Vielfachen** ist

$$\mathrm{KGV} = \mathrm{KGV}(a_1, \dots, a_n) := \{\, v \in \mathrm{GV} \mid \forall u \in \mathrm{GV} : v \mid_R u \,\}.$$

Hier verstehen wir „kleiner“ im Sinne der Präordnung $\mid_R$ auf R. (F1H)

Übung: Alle Elemente der Menge KGV sind zueinander assoziiert: Für jeden Repräsentanten $v \in \mathrm{KGV}$ gilt demnach $\mathrm{KGV} = K^\times v$.

Konvention: Wir betrachten insbesondere die Ringe $\mathbb{Z}$ und $K[X]$. Ist v unser kanonischer Repräsentant, so schreiben wir kurz $\mathrm{kgV} := v$.

Beispiel: In $\mathbb{Z}$ gilt $\mathrm{GV}(45, 60) = \{\pm 180, \pm 360, \dots\}$ und $\mathrm{KGV} = \{\pm 180\}$. Wir nennen $\mathrm{kgV}(45, 60) = +180$ *das* kleinste gemeinsame Vielfache.

⚠ Ohne diese Normierung nennen wir $v \in \mathrm{KGV}$ vorsichtig *ein* kgV.

Teilbarkeit, ggT und kgV

G355
Erläuterung

Aufgabe: Zeigen Sie die folgenden Eigenschaften und Rechenregeln:

(0) Die Präordnung $\mid$ auf R ist im Allgemeinen nur partiell, nicht total.

(1) Immer ist 0 das kleinste Element und 1 ein größtes Element.

Teilbarkeit ist verträglich mit Addition und Multiplikation:

(2) Aus $a \mid b$ und $a \mid c$ folgt $a \mid b + c$, allgemein $a \mid bu + cv$ für alle $u, v \in R$.

(3) Aus $a \mid b$ und $c \mid d$ folgt $ac \mid bd$, insbesondere dank $c \mid c$ auch $ac \mid bc$.

(4) Kürzungsregel: Für $c \neq 0$ sind $ac \mid bc$ und $a \mid b$ äquivalent.

Vorsicht bei gemeinsamen Teilern und Vielfachen in exotischen Ringen:

(5) Untersuchen Sie X^a, X^{a+1} im Polynomring $R = \mathbb{Q}[X]$ und im Teilring $S = \mathbb{Q}[X^2, X^3] = \{\, p_0 + p_2 X^2 + \dots + p_n X^n \mid n \in \mathbb{N},\ p_0, p_2, \dots, p_n \in \mathbb{Q} \,\}$.

(6) Die Mengen $\mathrm{GGT}(a, b)$ und $\mathrm{KGV}(a, b)$ können leer sein.

(7) Sei t ein ggT von a und b. Ist dann $v = ab/t$ ein kgV von a und b?

(8) Sei v ein kgV von a und b. Ist dann $t = ab/v$ ein ggT von a und b?

Teilbarkeit, ggT und kgV

G356
Erläuterung

🙂 Für knifflige Fragen wie (6–8) benötigen Sie gute Beispiele wie (5).

Lösung: (5) In R gilt $\mathrm{GT}_R(X^a, X^{a+1}) = \{\, uX^i \mid u \in \mathbb{Q}^\times,\ 0 \leq i \leq a \,\}$, also $\mathrm{ggT}_R(X^a, X^{a+1}) = X^a$. Das war auch zu erwarten. Ebenso gilt $\mathrm{GV}_R(X^a, X^{a+1}) = \mathbb{Q}[X] \cdot X^{a+1}$, also $\mathrm{kgV}_R(X^a, X^{a+1}) = X^{a+1}$.

In S hingegen gilt $\mathrm{GT}_S(X^a, X^{a+1}) = \{\, u,\ uX^i \mid u \in \mathbb{Q}^\times,\ 2 \leq i \leq a - 2 \,\}$. Für $a = 0, 1, 2, 3$ gilt $\mathrm{ggT}_S(X^a, X^{a+1}) = 1$, dann $\mathrm{ggT}_S(X^4, X^5) = X^2$ und $\mathrm{GGT}_S(X^5, X^6) = \emptyset$, denn $X^2 \nmid_S X^3$. Das ist überaus merkwürdig!

Andererseits gilt $\mathrm{GV}_S(X^a, X^{a+1}) = \mathbb{Q}[X] \cdot X^{a+3}$. Erneut folgt daraus $\mathrm{KGV}_S(X^a, X^{a+1}) = \emptyset$, denn $X^{a+3} \nmid_S X^{a+4}$. Auch das ist merkwürdig!

(6) Für X^5, X^6 in $S = \mathbb{Q}[X^2, X^3]$ gilt $\mathrm{GGT} = \emptyset$ und $\mathrm{KGV} = \emptyset$ dank (5).

(7) Nein! Für X^2, X^3 in $S = \mathbb{Q}[X^2, X^3]$ gilt $\mathrm{GGT} = \mathbb{Q}^\times$ und $\mathrm{KGV} = \emptyset$.

(8) Ja, falls $v \neq 0$. Es gilt $t \mid a$ und $t \mid b$, denn $a = \frac{ab}{v} \cdot \frac{v}{b}$ und $b = \frac{ab}{v} \cdot \frac{v}{a}$. Angenommen ein weiteres Element $s \in R$ erfüllt ebenso $s \mid a$ und $s \mid b$. Dann folgt $a \mid ab/s$ und $b \mid ab/s$, also $v \mid ab/s$, somit $sv \mid ab$ und $s \mid ab/v$. Das zeigt $s \mid t$, also ist t tatsächlich ein ggT von a und b in R.

Unzerlegbar / irreduzibel vs prim

G357
Erläuterung

Wir zerlegen das Monoid $R^* = R^\times \sqcup R^{\mathrm{red}} \sqcup R^{\mathrm{irr}}$ in die invertierbaren $R^\times$, zerlegbaren / reduziblen R^{red} und unzerlegbaren / irreduziblen R^{irr}:

$$\begin{aligned} R^\times &:= \{\, a \in R^* \mid \exists b \in R^* : ab = 1 \,\}, \\ R^{\mathrm{red}} &:= \{\, a \in R^* \mid \exists b, c \in R^* \smallsetminus R^\times : a = bc \,\}, \\ R^{\mathrm{irr}} &:= \{\, a \in R^* \mid \forall b, c \in R^* : a = bc \;\Rightarrow\; b \sim 1 \veebar c \sim 1 \,\} \end{aligned}$$

Definition G3P: unzerlegbar / irreduzibel vs prim

(5a) Ein Element $a \in R^*$ heißt **unzerlegbar** / irreduzibel in R, falls gilt: Für alle $b, c \in R$ folgt aus $a = b \cdot c$ entweder $b \in R^\times$ oder $c \in R^\times$.

(5b) Hingegen nennen wir ein Element $a \in R \smallsetminus R^\times$ **prim** in R, falls gilt: Für je zwei Faktoren $b, c \in R$ folgt aus $a \mid b \cdot c$ stets $a \mid b$ oder $a \mid c$.

Beispiel: Das Nullelement ist besonders, $R = \{0\} \sqcup R^\times \sqcup R^{\mathrm{red}} \sqcup R^{\mathrm{irr}}$. Es ist zudem prim, denn $0 \mid ab$ bedeutet $ab = 0$, also $a = 0$ oder $b = 0$.

Im Monoid $(\mathbb{Z}^*, \cdot, 1)$ sind ±1 invertierbar, $\pm2, \pm3, \pm5, \pm7, \pm11, \pm13, \ldots$ unzerlegbar und $\pm4, \pm6, \pm8, \pm9, \pm10, \pm12, \pm14, \pm15, \pm16, \ldots$ zerlegbar.

Unzerlegbar / irreduzibel vs prim

G358
Erläuterung

Bemerkung: Im Monoid $(\mathbb{Z}^*.\cdot, 1)$ sind unzerlegbar und prim äquivalent dank dem Lemma von Euklid (A2M). Das gilt nicht in jedem Ring:

Beispiel: Im Ring $S = \mathbb{Q}[X^2, X^3] = \{\, p_0 + p_2 X^2 + \cdots + p_n X^n \mid p_i \in \mathbb{Q} \,\}$ sind X^2 und X^3 unzerlegbar, aber nicht prim: Es gilt $X^2 \mid X^3 \cdot X^3$, aber $X^2 \nmid X^3$. Ebenso gilt $X^3 \mid X^2 \cdot X^4$, aber weder $X^3 \mid X^2$ noch $X^3 \mid X^4$.

⚠ Das Element $X^6 = X^3 \cdot X^3 \cdot X^3 = X^2 \cdot X^2$ hat in $S = \mathbb{Q}[X^2, X^3]$ zwei völlig verschiedene Zerlegungen in unzerlegbare Elemente. Für „vernünftige“ Ringe wollen wir solche Pathologien ausschließen!

Lemma G3Q: Prim impliziert unzerlegbar.

Sei R ein Ring. Jedes Primelement $p \in R^*$ ist unzerlegbar in R.

Aufgabe: Beweisen Sie dies nach dem Vorbild von Lemma A2M(1).

Lösung: Sei $p \neq 0$ prim und $p = ab$ in R. Daraus folgt $p \mid a$ oder $p \mid b$. Nehmen wir $p \mid a$ an, also $a = pp'$ für ein $p' \in \mathbb{Z}$. Damit gilt $p = ab = pp'b$, nach Kürzung $1 = p'b$, also $b = \pm1$. Analog folgt aus $p \mid b$, dass $a = \pm1$.

Zerlegung in irreduzible Faktoren

G359
Erläuterung

Definition G3P: Zerlegung in unzerlegbare Faktoren

(6a) Zu $a \in R^*$ besteht eine **irreduzible Zerlegung** kurz **UProdukt** $(u; p_1, \ldots, p_n)$ aus $u \in R^\times$ und $p_1, \ldots, p_n \in R^{\mathrm{irr}}$ mit $a = up_1 \cdots p_n$.

(6b) Zwei irreduzible Zerlegung $(u; p_1, \ldots, p_n)$ und $(v; q_1, \ldots, q_m)$ heißen **assoziiert**, wenn $m = n$ und nach Umordnung $p_1 \sim q_1, \ldots, p_n \sim q_n$ gilt.

(7a) Ein Element $a \in R^*$ ist **zerlegbar in unzerlegbare Faktoren** in R, falls ein solches UProdukt existiert. (Für $n = 0$ gilt $a = u$, also $a \in R^\times$.)

(7b) Wir nennen a in R **eindeutig zerlegbar in irreduzible Faktoren**, wenn zudem je zwei irreduzible Zerlegungen von a assoziiert sind.

(8) Ein Integritätsring R heißt **faktoriell** wenn jedes Element $a \in R^*$ eindeutig in irreduzible Faktoren zerlegbar ist wie in (7) erklärt.

(9) Wir nennen $\mathbb{P} \subset R^{\mathrm{irr}}$ ein **Repräsentantensystem** der unzerlegbaren Elemente in R, falls jedes unzerlegbare Element $q \in R^{\mathrm{irr}}$ assoziert ist zu genau einem Element $p \in \mathbb{P}$, als **kanonischem Repräsentanten**.

Zerlegung in irreduzible Faktoren

G360
Erläuterung

Dank Kommutativität können wir Produkte in R beliebig umordnen. Ebenso können wir von jeder irreduziblen Zerlegung $a = up_1 \cdots p_n$ übergehen zu $a = (uu_1^{-1} \cdots u_n^{-1})(u_1 p_1) \cdots (u_n p_n)$ mit $u_1, \ldots, u_n \in R^\times$.

Diese offensichtliche Umformung können und wollen wir nicht verbieten. Wir nennen die Zerlegung von a eindeutig, wenn je zwei Zerlegungen allein durch diese offensichtlichen Umformungen ineinander übergehen.

Beispiel: Der Fundamentalsatz der Arithmetik (A2J) besagt: Der Ring $\mathbb{Z}$ der ganzen Zahlen ist faktoriell. Jede ganze Zahl lässt sich zerlegen in irreduzible Fakoren, eindeutig bis auf Reihenfolge und Vorzeichen.

$$-60 = (-1) \cdot 2 \cdot 2 \cdot 3 \cdot 5 = (+1) \cdot (-5) \cdot 2 \cdot (-3) \cdot (-2)$$

Beispiel: Der Ring $\mathbb{Q}[X^2, X^3]$ ist nicht faktoriell, denn für Elemente wie $X^6 = X^3 \cdot X^3 \cdot X^3 = X^2 \cdot X^2$ gibt es mehr als eine Zerlegung.

Übung: Genau dann ist R faktoriell, wenn jedes Element $a \in R$ eine irreduzible Zerlegung erlaubt und jedes irreduzible Element prim ist.

Faktorisierung als Isomorphismus

Beispiel: Im Ring $\mathbb{Z}$ wählen wir als kanonische Repräsentanten traditionell die positiven Primzahlen, $\mathbb{P} = \mathbb{Z}_{>0}^{\text{irr}} = \{2, 3, 5, 7, 11, 13, \ldots\}$.

Satz G3R: Faktorisierung als Isomorphismus

Sei R ein Ring und $\mathbb{P} \subset R$ eine Teilmenge. Dann sind äquivalent:

(1) Der Ring R ist faktoriell, erlaubt also eindeutige UProdukte, und $\mathbb{P} \subset R$ ist ein Repräsentantensystem der unzerlegbaren Elemente.

$$\Phi = \Phi_R^{\mathbb{P}} : (R^\times, \cdot) \times (\mathbb{N}^{(\mathbb{P})}, +) \to (R^*, \cdot) : (u, \nu) \mapsto u \cdot \textstyle\prod_{p \in \mathbb{P}} p^{\nu(p)}$$

(2) Der Monoidhomomorphismus Φ ist bijektiv, also ein Isomorphismus.

Als Dreingabe erhalten wir dank $\mathbb{P}$ in R kanonische ggT und kgV:

$$\operatorname{ggT}(a,b) = \textstyle\prod_p p^{\min(\nu_a(p),\nu_b(p))} \quad \text{und} \quad \operatorname{kgV}(a,b) = \textstyle\prod_p p^{\max(\nu_a(p),\nu_b(p))}$$

Insbesondere folgt die schöne Beziehung $\operatorname{ggT}(a,b) \cdot \operatorname{kgV}(a,b) \sim a \cdot b$.

Faktorisierung als Isomorphismus

Aufgabe: Beweisen Sie die Äquivalenz des Satzes G3R.

Lösung: „(1) $\Rightarrow$ (2)“: Die Abbildung Φ ist ein Monoidhomomorphismus. Surjektivität bedeutet, jedes Element $a \in R^*$ lässt sich als UProdukt schreiben; Injektivität bedeutet, je zwei UProdukte zu a sind assoziiert.
„(2) $\Rightarrow$ (1)“: Wir vergleichen $a = u \prod_p p^{\nu_a(p)}$ und $b = v \prod_p p^{\nu_b(p)}$ in R. Dann ist Teilbarkeit $a \mid b$ in R äquivalent zur Relation $\nu_a \le \nu_b$ in $\mathbb{N}^{(\mathbb{P})}$. Somit ist $\mathbb{P}$ ein Repräsentantensystem der unzerlegbaren Elemente in R, und der Ring R ist faktoriell, da in R eindeutige UProdukte existieren.

🙂 Der Isomorphismus Φ_R klärt die Struktur des Monoids $(R^*, \cdot)$.

⚠ Das Produkt $\Phi_{\mathbb{Z}}$ ist leicht, die Primfaktorzerlegung $\Phi_{\mathbb{Z}}^{-1}$ ist notorisch schwer zu berechnen. Genau darauf beruhen Cryptosysteme wie RSA.

🙂 Glücklicherweise gibt es für ggT und kgV in euklidischen Ringen weit effizientere Algorithmen, und diesen wenden wir uns nun zu.

Eindeutigkeit der Zerlegung

Lemma G3S: Eindeutigkeit der Zerlegung

Sei R ein Integritätsring und jedes unzerlegbare Element sei prim. Dann sind zu jedem Element $a \in R^*$ je zwei UProdukte assoziiert.

Aufgabe: Beweisen Sie dies nach dem Vorbild $\mathbb{Z}$ (Satz A2J).

Lösung: In R betrachten wir zwei UProdukte

$$a \;=\; up_1p_2\cdots p_n \;=\; vq_1q_2\cdots q_m.$$

Wir behaupten, dass $n = m$ gilt und nach Umordnung $p_i \sim q_i$ für alle i. Wir führen Induktion über n. Für $n = 0$ gilt $a \in R^\times$, also auch $m = 0$. Für $n \ge 1$ ist p_n ist unzerlegbar, nach Voraussetzung somit auch prim. Also gilt $p_n \mid q_i$ für ein $i \in \{1, \ldots, m\}$. Nach Umordnung gilt $i = m$. Da auch q_m unzerlegbar ist, folgt $p_n \sim q_m$. Kürzen ergibt

$$a/p_n \;=\; up_1p_2\cdots p_{n-1} \;=\; v'q_1q_2\cdots q_{m-1}.$$

Nach Induktionsvoraussetzung gilt für diese gekürzten Produkte $n - 1 = m - 1$ und nach Umordnung $p_i \sim q_i$ für alle $i = 1, \ldots, n-1$.

Existenz und Eindeutigkeit der Zerlegung

🙂 Dieses schöne Argument ist der übliche Weg, um die Eindeutigkeit der Primfaktorzerlegung in R zu beweisen. Die wesentliche Zutat ist: Jedes unzerlegbare Element ist prim. Zum Verständnis des Rings R wollen wir daher das genaue Verhältnis von unzerlegbaren und primen Elementen untersuchen. Unser Ziel ist das Lemma von Euklid (G3X).

Für den Ring $\mathbb{Z}$ kennen wir den Fundamentalsatz der Arithmetik A2J: Jede ganze Zahl $a \in \mathbb{Z}^*$ ist ein Produkt von Primzahlen, und diese Zerlegung ist eindeutig bis auf Reihenfolge und Vorzeichen.

Dies wollen wir nun ebenfalls für jeden Polynomring $K[X]$ über einem Körper K beweisen: Jedes Polynom $a \in K[X]^*$ ist ein Produkt von unzerlegbaren Polynomen in $K[X]$, und diese Zerlegung ist eindeutig bis auf Reihenfolge und Assoziiertheit der Faktoren.

Die gute Nachricht: Der Beweis verläuft genau so, wie Sie dies im Vorbild $\mathbb{Z}$ gesehen haben. Wir nutzen die Gelegenheit, diese schönen Argumente noch einmal genau nachzuvollziehen, und die wesentlichen Ideen als allgemeine Definitionen und Sätze zu formulieren.

Euklidische Ringe: Division mit Rest

Definition G3T: euklidischer Ring

Sei R ein Integritätsring. Eine **euklidische Division** auf dem Ring R ist ein Paar (ν, δ) aus einer Funktion $\nu : R \to \mathbb{N}$ mit $\nu(0) = 0 = \min \mathbb{N}$ und einer Abbildung $\delta : R \times R^* \to R \times R : (a, b) \mapsto (q, r)$, so dass gilt:

$$a = bq + r \quad \text{und} \quad \nu(r) < \nu(b).$$

Statt $(\mathbb{N}, \leq)$ genügt eine beliebige wohlgeordnete Menge $(N, \leq)$.

Wir nennen das Tripel (R, ν, δ) dann einen **euklidischen Ring** mit **(euklidischer) Division** δ und **(euklidischer) Normfunktion** ν.

Wir definieren $\operatorname{quo}, \operatorname{rem} : R \times R^* \to R$ durch $\delta(a, b) = (a \operatorname{quo} b, a \operatorname{rem} b)$ und nennen dies **Quotient** und **Rest** der Division von a durch b.

Beispiele: Der Ring $\mathbb{Z}$ ist euklidisch mit der Norm $\nu : \mathbb{Z} \to \mathbb{N} : b = |b|$ und der Division mit Rest $\delta : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{N}$ aus Satz A2A.

Über jedem Körper K ist der Polynomring $K[X]$ euklidisch mit der Norm $\deg : K[X] \to \mathbb{N} \cup \{-\infty\}$ und der Division δ aus Satz G3H.

Euklidische Ringe: Division mit Rest

Wir dividieren $a \in R$ durch $b \in R^*$ und erhalten gemäß $a = bq + r$ einen Quotienten $q \in R$ und einen Rest $r \in R$. Dabei müssen wir sicherstellen, dass der Rest r „kleiner“ als b ist. Dies messen wir mit der Norm ν.

Abkürzend nennen wir einen Integritätsring R **euklidisch**, wenn auf R eine euklidische Division (ν, δ) wie in G3T existiert.

Manche Autoren nennen das Paar (R, ν) einen **euklidischen Ring** und fordern dann, dass dazu eine geeignete Division δ existiert.

Ist R euklidisch, so gibt es im Allgemeinen mehrere Normfunktionen ν und zu jeder Normfunktion ν auch mehrere euklidische Divisionen δ.

Zur Formulierung von Algorithmen nutzen wir sowohl die Norm ν als auch die Division δ, daher betrachten wir explizit das Tripel (R, ν, δ).

Nicht jeder Ring ist euklidisch, zum Beispiel ist der Polynomring $\mathbb{Z}[X]$ nicht euklidisch. (Später genauer: $\mathbb{Z}[X]$ ist kein Hauptidealring.)

Euklidische Ringe: Division mit Rest

Bemerkung: (1) Statt $(\mathbb{N}, \leq)$ genügt jede wohlgeordnete Menge $(N, \leq)$. Für Polynome etwa nutzen wir die Norm $\deg : K[X] \to \mathbb{N} \cup \{-\infty\}$. Genau so gut können wir $\nu : K[X] \to \mathbb{N}$ betrachten mit $\nu(0) = 0$ und $\nu(P) = 1 + \deg(P)$ für $P \neq 0$. Das Ergenis ist dasselbe.

(2) In Definition G3T fordern wir zunächst $\nu(0) = 0 = \min \mathbb{N}$. Wir folgern nun, dass für $b \in R^*$ stets $\nu(b) > 0$ gilt: Jede Division $\delta : (a, b) \mapsto (q, r)$, etwa für $a = 0$, ergibt $\nu(r) < \nu(b)$, also gilt $\nu(b) > 0$.

(3) In $\mathbb{Z}$ und $K[X]$ gilt die schöne Eigenschaft: Aus $a \mid b$ folgt $a \operatorname{rem} b = 0$. Es schadet nichts, dies sogar für jeden euklidischen Ring zu fordern, wir können δ notfalls immer so anpassen, und (R, ν, δ) bleibt euklidisch.

Wir haben in G3T zunächst nur die minimalen Forderungen formuliert. Man kann weitere gute Eigenschaften fordern oder herleiten. Eine ausführliche Diskussion verschieben wir auf später.

Euklidische Ringe: Division mit Rest

Wozu führen wir den abstrakten Begriff eines „euklidischen Rings“ ein?

Zunächst wollen wir die beiden Beispiele $\mathbb{Z}$ und $K[X]$ zusammenfassen, wesentliche Gemeinsamkeiten benennen und einheitlich behandeln. Das ist in der Mathematik ein allgegenwärtiger Trick zur Denkökonomie, zudem wird dadurch die Struktur noch wesentlich klarer und einfacher.

Es gibt darüber hinaus noch viele weitere euklidische Ringe. Auf diese wollen wir hier noch nicht eingehen, aber wir können alles vorbereiten. So sind Sie für die Zukunft bestens gewappnet: Wann immer Ihnen ein euklidischer Ring begegnet, haben Sie sofort passende Werkzeuge.

Ist Abstraktion etwas Gutes? Ich denke schon! Sie klärt und vereinfacht, sie bündelt viele Beispiele und verhilft uns zu wesentlich mehr Effizienz. Und sie schadet nicht: Wenn Sie möchten, können Sie bei „euklidischer Ring“ immer an die beiden wichtigsten Beispiele denken: $\mathbb{Z}$ und $K[X]$.

☺ Wir formulieren und beweisen im Allgemeinen, wir illustrieren und rechnen im Konkreten. Beides ergänzt sich wie linke und rechte Hand.

Der euklidische Algorithmus

☺ Der von den ganzen Zahlen $\mathbb{Z}$ bekannte euklidische Algorithmus überträgt sich wörtlich auf $K[X]$ und jeden euklidischen Ring (R, ν, δ):

Algo G3U: euklidischer Algorithmus

Eingabe: zwei Elemente $a_0, b_0 \in R$ in einem euklidischen Ring (R, ν, δ)
Ausgabe: ein größter gemeinsame Teiler $a \in \mathrm{GGT}(a_0, b_0)$ im Ring R

1: $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix} a_0 \\ b_0 \end{smallmatrix}\right]$ // $\mathrm{GT}(a,b) = \mathrm{GT}(a_0, b_0)$
2: while $b \neq 0$ do $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix} b \\ a \operatorname{rem} b \end{smallmatrix}\right]$ // $\mathrm{GT}(a,b) = \mathrm{GT}(b, a - qb)$
3: wähle $\varepsilon \in R^\times$, notfalls $\varepsilon = 1$ // optional zur Normierung
4: return εa // $\mathrm{GGT}(a,0) = R^\times a$

Satz G3U: ggT in einem euklidischen Ring

Sei (R, ν, δ) ein euklidischer Ring, etwa $\mathbb{Z}$ oder $K[X]$.
(1) Zu je zwei Elementen $a, b \in R$ existiert ein ggT in R.
(2) Der obige Algorithmus berechnet einen solchen ggT.

Der euklidische Algorithmus

Wir müssen zeigen, dass der angegebene Algorithmus korrekt ist, also dass die Methode tatsächlich liefert, was die Spezifikation verspricht.

Die Methode terminiert: Die Norm $\nu(b) \in \mathbb{N}$ nimmt in jedem Schritt ab, bis mit $\nu(b) = 0$ schließlich $b = 0$ erreicht ist und der Algorithmus endet.

Das gelieferte Ergebnis erfüllt die geforderten Bedingungen:
Die Initialisierung $(a, b) \leftarrow (a_0, b_0)$ garantiert $\mathrm{GT}(a,b) = \mathrm{GT}(a_0, b_0)$.
Jede Iteration erhält $\mathrm{GT}(a,b) = \mathrm{GT}(b, a - qb)$. Zum Schluss gilt also $\mathrm{GT}(a_0, b_0) = \mathrm{GT}(a, 0)$, somit $\mathrm{GGT}(a_0, b_0) = \mathrm{GGT}(a, 0) = R^\times a$. QED

☺ Das ist genial-einfach und einfach-genial. Zudem ist die Methode sehr effizient, das heißt, auch für große Eingaben (a_0, b_0) geeignet.

☺ Wir können das Ergebnis zu „dem“ kanonischen ggT normieren:
Beispiele: In $\mathbb{Z}$ wählen wir $a \geq 0$. In $K[X]$ wählen wir a mit $\mathrm{lc}(a) = 1$.

☺ Auch der erweiterte Algorithmus A2I zur Berechnung eines ggT mit Bézout–Koeffizienten überträgt sich von $\mathbb{Z}$ auf $K[X]$ und (R, ν, δ).

Übung: Wiederholen Sie A2I und formulieren Sie dies nun allgemein.

Der erweiterte euklidische Algorithmus nach Bézout

Algo G3V: euklidischer Algorithmus mit Bézout–Koeffizienten

Eingabe: zwei Elemente $a_0, b_0 \in R$ in einem euklidischen Ring (R, ν, δ)
Ausgabe: drei Elemente $a, u, v \in R$ mit $a = a_0 u + b_0 v \in \mathrm{GGT}(a_0, b_0)$

1: $\left[\begin{smallmatrix} a & u & v \\ b & s & t \end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \end{smallmatrix}\right]$ // Invariante $\begin{cases} a = a_0 u + b_0 v \\ b = a_0 s + b_0 t \end{cases}$
2: while $b \neq 0$ do $q \leftarrow a \operatorname{quo} b$ // euklidische Division
3: $\left[\begin{smallmatrix} a & u & v \\ b & s & t \end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix} b & s & t \\ a - qb & u - qs & v - qt \end{smallmatrix}\right]$ // Invariante $\begin{cases} a = a_0 u + b_0 v \\ b = a_0 s + b_0 t \end{cases}$
4: wähle $\varepsilon \in R^\times$, notfalls $\varepsilon = 1$ // optional zur Normierung
5: return $(\varepsilon a, \varepsilon u, \varepsilon v)$ // $a = a_0 u + b_0 v \in \mathrm{GGT}(a_0, b_0)$

Satz G3V: ggT mit Bézout–Koeffizienten

Sei (R, ν, δ) ein euklidischer Ring. (1) Zu je zwei Elementen $a, b \in R$ existieren **Bézout–Koeffizienten** $u, v \in R$ mit $d = au + bv \in \mathrm{GGT}(a, b)$.
(2) Obiger Algorithmus berechnet einen ggT mit Bézout–Koeffizienten.
(3) Das ist ein Zertifikat: Aus $t = au + bv \in \mathrm{GT}(a, b)$ folgt $t \in \mathrm{GGT}(a, b)$.

Der erweiterte euklidische Algorithmus nach Bézout

Bemerkung: Die Operationen $q \leftarrow a \operatorname{quo} b$ und

$$\begin{bmatrix} a & u & v \\ b & s & t \end{bmatrix} \leftarrow \begin{bmatrix} b & s & t \\ a - qb & u - qs & v - qt \end{bmatrix}$$

erinnern uns an Zeilenoperationen für lineare Gleichungssysteme, hier die invarianten Gleichungen. $R_1 \leftrightarrow R_2$: Wir tauschen die beiden Zeilen. $R_2 \leftarrow R_2 - qR_1$: Von der zweiten Zeile ziehen wir q mal die erste ab. Die Gleichungen $a = a_0 u + b_0 v$ und $b = a_0 s + b_0 t$ bleiben erhalten.

Beweis: (2) In der ersten Spalte wird der euklidische Algorithmus G3U zur Berechnung des ggT ausgeführt. Die Invarianten garantieren in jedem Schritt die Gleichungen $a = a_0 u + b_0 v$ und $b = a_0 s + b_0 t$.

(3) Sei $d = au + bv$ sowie $d \mid a$ und $d \mid b$. Wir zeigen $d \in \mathrm{GGT}(a, b)$: Angenommen $c \mid a$ und $c \mid b$, also $ca' = a$ und $cb' = b$. Dann gilt $c(a'u + b'v) = d$, also $c \mid d$. Das heißt, d ist ein ggT von a und b. QED

Die Primfaktorzerlegung im Polynomring $K[X]$

Für den Ring $\mathbb{Z}$ gilt der Fundamentalsatz der Arithmetik (A2J). Dieser Satz gilt genauso für jeden Polynomring $K[X]$ über einem Körper K:

Satz G3W: Primfaktorzerlegung im Polynomring $K[X]$

Sei K ein Körper. Dann ist der Polynomring $K[X]$ faktoriell.

Explizit ausformuliert bedeutet das folgendes:

(1) Jedes Polynom $a \in K[X]^*$ können wir zerlegen in ein Produkt

$$a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_\ell$$

mit $u = \mathrm{lc}(a) \in K^\times$ und $p_1, p_2, \ldots, p_\ell \in K[X]$ unzerlegbar und normiert.

(2) Diese Zerlegung ist eindeutig bis auf Umordnung: Gilt

$$p_1 \cdot p_2 \cdot \ldots \cdot p_\ell = q_1 \cdot q_2 \cdot \ldots \cdot q_k$$

mit unzerlegbaren normierten Polynomen $p_1, p_2, \ldots, p_\ell$ und $q_1, q_2, \ldots, q_k$, so folgt $\ell = k$ und nach Umordnung $p_1 = q_1$, $p_2 = q_2$, …, $p_\ell = q_\ell$.

Die Primfaktorzerlegung im Polynomring $K[X]$

Sei $\mathbb{P} \subset K[X]$ die Teilmenge der unzerlegbaren normierten Polynome. Gemäß Satz G3R haben wir den Monoidhomomorphismus

$$\Phi = \Phi_{K[X]} : (K^\times, \cdot) \times (\mathbb{N}^{(\mathbb{P})}, +) \to (K[X]^*, \cdot) : (u, \nu) \mapsto u \cdot \textstyle\prod_{p \in \mathbb{P}} p^{\nu(p)},$$
$$(\mathbb{N}^{(\mathbb{P})}, +) \to (K[X]^1, \cdot).$$

Dank Satz G3W ist Φ bijektiv, also ein Isomorphismus. Das beinhaltet zwei Aussagen: (1) Surjektivität bedeutet, jedes Polynom $a \in K[X]^*$ lässt sich als ein Produkt unzerlegbarer Polynome in $K[X]$ schreiben. Diese können wir normieren zu $a = up_1 \cdots p_\ell$ mit $u = \mathrm{lc}(a) \in K^\times$ und $p_1, \ldots, p_\ell \in \mathbb{P}$. (2) Injektivität bedeutet, je zwei solche Zerlegungen zu a sind assoziiert.

🙂 Für den Polynomring $K[X]$ können wir dies nun leicht beweisen, da wir alle Werkzeuge zur Hand haben. Der Beweis verläuft genau so, wie Sie dies im Vorbild $\mathbb{Z}$ gesehen haben. Diese Wiederholung ist eine wunderbare Gelegenheit, das Verständnis zu festigen und zu vertiefen.

Existenz einer Primfaktorzerlegung in $K[X]$

Aufgabe: Beweisen Sie die Existenz (1) nach dem Vorbild $\mathbb{Z}$ (A2J).

🙂 Die Existenz ist ein recht naheliegendes Induktionsargument: Wir zerlegen bis es aus Gradgründen nicht weiter geht. Ausführlich:

Lösung: Wir führen Induktion über den Polynomgrad $n = \deg(a)$.
Für $n = 0$ gilt $a = u \in K^\times$; dies ist eine Zerlegung der Länge $\ell = 0$.

Sei nun $n \geq 1$. Entweder a ist unzerlegbar oder echt zerlegbar.
Ist a unzerlegbar, so gilt $a = up_1$ mit $u = \mathrm{lc}(a)$ und $p_1 = a/u \in \mathbb{P}$.
Ist a in $K[X]^*$ echt zerlegbar, so gilt $a = bc$ mit $a, b \in K[X]^* \smallsetminus K^\times$.
Für die Polynomgrade bedeutet dies $\deg(b) \geq 1$ und $\deg(c) \geq 1$.
Wegen $n = \deg(a) = \deg(b) + \deg(c)$ folgt $\deg(b) < n$ und $\deg(c) < n$.
Nach Induktionsvoraussetzung existieren Zerlegungen $b = up_1 \cdots p_k$ und $c = vp_{k+1} \cdots p_\ell$. Somit ist $a = (uv)p_1 \cdots p_\ell$ eine Zerlegung von a.

Übung: Übertragen Sie Euklids Lemma (A2M) von $\mathbb{Z}$ auf $K[X]$. Folgern Sie daraus die Eindeutigkeit der Primfaktorzerlegung (G3S).

🙂 Damit ist Satz G3W zur Primfaktorzerlegung in $K[X]$ bewiesen!

Eindeutigkeit der Primfaktorzerlegung in $K[X]$

Weiterhin sei K ein Körper und $K[X]$ der Polynomring über K.

Lemma G3X: Lemma von Euklid für $K[X]$

Jedes unzerlegbare Element $p \in K[X]^*$ ist prim in $K[X]$.

Beweis: Sei $p \in K[X]^*$ ein unzerlegbares Polynom in $K[X]$. Gegeben seien zwei Polynome $a, b \in K[X]$ mit $p \mid ab$. Wir zeigen $p \mid a$ oder $p \mid b$:
Hierzu sei $d = \mathrm{ggT}(p, a)$. Es gilt $d \mid p$; da p unzerlegbar ist, gilt entweder $d = 1$ oder $d \sim p$. (a) Im Falle $d \sim p$ gilt dank $d \mid a$ sofort $p \mid a$.
(b) Im Falle $d = 1$ folgt $p \mid b$ mit dem Lemma von Gauß. QED

Lemma G3Y: Lemma von Gauß für $K[X]$

Seien $p, a, b \in K[X]$ mit $\mathrm{ggT}(p, a) = 1$. Dann folgt aus $p \mid ab$ bereits $p \mid b$.

Beweis: Dank Bézout G3V existieren $u, v \in K[X]$, sodass $pu + av = 1$.
Die Teilbarkeit $p \mid ab$ bedeutet $ab = pq$ für ein $q \in K[X]$. Daraus folgt $b = (pu + av)b = pub + abv = p(ub + qv)$, also $p \mid b$. QED

Kapitel H

Halbzeit

Frohe Weihnachten!

Inhalt dieses Kapitels H

Motivation und Überblick

Liebe Studierende,

unser außergewöhnliches Semester befindet sich nun in der Halbzeit. Dieses Kapitel H markiert diesen kurzen Moment des Innehaltens.

Ich freue mich weiterhin sehr, dass Sie dieser Veranstaltung die Treue halten und Woche für Woche engagiert mitarbeiten. Das kostet Sie viel Zeit und Mühe, ich weiß es sehr zu schätzen und darf Ihnen versichern: Es lohnt sich!

Die Mathematik ist wunderschön und überall nützlich.
Bitte bleiben Sie dran!

Motivation und Überblick

Schritt für Schritt gewinnen Sie mehr Erfahrung und finden immer besser in Ihr Studium hinein. Sie haben in den vergangenen Wochen schon viel geleistet und den schwierigen Übergang von der Schule zur Universität gemeistert, zudem unter widrigen äußeren Umständen. Darauf dürfen Sie stolz sein.

Auch für uns, das LinA-Team, ist die digitale Lehre extrem fordernd und aufreibend, doch wir sehen auch Ihre ersten Erfolge, Ihre konstruktive Mitarbeit und freundlichen Rückmeldungen geben uns immer wieder Mut und machen Hoffnung: Unsere gemeinsame Mühe lohnt sich.

Wir werden Sie auch im nächsten Jahr bestmöglich beim Lernen unterstützen, zunächst weiter digital, sobald möglich in Präsenz.

Im Namen Ihres LinA-Teams wünsche ich Ihnen
frohe Weihnachten!

Kapitel I

Lineare Räume und lineare Abbildungen

In der Geschichte der Mathematik zeigt sich uns ein großer Reichtum in der Entstehung verschiedenartiger Strukturen, die sich entfalten, durchdringen und vereinen. Die besonders einfachen und grundlegenden Strukturen treten dabei oft erst zum Schluss hervor.

Egbert Brieskorn (1936–2013)

Inhalt dieses Kapitels I

Motivation und Überblick

In diesem Kapitel beginnen wir das Kerngeschäft der Linearen Algebra: lineare Räume (speziell Vektorräume) und ihre linearen Abbildungen.

Unser leuchtendes Vorbild ist dabei zunächst der Vektorraum $\mathbb{R}^n$ mit koordinatenweiser Addition und Skalierung (aka Skalarmultiplikation). Dieselbe Konstruktion gelingt ganz allgemein über jedem Ring R, wir erhalten so den linearen Raum R^I über R, siehe Beispiel I1A.

Aus diesen motivierenden Beispielen extrahieren wir die wesentlichen Rechenregeln und erheben diese anschließend zur Definition I1B. Zahlreiche relevante Beispiele und erste Eigenschaften belegen, dass wir damit einen nützlichen Begriff geschaffen haben.

Das Konzept der linearen Räume wird sich als sehr wirkungsvoll und praktisch erweisen, es ist eine gute Grundlage für alles Weitere.

Motivation und Überblick

Eine R–lineare Abbildung $f : U \to V$ zwischen R–linearen Räumen U und V erhält ihre Struktur, das heißt, f ist additiv und R–homogen.

Wir gelangen so zum Konzept des Homomorphismus von R–linearen Räumen (I1F), analog zu Homomorphismen von Gruppen (G1O). Auch hier belegen relevante Beispiele und erste Eigenschaften, dass wir damit einen nützlichen Begriff geschaffen haben.

Die Frage nach sinnvoller Verallgemeinerung ist meist nicht leicht und lässt sich wenn überhaupt immer nur rückblickend beantworten: Letztlich entscheiden darüber gute Erfahrungen im Aufbau der Theorie und zahlreicher Anwendungen, die Sie nach und nach sehen werden.

Hierzu legen wir in diesem Kapitel die Grundlagen und bauen Theorie und Anwendungen im weiteren Verlauf schrittweise immer weiter aus.

Motivation und Überblick

Im Vergleich mit der Literatur werden Sie feststellen, dass ich zunächst allgemein mit linearen Räumen über Ringen arbeite, wo andere Autoren lieber speziell mit Vektorräumen über Körpern beginnen. Beides hat gewisse Vor- und Nachteile, die Abwägung ist eine spannende Frage.

Zu Ihrer wohlwollenden Einstimmung will ich mein Vorgehen erklären und stelle dazu meine mathematisch-didaktischen Überlegungen voran.

Zugegeben, am liebsten wäre mir Lineare Algebra allein über Körpern, und geometrisch interessieren mich dabei $\mathbb{R}$ und $\mathbb{C}$ ganz besonders.

Doch dieser Wunsch nach Einfachheit stößt sich schnell an der Realität: Eher früher als später benötigen wir Matrixringe und Polynomringe, etc.

Die zugehörigen linearen Räume sind „so gut wie“ Vektorräume, aber eben nicht mehr über einem Körper, sondern nur noch einem Ring.

Das liegt in der Natur der Sache, die Realität ist manchmal kompliziert, und die mathematische Beschreibung soll ihr gerecht werden.

Motivation und Überblick

Ich beginne daher mit dem großen, recht weit gesteckten Rahmen der linearen Räume über Ringen. Das ermöglicht uns ein wesentlich größeres Spektrum an illustrativen und relevanten Beispielen.

Allein das halte ich bereits für ein starkes Argument, denn ein gut verstandenes Beispiel ist mehr wert als drei schlecht verstandene Sätze. Zudem sind die grundlegenden Begriffe und Techniken dieselben, daher verspüren wir anfangs kaum Drang und Zwang zu Körpern.

Wo wir Kommutativität und Invertierbarkeit wirklich benötigen, da macht der allgemeine Rahmen dies klar und verständlich. Zugegeben, wir müssen besonders sorgfältig arbeiten und genau hinsehen, aber das ist ja nicht schlecht, sondern eher zu begrüßen.

Auch den besonders schönen kommutativen Fall versteht man besser im nicht-kommutativen Kontext. So wissen Sie seine Annehmlichkeiten erst zu schätzen. *You don't know what you have until it's gone.*

Motivation und Überblick

Es wäre möglich, zunächst im kleinen Rahmen anzufangen, und dann schrittweise die Begriffe zu erweitern, je nach dem wachsenden Bedarf.

Das ist in gewisser Weise die historische Entwicklung; dieses Vorbild kann ein guter Ratgeber zur Didaktik sein, muss es aber nicht.

Unsere Zeit ist kostbar, daher müssen wir aus der historischen Entwicklung eine effiziente logische Entwicklung destillieren.

Sollte man dennoch klein anfangen, mit Körpern und Vektorräumen, oder gar, wie manche denken, allein mit $\mathbb{R}$ und $\mathbb{R}^n$ sowie $\mathbb{C}$ und $\mathbb{C}^n$?

Ein Vorteil ist, dass Körper und Vektorräume näher am geometrischen Modell der reellen Zahlen $\mathbb{R}$ und des euklidischen Raumes $\mathbb{R}^n$ sind.

Dieses hilfreiche Modell schult die geometrische Anschauung und verhilft uns zu einer Intuition, doch diese kann leider auch trügen.

Über allgemeinen Körpern oder gar Ringen sind voreilige Annahmen und falsche Vorstellungen eher hinderlich als hilfreich, sie müssen erst verlernt werden bevor sie dann erst richtig gelernt werden können.

Motivation und Überblick

Das Problem bei der schrittweisen Erweiterung der Begriffe ist nicht so sehr die Redundanz, die mag sogar helfen, sondern das Umstürzen liebgewonnener Gewissheiten, die plötzlich nicht mehr gelten, und die nötige Zeit des Umdenkens und neu Lernens.

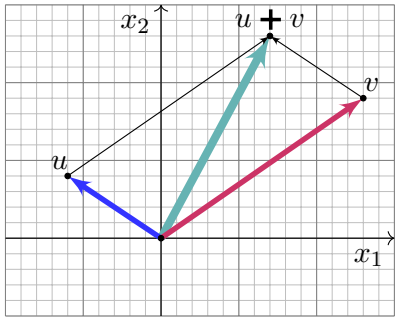
Letztendlich sind beide Wege durchaus möglich und auch erfolgreich. Die Wahl ist eine Entscheidung zwischen kurzfristiger Erleichterung und langfristigem Nutzen. Es ist wie bei der vollständigen Induktion:

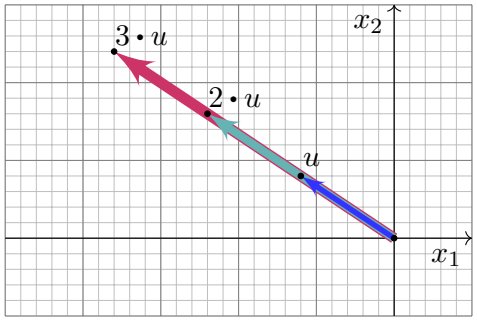
Ihre Investition von heute ist Ihr Ertrag von morgen!

Ich halte es daher für besser, Sie von Anfang an auf die nötige Vielfalt sanft vorzubereiten. Umso mehr schätzen wir die heile Welt der Körper.

If people do not believe that mathematics is simple,
it is only because they do not realize how complicated life is.
John von Neumann (1903–1957)

Addition und Skalierung von Vektoren im $\mathbb{R}^n$





Auf der Menge $\mathbb{R}^n = \{\, x = (x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R} \,\}$ nutzen wir die koordinatenweise Addition und Skalierung / Skalarmultiplikation:

$$+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n : (u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1 + v_1, \ldots, u_n + v_n)$$

$$\cdot : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n : \lambda \cdot (u_1, \ldots, u_n) = (\lambda \cdot u_1, \ldots, \lambda \cdot u_n)$$

Damit ist $(\mathbb{R}^n, +)$ eine abelsche Gruppe und $(\mathbb{R}^n, +, \cdot)$ ein Vektorraum über dem Körper $(\mathbb{R}, +, \cdot)$. Die Skalierung schreiben wir auch rechts:

$$\cdot : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n : (u_1, \ldots, u_n) \cdot \lambda = (u_1 \cdot \lambda, \ldots, u_n \cdot \lambda)$$

Addition und Skalierung von Vektoren im $\mathbb{R}^n$

Jedes n–Tupel $x = (x_1, \ldots, x_n)$ können wir auf zwei Arten betrachten:

1. Als einen Punkt im Raum $\mathbb{R}^n$, so wie oben als Kreis markiert.
2. Als Verschiebung des Raumes $\mathbb{R}^n$, oben als Pfeil dargestellt.

In der zweiten Sichtweise sind Addition und (ganzzahlige) Skalierung anschaulich die Hintereinanderausführung von Verschiebungen.

Physikalische Interpretation: Vektoren $x \in \mathbb{R}^n$ mit der oben erklärten Addition und Skalierung treten in Anwendungen auf als Verschiebungen, Geschwindigkeiten, Beschleunigungen, Kräfte, Felder, etc. Daher ist die Vektorrechnung grundlegend in Natur- und Ingenieurwissenschaften.

Wir nennen jedes Element $a \in \mathbb{R}$ des Grundkörpers $\mathbb{R}$ einen **Skalar** und jedes Element $x \in \mathbb{R}^n$ einen **Vektor**. Die Verknüpfung $+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ heißt daher auch **Vektoraddition**. Die Operation $\cdot : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ bzw. $\cdot : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ heißt **Skalierung** oder **Skalarmultiplikation**.

⚠ Der Begriff **Skalarprodukt** bezeichnet später etwas ganz anderes, nämlich eine Abbildung $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ mit *Werten* in den Skalaren.

Addition und Skalierung von Vektoren im $\mathbb{R}^n$

Notation: Zur Betonung oder als Gedächtnisstütze schreiben manche statt v gerne ein Vektorpfeilchen $\vec{v}$ oder Unterstrich $\underline{v}$ oder Fettdruck $\boldsymbol{v}$. Redundanz schadet selten, oft bietet sie eine willkommene Hilfestellung. Zudem setzt die Notation $\vec{v}$, $\underline{v}$, $\boldsymbol{v}$ o.ä. das einfache Symbol v wieder frei, das wird etwa in physikalischen Anwendungen gerne genutzt.

Schreiben und Sprechen beeinflussen unser Denken und Verstehen. Eine gute Notation vermeidet Missverständnisse und Fehlanwendung. Klarheit ist ein zentrales mathematisches Anliegen, darüber hinaus ist es meist eine Frage der Bequemlichkeit, des individuellen Geschmacks und der jeweils vorherrschenden Tradition, also eine soziale Konvention.

Für die Praxis empfiehlt sich, überflüssige Schnörkel wegzulassen und nur das Wesentliche so klar und präzise zu notieren, dass Lese- und Rechenfehler möglichst vermieden werden. Alle obigen Schreibweisen haben sich hierzu bewährt. Die wahre Kraft mathematischer Begriffe liegt nicht in ihrer *Schreibung*, sondern in ihrer *Bedeutung*!

Addition und Skalierung von Vektoren im $\mathbb{R}^n$

Wir wollen im Folgenden klären, wie man mit Vektoren effizient rechnet. Das gehört für viele Anwendungen zu den grundlegenden Werkzeugen. Oft wird dabei jedoch nicht nur der Körper $\mathbb{R}$ der reellen Zahlen genutzt, sondern etwa der Körper $\mathbb{C}$ oder $\mathbb{Q}$ oder $\mathbb{F}_p = \mathbb{Z}/p$, wie bereits gesehen.

Sehr häufig bilden die Skalare keinen Körper, sondern nur einen Ring, etwa die ganzen Zahlen $\mathbb{Z}$ oder Polynome $K[X]$ über einem Körper K. Die grundlegenden Rechenregeln sind auch hier zunächst dieselben! Es lohnt sich daher, zunächst die allgemeinen Grundlagen zu klären.

In den folgenden Kapiteln werden wir die Techniken weiter ausbauen: Über Divisionsringen haben wir den Gauß–Algorithmus B2C, den Sie bereits aus Kapitel B kennen. Über kommutativen Ringen verfügen wir über die Determinante, siehe Kapitel L. Über Körpern haben wir alles!

Wir werden unseren Werkzeugkasten nun schrittweise aufbauen.

Fundamentalbeispiel: Addition und Skalierung auf R^I

Beispiel I1A: Addition und Skalierung auf R^I

Sei $(R, +, 0, \cdot, 1)$ ein Ring, etwa $\mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \dots$, und I eine Menge.
Auf der Menge $R^I = \mathrm{Abb}(I, R) = \{\, u : I \to R : i \mapsto u_i \,\}$ der I–Tupel in R nutzen wir die koordinatenweise Addition und Skalarmultiplikation:

$$\begin{aligned} \boldsymbol{+} &: R^I \times R^I \to R^I : (u, v) \mapsto u \boldsymbol{+} v, \quad (u \boldsymbol{+} v)_i := u_i + v_i, \\ \boldsymbol{\cdot} &: R \times R^I \to R^I : (a, u) \mapsto a \boldsymbol{\cdot} u, \qquad (a \boldsymbol{\cdot} u)_i := a \cdot u_i. \end{aligned}$$

So ist $(R^I, \boldsymbol{+})$ eine abelsche Gruppe und $\boldsymbol{\cdot}$ eine distributive Operation:

$$\begin{aligned} a \boldsymbol{\cdot} (u \boldsymbol{+} v) &= (a \boldsymbol{\cdot} u) \boldsymbol{+} (a \boldsymbol{\cdot} v), \qquad 1 \boldsymbol{\cdot} u = u, \\ (a + b) \boldsymbol{\cdot} u &= (a \boldsymbol{\cdot} u) \boldsymbol{+} (b \boldsymbol{\cdot} u), \qquad (a \cdot b) \boldsymbol{\cdot} u = a \boldsymbol{\cdot} (b \boldsymbol{\cdot} u). \end{aligned}$$

Beispiele: Für den Körper $\mathbb{R}$ der reellen Zahlen und $I = \{1, \dots, n\}$ erhalten wir den Vektorraum $(\mathbb{R}^n, \boldsymbol{+}, \boldsymbol{\cdot})$ über $\mathbb{R}$ wie zuvor erklärt;
für $I = \mathbb{N}$ den Vektorraum $(\mathbb{R}^{\mathbb{N}}, \boldsymbol{+}, \boldsymbol{\cdot})$ aller Folgen $u : \mathbb{N} \to \mathbb{R} : n \mapsto u_n$;
für $I = \mathbb{R}$ den Vektorraum $(\mathbb{R}^{\mathbb{R}}, \boldsymbol{+}, \boldsymbol{\cdot})$ aller reellen Funktionen $u : \mathbb{R} \to \mathbb{R}$.

Fundamentalbeispiel: Addition und Skalierung auf R^I

Beispiel I1A: Addition und Skalierung auf R^I

Die Skalarmultiplikation schreiben wir links oder alternativ auch rechts:

$$\begin{aligned} \boldsymbol{+} &: R^I \times R^I \to R^I : (u, v) \mapsto u \boldsymbol{+} v, \quad (u \boldsymbol{+} v)_i := u_i + v_i, \\ \boldsymbol{\cdot} &: R^I \times R \to R^I : (u, a) \mapsto u \boldsymbol{\cdot} a, \qquad (u \boldsymbol{\cdot} a)_i := u_i \cdot a. \end{aligned}$$

Auch dies ist eine distributive Operation des Rings R auf $(R^I, \boldsymbol{+})$:

$$\begin{aligned} (u \boldsymbol{+} v) \boldsymbol{\cdot} a &= (u \boldsymbol{\cdot} a) \boldsymbol{+} (v \boldsymbol{\cdot} a), \qquad u \boldsymbol{\cdot} 1 = u, \\ u \boldsymbol{\cdot} (a + b) &= (u \boldsymbol{\cdot} a) \boldsymbol{+} (u \boldsymbol{\cdot} b), \qquad u \boldsymbol{\cdot} (b \cdot a) = (u \boldsymbol{\cdot} b) \boldsymbol{\cdot} a. \end{aligned}$$

Beide Schreibweisen sind nützlich und üblich, je nach Situation.
Ist der Ring R kommutativ, so sind beide Operationen gleich.

Beispiele: Diese Konstruktion gelingt über jedem Ring R:
So erhalten wir den Vektorraum $\mathbb{R}^I$ über dem Körper $\mathbb{R}$
und ebenso den Vektorraum $\mathbb{Q}^I$ über dem Körper $\mathbb{Q}$
sowie den linearen Raum $\mathbb{Z}^I$ über dem Ring $\mathbb{Z}$.

Fundamentalbeispiel: Addition und Skalierung auf R^I

Wir nennen $(R^I, \boldsymbol{+}, \boldsymbol{\cdot})$ einen linearen Raum über dem Ring $(R, +, \cdot)$.
Zur Betonung habe ich hier die Addition $\boldsymbol{+}$ und die Skalierung $\boldsymbol{\cdot}$ auf der Menge $V = R^I$ fett hervorgehoben. So unterscheiden wir sie graphisch von der zugrundeliegenden Addition $+$ und Multiplikation $\cdot$ der Skalare im Koeffizientenring $(R, +, \cdot)$. Das ist insbesondere für die ersten Rechnungen didaktisch sinnvoll, wie hier ausgeführt.

Diese pedantische Unterscheidung ist mathematisch gerechtfertigt: Streng genommen sind $\boldsymbol{+}$ und $+$ bzw. $\boldsymbol{\cdot}$ und $\cdot$ verschiedene Operationen, daher verdienen sie zur Klarheit auch verschiedene Bezeichnungen.

Auf Dauer wird diese Schreibweise jedoch lästig. Aus dem Kontext ist ohnehin jeweils klar, was gemeint ist, daher schreiben wir später beide Additionen kurz $+$ und beide Multiplikationen kurz $\cdot$. Das ist bequemer, daher ist diese *überladene Notation* allgemein beliebt und üblich.

Für die grundlegenden Rechnungen dieses Abschnitts betone ich weiterhin den Unterschied. Ich hoffe, diese Genauigkeit hilft Ihnen. Anschließend wird Ihnen die Unterscheidung dann leicht fallen.

Fundamentalbeispiel: Addition und Skalierung auf R^I

Hier wirken zwei algebraische Strukturen wunderbar zusammen:
einerseits die abelsche Gruppe $(V, \boldsymbol{+})$ auf der Menge $V = R^I$ mit der punktweise Addition $\boldsymbol{+} : V \times V \to V$, und andererseits die distributive Operation des Rings $(R, +, \cdot)$ von links / rechts auf dieser Gruppe $(V, \boldsymbol{+})$.

Gruppen haben wir zuvor schon ausführlich diskutiert, das hilft uns jetzt, denn all diese Begriffe und Techniken fließen hier nun unmittelbar ein.
Neu ist die Operation der Skalare $a \in R$ auf den Vektoren $u \in R^I$ durch Skalarmultiplikation $(a, u) \mapsto a \boldsymbol{\cdot} u$ bzw. $(u, a) \mapsto u \boldsymbol{\cdot} a$.

Das ist eine zusätzliche Struktur und unterscheidet die abelsche Gruppe $(V, \boldsymbol{+})$ vom linearen Raum $(V, \boldsymbol{+}, \boldsymbol{\cdot})$. Dies bietet wertvolle Möglichkeiten, wie wir im Folgenden immer wieder sehen werden:

Gute Eigenschaften des Rings R übertragen sich weitgehend auf den linearen Raum V, wir können daher unsere Rechentechniken für R auch für V nutzen! Dies gilt insbesondere für jeden Körper R.

Wir kehren die Sichtweise um und erheben diese Daten mit ihren grundlegenden Eigenschaften zur Definition:

Lineare Räume, links und rechts

Definition I1B: linearer Raum über einem Ring

Ein **linkslinearer Raum** $(V, \mathbf{+}, \bullet)$ über dem Ring $(R, +, \cdot)$ besteht aus einer abelschen Gruppe $(V, \mathbf{+})$ und einer Skalierung $\bullet : R \times V \to V$ von links, sodass für alle $a, b \in R$ und $u, v \in V$ gilt:

$$a \bullet (u \mathbf{+} v) = (a \bullet u) \mathbf{+} (a \bullet v), \qquad 1 \bullet v = v,$$
$$(a + b) \bullet v = (a \bullet v) \mathbf{+} (b \bullet v), \qquad (a \cdot b) \bullet v = a \bullet (b \bullet v).$$

Ein **rechtslinearer Raum** $(V, \mathbf{+}, \bullet)$ über dem Ring $(R, +, \cdot)$ besteht aus einer abelschen Gruppe $(V, \mathbf{+})$ und einer Skalierung $\bullet : V \times R \to V$ mit

$$(u \mathbf{+} v) \bullet a = (u \bullet a) \mathbf{+} (v \bullet a), \qquad v \bullet 1 = v,$$
$$v \bullet (a + b) = (v \bullet a) \mathbf{+} (v \bullet b), \qquad v \bullet (b \cdot a) = (v \bullet b) \bullet a.$$

Eine solche Skalarmultiplikation $\bullet$ ist eine **distributive Operation** des Rings $(R, +, \cdot)$ von links bzw. rechts auf der Gruppe $(V, \mathbf{+})$.

Wir nennen $(V, \mathbf{+}, \bullet)$ einen **Vektorraum** über R, falls R ein Divisionsring ist, also ein Körper wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ oder ein Schiefkörper wie $\mathbb{H}$.

Lineare Räume, links und rechts

Die Skalierung schreiben wir je nach Anwendung links oder rechts, das ergibt sich oft zwangsläufig aus der vorliegenden Situation.

Beides nennen wir kurz einen R–linearen Raum; ob die Skalierung rechts oder links geschrieben wird, ergibt sich dann aus dem Kontext.

Pars pro toto: Oft sagt man „der Ring R“, meint aber $\underline{R} = (R, +, \cdot)$, oder entsprechend „der R–lineare Raum V“, meint aber $\underline{V} = (V, \mathbf{+}, \bullet)$.

Ist $(V, \mathbf{+}, \bullet)$ ein linearer Raum über dem Ring $(R, +, \cdot)$, so schreiben wir kurz $(V, \mathbf{+}, \bullet) \in {}_R\mathbf{Lin}$ für linkslinear und $(V, \mathbf{+}, \bullet) \in \mathbf{Lin}_R$ für rechtslinear. Ist R kommutativ, so ist beides gleich und wir schreiben meist $\mathbf{Lin}_R$.

Die traditionell üblichen Bezeichnungen hierzu sind die folgenden: Statt linearer Raum nennt man V auch einen **Modul** über dem Ring R, kurz R–Modul, geschrieben links $V \in {}_R\mathbf{Mod}$ oder rechts $V \in \mathbf{Mod}_R$.

Ist der Skalarring R ein Körper wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \ldots$ oder ein Schiefkörper wie $\mathbb{H}$, so nennen wir V einen **Vektorraum** über R, kurz R–Vektorraum, geschrieben links $V \in {}_R\mathbf{Vec}$ oder rechts $V \in \mathbf{Vec}_R$.

Lineare Räume: erste Beispiele

Sei weiterhin $(R, +, \cdot)$ ein Ring, etwa $\mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \ldots$.

Beispiel: Die triviale Gruppe $(\{\mathbf{0}\}, \mathbf{+})$ ist ein linearer Raum über R. Die einzig mögliche Skalierung ist hier $\bullet : R \times \{\mathbf{0}\} \to \{\mathbf{0}\} : a \bullet \mathbf{0} = \mathbf{0}$. Wir nennen $(\{\mathbf{0}\}, \mathbf{+}, \bullet)$ den **Nullraum**, geschrieben $\{\mathbf{0}\}$ oder kurz $\mathbf{0}$.

Beispiel: Die abelsche Gruppe $(R^I, \mathbf{+})$ wird zu einem linearen Raum über dem Ring $(R, +, \cdot)$ durch die Skalierung $\bullet$ wie oben erklärt (I1A). Insbesondere erhalten wir so den R–linearen Raum R^n und $R^1 = R$.

Beispiel: Ist $S \leq R$ ein Teilring, so ist $(R, +, \bullet)$ ein linearer Raum über S dank $\bullet : S \times R \to R : (a, v) \mapsto a \cdot v$ bzw. $\bullet : R \times S \to R : (v, a) \mapsto v \cdot a$. So sind die Polynome $\mathbb{R}[X]$ ein Vektorraum über $\mathbb{R} \leq \mathbb{R}[X]$.

Beispiel: Die komplexen Zahlen $\mathbb{C}$ sind ein Vektorraum über $\mathbb{R} \leq \mathbb{C}$. Ebenso sind die reellen Zahlen $\mathbb{R}$ ein Vektorraum über $\mathbb{Q} \leq \mathbb{R}$ und die rationalen Zahlen $\mathbb{Q}$ ein linearer Raum über $\mathbb{Z} \leq \mathbb{Q}$.

Lineare Räume: erste Beispiele

Beispiel: Auf der abelschen Gruppe $(\mathbb{C}^I, \mathbf{+})$ haben wir die Skalierung

$$\bullet : \mathbb{C} \times \mathbb{C}^I \to \mathbb{C}^I \; : \; (a \bullet v)_i = a \cdot v_i.$$

Damit ist $(\mathbb{C}^I, \mathbf{+}, \bullet)$ ein Vektorraum über $\mathbb{C}$, wie oben gesehen.

Ebenso können wir mit der komplex-konjugierten Zahl multiplizieren:

$$\odot : \mathbb{C} \times \mathbb{C}^I \to \mathbb{C}^I \; : \; (a \bullet v)_i = \overline{a} \cdot v_i.$$

Damit ist $(\mathbb{C}^I, \mathbf{+}, \odot)$ ebenfalls ein Vektorraum über $\mathbb{C}$, denn es gilt

$$a \odot (u \mathbf{+} v) = (a \odot u) \mathbf{+} (a \odot v), \qquad 1 \odot v = v,$$
$$(a + b) \odot v = (a \odot v) \mathbf{+} (b \odot v), \qquad (a \cdot b) \odot v = a \odot (b \odot v).$$

⚠ Die jeweils betrachtete Skalarmultiplikation $R \times V \to V$ ist eine zusätzliche Struktur, sie folgt i.A. nicht allein aus der Gruppe $(V, \mathbf{+})$.

Zur Präzisierung müssen wir explizit angeben, was genau gemeint ist. Lineare Räume $(V, \mathbf{+}, \bullet)$ sind daher Tripel, nicht bloß Paare $(V, \mathbf{+})$.

Lineare Räume: erste Beispiele

Beispiel: Sei $(R, +, \cdot)$ ein Ring und $p, q \in \mathbb{N}_{\geq 1}$ natürliche Zahlen.
Die Menge der $p \times q$–Matrizen bildet die abelsche Gruppe $(R^{p\times q}, \mathbf{+})$.

Sie wird ein linkslinearer bzw. rechtslinearer Raum über R vermöge

$$\bullet : R \times R^{p\times q} \to R^{p\times q} : (\lambda, A) \mapsto B = \lambda \bullet A, \;\; b_{ij} = \lambda \cdot a_{ij},$$
$$\bullet : R^{p\times q} \times R \to R^{p\times q} : (A, \lambda) \mapsto C = A \bullet \lambda, \;\; c_{ij} = a_{ij} \cdot \lambda.$$

Sie wird ein linkslinearer Raum über dem Ring $(R^{p\times p}, +, \cdot)$ vermöge

$$\bullet : R^{p\times p} \times R^{p\times q} \to R^{p\times q} : (S, A) \mapsto B = S \bullet A, \;\; b_{ik} = \textstyle\sum_{j=1}^{p} s_{ij} \cdot a_{jk}.$$

Sie wird ein rechtslinearer Raum über dem Ring $(R^{q\times q}, +, \cdot)$ vermöge

$$\bullet : R^{p\times q} \times R^{q\times q} \to R^{p\times q} : (A, T) \mapsto C = A \bullet T, \;\; c_{ik} = \textstyle\sum_{j=1}^{q} a_{ij} \cdot t_{jk}.$$

Speziell $q = 1$: Spaltenvektoren bilden die abelsche Gruppe $(R^{p\times 1}, \mathbf{+})$.
Sie ist ein linkslinearer Raum über $R^{p\times p}$, rechtslinear über $R^{1\times 1} = R$.

Speziell $p = 1$: Zeilenvektoren bilden die abelsche Gruppe $(R^{1\times q}, \mathbf{+})$.
Sie ist ein linkslinearer Raum über $R^{1\times 1} = R$, rechtslinear über $R^{q\times q}$.

Lineare Räume: erste Beispiele

🙂 Dieses Beispiel von Matrizen und Vektoren zeigt sehr eindrücklich, warum wir links und rechts im Allgemeinen sorgsam unterscheiden.

Jede Linksoperation des Rings $(R, +, \cdot)$ ist eine Rechtsoperation des entgegengesetzten Rings $(R, +, \cdot^{\mathrm{op}})$ und ebenso umgekehrt.

Ist der Ring $(R, +, \cdot)$ kommutativ, also $a \cdot b = b \cdot a$ für alle $a, b \in R$, so ist die Skalierung links oder rechts nur eine Frage der Vorliebe.

Beide Notation sind üblich und bequem, daher bereite ich sie hier vor, damit Sie anschließend problemlos darauf zurückgreifen können.

Oft wird nur eine Seite erklärt, typischerweise links, und das ist aus logischer Sicht auch vollkommen ausreichend. In der Praxis werden dann aber doch beide Seiten verwendet, und jede/r muss sich dann seinen Teil denken. Dieses Vorgehen ist möglich, aber nicht ideal.

Beispiel: Der Schiefkörper $\mathbb{H} = \mathbb{R}[\mathrm{i}, \mathrm{j}, \mathrm{k}]$ der Quaternionen ist ein Vektorraum über dem Teilkörper $\mathbb{C} = \mathbb{R}[\mathrm{i}] \leq \mathbb{H}$ der komplexen Zahlen. Obwohl $\mathbb{C}$ kommutativ ist, müssen wir dennoch die Skalierungen von links und rechts sorgsam unterscheiden, denn $\mathrm{i} \cdot \mathrm{j} = -\mathrm{j} \cdot \mathrm{i}$.

Lineare Räume, links und rechts

Muss es wirklich so allgemein sein? Dazu gibt es sehr verschiedene Ansichten. Am liebsten wäre mir Lineare Algebra allein über Körpern.

Doch dieser Wunsch nach Einfachheit stößt sich schnell an der Realität: Eher früher als später benötigen wir Matrixringe und Polynomringe, etc.

Die zugehörigen linearen Räume sind „so gut wie“ Vektorräume, aber eben nicht mehr über einem Körper, sondern nur noch einem Ring.

Das liegt in der Natur der Sache, die Realität ist manchmal kompliziert, und die mathematische Beschreibung soll ihr gerecht werden.

Es wäre möglich, zunächst im kleinen Rahmen anzufangen, und dann schrittweise die Begriffe zu erweitern, je nach dem wachsenden Bedarf.

Das Problem dabei ist nicht die Redundanz, die mag sogar helfen, sondern dass liebgewonnene Gewissheiten plötzlich nicht mehr gelten.

Ich halte es daher für besser, Sie von Anfang an auf die nötige Vielfalt sanft vorzubereiten. Umso mehr schätzen wir die heile Welt der Körper.

Lineare Räume, links und rechts

Müssen wir wirklich links und rechts unterscheiden? Über kommutativen Ringen ist dies nur ein rein formaler Unterschied in der Schreibweise:

Jede Linksskalierung kann ebenso gut rechts geschrieben werden, und umgekehrt; die geforderten Axiome bleiben dabei erhalten.

Über nicht-kommutativen Ringen, zum Beispiel Matrixringen wie oben, ist die Unterscheidung jedoch wesentlich. . . und nicht weiter schwer.

Eine gewisse Selbstdisziplin bei der Notation ist erfahrungsgemäß hilfreich, begründete Vereinfachungen sind umso mehr willkommen.

Es scheint mir daher auch hier ehrlich, zunächst sorgsam vorzugehen und nicht voreilig „links gleich rechts“ auszurufen.

„Na prima“, sagt der Mensch, „das war ja einfach“,
und beweist, weil’s gerade so schön ist, dass schwarz gleich weiß ist,
und kommt wenig später auf einem Zebrastreifen unter die Räder.
Douglas Adams (1952–2001), *Per Anhalter durch die Galaxis*

Rechenregeln für lineare Räume

Lemma I1C: Null und Negation

Sei $(V, \mathbf{+}, \cdot)$ ein linearer Raum über dem Ring $(R, +, 0, \cdot, 1)$, also eine abelsche Gruppe $(V, \mathbf{+}, \mathbf{0}, \mathbf{-})$ mit distributiver Operation $\cdot : R \times V \to V$ von links bzw. $\cdot : V \times R \to V$ von rechts. Für alle $a \in R$ und $v \in V$ gilt:

1. $a \cdot \mathbf{0} = \mathbf{0}$ bzw. $\mathbf{0} \cdot a = \mathbf{0}$
2. $0 \cdot v = \mathbf{0}$ bzw. $v \cdot 0 = \mathbf{0}$
3. $(-1) \cdot v = \mathbf{-}v$ bzw. $v \cdot (-1) = \mathbf{-}v$

Beweis: (1) Es gilt $a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = (a \cdot \mathbf{0}) + (a \cdot \mathbf{0})$.
Addition von $\mathbf{-}(a \cdot \mathbf{0})$ ergibt $\mathbf{0} = a \cdot \mathbf{0}$, wie behauptet.

(2) Es gilt $0 \cdot v = (0 + 0) \cdot v = (0 \cdot v) + (0 \cdot v)$.
Addition von $\mathbf{-}(0 \cdot v)$ ergibt $\mathbf{0} = 0 \cdot v$.

(3) Es folgt $v + ((-1) \cdot v) = (1 \cdot v) + ((-1) \cdot v) = (1 - 1) \cdot v = 0 \cdot v = \mathbf{0}$.
In der Gruppe $(V, \mathbf{+}, \mathbf{0})$ ist somit $(-1) \cdot v = \mathbf{-}v$ das Inverse zu v. QED

Konvention: Wir sparen Klammern und schreiben $u + (a \cdot v) = u + a \cdot v$ (Punkt vor Strich). Für die Multiplikation schreiben wir statt $a \cdot v$ kurz av.

Kürzungsregeln für Vektorräume

Lemma I1D: Kürzungsregel

Sei $(V, \mathbf{+}, \cdot)$ ein linearer Raum über dem Divisionsring $(R, +, \cdot)$, etwa von links vermöge $\cdot : R \times V \to V$. Für alle $a, b \in R$ und $u, v \in V$ gilt:

1. Torsionsfreiheit:
   $a \neq 0 \wedge v \neq \mathbf{0} \;\Rightarrow\; a \cdot v \neq \mathbf{0}$
   $a \cdot v = \mathbf{0} \;\Rightarrow\; a = 0 \vee v = \mathbf{0}$
2. Kürzungsregel:
   $a \cdot u = a \cdot v \wedge a \neq 0 \;\Rightarrow\; u = v$
   $a \cdot v = b \cdot v \wedge v \neq \mathbf{0} \;\Rightarrow\; a = b$

Beweis: (1) Gilt $a \cdot v = \mathbf{0}$ und $a \neq 0$, so können wir mit a^{-1} multiplizieren:

$$\mathbf{0} = a^{-1} \cdot \mathbf{0} = a^{-1} \cdot (a \cdot v) = (a^{-1} \cdot a) \cdot v = 1 \cdot v = v$$

(2a) Aus $a \cdot u = a \cdot v$ folgt $\mathbf{0} = (a \cdot u) - (a \cdot v) = a \cdot (u - v)$.
Dank (1) und $a \neq 0$ folgt $u - v = \mathbf{0}$, somit $u = v$.

(2b) Aus $a \cdot v = b \cdot v$ folgt $\mathbf{0} = (a \cdot v) - (b \cdot v) = (a - b) \cdot v$.
Dank (1) und $v \neq \mathbf{0}$ folgt $a - b = 0$, somit $a = b$. QED

Rechenregeln für lineare Räume

☺ Wir sehen in der Rechnung noch einmal sehr schön, wie die Axiome des linearen Raumes $(V, \mathbf{+}, \cdot)$ hier wunderbar zusammenarbeiten!

☺ Das Lemma gilt wörtlich genauso bei distributiver Operation $\cdot : V \times R \to V$ des Rings R von rechts auf der abelschen Gruppe $(V, \mathbf{+})$.

Aussage (1) ist eine Besonderheit über Divisionsringen, für beliebige Ringe gilt dies nicht. Zur Illustration betrachten wir die Spaltenvektoren $(R^{n\times 1}, \mathbf{+}, \cdot)$ als linkslinearen Raum über dem Matrixring $(R^{n\times n}, +, \cdot)$:

Beispiel: Für 2×2–Matrizen über den reellen Zahlen $\mathbb{R}$ gilt:

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \text{und} \quad \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Hier lässt sich die Linkskürzungsregel nicht anwenden! Ebenso gilt:

$$\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \quad \text{und} \quad \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

Auch die Rechtskürzungsregel lässt sich demnach hier nicht anwenden!

Rechenregeln für lineare Räume

Beispiel: Die abelsche Gruppe $(\mathbb{Z}/n, +)$ wird zu einem $\mathbb{Z}$–linearen Raum vermöge der (einzig möglichen) Skalarmultipikation

$$\cdot : \mathbb{Z} \times \mathbb{Z}/n : a \cdot [b] = [a \cdot b].$$

Für $n \in \mathbb{N}_{\geq 2}$ finden wir Torsion: Für $n \neq 0$ und $[b] \neq [0]$ gilt

$$n \cdot [b] = [n \cdot b] = [0].$$

Noch etwas konkreter betrachten wir $\mathbb{Z}/6$ und

$$3 \cdot [2] = [0].$$

Ebenso ist $(\mathbb{Z}/n, +)$ ein $\mathbb{Z}/n$–linearer Raum. Hier entspricht Torsion den Nullteilern des Rings $\mathbb{Z}/n$. Zu Illustration betrachten wir wieder $\mathbb{Z}/6$ und

$$[3] \cdot [2] = [0].$$

Diese Schwierigkeiten können über einem Divisionsring R nicht auftreten, das ist genau die Aussage des obigen Lemmas.

Lineare Räume: logische Spitzfindigkeit

☺ In Definition I1B des linearen Raumes $(V, +, \cdot)$ sind manche der acht Axiome redundant und folgen automatisch aus den anderen Axiomen:

Insbesondere müssen additive Inverse und Kommutativität nicht explizit gefordert werden, wir können sie aus den anderen Axiomen folgern.

Wenn Sie also spitzfindig sein wollen, oder besonders effizient und ökonomisch arbeiten, dann können Sie noch etwas Arbeit sparen.

Sollten wir die Axiome auf ein logisches Minimum reduzieren?
Hier gehen die Ansichten und Vorlieben etwas auseinander...

Ich formuliere Definition I1B nach ästhetisch-didaktischem Empfinden, so lässt sie sich besser aussprechen und auch leichter einprägen.

Die minimalistische Strenge formuliere ich lieber aus Übung:

Aufgabe: Sei $(V, +)$ eine Halbgruppe und $(R, +, 0, \cdot, 1)$ ein Ring mit einer distributiven Operation $\cdot : R \times V \to V$, sodass $0 \cdot V = \{0\}$ gilt.

Dann ist $(V, +)$ eine abelsche Gruppe und $(V, +, \cdot)$ ein R–linearer Raum. Dasselbe gilt bei distributiver Operation $\cdot : V \times R \to V$ von rechts.

Lineare Räume: logische Spitzfindigkeit

Lösung: (0) Das Element 0 ist beidseitig neutral zu $u \in V$:

$$u + 0 = (1 \cdot u) + (0 \cdot u) = (1 + 0) \cdot u = 1 \cdot u = u.$$
$$0 + u = (0 \cdot u) + (1 \cdot u) = (0 + 1) \cdot u = 1 \cdot u = u.$$

(1) Das Element $-u = (-1) \cdot u$ ist beidseitig invers zu u:

$$u + (-u) = 1 \cdot u + (-1) \cdot u = (1 + (-1)) \cdot u = 0 \cdot u = 0.$$
$$(-u) + u = (-1) \cdot u + 1 \cdot u = ((-1) + 1) \cdot u = 0 \cdot u = 0.$$

(2) Zur Kommutativität entwickeln wir $(1 + 1) \cdot (u + v)$ auf zwei Arten:

$$(1 + 1) \cdot (u + v) \overset{\text{DR}}{=} 1 \cdot (u + v) + 1 \cdot (u + v) \overset{\text{Ntr}}{=} u + v + u + v$$
$$(1 + 1) \cdot (u + v) \overset{\text{DL}}{=} (1 + 1) \cdot u + (1 + 1) \cdot v$$
$$\overset{\text{DR}}{=} 1 \cdot u + 1 \cdot u + 1 \cdot v + 1 \cdot v \overset{\text{Ntr}}{=} u + u + v + v$$

Wir addieren $-u$ von links, $-v$ von rechts und erhalten $u + v = v + u$.

Linearer Raum als abelsche Gruppe mit Ringoperation

Satz I1E: abelsche Gruppe mit Ringoperation

(0) Sei $(V, +)$ eine abelsche Gruppe. Die Menge $E = \mathrm{End}(V, +)$ bildet einen Ring $(E, +, \circ)$ mit punktweiser Addition $+$ und Komposition $\circ$:

$$+ : E \times E \to E : (f + g)(x) = f(x) + g(x),$$
$$\circ : E \times E \to E : (f \circ g)(x) = f(g(x)).$$

Sei $(R, +, \cdot)$ ein Ring und $\varphi : R \to E$ eine Abbildung. Äquivalent sind:

(1) Die Abbildung $\varphi : (R, +, \cdot) \to (E, +, \circ)$ ist ein Ringhomomorphismus.

(2) Die Verknüpfung $\cdot : R \times V \to V : (a, v) \mapsto a \cdot v = \varphi(a)(v)$ ist eine distributive Operation. Das heißt, für alle $a, b \in R$ und $u, v \in V$ gilt

$$a \cdot (u + v) = (a \cdot u) + (a \cdot v), \qquad 1 \cdot v = v,$$
$$(a + b) \cdot v = (a \cdot v) + (b \cdot v), \qquad (a \cdot b) \cdot v = a \cdot (b \cdot v).$$

Ebenso entspricht jeder Ringhomomorphismus $\varphi : (R, +, \cdot) \to (E, +, \bullet)$ einer Operation des Rings $(R, +, \cdot)$ von rechts auf der Gruppe $(V, +)$.

Linearer Raum als abelsche Gruppe mit Ringoperation

Übung: Führen Sie Aussage (0) und die Äquivalenz (1) ⇔ (2) aus. Sie müssen hierzu nichts Neues erfinden, sondern nur gewissenhaft die Definitionen anwenden, also einsetzen und ausrechnen!

Dieser Satz erklärt noch einmal auf eine weitere, unabhängige Weise, warum unsere Axiome I1B eines linearen Raumes „natürlich“ sind, also eine / die „richtige“ Verallgemeinerung unserer vorigen Beispiele:

☺ *Jede distributive Operation* $\cdot : R \times V \to V$ *auf* $(V, +)$ *entspricht einem Ringhomomorphismus* $\varphi : R \to \mathrm{End}(V, +)$*, und umgekehrt.*

Inzwischen sind uns Ringe und ihre Homomorphismen recht vertraut, und wir halten die vereinbarten Axiome für eine sinnvolle Grundlage. Diese Zuversicht übertragen wir nun von Ringen auf lineare Räume.

Die Frage nach sinnvoller Verallgemeinerung ist meist nicht leicht und lässt sich wenn überhaupt immer nur rückblickend beantworten: Letztlich entscheiden darüber gute Erfahrungen im Aufbau der Theorie und zahlreicher Anwendungen, die Sie nach und nach sehen werden.

Lineare Abbildungen erhalten die lineare Struktur.

Definition I1F: R–lineare Abbildung

Seien $(U,+,\cdot)$ und $(V,+,\cdot)$ lineare Räume über dem Ring $(R,+,\cdot)$.

(1) Ein **Gruppenhomomorphismus** $f:(U,+)\to(V,+)$ ist

$$\textbf{additiv:}\quad f(u+v)=f(u)+f(v)\quad \text{für alle } u,v\in U.$$

Hierfür schreiben wir kurz $f\in\mathrm{Hom}(U,V):=\mathrm{Hom}(U,+;V,+)$.

(2) Eine **R–lineare Abbildung** $f:(U,+,\cdot)\to(V,+,\cdot)$ ist additiv und

$$R\textbf{–homogen:}\quad f(a\cdot v)=a\cdot f(v)\quad \text{bzw.}\quad f(v\cdot a)=f(v)\cdot a$$

für alle $a\in R$ und $v\in U$. Wir nennen dann f einen **Homomorphismus von R–linearen Räumen** oder kurz einen **R–Homomorphismus**, geschrieben $f\in\mathrm{Hom}_R(U,V):=\mathrm{Hom}_{(R,+,\cdot)}(U,+,\cdot\,;V,+,\cdot)$.

Bemerkung: Zusammengefasst sind (1) und (2) äquivalent zu
(3) $f(u+a\cdot v)=f(u)+a\cdot f(v)$ bzw. $f(u+v\cdot a)=f(u)+f(v)\cdot a$.

Beweis: Für „(3) $\Rightarrow$ (1)“ wähle $a=1$. Für „(3) $\Rightarrow$ (2)“ wähle $u=0$.

Lineare Abbildungen erhalten die lineare Struktur.

Bitte beachten Sie, dass jedes der beiden Symbole $+$ und $\cdot$ hier in drei verschiedenen Bedeutungen auftritt: Für den Skalarring R als Addition und Multiplikation, zudem auf der Menge U als Addition $+:U\times U\to U$ und Skalarmultiplikation $\cdot:U\times R\to U$, ebenso auf der Menge V als Addition $+:V\times V\to V$ und Skalarmultiplikation $\cdot:V\times R\to V$.

Für die Homomorphismen der abelschen Gruppen schreiben wir kurz

$$\mathrm{Hom}(U,V)=\mathrm{Hom}(U,+;V,+).$$

Die zusätzliche Bedingung der R–Homogenität vermerken wir explizit durch die Angabe des Rings $(R,+,\cdot)$, meist kurz als Subskript R:

$$\mathrm{Hom}_R(U,V)=\mathrm{Hom}_{(R,+,\cdot)}(U,+,\cdot\,;V,+,\cdot).$$

Die lange Schreibweise rechts ist korrekt, aber lästig. Die Kurzform links genügt, solange die fehlenden Daten aus dem Kontext hervorgehen.

Sender und Empfänger treffen dabei eine wohlwollende Übereinkunft: Alle fehlenden Daten müssen aus dem Kontext erschlossen werden.

Komposition linearer Abbildungen

Schreibweise für R–**Homomorphismen** und R–**Isomorphismen**:

$$\begin{aligned}\mathrm{Hom}_R(U,V)&=\{\,f:U\to V \text{ linear}\,\}\\ \mathrm{Iso}_R(U,V)&=\{\,f:U\to V \text{ linear und bijektiv}\,\}\end{aligned}$$

Schreibweise für R–**Endomorphismen** und R–**Automorphismen**:

$$\begin{aligned}\mathrm{End}_R(V)&=\mathrm{Hom}_R(V,V)\\ \mathrm{Aut}_R(V)&=\mathrm{Iso}_R(V,V)=\mathrm{GL}(V)\end{aligned}$$

Lemma I1G: Komposition und Umkehrung

(0) Für jeden R–linearen Raum $(V,+,\cdot)$ ist die Identität $\mathrm{id}_V:V\to V$ ein Homomorphismus (und somit ein Iso-/Endo-/Automorphismus).

(1) Sind $f:(U,+,\cdot)\to(V,+,\cdot)$ und $g:(V,+,\cdot)\to(W,+,\cdot)$ Homomorphismen von R–linearen Räumen, so auch $g\circ f:(U,+,\cdot)\to(W,+,\cdot)$.

(2) Ist $f:(U,+,\cdot)\to(V,+,\cdot)$ ein bijektiver R–Homomorphismus, so auch die Umkehrabbildung $g=f^{-1}:(V,+,\cdot)\to(U,+,\cdot)$.

Aufgabe: Beweisen Sie dies zur Wiederholung (wie Lemma G1P).

Komposition linearer Abbildungen

Lösung: Aussage (0) ist klar.

Zum Beweis von (1) seien $u,v\in U$ und $a\in R$:

$$\begin{aligned}(g\circ f)(u+v\cdot a)&\overset{\text{Def}}{=}g(f(u+v\cdot a))\\ &\overset{\text{Lin}}{=}g(f(u)+f(v)\cdot a)\\ &\overset{\text{Lin}}{=}g(f(u))+g(f(v))\cdot a\\ &\overset{\text{Def}}{=}(g\circ f)(u)+(g\circ f)(v)\cdot a\end{aligned}$$

(2) Dank G1P wissen wir bereits, dass $g(x+y)=g(x)+g(y)$ gilt.

Erinnerung: Zu $x,y\in V$ sei $u=g(x)$ und $v=g(y)$. Damit folgt:

$$g(x+y)=g(f(u)+f(u))=g(f(u+v))=u+v=g(x)+g(y)$$

Für jeden Skalar $a\in R$ gilt nun ganz analog:

$$g(x\cdot a)=g(f(u)\cdot a)=g(f(u\cdot a))=u\cdot a=g(x)\cdot a$$

Somit ist auch g linear über R, also ein R–Homomorphismus.
Die Rechnung gilt genauso bei Skalarmultiplikation von links.

Lineare Abbildungen: erste Beispiele

Beispiel: Die Abbildung $f:\mathbb{R}\to\mathbb{R}:x\mapsto 3x$ ist $\mathbb{R}$–linear.
Sie ist ein $\mathbb{R}$–Automorphismus mit $f^{-1}:\mathbb{R}\to\mathbb{R}:x\mapsto \frac{1}{3}x$.

🙂 Rechnen Sie es nach! Es genügt einsetzen und ausrechnen.
Wir führen dies in Beispiel I1H ganz allgemein für Matrizen aus.

Beispiel: Die Abbildung $g:\mathbb{R}\to\mathbb{R}:x\mapsto 3x+2$ ist nicht $\mathbb{R}$–linear, nicht einmal additiv, denn insbesondere gilt $g(0)=2\neq 0$.

⚠ Im lässigen Sprachgebrauch wird oft auch g als lineare Funktion bezeichnet. Genauer (und richtig!) sollte man **affin-linear** sagen.

Beispiel: Die Betragsfunktion $h:\mathbb{R}\to\mathbb{R}:x\mapsto|x|$ ist nicht $\mathbb{R}$–linear, nicht einmal additiv: Es gilt $h(1+(-1))=0$ vs $h(1)+h(-1)=2$.

⚠ Positive Homogenität: Für alle $a\in\mathbb{R}_{\geq 0}$ gilt $h(a\cdot u)=a\cdot h(u)$.
Für $a<0$ gilt dies nicht mehr: $h(-1\cdot 7)=7$ vs $-1\cdot h(7)=-7$.

🙂 Zum Nachweis der Nicht-Linearität genügt *ein* Gegenbeispiel, so wie hier für die Funktionen g und h exemplarisch vorgeführt.

Lineare Abbildungen: erste Beispiele

Übung: Welche der folgenden Abbildungen sind $\mathbb{R}$–linear?

$$f_1:\mathbb{R}^2\to\mathbb{R}:\quad f_1\begin{pmatrix}x\\y\end{pmatrix}=\begin{cases}\frac{4x^2-9y^2}{2x-3y} & \text{falls } 2x\neq 3y,\\ 4x & \text{falls } 2x=3y,\end{cases}$$

$$f_2:\mathbb{R}^2\to\mathbb{R}:\quad f_2\begin{pmatrix}x\\y\end{pmatrix}=\begin{cases}\frac{4x^2-9y^2}{2x-3y} & \text{falls } 2x\neq 3y,\\ 5x & \text{falls } 2x=3y.\end{cases}$$

$$g_1:\mathbb{R}^2\to\mathbb{R}^2:\ g_1\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}|\sin(y)|-\sqrt{1-\cos(y)^2}\\ \sin(x)+\cos(x+\pi/2)\end{pmatrix}$$

$$g_2:\mathbb{R}^2\to\mathbb{R}^2:\ g_2\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}|\sin(y)|-\sqrt{1-\cos(y)^2}\\ \sin(x)+\cos(x-\pi/2)\end{pmatrix}$$

⚠ Gefordert ist nicht, dass die Abbildungsvorschrift linear „aussieht“, sondern einzig und allein, dass die Abbildung die Definition I1F erfüllt.

Lösung: $f_1(x,y)=2x+3y$ und $g_1(x,y)=(0,0)$ sind $\mathbb{R}$–linear, jedoch nicht f_2 und g_2: Es gilt $f_2(3,0)=6$ und $f_2(0,2)=6$ vs $f_2(3,2)=10$.
Für $u=(\pi/2,0)$ gilt $g_2(u+u)=(0,0)$ vs $g_2(u)+g_2(u)=(0,4)$.

Lineare Abbildungen: erste Beispiele

Beispiel: Seien $(U,+,\cdot)$ und $(V,+,\cdot)$ lineare Räume über dem Ring R.
Die Nullabbildung $\mathbf{0}:U\to V:u\mapsto 0$ ist R–linear, also $\mathbf{0}\in\mathrm{Hom}_R(U,V)$.

Beispiel: Die Projektion $\mathrm{pr}_i:R^n\to R:x\mapsto x_i$ ist R–linear, ebenso die Projektion $p_n^m:R^n\to R^m:(x_1,\ldots,x_n)\mapsto(x_1,\ldots,x_m)$ für $1\leq m\leq n$.

Beispiel: Die Auswertung $\delta_a:R^X\to R:f\mapsto f(a)$ ist R–linear, ebenso die Einschränkung $R^X\to R^Y:f\mapsto f|_Y$ für $Y\subseteq X$.

Beispiel: Die komplexe Konjugation

$$\mathrm{conj}\ :\ \mathbb{C}\to\mathbb{C}\ :\ z=x+\mathrm{i}y\ \mapsto\ \overline{z}=x-\mathrm{i}y$$

ist $\mathbb{R}$–linear, aber nicht $\mathbb{C}$–linear: Es gilt $\mathrm{conj}(\mathrm{i}\cdot 1)=-\mathrm{i}$ vs $\mathrm{i}\cdot\mathrm{conj}(1)=\mathrm{i}$.

🙂 Geometrische Anschauung, mathematische Intuition oder schlicht Erfahrung sind oft hilfreich. Lassen Sie sich davon ruhig inspirieren! Präzise Definitionen wirken und helfen Ihnen weit darüber hinaus: Sie schaffen Klarheit, wo uns Anschauung und Intuition verlassen!

Lineare Abbildungen: erste Beispiele

Übung: Sind die folgenden Abbildungen linear über $\mathbb{R}$? über $\mathbb{R}[X]$?

$$f\ :\ \mathbb{R}[X]\to\mathbb{R}[X]\ :\ P(X)\mapsto P(X)\cdot X^2,$$
$$g\ :\ \mathbb{R}[X]\to\mathbb{R}[X]\ :\ P(X)\mapsto P(X^2),$$
$$h\ :\ \mathbb{R}[X]\to\mathbb{R}[X]\ :\ P(X)\mapsto P(X)^2.$$

Antwort: (1) f ist linear über $\mathbb{R}[X]$ und somit $\mathbb{R}$. (2) g ist linear über $\mathbb{R}$; wir erkennen g als einen Einsetzungshomomorphismus (Satz G3E).
Aber g ist nicht $\mathbb{R}[X]$–homogen: etwa $g(X\cdot 1)=X^2$ vs $X\cdot g(1)=X$.
(3) h ist nicht additiv: etwa $h(X+X)=4X^2$ vs $h(X)+h(X)=2X^2$.

Übung: Jedes Polynom $P\in\mathbb{R}[X]^*$ definiert zwei Abbildungen

$$q\ :\ \mathbb{R}[X]\to\mathbb{R}[X]\ :\ S\mapsto S\ \mathrm{quo}\ P,$$
$$r\ :\ \mathbb{R}[X]\to\mathbb{R}[X]\ :\ S\mapsto S\ \mathrm{rem}\ P.$$

Sind diese linear über $\mathbb{R}$? und über $\mathbb{R}[X]$?

Antwort: Beide sind linear über $\mathbb{R}$, aber nicht linear über $\mathbb{R}[X]$.
Formulieren Sie dies explizit aus mit Hilfe von Satz G3H.

Matrizen wirken als lineare Abbildungen.

Beispiel I1H: Matrizen wirken als lineare Abbildungen.

Weiterhin sei $(R, +, \cdot)$ ein Ring, etwa $\mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \ldots$.
Jede Matrix $A \in R^{m\times n}$ definiert die zugehörige Abbildung

$$f = f_A : R^n \to R^m : v \mapsto Av.$$

(0) Dabei gilt $f_A \circ f_B = f_{AB}$ dank Assoziativität $A(Bv) = (AB)v$.
Genau dann ist f_A bijektiv, wenn A invertierbar ist (Satz B2D).

(1) Die Abbildung f ist additiv, denn für alle $u, v \in R^n$ gilt:

$$A(u + v) = Au + Av$$

(2) Zudem ist f rechtshomogen, denn für alle $v \in R^n$ und $\lambda \in R$ gilt:

$$A(v\lambda) = (Av)\lambda$$

(3) Ist der Ring R zudem kommutativ, so ist f auch linkshomogen:

$$A(\lambda v) = (A\lambda)v = (\lambda A)v = \lambda(Av)$$

Matrizen wirken als lineare Abbildungen.

Wir identifizieren R^n hier mit Spaltenvektoren $R^{n\times 1}$ und nutzen die Matrixmultiplikation, spezialisiert zu „Matrix mal Vektor“ vermöge

$$\bullet : R^{m\times n} \times R^{n\times 1} \to R^{m\times 1} : (A, v) \mapsto w = A \bullet v, \quad w_{i1} = \textstyle\sum_{j=1}^{n} a_{ij} \cdot v_{j1}.$$

Die Rechenregeln haben wir in Kapitel B sorgsam nachgerechnet.

🙂 Das ist für Sie bereits jetzt ein großer Vorteil: Sie verfügen über ein reichhaltiges Repertoire an illustrativen und relevanten Beispielen!

Für Beispiele wie I1H ist demnach nichts weiter zu tun; wenn Sie dies jedoch wünschen, kann eine explizite Wiederholung nicht schaden.

🙂 Fast alle Illustrationen dieses Kapitels sind ebenso direkt und leicht: Es genügt, die Definitionen einzusetzen und sorgsam auszurechnen.

Ich ermutige Sie, dies selbst zu versuchen und Routine zu entwickeln.
So werden Ihnen die neuen Begriffe und Techniken schnell vertraut.

Matrizen wirken als lineare Abbildungen.

Beispiel I1H illustriert eine wichtige Beobachtung:

⚠ Wenn wir über einem nicht-kommutativen Ring R arbeiten, dann sollten Matrizen und Skalare von entgegengesetzten Seiten operieren.

🙂 Über einem kommutativen Ring ist diese Unterscheidung unnötig.

In den anfänglichen Beispielen arbeiten wir meist über kommutativen Ringen, sogar über Körpern, das ist besonders einfach und elegant.

Aller Voraussicht nach werden Ihnen bald auch nicht-kommutative Situationen begegnen, spätestens wenn Sie mit Matrizen arbeiten. Dann sollten Sie wissen, wie man korrekt damit umgeht.

Auch den besonders schönen kommutativen Fall versteht man besser im nicht-kommutativen Kontext. So wissen Sie seine Annehmlichkeiten erst zu schätzen. *You don't know what you have until it's gone.*

Von Matrizen zu Homomorphismen

🙂 Matrizen und Homomorphismen über R verhalten sich ähnlich.
Diese Analogie werden wie im Folgenden immer weiter ausbauen.

Warum bleiben wir nicht gleich bei Matrizen? Nun, die Erfahrung zeigt:
Matrizen sind wunderbar konkret, aber nur eingeschränkt nutzbar.
Homomorphismen sind allgemeiner und viel flexibler einsetzbar.

Für Matrizen über R haben wir hilfreiche Rechenregeln, die Sie aus Kapitel B kennen, und die uns seitdem stets gute Dienste leisten.

Diese nützlichen Rechenregeln wollen wir nun auf R–Homomorphismen übertragen, soweit möglich. Das ist das Ziel der beiden folgenden Sätze.

Den ersten Satz werde ich für Sie hier ausführlich beweisen,
den Beweis des zweiten Satzes empfehle ich Ihnen als Übung.

Auch Homomorphismen wollen Vektoren sein.

Satz I1I: die Homomorphismengruppe $\mathrm{Hom}(U,V) \geq \mathrm{Hom}_R(U,V)$

Weiterhin seien $(U,+,\cdot)$ und $(V,+,\cdot)$ lineare Räume über dem Ring R.

(1) Die Menge $V^U = \mathrm{Abb}(U,V)$ aller Abbildungen $f,g : U \to V$ wird zu einer abelschen Gruppe $(\mathrm{Abb}(U,V),+)$ mit der punktweisen Addition:

$$(f+g)(u) := f(u) + g(u) \quad \text{für alle } u \in U$$

Darin liegen die Homomorphismen als Untergruppe:

$$\mathrm{Abb}(U,V) \geq \mathrm{Hom}(U,V) \geq \mathrm{Hom}_R(U,V)$$

(2) Zudem sind $\mathrm{Abb}(U,V) \geq \mathrm{Hom}(U,V)$ lineare Räume über R vermöge der punktweisen Skalarmultiplikation mit $\lambda \in R$:

$$(\lambda \cdot f)(u) := \lambda \cdot f(u) \quad \text{bzw.} \quad (f \cdot \lambda)(u) := f(u) \cdot \lambda.$$

Ist R zudem kommutativ, so ist auch $\mathrm{Hom}_R(U,V)$ ein R–linearer Raum.

🙂 Sind U, V Vektorräume über einem Körper K, so auch $\mathrm{Hom}_K(U,V)$.

Auch Homomorphismen wollen Vektoren sein.

Beweis: (1) Für jede Menge U ist $(\mathrm{Abb}(U,V),+)$ eine Gruppe (G1Y).

Sind $f,g : U \to V$ additiv, so auch $f+g$, denn für alle $u,v \in U$ gilt:

$$\begin{aligned}(f+g)(u+v) &\overset{\text{Def}}{=} f(u+v)+g(u+v) \overset{\text{Add}}{=} f(u)+f(v)+g(u)+g(v)\\ &\overset{\text{Com}}{=} f(u)+g(u)+f(v)+g(v) \overset{\text{Def}}{=} (f+g)(u)+(f+g)(v)\end{aligned}$$

Sind $f,g : U \to V$ sogar R–linear, so auch $f+g$, denn für alle $a \in R$ gilt:

$$\begin{aligned}(f+g)(u\cdot\lambda) &\overset{\text{Def}}{=} f(u\cdot\lambda)+g(u\cdot\lambda) \overset{\text{Lin}}{=} f(u)\cdot\lambda+g(u)\cdot\lambda\\ &\overset{\text{DL}}{=} (f(u)+g(u))\cdot\lambda \overset{\text{Def}}{=} (f+g)(u)\cdot\lambda\end{aligned}$$

(2) Für jede Menge U ist $(\mathrm{Abb}(U,V),+,\cdot)$ ein R–linearer Raum wie im Fundamentalbeispiel I1A. Ist $f : U \to V$ additiv, so auch $f \cdot \lambda$, denn:

$$\begin{aligned}(f\cdot\lambda)(u+v) &\overset{\text{Def}}{=} f(u+v)\cdot\lambda \overset{\text{Add}}{=} (f(u)+f(v))\cdot\lambda\\ &\overset{\text{DL}}{=} f(u)\cdot\lambda+f(v)\cdot\lambda \overset{\text{Def}}{=} (f\cdot\lambda)(u)+(f\cdot\lambda)(v)\end{aligned}$$

Ist R kommutativ und $f : U \to V$ linear über R, so auch $f \cdot \lambda$, denn:

$$\begin{aligned}(f\cdot\lambda)(u\cdot\mu) &\overset{\text{Def}}{=} f(u\cdot\mu)\cdot\lambda \overset{\text{Lin}}{=} f(u)\cdot\mu\cdot\lambda\\ &\overset{\text{Com}}{=} f(u)\cdot\lambda\cdot\mu \overset{\text{Def}}{=} (f\cdot\lambda)(u)\cdot\mu\end{aligned}$$

Die Rechnungen gelten genauso bei Skalarmultiplikation von links. QED

Endomorphismenringe

Satz I1J: der Endomorphismenring $\mathrm{End}(V) \geq \mathrm{End}_R(V)$

Weiterhin seien $(U,+,\cdot)$, $(V,+,\cdot)$, $(W,+,\cdot)$ lineare Räume über R.
Wir betrachten die Komposition von Homomorphismen:

$$\begin{aligned}\circ &: \mathrm{Hom}(V,W) \times \mathrm{Hom}(U,V) \to \mathrm{Hom}(U,W) : (g,f) \mapsto g \circ f\\ \circ &: \mathrm{Hom}_R(V,W) \times \mathrm{Hom}_R(U,V) \to \mathrm{Hom}_R(U,W) : (g,f) \mapsto g \circ f\end{aligned}$$

(1) Komposition ist additiv in jedem der beiden Faktoren:

$$\begin{aligned}(g_1+g_2)\circ f &= g_1\circ f + g_2 \circ f,\\ g\circ(f_1+f_2) &= g\circ f_1 + g\circ f_2.\end{aligned}$$

(2) Die Endomorphismenmenge $\mathrm{End}(V) = \mathrm{End}(V,+)$ wird zu einem Ring $(\mathrm{End}(V),+,\circ)$ mit punktweiser Addition $+$ und Komposition $\circ$. Darin liegt $(\mathrm{End}_R(V),+,\circ) \leq (\mathrm{End}(V),+,\circ)$ als Unterring.

(3) Ist R kommutativ, so ist die Komposition von R–Homomorphismen sogar R–linear in jedem der beiden Faktoren, und wir haben zudem den zentralen Ringhomomorphismus $R \to \mathrm{End}_R(V) : \lambda \mapsto \lambda \cdot \mathrm{id}_V$.

Endomorphismenringe

Bemerkung: Additivität (1) gilt für Gruppenhomomorphismen Hom, somit insbesondere für R–lineare Abbildungen $\mathrm{Hom}_R \leq \mathrm{Hom}$.

Daraus folgt die Ringeigenschaft (2) von $\mathrm{End}(V) \geq \mathrm{End}_R(V)$.
Für die R–Linearität (3) benötigen wir, dass R kommutativ ist.

Im Endomorphismenring $\mathrm{End}(V) \geq \mathrm{End}_R(V)$ ist $\mathrm{Aut}(V) = \mathrm{End}(V)^\times$ bzw. $\mathrm{Aut}_R(V) = \mathrm{End}_R(V)^\times$ die Gruppe der invertierbaren Elemente.

Übung: Rechnen Sie die Aussagen dieses Satzes sorgsam nach.
Dies ist eine hilfreiche Übung zum Verständnis der Definitionen.

Wie in der vorigen Aufgabe müssen Sie hierzu nichts Neues erfinden, sondern nur gewissenhaft die Definitionen einsetzen und ausrechnen.

Das ist anfangs schwierig, solange die Begriffe noch ungewohnt sind.
Ich ermutige Sie, es selbst zu versuchen und Routine zu entwickeln.

🙂 Sie sollten vor solchen allgemeinen Sätzen keine Angst haben, sondern sie freudig begrüßen und als schön und nützlich erkennen.
Die Rechnungen sind zwar länglich, aber nicht wirklich schwierig, und sie belegen: Alle Begriffe fügen sich wunderbar zusammen!

Lineare Räume über $\mathbb{Z}$

Beispiel I1K: $\mathbb{Z}$–lineare Räume und Abbildungen

(0) Jede abelsche Gruppe $(V,+)$ ist ein $\mathbb{Z}$–linearer Raum vermöge

$$\bullet : V \times \mathbb{Z} \to V \ : \ (v,n) \mapsto v \bullet n = \begin{cases} \sum_{k=1}^{+n} (+v) & \text{falls } n \geq 0, \\ \sum_{k=1}^{-n} (-v) & \text{falls } n \leq 0. \end{cases}$$

Dies ist die einzige distributive Operation des Rings $\mathbb{Z}$ auf $(V,+)$.

(1) Zu jedem $\mathbb{Z}$–linearen Raum $(V,+,\bullet)$ können wir allein aus $(V,+)$ die Skalarmultiplikation $\bullet : V \times \mathbb{Z} \to V$ eindeutig rekonstruieren.

(2) Jeder Gruppenhomomorphismus $f : (V,+) \to (W,+)$ zwischen abelschen Gruppen $(V,+)$ und $(W,+)$ ist automatisch $\mathbb{Z}$–linear:

$$f(v \bullet n) = f(v) \bullet n$$

Wörtlich dasselbe gilt für die Schreibweise als Vielfaches von links.

Lineare Räume über $\mathbb{Z}$

Dank Satz I1E wissen wir: Jede distributive Operation $\bullet : V \times R \to V$ entspricht einem Ringhomomorphismus $\varphi : (R,+,\cdot) \to (\mathrm{End}(V),+,\bullet)$.

Die obige Operation entspricht dem eindeutigen Ringhomomorphismus

$$\varphi \ : \ (\mathbb{Z},+,\cdot) \to (\mathrm{End}(V,+),\mathbf{+},\bullet) \ : \ n \mapsto \mathrm{id}_V \bullet n.$$

Bei Schreibweise als Vielfaches von links erhalten wir entsprechend

$$\varphi \ : \ (\mathbb{Z},+,\cdot) \to (\mathrm{End}(V,+),\mathbf{+},\circ) \ : \ n \mapsto n \bullet \mathrm{id}_V.$$

Das ist dieselbe Abbildung, denn $\mathrm{id}_V \bullet n = n \bullet \mathrm{id}_V = \mathrm{id}_V + \cdots + \mathrm{id}_V$.

Aus Satz G2H kennen wir die **Charakteristik** $k = \mathrm{char}(\mathrm{End}(V,+))$.
Positive Charakteristik $k > 0$ bedeutet $\mathrm{id}_V \bullet k = \sum_{i=1}^{k} \mathrm{id}_V = 0$.
Das bedeutet, für jedes Element $v \in V$ gilt $v \bullet k = \sum_{i=1}^{k} v = 0$.
Dabei ist $k \in \mathbb{N}_{\geq 1}$ die kleinste Zahl mit dieser Eigenschaft.

Diese Betrachtung für uns direkt zum nächsten Beispiel.

Lineare Räume über $\mathbb{Z}/p$

Beispiel I1L: $\mathbb{Z}/p$–lineare Räume und Abbildungen

Wie zuvor sei $(V,+)$ eine abelsche Gruppe mit $\bullet : V \times \mathbb{Z} \to V$.

(0) Gegeben sei $p \in \mathbb{N}$, sodass $v \bullet p = 0$ für alle $v \in V$ gilt.
Dann ist $(V,+)$ ein linearer Raum über dem Ring $\mathbb{Z}/p\mathbb{Z}$ vermöge

$$\bullet : V \times \mathbb{Z}/p\mathbb{Z} \to V \ : \ (v,[n]) \mapsto v \bullet [n] := v \bullet n.$$

Dies ist die einzige distributive Operation des Rings $\mathbb{Z}/p$ auf $(V,+)$.

Für $p = 0$ erhalten wir die Skalierung durch $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ wie zuvor.
Ist $p > 0$ prim, so ist $(V,+)$ ein Vektorraum über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(1) Zu jedem $\mathbb{Z}/p$–linearen Raum $(V,+,\bullet)$ können wir allein aus $(V,+)$ die Skalarmultiplikation $\bullet : V \times \mathbb{Z}/p \to V$ eindeutig rekonstruieren.

(2) Jeder Gruppenhomomorphismus $f : (V,+) \to (W,+)$ zwischen $\mathbb{Z}/p$–linearen Räumen $(V,+)$ und $(W,+)$ ist automatisch $\mathbb{Z}/p$–linear:

$$f(v \bullet [n]) = f(v) \bullet [n]$$

Lineare Räume über $\mathbb{Z}/2$

Beispiel: Sei X eine Menge. Die Potenzmenge $V = \mathfrak{P}(X)$ bildet die abelsche Gruppe $(V,\triangle,\emptyset)$ bezüglich der symmetrischen Differenz

$$A \triangle B = (A \smallsetminus B) \cup (B \smallsetminus A).$$

Für jedes Element $A \in V$, also jede Teilmenge $A \subseteq X$, gilt $A \triangle A = \emptyset$.
Somit ist $(V,\triangle)$ ein $\mathbb{F}_2$–Vektorraum, vermöge $A \bullet [0] = \emptyset$ und $A \bullet [1] = A$.

Wir haben die (kanonische, natürliche) Bijektion

$$(\mathbf{I}, \mathrm{supp}) \ : \ \mathfrak{P}(X) \ \cong \ \mathrm{Abb}(X,\{0,1\}).$$

Diese ist ein Isomorphismus von $\mathbb{F}_2$–Vektorräumen $(V,\triangle) \cong (\mathbb{F}_2^X,+)$.

Übung: Dies ist sogar ein Ringisomorphismus $(V,\triangle,\cap) \cong (\mathbb{F}_2^X,+,\cdot)$.

Lineare Räume über $\mathbb{Q}$

Beispiel I1M: $\mathbb{Q}$–lineare Räume und Abbildungen

Wie zuvor sei $(V,+)$ eine abelsche Gruppe mit $\bullet : V \times \mathbb{Z} \to V$.

(0) Zu jedem $n \in \mathbb{N}_{\geq 2}$ sei die Ver–n–fachung bijektiv,

$$\mu_n \,:\, V \xrightarrow{\sim} V \,:\, u \mapsto u \bullet n.$$

Das bedeutet: Zu jedem $v \in V$ existiert also genau eine n–Teilung $u \in V$ mit $u \bullet n = v$; wir definieren so $v/n := u = \mu_n^{-1}(v)$ und

$$\bullet \,:\, V \times \mathbb{Q} \to V \,:\, (v, z/n) \mapsto v \bullet (z/n) = (v \bullet z)/n.$$

Dies ist die einzige distributive Operation des Körpers $\mathbb{Q}$ auf $(V,+)$.

(1) Zu jedem $\mathbb{Q}$–Vektorraum $(V,+,\bullet)$ können wir allein aus $(V,+)$ die Skalarmultiplikation $\bullet : V \times \mathbb{Q} \to V$ eindeutig rekonstruieren.

(2) Jeder Gruppenhomomorphismus $f : (V,+) \to (W,+)$ zwischen $\mathbb{Q}$–Vektorräumen $(V,+)$ und $(W,+)$ ist automatisch $\mathbb{Q}$–linear:

$$f(v \bullet z/n) = f(v) \bullet z/n$$

Lineare Räume über $\mathbb{Q}$

Jeder der Ringe $R = \mathbb{Z}, \mathbb{Z}/p, \mathbb{Q}$ hat diese besondere Eigenschaft!

Die Aussage, dass $(V,+,\cdot)$ ein R–linearer Raum ist, stellt eine ganz konkrete Bedingung an die zu Grunde liegende Gruppe $(V,+)$.

- Für $R = \mathbb{Z}$ fordern wir nur die Kommutativität,
- für $R = \mathbb{Z}/p$ fordern wir zudem $v \bullet p = 0$ für alle $v \in V$,
- für $R = \mathbb{Q}$ stattdessen $\mu_n : u \mapsto u \bullet n$ bijektiv für alle $n \in \mathbb{N}_{\geq 2}$.

Die zusätzliche Struktur der Skalarmultiplikation $\bullet : V \times R \to V$ lässt sich dann allein aus $(V,+)$ eindeutig rekonstruieren.

⚠ Das ist eine Besonderheit der Ringe $R = \mathbb{Z}, \mathbb{Z}/p, \mathbb{Q}$, allgemein gilt dies nicht. Hierzu erinnern wir an das folgende Beispiel über $\mathbb{R}$ bzw. $\mathbb{C}$.

Lineare Räume über $\mathbb{R}$ und $\mathbb{C}$

Beispiel I1N: lineare Räume über $\mathbb{R}$ und $\mathbb{C}$

(1) Sei $(V,+,\bullet)$ ein $\mathbb{C}$–linearer Raum vermöge $\bullet : \mathbb{C} \times V \to V$.
Dann ist $(V,+,\cdot)$ ein $\mathbb{R}$–linearer Raum dank der Einschränkung

$$\cdot \,:\, \mathbb{R} \times V \to V \,:\, (\lambda, v) \mapsto \lambda \bullet v.$$

Die Abbildung $J : V \to V : v \mapsto \mathrm{i} \bullet v$ ist $\mathbb{R}$–linear und erfüllt $J \circ J = -\mathrm{id}_V$.

(2) Sei $(V,+,\cdot)$ ein $\mathbb{R}$–linearer Raum vermöge $\cdot : \mathbb{R} \times V \to V$.
Gegeben sei eine $\mathbb{R}$–lineare Abbildung $J : V \to V$ mit $J \circ J = -\mathrm{id}_V$.
Mit diesen Daten definieren wir

$$\bullet \,:\, \mathbb{C} \times V \to V \,:\, (x + y\mathrm{i}) \bullet v = x \cdot v + y \cdot J(v)$$

Dies ist eine distributive Operation des Körpers $\mathbb{C}$ auf $(V,+)$.

Dies zeigt noch einmal, dass die $\mathbb{C}$–Operation $\bullet$ nicht allein aus $(V,+,\cdot)$ eindeutig rekonstruierbar ist: Neben J erfüllt auch $-J$ die Forderung, wir erhalten so die Operation durch das komplex-konjugierte (I112).

Lineare Räume über $K[X]$

Beispiel I1O: lineare Räume über $K[X]$

Sei K ein kommutativer Ring und $K[X]$ der Polynomring.

(1) Sei $(V,+,\bullet)$ ein $K[X]$–linearer Raum vermöge $\bullet : K[X] \times V \to V$.
Dann ist $(V,+,\cdot)$ ein K–linearer Raum dank der Einschränkung

$$\cdot \,:\, K \times V \to V \,:\, (\lambda, v) \mapsto \lambda \bullet v.$$

Die Abbildung $T : V \to V : v \mapsto X \bullet v$ ist K–linear, kurz $T \in \mathrm{End}_K(V)$.

(2) Sei $(V,+,\cdot)$ ein K–linearer Raum vermöge $\cdot : K \times V \to V$.
Gegeben sei eine K–lineare Abbildung $T : V \to V$.
Mit diesen Daten definieren wir

$$\bullet \,:\, K[X] \times V \to V \,:\, (\textstyle\sum_i p_i X^i) \bullet v = \sum_i p_i \cdot T^i(v)$$

Dies ist eine distributive Operation des Rings $K[X]$ auf $(V,+)$.

🙂 Dies entspricht der universellen Abbildungseigenschaft G3E des Polynomrings $K[X]$, hier angewendet auf $K[X] \to \mathrm{End}_K(V) : X \mapsto T$.

Definition I1P: linearer Unterraum

Sei $(V,+,\cdot)$ ein R–linearer Raum. Ein **R–linearer Unterraum** $U \leq (V,+,\cdot)$ ist eine Untergruppe $U \leq (V,+)$ mit der Eigenschaft

$$R \cdot U \subseteq U \quad \text{bzw.} \quad U \cdot R \subseteq U.$$

Äquivalent umformuliert: $U \subseteq V$ ist eine Teilmenge, sodass gilt:

$$(0)\ 0 \in U, \quad (1)\ U+U \subseteq U, \quad (2)\ R \cdot U \subseteq U \ \text{ bzw. } \ U \cdot R \subseteq U.$$

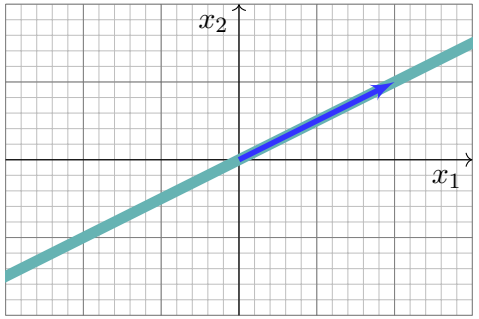
Dank Lemma I1C beinhaltet Bedingung (2) die Negation $-U \subseteq U$.

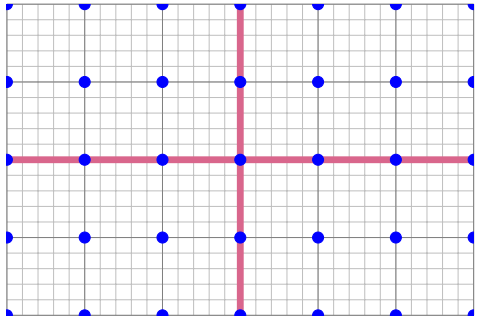
Durch Einschränkung ist dann $(U,+_U,\cdot_U)$ selbst ein R–linearer Raum und die Inklusion $\iota : (U,+_U,\cdot_U) \hookrightarrow (V,+,\cdot)$ eine R–lineare Abbildung.

Beispiel: In $(V,+,\cdot)$ sind die Mengen $\{0\}$ und V lineare Unterräume.

Beispiel: Die $\mathbb{Z}$–linearen Unterräume von $\mathbb{Z}$ sind $n\mathbb{Z}$ mit $n \in \mathbb{N}$ (G1V).

Übung: Sind $U_1, U_2 \leq V$ Unterräume, so auch U_1+U_2 und $U_1 \cap U_2$. Zur Lösung, auch für beliebige Summen und Schnitte, siehe Satz I1X.





Beispiele: Wir betrachten den $\mathbb{R}$–Vektorraum $\mathbb{R}^n$.

1. Die Gerade $G = (2,1)\cdot\mathbb{R}$ ist ein $\mathbb{R}$–linearer Unterraum von $\mathbb{R}^2$.
2. Die Ebene $E = (1,2,5)\cdot\mathbb{R} + (0,3,2)\cdot\mathbb{R}$ ist ein $\mathbb{R}$–Unterraum von $\mathbb{R}^3$.

Gegenbeispiele: Wir betrachten den $\mathbb{R}$–Vektorraum $\mathbb{R}^2$.

3. Die Untergruppe $U = \mathbb{Z}^2$ ist kein $\mathbb{R}$–Unterraum, denn $U \cdot \mathbb{R} \not\subseteq U$.
4. $V = (\mathbb{R}\times\{0\}) \cup (\{0\}\times\mathbb{R})$ erfüllt $V\cdot\mathbb{R} \subseteq V$, aber $V+V \not\subseteq V$.

Beispiel: Die Teilmenge $W = \mathrm{i}\mathbb{R}$ in $\mathbb{C}$ ist ein $\mathbb{R}$–linearer Unterraum. Hingegen ist W kein $\mathbb{C}$–linearer Unterraum, denn $W \cdot \mathrm{i} \not\subseteq W$.

Definition I1P ist klar und einfach: Ein R–linearer Unterraum $U \leq (V,+,\cdot)$ ist eine Untergruppe $U \leq (V,+)$ mit $R\cdot U \subseteq U$ bzw. $U \cdot R \subseteq U$.

Äquivalent umformuliert: $U \subseteq V$ ist eine Teilmenge, sodass gilt:
$(0)\ 0 \in U$, $(1)\ U+U \subseteq U$, $(2)\ R\cdot U \subseteq U$ bzw. $U\cdot R \subseteq U$.

Zum Verständnis helfen Beispiele und Gegenbeispiele wie oben:

(3) Die Teilmenge $U = \mathbb{Z}^2$ in $\mathbb{R}^2$ erfüllt zwar $0 \in U$ und $-U \subseteq U$ sowie $U+U \subseteq U$, aber $U\cdot\mathbb{R} \not\subseteq U$. Konkretes Gegenbeispiel: Es gilt $(1,0) \in U$, aber $(1,0)\cdot{}^1\!/_2 \notin U$. Somit ist $U \leq \mathbb{R}^2$ zwar eine Untergruppe, also ein $\mathbb{Z}$–linearer Unterraum, aber kein $\mathbb{R}$–linearer Unterraum.

(4) Die Teilmenge $V = (\mathbb{R}\times\{0\}) \cup (\{0\}\times\mathbb{R})$ besteht aus der x–Achse $\mathbb{R}\times\{0\}$ und der y–Achse $\{0\}\times\mathbb{R}$. Es gilt $V\cdot\mathbb{R} \subseteq V$, aber $V+V \not\subseteq V$. Konkretes Gegenbeispiel: $(1,0),(0,1) \in V$, aber $(1,0)+(0,1) \notin V$. Somit ist V keine Untergruppe, erst recht kein $\mathbb{R}$–linearer Unterraum.

Das folgende Beispiel des Unterraums $R^{(I)} \leq R^I$ ist etwas allgemeiner und wird uns im Folgenden immer wieder gute Dienste erweisen.

Beispiel I1Q: der lineare Raum $R^{(I)} \leq R^I$ über R

Sei $(R,+,0,\cdot,1)$ ein Ring, etwa $\mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \ldots$, und I eine Menge.
(0) Die Abbildungsmenge $R^I = \mathrm{Abb}(I,R) = \{\, u : I \to R : i \mapsto u_i \,\}$ ist ein R–linearer Raum mit koordinatenweiser Addition und Skalierung.

(1) Für den Träger $\mathrm{supp}(u) = \{\, i \in I \mid u_i \neq 0 \,\}$ gilt

$$\mathrm{supp}(a\cdot u) \subseteq \mathrm{supp}(u), \qquad \mathrm{supp}(0) = \emptyset,$$
$$\mathrm{supp}(u\cdot a) \subseteq \mathrm{supp}(u), \qquad \mathrm{supp}(u+v) \subseteq \mathrm{supp}(u) \cup \mathrm{supp}(v).$$

(2) Wir erhalten so den R–linearen Unterraum

$$R^{(I)} := \{\, u : I \to R \mid \sharp\,\mathrm{supp}(u) < \infty \,\} \leq R^I$$

der Funktionen mit endlichem Träger. Ist I endlich, so gilt $R^{(I)} = R^I$.

(3) Zu $i \in I$ definieren wir $e_i : I \to R$ durch $e_i(i) = 1$ und $e_i(j) = 0$ sonst. Jedes Element $u \in R^{(I)}$ schreibt sich eindeutig als Linearkombination $u = \sum_{i\in I} u_i e_i$ (linkslinear) bzw. $u = \sum_{i\in I} e_i u_i$ (rechtslinear).

Bild und Kern einer linearen Abbildung

Satz I1R: Bild und Kern, surjektiv und injektiv

Sei $f : V \to W$ eine R–lineare Abbildung.

(1) Ist $U \leq V$ ein Unterraum, so auch das Bild $f(U) \leq W$.
Insbesondere ist das Bild $\operatorname{im}(f) = f(V) \leq W$ ein Unterraum.

(2) Genau dann ist f surjektiv, wenn $\operatorname{im}(f) = W$ gilt.

(3) Ist $U \leq W$ ein Unterraum, so auch $f^{-1}(U) \leq V$.
Somit ist der Kern $\ker(f) := f^{-1}(\{0\}) \leq V$ eine Unterraum.

(4) Genau dann ist f injektiv, wenn $\ker(f) = \{0\}$ gilt. Allgemein:

(5) Für $v \in V$ und $w = f(v) \in \operatorname{im}(f)$ gilt $f^{-1}(\{w\}) = v + \ker(f)$.
Jede Faser ist entweder leer oder eine Translation des Kerns.

🙂 Das unscheinbare Injektivitätskriterium (4) ist überaus praktisch und wird sich im Folgenden immer wieder als hilfreich erweisen.

Arbeitsersparnis: Für die Injektivität einer R–linearen Abbildung $f : V \to W$ müssen wir nicht alle Fasern $f^{-1}(\{w\})$ prüfen, sondern nur eine einzige Faser, nämlich $\ker(f) = f^{-1}(\{0\})$.

Bild und Kern einer linearen Abbildung

Beweis: (1) Dank G1R(1) ist $f(U) \leq W$ eine Untergruppe. Zu $w \in f(U)$ existiert $u \in U$ mit $w = f(u)$. Für $a \in R$ gilt $wa = f(u)a = f(ua) \in f(U)$.

(2) Die Aussage $\operatorname{im}(f) = W$ ist die Definition von Surjektivität.

(3) Dank G1R(3) ist $f^{-1}(U) \leq V$ eine Untergruppe. Für $a \in R$ und $v \in f^{-1}(U)$ gilt $f(v) \in U$, also $f(va) = f(v)a \in U$, somit $va \in f^{-1}(U)$.

(4) Die Implikation „f injektiv $\Rightarrow \ker(f) = \{0\}$“ ist klar. Umgekehrt:

(5) Für $v, v' \in V$ mit $f(v) = f(v')$ gilt $0 = f(v') - f(v) = f(v' - v)$, also $v' - v \in \ker(f)$, somit $v' \in v + \ker(f)$. Mit $\ker(f) = \{0\}$ folgt $v' = v$.
Allgemein: Für $w = f(v) \in \operatorname{im}(f)$ folgt $f^{-1}(\{w\}) = v + \ker(f)$. QED

🙂 Jede Faser ist entweder leer oder eine Translation des Kerns.

Das hilft uns beim Lösen von linearen Gleichungssystemen $f(x) = y$, es gibt uns Struktur und Überblick. Abstraktion wirkt ganz konkret:
Zur homogenen Gleichung $f(x) = 0$ heißt $x_h \in \ker(f)$ eine homogene Lösung. Zur inhomogenen Gleichung $f(x) = y$ heißt $x_p \in f^{-1}(\{y\})$ eine partikuläre Lösung. Damit gilt $f^{-1}(\{y\}) = x_p + \ker(f)$: **Die allgemeine Lösung ist eine partikuläre plus eine beliebige homogene Lösung.**

Superposition: partikuläre und homogene Lösungen

Aufgabe: Bestimmen Sie in $\mathbb{Q}^5$ die Lösungsmenge zu $Ax = b$ mit

$$A = \begin{bmatrix} 2 & 0 & 1 & -3 & 3 \\ 1 & 1 & 0 & -2 & 5 \\ 2 & 1 & 5 & 1 & 5 \\ 1 & -3 & 2 & 0 & -9 \end{bmatrix} \in \mathbb{Q}^{4\times 5}, \quad b = \begin{bmatrix} 0 \\ -1 \\ 2 \\ 3 \end{bmatrix} \in \mathbb{Q}^4.$$

Lösung: Wir bringen die erweiterte Koeffizientenmatrix $(A|b)$ in RZSF:

$$\left[\begin{array}{ccccc|c} 2 & 0 & 1 & -3 & 3 & 0 \\ 1 & 1 & 0 & -2 & 5 & -1 \\ 2 & 1 & 5 & 1 & 5 & 2 \\ 1 & -3 & 2 & 0 & -9 & 3 \end{array}\right] \xrightarrow[\text{B2c}]{\text{Gauß}} \left[\begin{array}{ccccc|c} 1 & 0 & 0 & -2 & 5/3 & -1/3 \\ 0 & 1 & 0 & 0 & 10/3 & -2/3 \\ 0 & 0 & 1 & 1 & -1/3 & 2/3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Die Lösungsmenge $L(A, b) = \{ x \in \mathbb{Q}^5 \mid Ax = b \}$ ist demnach explizit

$$L(A,b) = \begin{bmatrix} -1/3 \\ -2/3 \\ 2/3 \\ 0 \\ 0 \end{bmatrix} + \mathbb{Q} \begin{bmatrix} -2 \\ 0 \\ 1 \\ -1 \\ 0 \end{bmatrix} + \mathbb{Q} \begin{bmatrix} 5/3 \\ 10/3 \\ -1/3 \\ 0 \\ -1 \end{bmatrix} = v + \ker(A).$$

Superposition: partikuläre und homogene Lösungen

Aufgabe: Sei R ein Ring, etwa $R = \mathbb{Q}$ wie im vorigen Beispiel. Gegeben sei $A \in R^{p\times q}$ und $b \in R^p$. Das lineare Gleichungssystem $Ax = b$ hat die Lösungsmenge $L(A, b) := \{ x \in R^q \mid Ax = b \}$.

1. Es gilt $L(A, b) + L(A, c) \subseteq L(A, b + c)$ für alle $b, c \in R^p$ sowie $L(A, b) \cdot \lambda \subseteq L(A, b \cdot \lambda)$ für alle $\lambda \in R$.
2. Der wichtigste Spezialfall ist die homogene Gleichung $Ax = 0$: Die Menge $L(A, 0) = \ker(A)$ ist ein R–linearer Unterraum von R^q.
3. Ist $x_p \in L(A, b)$ eine „partikuläre“ Lösung der Gleichung $Ax = b$, so erhalten wir die gesamte Lösungsmenge $L(A, b) = x_p + L(A, 0)$.

Man sagt hierzu zusammenfassend: **Die allgemeine Lösung ist eine partikuläre plus eine beliebige homogene Lösung.**

Lösung: Das ist genau die Rechnung zum vorigen Satz I1R, hier spezialisiert für die lineare Abbildung $f : R^q \to R^p : x \mapsto Ax$.

🙂 Das hilft uns beim Lösen von linearen Gleichungssystemen, es gibt uns Struktur und Überblick. Abstraktion wirkt ganz konkret.

Beispiel: Grenzwert von Folgen

Wir betrachten $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Die Menge aller $\mathbb{K}$–wertigen Folgen,

$$\mathbb{K}^{\mathbb{N}} = \{\, a : \mathbb{N} \to \mathbb{K} : n \mapsto a_n \,\},$$

ist ein $\mathbb{K}$–Vektorraum mit punktweiser Addition und Skalierung (I1A).

Darin liegt der Untervektorraum $c(\mathbb{N}, \mathbb{K})$ der $\mathbb{K}$–konvergenten Folgen, und der Grenzwert $\lim : c(\mathbb{N}, \mathbb{K}) \to \mathbb{K}$ ist eine $\mathbb{K}$–lineare Abbildung:

$$\lim_{n\to\infty} (a_n + b_n) = (\lim_{n\to\infty} a_n) + (\lim_{n\to\infty} b_n)$$
$$\lim_{n\to\infty} (\lambda \cdot a_n) = \lambda \cdot \lim_{n\to\infty} a_n$$

Ihr Bild ist $\mathbb{K}$, der Kern ist der Unterraum $c_0(\mathbb{N}, \mathbb{K})$ aller Nullfolgen.
Der Grenzwert $\lim : c(\mathbb{N}, \mathbb{K}) \to \mathbb{K}$ ist zudem sogar multiplikativ

$$\lim_{n\to\infty} (a_n \cdot b_n) = (\lim_{n\to\infty} a_n) \cdot (\lim_{n\to\infty} b_n)$$

Diese Rechenregeln vereinfachen die Bestimmung von Grenzwerten.
🙂 Ausführliche Beweise und Beispiele lernen Sie in der Analysis.

Beispiel: Grenzwert von Reihen

Zu $a : \mathbb{N} \to \mathbb{K}$ definieren wir die Folge $s : \mathbb{N} \to \mathbb{K}$ der **Partialsummen** $s_n = \sum_{k=0}^{n} a_k$. Wir erhalten den $\mathbb{K}$–Isomorphismus $(\Sigma, \Delta) : \mathbb{K}^{\mathbb{N}} \cong \mathbb{K}^{\mathbb{N}}$:

$$\Sigma \;:\; \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}} \;:\; a \mapsto s = \Sigma a, \quad s_n = \sum_{k=0}^{n} a_k,$$
$$\Delta \;:\; \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}} \;:\; s \mapsto a = \Delta s, \quad a_n = s_n - s_{n-1}.$$

Eine Folge $a \in \mathbb{K}^{\mathbb{N}}$ heißt **summierbar**, falls $\Sigma a \in c(\mathbb{N}, \mathbb{K})$ gilt, also die Partialsummen $s_n = \sum_{k=0}^{n} a_k$ für $n \to \infty$ konvergieren.
Für jede summierbare Folge $a : \mathbb{N} \to \mathbb{K}$ definieren wir die **Summe**

$$\textstyle\sum_{k=0}^{\infty} a_k := \lim_{n\to\infty} \sum_{k=0}^{n} a_k$$

Auch diese Zuordnung ist linear:

$$\textstyle\sum_{k=0}^{\infty} (a_k + b_k) = \sum_{k=0}^{\infty} a_k + \sum_{k=0}^{\infty} b_k$$
$$\textstyle\sum_{k=0}^{\infty} (\lambda \cdot a_k) = \lambda \cdot \sum_{k=0}^{\infty} a_k$$

Diese Rechenregeln vereinfachen die Bestimmung von Summen.
🙂 Ausführliche Beweise und Beispiele lernen Sie in der Analysis.

Beispiel: Ableitung und Integral

Beispiel I1S: Hauptsatz der Differential- und Integralrechnung

Sei $X =]a, b[$ ein reelles Intervall mit $a < x_0 < b$ in $\bar{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$.
In $\mathbb{R}^X = \mathrm{Abb}(X, \mathbb{R}) = \{\, f : X \to \mathbb{R} \,\}$ liegen die Untervektorräume

$$\mathscr{C}^0(X, \mathbb{R}) = \mathscr{C}(X, \mathbb{R}) = \{\, f : X \to \mathbb{R} \text{ stetig} \,\},$$
$$\mathscr{C}^1(X, \mathbb{R}) = \{\, F : X \to \mathbb{R} \text{ stetig differenzierbar} \,\}.$$

Darauf sind Differenzieren und Integrieren $\mathbb{R}$–lineare Abbildungen:

$$D \;:\; \mathscr{C}^1 \to \mathscr{C}^0 \;:\; F \mapsto f, \qquad f(x) = \lim_{t\to x} \frac{F(t) - F(x)}{t - x},$$
$$I \;:\; \mathscr{C}^0 \to \mathscr{C}^1 \;:\; f \mapsto F, \qquad F(x) = \int_{t=x_0}^{x} f(t)\,\mathrm{d}t.$$

Dank Hauptsatz (HDI) gilt $DI(f) = f$ und $ID(F) = F - F(x_0)$.
Wir erhalten so den Isomorphismus von $\mathbb{R}$–Vektorräumen

$$(I, D) \;:\; \mathscr{C}^0 \cong \mathscr{C}^1_0 \;:= \{\, F \in \mathscr{C}^1 \mid F(x_0) = 0 \,\}.$$

Beispiel: Ableitung und Integral

Die $\mathbb{R}$–Linearität der Ableitung $D : \mathscr{C}^1 \to \mathscr{C}^0 : F \mapsto F'$ bedeutet

$$(F + G)' = F' + G' \quad \text{und} \quad (\lambda F)' = \lambda F'$$

für alle $\lambda \in \mathbb{R}$. Die $\mathbb{R}$–Linearität des Integrals $I : \mathscr{C}^0 \to \mathscr{C}^1$ bedeutet

$$\int_{t=x_0}^{x} f(t) + g(t)\,\mathrm{d}t = \int_{t=x_0}^{x} f(t)\,\mathrm{d}t + \int_{t=x_0}^{x} g(t)\,\mathrm{d}t \quad \text{und}$$
$$\int_{t=x_0}^{x} \lambda f(t)\,\mathrm{d}t = \lambda \int_{t=x_0}^{x} f(t)\,\mathrm{d}t.$$

🙂 Aus $DI(f) = f$ folgt sofort: D ist surjektiv, also $\mathrm{im}(D) = \mathscr{C}^0$, und I ist injektiv, also $\ker(I) = \{0\}$. Aus $ID(F) = F - F(x_0)$ folgt $\ker(D) = \{\, F = \mathrm{const} \,\}$ und $\mathrm{im}(I) = \mathscr{C}^1_0 = \{\, F \in \mathscr{C}^1 \mid F(x_0) = 0 \,\}$.

🙂 Je zwei Stammfunktionen F, G zu f unterscheiden sich nur durch eine Konstante: $(F - G)' = F' - G' = f - f = 0$, also $F - G = \mathrm{const}$.

🙂 Durch die Integralfunktion $F(x) = \int_{t=x_0}^{x} f(t)\,\mathrm{d}t$ mit Start in x_0 wird die Integrationskonstante durch $F(x_0) = 0$ eindeutig festgelegt.

Beispiel: Ableitung und Integral

Sei $\mathscr{C}^0(X,\mathbb{R})$ die Menge der stetigen Funktionen $f : X \to \mathbb{R}$ und $\mathscr{C}^n(X,\mathbb{R})$ die Menge der n–mal stetig differenzierbaren Funktionen:

$$\begin{aligned}
\mathscr{C}^0(X,\mathbb{R}) &= \mathscr{C}(X,\mathbb{R}) = \{\, f : X \to \mathbb{R} \text{ stetig} \,\} \\
\mathscr{C}^n(X,\mathbb{R}) &= \{\, f : X \to \mathbb{R} \text{ diff'bar und } f' \in \mathscr{C}^{n-1}(X,\mathbb{R}) \,\} \\
\mathscr{C}^\infty(X,\mathbb{R}) &= \textstyle\bigcap_{n\in\mathbb{N}} \mathscr{C}^n(X,\mathbb{R}) \\
\mathrm{Poly}(X,\mathbb{R}) &= \{\, f : X \to \mathbb{R} \mid \exists P \in \mathbb{R}[t]\ \forall x \in X : f(x) = P(x) \,\}
\end{aligned}$$

Dies sind $\mathbb{R}$–lineare Unterräume von $\mathrm{Abb}(X,\mathbb{R}) = \mathbb{R}^X$:

$$\mathbb{R}^X > \mathscr{C}^0 > \mathscr{C}^1 > \cdots > \mathscr{C}^n > \cdots > \mathscr{C}^\infty > \mathrm{Poly}\,.$$

Hierzu beweisen Sie in der Analysis: Sind $f, g : X \to \mathbb{R}$ stetig so auch $f + g$ und λf für alle $\lambda \in \mathbb{R}$. Sind $f, g : X \to \mathbb{R}$ sogar differenzierbar, so auch $f + g$ und λf, und es gilt $(f + g)' = f' + g'$ und $(\lambda f)' = \lambda f'$.

Beispiel: Ableitung und Integral

Aufgabe: Nennen Sie jeweils ein Beispiel für die strikte Inklusion

$$\mathbb{R}^I > \mathscr{C}^0 > \mathscr{C}^1 > \cdots > \mathscr{C}^n > \cdots > \mathscr{C}^\infty > \mathrm{Poly}\,.$$

Lösung: Zur Vereinfachung betrachten wir $X =]a, b[$ mit $a < 0 < b$.

- Die Vorzeichenfunktion $h : X \to \mathbb{R} : x \mapsto \mathrm{sign}(x)$ ist unstetig, liegt also in $\mathrm{Abb}(X,\mathbb{R}) = \mathbb{R}^X$, aber nicht in $\mathscr{C}(X,\mathbb{R})$.
- Die Betragsfunktion $f_0 : \mathbb{R} \to \mathbb{R} : x \mapsto |x|$ liegt in $\mathscr{C}^0(X,\mathbb{R})$, aber nicht in $\mathscr{C}^1(X,\mathbb{R})$.
- Die Funktion $f_n : \mathbb{R} \to \mathbb{R} : x \mapsto |x|x^n$ liegt in $\mathscr{C}^n(X,\mathbb{R})$, aber nicht in $\mathscr{C}^{n+1}(X,\mathbb{R})$.
- Die Exponentialfunktion $g : \mathbb{R} \to \mathbb{R} : x \mapsto \mathrm{e}^x$ liegt in $\mathscr{C}^\infty(X,\mathbb{R})$, aber nicht in $\mathrm{Poly}(X,\mathbb{R})$.

Beispiel: Ableitung und Integral

Ableitung und Integral stiften hierauf den $\mathbb{R}$–Isomorphismus

$$(I, D) \,:\, \mathscr{C}^n \cong \mathscr{C}^{n+1}_0 := \{\, F \in \mathscr{C}^{n+1} \mid F(x_0) = 0 \,\}.$$

Beim Differenzieren verlieren wir eine Stufe an Glattheit, beim Integrieren gewinnen wir eine Stufe an Glattheit.

Slogan: Integrieren glättet, Differenzieren raut auf.

Der $\mathbb{R}$–Isomorphismus gilt auch für $n = \infty$:

$$(I, D) \,:\, \mathscr{C}^\infty \cong \mathscr{C}^\infty_0 := \{\, F \in \mathscr{C}^\infty \mid F(x_0) = 0 \,\}.$$

Beispiel: Ableitung und Integral

Zur Vereinfachung betrachten wir $X =]a, b[$ mit $a < 0 < b$ und $x_0 = 0$.
Speziell für Polynomfunktionen erhalten wir die expliziten Formeln

$$\begin{aligned}
D \,:\, F(x) = \sum_{k=0}^{n} a_k x^k \;&\mapsto\; f(x) = \sum_{k=1}^{n} k a_k x^{k-1}, \\
I \,:\, f(x) = \sum_{k=0}^{n} b_k x^k \;&\mapsto\; F(x) = \sum_{k=0}^{n} \frac{1}{k+1} b_k x^{k+1}.
\end{aligned}$$

Daraus folgt unmittelbar $DI(f) = f$ und $ID(F) = F - F(0)$.
Wir erhalten so den Isomorphismus von $\mathbb{R}$–Vektorräumen

$$(I, D) \,:\, \mathrm{Poly} \cong \mathrm{Poly}_0 := \{\, F \in \mathrm{Poly} \mid F(0) = 0 \,\}.$$

Endlich erzeugte Unterräume

Satz I1T: endlich erzeugter Unterraum

Sei $(V,+,\cdot)$ ein (rechts)linearer Raum über dem Ring $(R,+,\cdot)$.
Gegeben sei zudem eine endliche Familie $u_1,\ldots,u_n \in V$.

(1) Diese Familie $F=(u_1,\ldots,u_n)$ definiert die R–lineare Abbildung

$$\Phi_F : R^n \to V : (\lambda_1,\ldots,\lambda_n) \mapsto u_1\lambda_1+\cdots+u_n\lambda_n.$$

(2) Ihr Bild ist der von $F=(u_1,\ldots,u_n)$ in V **erzeugte Unterraum**:

$$V \geq \operatorname{im}(\Phi_F) = u_1R+\cdots+u_nR =: \langle\, u_1,\ldots,u_n \,\rangle_R = U$$

Er besteht aus allen **Linearkombinationen** der Familie F über R.

(3) Diese Teilmenge $U \subseteq V$ ist ein R–linearer Unterraum $U \leq (V,+,\cdot)$ und zudem der kleinste, der die Elemente $u_1,\ldots,u_n$ enthält.

Beispiele: Im Vektorraum $\mathbb{R}^3$ über $\mathbb{R}$ erhalten wir so als Unterräume

- die Gerade $G = \langle\,(2,1,0)\,\rangle_{\mathbb{R}} = \langle\,(6,3,0)\,\rangle_{\mathbb{R}} = \langle\,(4,2,0),(6,3,0)\,\rangle_{\mathbb{R}}$,
- die Ebene $E = \langle\,(1,2,5),(0,3,2)\,\rangle_{\mathbb{R}} = \langle\,(1,2,5),(0,3,2),(1,5,7)\,\rangle_{\mathbb{R}}$.

Endlich erzeugte Unterräume

Beispiel I1U: Unterräume in $\mathbb{Z}$

In $\mathbb{Z}$ gilt $\langle\,3,5\,\rangle_{\mathbb{Z}} = \mathbb{Z}$ und $\langle\,8,12\,\rangle_{\mathbb{Z}} = 4\mathbb{Z}$ und $\langle\,24,42\,\rangle = 6\mathbb{Z}$.
Allgemein gilt $\langle\,u_1,\ldots,u_n\,\rangle_{\mathbb{Z}} = \operatorname{ggT}(u_1,\ldots,u_n)\mathbb{Z}$.

Beweis: Für $n=1$ ist die Aussage trivial. Wie betrachten daher $n=2$.
Sei $U = \langle\,u_1,u_2\,\rangle = u_1\mathbb{Z}+u_2\mathbb{Z}$ und $d=\operatorname{ggT}(u_1,u_2)$. Wir zeigen $U=d\mathbb{Z}$:

Dank $d \mid u_1$ und $d \mid u_2$ existieren $d_1,d_2\in\mathbb{Z}$ mit $dd_1=u_1$ und $dd_2=u_2$.
Daraus folgt $u_1a_1+u_2a_2 = d(d_1a_1+d_2a_2) \in d\mathbb{Z}$, also $U \subseteq d\mathbb{Z}$.

Zu $u_1,u_2\in\mathbb{Z}$ existieren dank Satz A2I Bézout–Koeffizienten $a_1,a_2\in\mathbb{Z}$, sodass $u_1a_1+u_2a_2=d$ gilt. Dies zeigt $d\in U$, also $d\mathbb{Z}\subseteq U$.

Die allgemeine Aussage folgt nun per Induktion über n:
Wir zeigen $\langle\,u_1,\ldots,u_n\,\rangle_{\mathbb{Z}} = d\mathbb{Z}$ mit $d=\operatorname{ggT}(u_1,\ldots,u_n)$.

Nach Induktionsvoraussetzung haben wir $\langle\,u_2,\ldots,u_n\,\rangle_{\mathbb{Z}} = v\mathbb{Z}$ mit $v=\operatorname{ggT}(u_2,\ldots,u_n)$. Daraus folgt $\langle\,u_1,u_2,\ldots,u_n\,\rangle_{\mathbb{Z}} = u_1\mathbb{Z}+v\mathbb{Z} = d\mathbb{Z}$ mit $d=\operatorname{ggT}(u_1,v)=\operatorname{ggT}(u_1,u_2,\ldots,u_n)$. QED

Erzeugte Unterräume

Satz I1V: erzeugter Unterraum

Sei $(V,+,\cdot)$ ein (rechts)linearer Raum über dem Ring $(R,+,\cdot)$.
Gegeben sei eine Familie $F=(u_i)_{i\in I}$ von Vektoren $u_i\in V$.

(1) Diese Familie F definiert die R–lineare Abbildung

$$\Phi_F : R^{(I)} \to V : (\lambda_i)_{i\in I} \mapsto \textstyle\sum_{i\in I} u_i\lambda_i.$$

(2) Ihr Bild ist der von $F=(u_i)_{i\in I}$ in V **erzeugte Unterraum**:

$$V \geq \operatorname{im}(\Phi_F) = \left\{\, \textstyle\sum_{i\in I} u_i\lambda_i \;\middle|\; \lambda\in R^{(I)} \,\right\} =: \langle\, u_i \mid i\in I\,\rangle_R = U$$

Er besteht aus allen **Linearkombinationen** der Familie F über R.

(3) Diese Teilmenge $U\subseteq V$ ist ein R–linearer Unterraum $U\leq(V,+,\cdot)$ und zudem der kleinste, der alle Elemente u_i mit $i\in I$ enthält.

Im Spezialfall $I=\{1,\ldots,n\}$ und $F=(u_1,\ldots,u_n)$ gilt wie zuvor

$$\Phi_F : R^n \to V : (\lambda_1,\ldots,\lambda_n) \mapsto u_1\lambda_1+\cdots+u_n\lambda_n,$$
$$U = \langle\,u_1,\ldots,u_n\,\rangle_R = u_1R+\cdots+u_nR.$$

Erzeugte Unterräume

Für R–lineare Unterräume $U_i\leq V$ definieren wir ihre Summe durch

$$U = \textstyle\sum_{i\in I} U_i := \left\{\, \sum_{i\in I} u_i \;\middle|\; u_i\in U_i \wedge \sharp\operatorname{supp}(u) < \infty \,\right\}.$$

Damit ist $U\leq V$ ein R–linearer Unterraum, und zwar der kleinste, der alle U_i mit $i\in I$ enthält (I1X). Somit gilt $\langle\, u_i \mid i\in I\,\rangle = \sum_{i\in I} u_iR$.

Beweis des Satzes: (0) Die Abbildung

$$\Phi_F : R^{(I)} \to V : (\lambda_i)_{i\in I} \mapsto \textstyle\sum_{i\in I} u_i\lambda_i$$

ist wohldefiniert, denn die Summe ist (im Wesentlichen) endlich.

(1) Die Abbildung Φ_F ist R–linear. Für alle $\lambda,\mu\in R^{(I)}$ und $a\in R$ gilt:

$$\begin{aligned}\Phi_F(\lambda+\mu\cdot a) &= \textstyle\sum_{i\in I} u_i(\lambda_i+\mu_i a) = \sum_{i\in I} u_i\lambda_i + u_i\mu_i a \\ &= \textstyle\sum_{i\in I}(u_i\lambda_i) + \sum_{i\in I}(u_i\mu_i)a = \Phi_F(\lambda)+\Phi_F(\mu)\cdot a\end{aligned}$$

(2) Dank Satz I1R ist die Bildmenge $U=\operatorname{im}(\Phi_F)\leq V$ ein Unterraum.

(3) Jeder Unterraum $U'\leq V$, der alle u_i mit $i\in I$ umfasst, enthält auch u_iR für jedes $i\in I$ und somit $U=\langle\, u_i \mid i\in I\,\rangle = \sum_{i\in I} u_iR$. QED

Beispiel: Polynome

Die folgenden ehrlichen Anwendungsbeispiele sind wunderbar konkret und anschaulich, doch etwas vertrackt. Sie illustrieren eindrücklich, warum wir nicht nur endlich erzeugte Unterräume betrachten wollen, denn viele natürliche Beispiele sind nun mal nicht endlich erzeugt.

Beispiel: Sei K ein kommutativer Ring und $K[X]$ der Polynomring.

Dann gilt $K[X] = \langle\, X^n \mid n \in \mathbb{N} \,\rangle_K$, denn jedes Polynom $P \in K[X]$ schreibt sich (sogar eindeutig) als eine Linearkombination

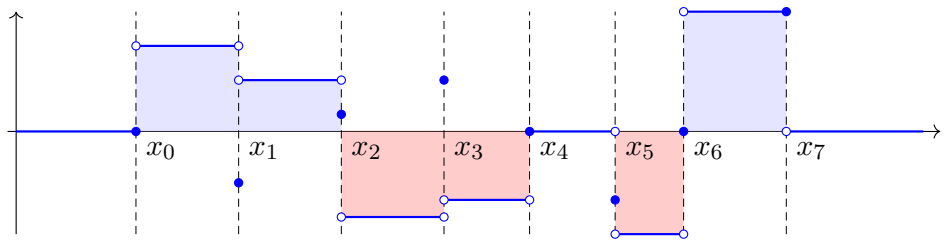
$$P = \textstyle\sum_{n\in\mathbb{N}} a_n X^n \quad \text{mit} \quad a \in K^{(\mathbb{N})}.$$

Der Raum $K[X]$ kann über K nicht endlich erzeugt werden, denn $\langle\, P_1, \ldots, P_n \,\rangle_K \leq K[X]_{\leq m}$ mit $m = \max\{\deg P_1, \ldots, \deg P_n\}$.

Übung: Dasselbe gilt allgemein für $R^{(I)} = \langle\, e_i \mid i \in I \,\rangle$, siehe I1Q: Ist die Menge I unendlich, so ist $R^{(I)}$ über R nicht endlich erzeugt.

Übung: Die reellen Zahlen $\mathbb{R}$ sind ein Vektorraum über $\mathbb{Q} \leq \mathbb{R}$. Dieser kann über $\mathbb{Q}$ nicht endlich oder abzählbar erzeugt werden.

Beispiel: Treppenfunktionen



Eine Treppenfunktion $f : \mathbb{R} \to \mathbb{R}$ ist stückweise konstant. Ausführlich:

Wir nennen $f : \mathbb{R} \to \mathbb{R}$ **Treppenfunktion**, wenn es eine Unterteilung $U = \{x_0 < x_1 < \cdots < x_\ell\} \subset \mathbb{R}$ gibt und Werte $f_1, \ldots, f_\ell \in \mathbb{R}$, so dass $f(x) = f_k$ für $x_{k-1} < x < x_k$ gilt, sowie $f(x) = 0$ für $x < x_0$ und $x > x_\ell$.

Wir schreiben hierfür kurz $f \in T_U$ und setzen $T = T(\mathbb{R}, \mathbb{R}) := \bigcup_U T_U$.

Satz I1W: eindimensionale Treppenfunktionen

Die Treppenfunktionen $T(\mathbb{R}, \mathbb{R}) \leq \mathbb{R}^{\mathbb{R}}$ bilden einen $\mathbb{R}$–Untervektorraum. Dieser wird erzeugt von den Indikatorfunktionen $\mathbf{I}_{[a,b]}$ mit $a \leq b$ in $\mathbb{R}$. Dabei gelten die Relationen $\mathbf{I}_{[a,c]} = \mathbf{I}_{[a,b]} + \mathbf{I}_{[b,c]} - \mathbf{I}_{[b,b]}$ für $a < b < c$.

Eindimensionale Treppenfunktionen

☺ Zu jeder Unterteilung $U \subset \mathbb{R}$ ist $T_U \leq \mathbb{R}^{\mathbb{R}}$ ein Untervektorraum.

⚠ Zu jeder Treppenfunktion f existieren unendlich viele angepasste Unterteilungen $U \subset \mathbb{R}$, insbesondere können wir jede Unterteilung $U \subset \mathbb{R}$ durch Einfügen weiterer Zwischenstellen zu $U' \supseteq U$ verfeinern.

Beweis des Satzes: Bei Verfeinerung $U \subseteq U' \subset \mathbb{R}$ gilt $T_U \leq T_{U'} \leq \mathbb{R}^{\mathbb{R}}$. Damit ist auch die Vereinigung $T = \bigcup_U T_U$ ein Untervektorraum in $\mathbb{R}^{\mathbb{R}}$:

- Sei $\lambda \in \mathbb{R}$. Für $f \in T$ gilt $f \in T_U$ für ein $U \subset \mathbb{R}$. Also liegt auch das Vielfache $\lambda f \in T_U$ in T.
- Seien $f, g \in T$. Somit gilt $f \in T_U$ und $g \in T_V$. Daraus folgt $f, g \in T_W$ mit $W = U \cup V$. Also liegt auch die Summe $f + g \in T_W$ in T.

Für jedes endliche Intervall $Q \subset \mathbb{R}$ ist $\mathbf{I}_Q : \mathbb{R} \to \mathbb{R}$ eine Treppenfunktion. Umgekehrt ist jede Treppenfunktion $f \in T$ eine Linearkombination

$$f = \textstyle\sum_{k=1}^{\ell} f_k\, \mathbf{I}_{]x_{k-1},x_k[} + \sum_{k=0}^{\ell} f(x_k)\, \mathbf{I}_{[x_k,x_k]}\,.$$

Für $a < b$ gilt $\mathbf{I}_{]a,b[} = \mathbf{I}_{[a,b]} - \mathbf{I}_{[a,a]} - \mathbf{I}_{[b,b]}$. Somit wird der $\mathbb{R}$–Vektorraum $T(\mathbb{R}, \mathbb{R})$ erzeugt von den Indikatorfunktionen $\mathbf{I}_{[a,b]}$ mit $a \leq b$ in $\mathbb{R}$. QED

Eindimensionale Treppenfunktionen

Vorsicht ist geboten: Die Schreibweise als Linearkombination von Indikatorfunktionen $\mathbf{I}_{[a,b]}$ ist keineswegs eindeutig. Zum Beispiel gilt

$$\mathbf{I}_{[0,2]} = \mathbf{I}_{[0,1]} + \mathbf{I}_{[1,2]} - \mathbf{I}_{[1,1]}\,.$$

☺ Dies ist ein schönes Beispiel für die (später ausgeführten) Begriffe *Erzeugendensystem* und *lineare Unabhängigkeit* und *Basis*:

Die Familie der Indikatorfunktionen $\mathbf{I}_{[a,b]}$ mit $a \leq b$ in $\mathbb{R}$ erzeugt $T(\mathbb{R}, \mathbb{R})$, aber sie ist, wie hier zu sehen, linear abhängig und somit keine Basis.

☺ In der Analysis sind Treppenfunktionen ein erster wichtiger Schritt zur Integration von Funktionen $f : \mathbb{R} \to \mathbb{R}$ und allgemein $f : \mathbb{R}^n \to \mathbb{R}$.

Zu diesem Zweck konstruiert man das Integral $\int_{\mathbb{R}} : T(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ als $\mathbb{R}$–lineare Abbildung mit der Normierung $\int_{\mathbb{R}} \mathbf{I}_{[a,b]}(x)\, \mathrm{d}x = b - a$.

Diese Bedingung legt das Integral auf ganz $T(\mathbb{R}, \mathbb{R})$ eindeutig fest, da die Indikatorfunktionen $\mathbf{I}_{[a,b]}$ den Vektorraum $T(\mathbb{R}, \mathbb{R})$ erzeugen!

Wir führen diese Konstruktion ab Seite I237 detailliert aus.

Schnitt und Summe von Unterräumen sind eine nützliche und allgegenwärtige Konstruktion, daher schauen wir genauer hin:

Satz I1X: Unterräume bilden einen vollständigen Verband.

Sei V ein R–linearer Raum über dem Ring R sowie $(U_i)_{i\in I}$ eine Familie von R–linearen Unterräumen $U_i \leq V$.

(1) Die Schnittmenge $A = \bigcap_{i\in I} U_i$ ist ein R–linearer Unterraum in V und zudem der größte, der in allen Unterräumen U_i enthalten ist.

(2) Die Summe $B = \sum_{i\in I} U_i$ ist ein R–linearer Unterraum in V und zudem der kleinste, der alle Unterräume U_i enthält.

Wir betrachten die Menge $X = \{\, U \leq V \,\}$ aller Unterräume von V. Bezüglich Inklusion ist $(X, \subseteq)$ eine geordnete Menge (Poset F1A).

Dank (1) und (2) ist $(X, \subseteq)$ ein vollständiger Verband (gemäß F1L) mit Infimum $\bigwedge_{i\in I} U_i = \bigcap_{i\in I} U_i$ und Supremum $\bigvee_{i\in I} U_i = \sum_{i\in I} U_i$.

Beispiel: Jede Menge Ω definiert den vollständigen Verband $(\mathfrak{P}(\Omega), \subseteq)$. Hierbei ist $\inf U = \bigcap U$ der Schnitt und $\sup U = \bigcup U$ die Vereinigung.

☺ Wir sehen nun für Unterräume von V eine ähnliche Struktur, mit Infimum $\bigwedge_{i\in I} U_i = \bigcap_{i\in I} U_i$ und Supremum $\bigvee_{i\in I} U_i = \sum_{i\in I} U_i$.

⚠ Die Vereinigung von Unterräumen ist i.A. kein Unterraum, eindrückliche Gegenbeispiele kennen Sie bereits von Seite I150.

Die Rolle des Supremums übernimmt hier die Summe; das ist nützlich zu wissen und erklärt die zuvor beobachteten Zusammenhänge.

Aufgabe: Rechnen Sie die Aussagen des Satzes anhand der zugehörigen Definitionen sorgsam nach.

Lösung: Für jeden Index $i \in I$ ist $U_i \leq V$ ein Unterraum. Gemäß I1P bedeutet das $0 \in U_i$ und $U_i + U_i \subseteq U_i$ und $U_i \cdot R \subseteq U_i$.

(1a) Wir zeigen, dass auch $A = \bigcap_{i\in I} U_i$ ein Unterraum ist.

Wir zeigen $0 \in A$: Da $0 \in U_i$ für alle $i \in I$ gilt, folgt sofort $0 \in A$.

Wir zeigen $A + A \subseteq A$: Hierzu seien $x, y \in A$. Das bedeutet $x, y \in U_i$ für alle $i \in I$. Daraus folgt $x + y \in U_i$ für alle $i \in I$. Wir schließen $x + y \in A$.

Wir zeigen $A \cdot R \subseteq A$: Hierzu seien $x \in A$ und $\lambda \in R$. Das bedeutet $x \in U_i$ für alle $i \in I$. Daraus folgt $x \cdot \lambda \in U_i$ für alle $i \in I$, also $x \cdot \lambda \in A$.

(1b) Sei $U \leq V$ ein Unterraum, sodass $A \subseteq U_i$ für alle $i \in I$ gilt. Daraus folgt $U \subseteq \bigcap_{i\in I} U_i = A$. Somit ist A der größte Unterraum, der in allen Unterräumen U_i enthalten ist.

(2a) Wir zeigen, dass auch $B = \sum_{i\in I} U_i$ ein Unterraum ist:

$$B = \textstyle\sum_{i\in I} U_i := \left\{ \sum_{i\in I} u_i \;\middle|\; u_i \in U_i \wedge \sharp\,\mathrm{supp}(u) < \infty \right\}$$

Wir haben $0 \in B$ dank $0 = \sum_i 0$ mit $0 \in U_i$ für alle $i \in I$.

Wir zeigen $B + B \subseteq B$: Hierzu seien $x, y \in B$. Das bedeutet $x = \sum_i x_i$ und $y = \sum_i y_i$ mit $x_i, y_i \in U_i$, und nur endlich viele Summanden sind ungleich Null. Daraus folgt $x + y = \sum_i (x_i + y_i) \in B$.

Wir zeigen $B \cdot R \subseteq B$: Hierzu seien $x \in B$ und $\lambda \in R$. Das bedeutet $x = \sum_i x_i$ wie oben. Daraus folgt $x \cdot \lambda = \sum_i (x_i \cdot \lambda) \in B$.

(2b) Nach Konstruktion der Summe gilt $B \supseteq U_i$ für alle $i \in I$. Sei $U \leq V$ ein Unterraum, sodass $U \supseteq U_i$ für alle $i \in I$ gilt. Daraus folgt $U \supseteq \sum_{i\in I} U_i = B$, da wir in U summieren können. Somit ist B der kleinste Unterraum, der alle Unterräume U_i enthält.

Jeder Unterraum $U \leq \mathbb{Z}$ ist von der Form $U = u\mathbb{Z}$ mit $u \in \mathbb{N}$. (G1v)
Daraus erhalten wir das folgende schöne und nützliche Ergebnis:

Satz I1y: Schnitt und Summe von Unterräumen in $\mathbb{Z}$

Zu jedem $i \in I$ sei $U_i = u_i\mathbb{Z} \leq \mathbb{Z}$ ein $\mathbb{Z}$–linearer Unterraum.

(1) Die Schnittmenge $A = \bigcap_{i\in I} U_i$ ist ein $\mathbb{Z}$–linearer Unterraum in $\mathbb{Z}$.
und zudem der größte, der in allen Unterräumen U_i enthalten ist.
Konkret gilt dabei $A = a\mathbb{Z}$ mit $a = \mathrm{kgV}(u_i : i \in I)$.

(2) Die Summe $B = \sum_{i\in I} U_i$ ist ein $\mathbb{Z}$–linearer Unterraum in $\mathbb{Z}$
und zudem der kleinste, der alle Unterräume U_i enthält.
Konkret gilt dabei $B = b\mathbb{Z}$ mit $b = \mathrm{ggT}(u_i : i \in I)$.

⚠ Beachten Sie, wie „kleinste“ und „größte“ vertauscht werden.
Der folgende Beweis erklärt ganz konkret, warum dies so sein muss.

Aufgabe: Beweisen Sie den vorigen Satz.

Zeigen Sie zunächst die folgende Äquivalenz:
(0) Genau dann gilt $b\mathbb{Z} \subseteq a\mathbb{Z}$, wenn $a \mid_{\mathbb{Z}} b$ gilt.

Lösung: „⇒“: Aus $b\mathbb{Z} \subseteq a\mathbb{Z}$ folgt insbesondere $b \in a\mathbb{Z}$.
Demnach gilt $b = aa'$ für ein $a' \in \mathbb{Z}$, und somit $a \mid_{\mathbb{Z}} b$.
„⇐“: Teilbarkeit $a \mid_{\mathbb{Z}} b$ bedeutet, es existiert $a' \in \mathbb{Z}$ mit $aa' = b$.
Demnach gilt $b \in a\mathbb{Z}$, und daraus folgt $b\mathbb{Z} \subseteq a\mathbb{Z}$.

Bemerkung: Die Definition der Teilbarkeit und die obige Rechnung übertragen sich von $\mathbb{Z}$ wörtlich auf jeden kommutativen Ring.

Die Besonderheit des Rings $\mathbb{Z}$ ist der Klassifikationssatz G1v:
Jeder Unterraum $U \leq \mathbb{Z}$ ist von der Form $U = u\mathbb{Z}$ mit $u \in \mathbb{N}$.

Beweis des Satzes:

(1) Sei $A = \bigcap_{i\in I} u_i\mathbb{Z}$. Dank G1v gilt $A = a\mathbb{Z}$ für ein $a \in \mathbb{N}$.

(a) Aus $A = a\mathbb{Z} \subseteq u_i\mathbb{Z}$ folgt $u_i \mid a$. Dies gilt für alle $i \in I$.

(b) Angenommen, $a' \in \mathbb{Z}$ erfüllt $u_i \mid a'$ für alle $i \in I$.
Dann gilt $a'\mathbb{Z} \subseteq u_i\mathbb{Z}$ für alle $i \in I$, also $a'\mathbb{Z} \subseteq A$.
Aus $a'\mathbb{Z} \subseteq A = a\mathbb{Z}$ wiederum folgt $a \mid a'$.

Das bedeutet, a ist ein kleinstes gemeinsames Vielfaches von $(u_i)_{i\in I}$.

(2) Sei $B = \sum_{i\in I} u_i\mathbb{Z}$. Dank G1v gilt $B = b\mathbb{Z}$ für ein $b \in \mathbb{N}$.

(a) Aus $u_i\mathbb{Z} \subseteq B = b\mathbb{Z}$ folgt $b \mid u_i$. Dies gilt für alle $i \in I$.

(b) Angenommen, $b' \in \mathbb{Z}$ erfüllt $b' \mid u_i$ für alle $i \in I$.
Dann gilt $u_i\mathbb{Z} \subseteq b'\mathbb{Z}$ für alle $i \in I$, also $B \subseteq b'\mathbb{Z}$.
Aus $B = b\mathbb{Z} \subseteq b'\mathbb{Z}$ wiederum folgt $b' \mid b$.

Das bedeutet, b ist ein größter gemeinsamer Teiler von $(u_i)_{i\in I}$.

Beispiel: Zur Illustration nenne ich

$$12\mathbb{Z} + 15\mathbb{Z} = 3\mathbb{Z},$$
$$12\mathbb{Z} \cap 15\mathbb{Z} = 60\mathbb{Z}.$$

Sie können sich leicht weitere Beispiele ausdenken wie

$$12\mathbb{Z} + 15\mathbb{Z} + 7\mathbb{Z} = 1\mathbb{Z},$$
$$12\mathbb{Z} \cap 15\mathbb{Z} \cap 7\mathbb{Z} = 420\mathbb{Z}.$$

🙂 Konkrete numerische Beispiele können wir wunderbar effizient mit dem euklidischen Algorithmus A2h berechnen.

🙂 Vergleichen Sie dies mit den Beipielen und dem Beweis von I1u.
Warum ist der Beweis des allgemeineren Satzes I1y so leicht?

Wann ist die Vereinigung von Unterräumen ein Unterraum?

Aufgabe: (1) Die Vereinigung von Unterräumen ist i.A. kein Unterraum. Nennen Sie möglichst einfache und anschauliche Gegenbeispiele!

(2) Seien $U_1, U_2 \leq V$ Unterräume. Genau dann ist $U := U_1 \cup U_2$ selbst ein Unterraum in V, wenn $U_1 \leq U_2$ oder $U_2 \leq U_1$ gilt.

(3) Wie sieht es aus für eine aufsteigende Kette $(U_i)_{i\in\mathbb{N}}$ von Unterräumen, also $U_0 \leq U_1 \leq U_2 \leq \cdots \leq V$?

Lösung: (1) Wir betrachten den Raum R^2 über einem Ring R. Hierin sind $U_1 = Re_1 = \{\, (x,0) \mid x \in R \,\}$ und $U_2 = Re_2 = \{\, (0,y) \mid y \in R \,\}$ Unterräume, doch $U = U_1 \cup U_2$ ist kein Unterraum von R^2:
Es gilt $(1,0) \in U$ und $(0,1) \in U$, aber $(1,0) + (0,1) \notin U$.

Wann ist die Vereinigung von Unterräumen ein Unterraum?

(2) Wir zeigen die Kontraposition:
Angenommen es gilt $U_1 \not\leq U_2$ und $U_2 \not\leq U_1$.
Dann ist $U := U_1 \cup U_2$ kein Unterraum in V.

Beweis hierzu: Es gibt Vektoren $v_1 \in U_1 \smallsetminus U_2$ und $v_2 \in U_2 \smallsetminus U_1$.
Wir betrachten $v = v_1 + v_2$. Wäre $v \in U$, so sind zwei Fälle möglich:
Im Falle $v \in U_1$ hätten wir $v_2 = v - v_1 \in U_1$; Widerspruch.
Im Falle $v \in U_2$ hätten wir $v_1 = v - v_2 \in U_2$; Widerspruch.
Wir schließen $v \notin U$. Somit ist U kein Unterraum in V.

(3) Sei $U_0 \leq U_1 \leq U_2 \leq \cdots \leq V$ eine Kette von Unterräumen in V.
Dann ist ihre Vereinigung $U = \bigcup_{i\in\mathbb{N}} U_i$ wiederum ein Unterraum in V.
Beweisen Sie dies als Übung, oder besser gleich den folgenden Satz.

Wann ist die Vereinigung von Unterräumen ein Unterraum?

Satz I1Z: Vereinigung einer gerichteten Familie von Unterräumen

Sei V ein R–linearer Raum. Hierin sei $(U_i)_{i\in I}$ eine gerichtete Familie von Unterräumen $U_i \leq V$, indiziert durch eine gerichtete Menge $(I, \leq)$:
(a) Für je zwei vergleichbare Indizes $i \leq j$ in I gelte $U_i \leq U_j$ in V.
(b) Zu je zwei Indizes $i, j \in I$ existiere ein $k \in I$ mit $i \leq k$ und $j \leq k$.
Dann ist die Vereinigung $U = \bigcup_{i\in I} U_i$ ein R–linearer Unterraum von V.

Bemerkung: Eine **prägeordnete Menge** $(I, \leq)$ besteht aus einer Menge I und einer Präordnung $\leq$ auf I, siehe Definition F1A.

Wir nennen $(I, \leq)$ eine **gerichtete Menge** und $\leq$ eine **Richtung**, falls jede endliche Teilmenge in I eine obere Schranke in I hat (F1G). Das bedeutet $I \neq \emptyset$ und zu $i, j \in I$ existiert $k \in I$ mit $i \leq k$ und $j \leq k$.

In Satz I1Z sprechen wir daher von einer **gerichteten Familie** $(U_i)_{i\in I}$ von Unterräumen $U_i \leq V$, indiziert durch die gerichtete Menge $(I, \leq)$.

Beispiele: Die geordneten Mengen $(\mathbb{N}, \leq)$ und $(\mathbb{R}, \leq)$ sind gerichtet.

Wann ist die Vereinigung von Unterräumen ein Unterraum?

Aufgabe: Beweisen Sie diesen Satz.

Lösung: Wir zeigen, dass $U \leq V$ ein R–linearer Unterraum ist.

(0) Dank $I \neq \emptyset$ existiert ein $i \in I$. Da $U_i \leq V$ ein Unterraum ist, haben wir den Nullvektor $0 \in U_i$. Somit gilt $0 \in U = \bigcup_{i\in I} U_i$.

(1) Zu je zwei Vektoren $u, v \in U$ existieren Indizes $i, j \in I$ mit $u \in U_i$ und $v \in U_j$. Hierzu wiederum existiert eine obere Schranke $k \in I$ mit $i \leq k$ und $j \leq k$, also $U_i \leq U_k$ und $U_j \leq U_k$, und somit $u, v \in U_k$.
Da $U_k \leq V$ ein Unterraum ist, gilt $u + v \in U_k$, also $u + v \in U$.

(2) Zu $u \in U$ existiert $i \in I$, sodass $u \in U_i$ gilt. Da $U_i \leq V$ ein Unterraum ist, gilt $Ru \leq U_i$ bzw. $uR \leq U_i$. Somit gilt $Ru \leq U$ bzw. $uR \leq U$.

🙂 Eigenschaften (0) und (2) gelten für jede nicht-leere Familie $(U_i)_{i\in I}$ von Unterräumen $U_i \leq V$. Für die Abgeschlossenheit unter Addition (1) benötigen wir mehr: Uns genügt eine gerichtete Familie $(U_i)_{i\in I}$.

Äquivalenz modulo eines Unterraumes $U \leq V$

Vorbild: Zum Unterraum $n\mathbb{Z} \leq \mathbb{Z}$ konstruieren wir den Quotienten $\mathbb{Z}/n\mathbb{Z}$.
Die Quotientenabbildung $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ ist $\mathbb{Z}$–linear mit $\ker(q) = n\mathbb{Z}$.

Allgemein: Sei V ein R–linearer Raum und $U \leq V$ ein Unterraum.
Insbesondere ist die Teilmenge $U \leq (V, +)$ eine Untergruppe,
es gilt also $0 \in U$ und $-U \subseteq U$ und $U + U \subseteq U$. Daraus folgt:

Der Unterraum $U \leq V$ definiert auf V die Äquivalenzrelation

$$x \sim y \quad :\Leftrightarrow \quad x - y \in U.$$

1. Reflexivität: Es gilt $x \sim x$, denn $x - x = 0 \in U$.
2. Symmetrie: $x \sim y$ bedeutet $x - y \in U$, also $y - x \in U$, somit $y \sim x$.
3. Transitivität: $x \sim y$ und $y \sim z$ bedeuten $x - y \in U$ und $y - z \in U$, daraus folgt $U \ni (x - y) + (y - z) = x - z$, somit $x \sim z$.

Beispiel: Für $n\mathbb{Z} \leq \mathbb{Z}$ erhalten wir die Kongruenz $x \equiv y \Leftrightarrow x - y \in n\mathbb{Z}$.
Die Äquivalenzklasse von x ist $[x] = x + n\mathbb{Z} = \{ x + nk \mid k \in \mathbb{Z} \}$.
Der Quotient ist demnach $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} : x \mapsto [x] = x + n\mathbb{Z}$.

Äquivalenzklassen modulo eines Unterraumes $U \leq V$

Die Menge V wird in Äquivalenzklassen bezüglich $\sim$ zerlegt (E318).
Zu jedem Vektor $x \in V$ haben wir die zugehörige Äquivalenzklasse:

$$[x] = x + U := \{ x + u \mid u \in U \}$$

Alle Äquivalenzklassen fassen wir zur Quotientenmenge zusammen:

$$V/U := \{ [x] = x + U \mid x \in V \}$$

Die zugehörige Quotientenabbildung ist demnach:

$$q : V \twoheadrightarrow V/U : x \mapsto [x] = x + U$$

Beispiel: Für $U = \{0\}$ erhalten wir $V/\{0\} = \{ \{x\} \mid x \in V \}$.
Die Quotientenabbildung $q : V \to V/\{0\} : x \mapsto \{x\}$ ist bijektiv.

Beispiel: Für $U = V$ erhalten wir $V/V = \{ V \}$.
Die Quotientenabbildung $q : V \to V/V : x \mapsto V$ ist konstant.

Diese beiden Extremfälle kommen also natürlich vor, siehe E321.
Interessant sind vor allem die Fälle dazwischen, also $0 < U < V$.

Konstruktion der Quotientengruppe $(U/V, +)$

Aus $x \sim x'$ und $y \sim y'$ folgt $x + y \sim x' + y'$, denn

$$(x + y) - (x' + y') = (x - x') + (y - y') \quad \in \quad U + U \quad \subseteq \quad U$$

Somit erhalten wir auf V/U eine wohldefinierte Addition

$$+ : V/U \times V/U \to V/U : ([x], [y]) \mapsto [x] + [y] := [x + y].$$

Wohldefiniert bedeutet hier: Das Ergebnis von $[x + y]$ hängt nur von den Klassen $[x], [y]$ ab, und nicht von der Wahl der Repräsentanten x, y.
Wählen wir statt x, y andere Repräsentanten x', y', so ist die Summe $x' + y' \sim x + y$ äquivalent, die Klasse $[x' + y'] = [x + y]$ also gleich.

Demnach ist $q : (V, +) \twoheadrightarrow (V/U, +)$ ein surjektiver Homomorphismus,
und die Gruppeneigenschaften übertragen sich von $(V, +)$ auf $(V/U, +)$.

Bemerkung: Wir können die Definition $[x] + [y] = [x + y]$ auch als Komplexverknüpfung betrachten (G1D), denn für alle $x, y \in V$ gilt

$$(x + U) + (y + U) = (x + y) + (U + U) = (x + y) + U.$$

Beispiel: Für $n\mathbb{Z} \leq \mathbb{Z}$ erhalten wir so die Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Konstruktion des Quotientenraumes $(U/V, +, \cdot)$

Aus $x \sim x'$ und $\lambda \in R$ folgt $x \cdot \lambda \sim x' \cdot \lambda$, denn

$$(x \cdot \lambda) - (x' \cdot \lambda) = (x - x') \cdot \lambda \quad \in \quad U \cdot R \quad \subseteq \quad U$$

Somit erhalten wir auf V/U eine wohldefinierte Skalarmultiplikation

$$\cdot : V/U \times R \to V/U : ([x], \lambda) \mapsto [x] \cdot \lambda = [x \cdot \lambda].$$

Nach Voraussetzung ist $\cdot : V \times R \to V$ eine distributive Operation (I1B),
und diese Eigenschaft überträgt sich auf $\cdot : V/U \times R \to V/U$. (Übung!)

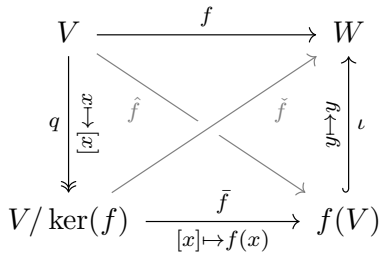
Die Rechnung gilt genauso bei Skalarmultiplikation von links.
Zusammenfassend erhalten wir das folgende schöne Ergebnis:

Satz I2A: Quotientenraum und Quotientenhomomorphismus

Sei V ein R–linearer Raum und $U \leq V$ ein R–linearer Unterraum.
Dann ist der Quotient V/U wie oben erklärt ein R–linearer Raum,
und die Quotientenabbildung $q : V \twoheadrightarrow V/U : x \mapsto x + U$ ist R–linear.
Nach Konstruktion ist q surjektiv mit $\ker(q) = U$.

🙂 Slogan: Wir können jeden Unteraum $U \leq V$ so „zu Null machen“.

Injektiv und surjektiv machen: die kanonische Faktorisierung



Satz I2B: die kanonische Faktorisierung

Jede R–lineare Abbildung $f : V \to W$ faktorisiert gemäß $f = \iota \circ \bar{f} \circ q$ in

1. die Quotientenabbildung $q : V \twoheadrightarrow V/\ker(f) : x \mapsto [x]$,
2. die Bijektion $\bar{f} : V/\ker(f) \xrightarrow{\sim} f(V) : [x] \mapsto f(x)$,
3. die Inklusion $\iota : f(V) \hookrightarrow W : y \mapsto y$.

Diese sind R–linear, insbesondere ist $\bar{f}$ ein R–Isomorphismus.
Wir nennen daher $\bar{f}$ den **kanonischen Isomorphismus** zu f.

Injektiv und surjektiv machen: die kanonische Faktorisierung

🙂 So können wir jede R–lineare Abbildung $f : V \to W$ kanonisch zerlegen in die drei einfacheren Abbildungen $q, \bar{f}, \iota$.
Diese heißen daher **kanonische Surjektion / Bijektion / Injektion**.

Beweis: Die Abbildungen q und $\bar{f}$ und ι sind wohldefiniert.
Für Quotient q und Inklusion ι ist dies klar nach Konstruktion.
Für $\bar{f}$ folgt dies aus dem Faktorisierungssatz I2E oder hier direkt:

(0) Wohldefiniertheit: Aus $[x] = [x']$ folgt $f(x) = f(x')$, denn $[x] = [x']$ $\Leftrightarrow$ $x - x' \in \ker(f)$ $\Leftrightarrow$ $0 = f(x - x') = f(x) - f(x')$ $\Leftrightarrow$ $f(x) = f(x')$.

(1) Injektivität: Gleichheit $\bar{f}(c) = \bar{f}(c')$ bedeutet: Für Repräsentanten $x \in c$ und $x' \in c'$ gilt $f(x) = f(x')$, somit $x - x' \in \ker(f)$, also $c = c'$.

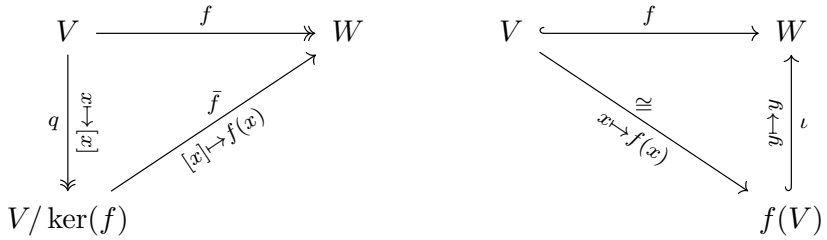
(2) Surjektivität: Zu jedem Bildelement $y \in f(V)$ existiert (mindestens) ein Urbild $x \in V$ mit $f(x) = y$. Somit gilt auch $\bar{f}([x]) = f(x) = y$.

Die R–Linearität von $q, \bar{f}, \iota$ folgt sofort aus der Konstruktion. QED

Bemerkung: So können wir f anschaulich „bijektiv machen“ zu $\bar{f}$.
Manchmal genügt surjektiv machen zu $\hat{f}$ oder injektiv machen zu $\check{f}$.

Injektiv und surjektiv machen: die kanonische Faktorisierung

Die einfachsten Beispiele ergeben sich wie folgt:



Beispiel: Ist $f : V \to W$ surjektiv, so erhalten wir $\bar{f} : V/\ker(f) \xrightarrow{\sim} W$.
Hier gilt $f(V) = W$ und die Inklusion $\iota : f(V) \hookrightarrow W$ ist die Identität.

Beispiel: Ist $f : V \to W$ injektiv, so erhalten wir $\bar{f} : V/\{0\} \xrightarrow{\sim} f(V)$.
Hier gilt $\ker(f) = \{0\}$ und $q : V \xrightarrow{\sim} V/\{0\}$ ist ein Isomorphismus.

Beispiel: Ist $f : V \to W$ bijektiv, so erhalten wir $\bar{f} : V/\{0\} \xrightarrow{\sim} W$.
Hier gilt sowohl $\ker(f) = \{0\}$ als auch $f(V) = W$.

Injektiv und surjektiv machen: die kanonische Faktorisierung

Aus Kapitel E kennen Sie als grundlegende Konstruktion die kanonische Faktorisierung für beliebige Abbildungen zwischen Mengen (Satz E3I):

Jede Abbildung $f : X \to Y$ faktorisiert gemäß $f = \iota \circ \bar{f} \circ q$ in

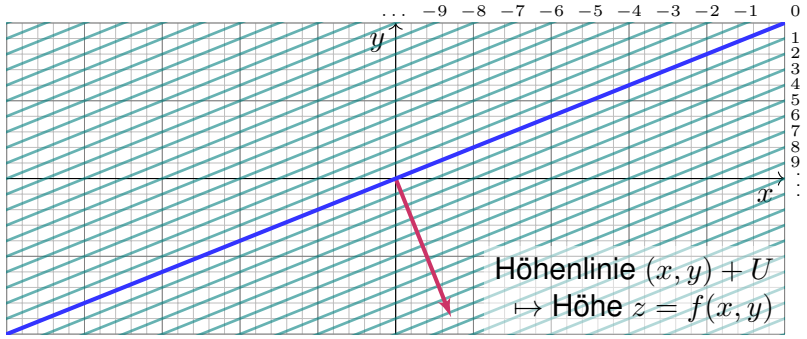
1. die Quotientenabbildung $q : X \twoheadrightarrow X/R_f : x \mapsto [x]$,
2. die Bijektion $\bar{f} : X/R_f \xrightarrow{\sim} f(X) : [x] \mapsto f(x)$,
3. die Inklusion $\iota : f(X) \hookrightarrow Y : y \mapsto y$.

Neu hinzu kommt hier nun, dass für jede lineare Abbildung $f : V \to W$ dabei die lineare Struktur erhalten bleibt. Den Quotienten V/R_f können wir zudem elegant als V/U formulieren mit dem Kern $U = \ker(f)$.

Beim ersten Kontakt ist das noch neu und ungewohnt und erfordert daher Gewöhnung und Übung. Davon abgesehen ist es nicht schwer.

Genau deshalb ist es wichtig, schon früh mit diesen Begriffen zu arbeiten. Bitte lesen Sie sich die schrittweise Konstruktion in Ruhe durch und illustrieren Sie dies mit Beispielen wie den folgenden.

Geometrisches Beispiel zur kanonischen Faktorisierung



Aufgabe: Führen Sie die kanonische Faktorisierung explizit aus für die $\mathbb{R}$–lineare Abbildung $f:\mathbb{R}^2\to\mathbb{R}:(x,y)\mapsto z=2x-5y$.

Lösung: (1) Es gilt $\mathrm{im}(f)=\mathbb{R}$: Zu $z\in\mathbb{R}$ finden wir $f(z/2,0)=z$.
(2) Es gilt $\ker(f)=(5,2)\cdot\mathbb{R}$. Die Inklusion „$\supseteq$“ folgt aus $f(5,2)=0$.
„$\subseteq$“: Aus $f(x,y)=0$ folgt $2x=5y$; für $t=x/5$ gilt $(x,y)=(5t,2t)$.
(3) Modulo $U=(5,2)\cdot\mathbb{R}$ induziert f den $\mathbb{R}$–Isomorphismus

$$\bar f\ :\ \mathbb{R}^2/U\xrightarrow{\sim}\mathbb{R}\ :\ (x,y)+U\mapsto f(x,y)=2x-5y.$$

Geometrisches Beispiel zur kanonischen Faktorisierung

🙂 Wir können uns $z=f(x,y)=2x+5y$ als Höhe vorstellen.
Der Kern $U=\ker(f)=(5,2)\cdot\mathbb{R}$ ist die Ursprungsgerade auf Höhe 0.
Die Äquivalenzklasse $(x,y)+U$ ist dann die Höhenlinie durch (x,y).
Die von f induzierte kanonische Bijektion

$$\bar f\ :\ \mathbb{R}^2/U\xrightarrow{\sim}\mathbb{R}\ :\ (x,y)+U\mapsto 2x-5y.$$

ordnet jeder Höhenlinie ihre Höhe zu. So gesehen ist alles ganz einfach und anschaulich. Am Anfang jedoch erfordert das etwas Gewöhnung und Einübung, bis es sich wirklich einfach und anschaulich anfühlt.

🙂 Die kanonische Faktorisierung gilt allgemein wie in Satz E3I:
Jede beliebige Abbildung $f:V\to W$ faktorisiert gemäß $f=\iota\circ\bar f\circ q$.
Wir betrachten hier speziell eine R–lineare Abbildung $f:V\to W$.
Damit wird die gesamte Konstruktion R–linear und somit besonders übersichtlich: Der Kern $U=\ker(f)\le V$ und das Bild $f(V)\le W$ sind R–lineare Unterräume, ebenso der Quotient V/U, und alle drei Abbildungen $q,\bar f,\iota$ sind R–linear wie in Satz I2B erklärt.

Analytisches Beispiel zur kanonischen Faktorisierung

Sie kennen die Schreibweise „$+\,\mathbf{const}$“ bei Stammfunktionen wie

$$\int x^n\,\mathrm{d}x=\frac{x^{n+1}}{n+1}+\mathbf{const},\qquad\int \mathrm{e}^x\,\mathrm{d}x=\mathrm{e}^x+\mathbf{const},\qquad\text{usw.}$$

Aufgabe: Erklären Sie dies mit Hilfe der kanonischen Faktorisierung!

Lösung: Auf dem Intervall $X=]a,b[\subseteq\mathbb{R}$ haben wir die Ableitung

$$D\ :\ \mathscr{C}^1(X,\mathbb{R})\to\mathscr{C}^0(X,\mathbb{R})\ :\ F\mapsto f=F'.$$

Diese $\mathbb{R}$–lineare Abbildung ist surjektiv, also $\mathrm{im}(D)=\mathscr{C}^0$, und ihr Kern $\ker(D)=\{\,F=\mathrm{const}\,\}=:U$ besteht aus allen konstanten Funktionen.
Dank kanonischer Faktorisierung erhalten wir den $\mathbb{R}$–Isomorphismus

$$\bar D\ :\ \mathscr{C}^1(X,\mathbb{R})/U\xrightarrow{\sim}\mathscr{C}^0(X,\mathbb{R})\ :\ F+U\mapsto f=F'.$$

Die Umkehrabbildung $\int$ ordnet jeder stetigen Funktion $f:X\to\mathbb{R}$ eine Stammfunktion F zu, genauer: ihre Äquivalenzklasse $\int f=F+U$.
⚠ Ohne den Quotienten modulo U ist die Umkehrung nicht definiert!
Genau dies steckt hinter der üblichen Schreibweise $\int f=F+\mathrm{const}$.

Analytisches Beispiel zur kanonischen Faktorisierung

Wir betrachten den Körper $\mathbb{K}=\mathbb{Q},\mathbb{R},\mathbb{C}$ und die $\mathbb{K}$–wertigen Folgen

$$\mathbb{K}^{\mathbb{N}}=\{\,a:\mathbb{N}\to\mathbb{K}:n\mapsto a_n\,\}.$$

Darin liegt der Unterraum $c=c(\mathbb{N},\mathbb{K})$ der $\mathbb{K}$–konvergenten Folgen, darin wiederum liegt der Unterraum $c_0=c_0(\mathbb{N},\mathbb{K})$ der Nullfolgen.

Aufgabe: Konstruieren Sie einen $\mathbb{K}$–Isomorphismus $c/c_0\cong\mathbb{K}$.

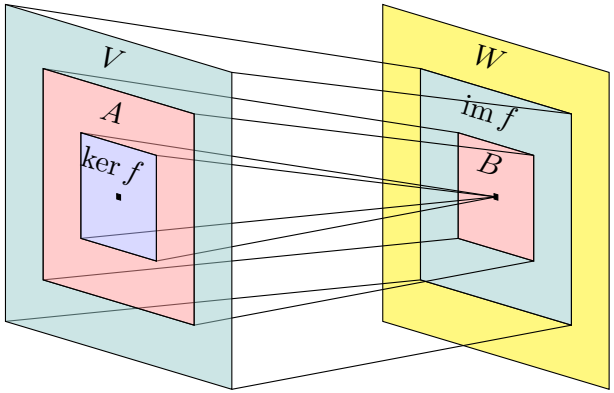
Lösung: Der Grenzwert $\lim:c(\mathbb{N},\mathbb{K})\to\mathbb{K}$ ist eine $\mathbb{K}$–lineare Abbildung.
Ihr Bild ist ganz $\mathbb{K}$, der Kern ist der Unterraum $c_0(\mathbb{N},\mathbb{K})$ aller Nullfolgen.
Dank kanonischer Faktorisierung induziert $\lim$ den $\mathbb{R}$–Isomorphismus

$$c(\mathbb{N},\mathbb{K})/c_0(\mathbb{N},\mathbb{K})\xrightarrow{\sim}\mathbb{K}\ :\ [a]\mapsto\lim a.$$

🙂 Diese Idee kann man nutzen zur Konstruktion der reellen Zahlen $\mathbb{R}$ aus den rationalen Zahlen $\mathbb{Q}$. Hierzu betrachtet man die Cauchy–Folgen $C(\mathbb{N},\mathbb{Q})\le\mathbb{Q}^{\mathbb{N}}$ und erhält so die ersehnte Vervollständigung

$$\mathbb{Q}\hookrightarrow C(\mathbb{N},\mathbb{Q})/c_0(\mathbb{N},\mathbb{Q})\xrightarrow{\sim}\mathbb{R}.$$

Der Korrespondenzsatz für Unterräume



Satz I2C: Korrespondenzsatz für Unterräume

(0) Jede R–lineare Abbildung $f : V \to W$ stiftet eine Bijektion

$$(f_*, f^*) \,:\, \{\, A \leq V \;\big|\; \ker(f) \leq A \,\} \;\cong\; \{\, B \leq \operatorname{im}(f) \,\}.$$

(1) Für jeden Unterraum $A \leq V$ gilt $f^{-1}(f(A)) = A + \ker(f)$.
(2) Für jeden Unterraum $B \leq W$ gilt $f(f^{-1}(B)) = B \cap \operatorname{im}(f)$.

Der Korrespondenzsatz für Unterräume

(0) Ausführlich besagt dieses Bijektionspaar (f_*, f^*):

1. Für jeden Unterraum $A \leq V$ mit $\ker(f) \leq A$ ist die Bildmenge $B := f(A) \leq \operatorname{im}(f)$ ein Unterraum, und es gilt $f^{-1}(B) = A$.
2. Für jeden Unterraum $B \leq \operatorname{im}(f)$ ist umgekehrt die Urbildmenge $A := f^{-1}(B) \leq V$ ein Unterraum mit $\ker(f) \leq A$ und $f(A) = B$.

Beweis: (1) Für jeden Unterraum $A \leq V$ gilt

$$f^{-1}(f(A)) \overset{\text{Def}}{=} \bigcup_{x \in A} f^{-1}(f(\{x\})) \overset{\text{IIR}}{=} \bigcup_{x \in A} x + \ker(f) \overset{\text{Def}}{=} A + \ker(f).$$

(0a) Zusammen mit $\ker(f) \leq A$ erhalten wir $f^{-1}(f(A)) = A$.

(2) Für jeden Unterraum $B \leq W$ gilt

$$f(f^{-1}(B)) \overset{\text{Def}}{=} \bigcup_{y \in B} f(f^{-1}(\{y\})) \overset{\text{Bild}}{=} B \cap \operatorname{im}(f).$$

(0b) Zusammen mit $B \leq \operatorname{im}(f)$ erhalten wir $f(f^{-1}(B)) = B$. QED

Der Isomorphiesatz für lineare Räume

Satz I2D: Isomorphiesatz für lineare Räume

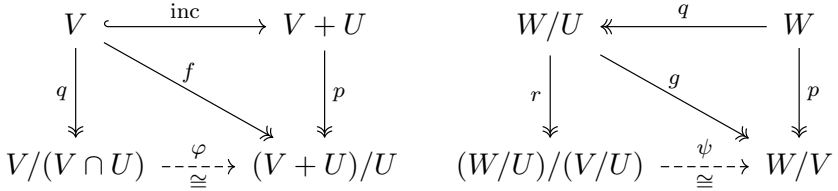
(1) Sind $U, V \leq W$ Unterräume, so auch $U + V$ und $U \cap V$, und es gilt:

$$\varphi \,:\, V/(V \cap U) \xrightarrow{\sim} (V + U)/U \,:\, v + (V \cap U) \mapsto v + U$$

(2) Sind $U \leq V \leq W$ lineare Räume, so gilt die Kürzungsregel:

$$\psi \,:\, (W/U)/(V/U) \xrightarrow{\sim} W/V \,:\, (w + U) + (V + U) \mapsto w + V$$

Beweis: Wir konstruieren zunächst zwei Hilfsabbildungen f und g:



Daran lesen wir ab (1) $\ker(f) = V \cap U$ und (2) $\ker(g) = V/U$.
Die kanonische Faktorisierung I2B erledigt nun die Arbeit. QED

Der Isomorphiesatz für lineare Räume

Aufgabe: Führen Sie die Details dieser Konstruktion aus! Wie sind die Abbildungen definiert? Warum gilt $\ker(f) = V \cap U$ und $\ker(g) = V/U$?

Lösung: (1) Wir definieren $f = p \circ \operatorname{inc} : V \hookrightarrow V + U \twoheadrightarrow (V + U)/U$.
Nach Konstruktion gilt $\operatorname{im}(f) = (V + U)/U$ und $\ker(f) = V \cap U$.
Die kanonische Faktorisierung I2B ergibt dann:

$$\varphi \,:\, V/(V \cap U) \xrightarrow{\sim} (V + U)/U \,:\, v + (V \cap U) \mapsto v + U$$

(2) Wir definieren $g : W/U \to W/V : x + U \mapsto x + V$, entweder direkt durch diese Formel oder mit dem folgenden Faktorisierungssatz I2E.
Nach Konstruktion gilt $\operatorname{im}(g) = W/V$ und $\ker(g) = V/U$.
Die kanonische Faktorisierung I2B ergibt dann:

$$\psi \,:\, (W/U)/(V/U) \xrightarrow{\sim} W/V \,:\, (w + U) + (V + U) \mapsto w + V$$

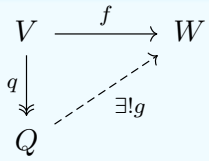
☺ Diese beiden Konstruktionen werden in den obigen Diagrammen zusammengefasst. Beide Darstellungen sind nützlich: Das Diagramm ist übersichtlich. Der Text ist ausführlich. Lernen Sie beides zu nutzen!

Faktorisierung über eine Surjektion

I217

Satz I2E: lineare Faktorisierung über eine Surjektion

Sei $q : V \twoheadrightarrow Q$ eine R–lineare Surjektion.
Gegeben sei eine R–lineare Abbildung $f : V \to W$.



Zu (f, q) suchen wir eine **Faktorisierung** $g : Q \to W$
mit $f = g \circ q$, also $f(x) = g(q(x))$ für alle $x \in V$.

Eindeutigkeit: Je zwei Faktorisierungen $g, g' : Q \to W$ sind gleich:
Zu jedem Element $\overline{x} \in Q$ existiert ein Urbild $x \in V$ mit $q(x) = \overline{x}$,
also gilt $g(\overline{x}) = g(q(x)) = (g \circ q)(x) = (g' \circ q)(x) = g'(q(x)) = g'(\overline{x})$.

Existenz: Genau dann existiert $g : Q \to W$ mit $f = g \circ q$, wenn
$\ker(q) \subseteq \ker(f)$ gilt. **Konstruktion:** Zu jedem $\overline{x} \in Q$ wählen wir
willkürlich ein Urbild $x \in V$ mit $q(x) = \overline{x}$ und setzen $g(\overline{x}) := f(x)$.

Diese Abbildung $g : Q \to W$ ist wohldefiniert und R–linear.
Der Bildraum $g(Q) = f(V)$ in W bleibt dabei unverändert.
Für den Kern gilt nach Konstruktion $\ker(g) = q(\ker f)$.
Genau dann ist g injektiv, wenn $\ker(q) = \ker(f)$ gilt.

Faktorisierung über eine Surjektion

I218
Erläuterung

Im Falle $f = g \circ q$ sagen wir **die Abbildung f faktorisiert über q zu g**
oder auch $f : V \to W$ **induziert** $g : Q \to W$ **über** $q : V \twoheadrightarrow Q$.

Beweis: Das ist die Faktorisierung $f = g \circ q$ aus Satz E3J.
Die R–Linearität von g rechnet man unmittelbar nach:

Linearität: Sei $\lambda \in R$. Zu $\overline{x}, \overline{y} \in Q$ wählen wir Urbilder $x, y \in V$.
Zu $\overline{x} + \overline{y} \cdot \lambda \in Q$ ist dann $x + y \cdot \lambda \in V$ ein Urbild, denn q ist R–linear.
Also gilt $g(\overline{x} + \overline{y} \cdot \lambda) = f(x + y \cdot \lambda) = f(x) + f(y) \cdot \lambda = g(\overline{x}) + g(\overline{y}) \cdot \lambda$.

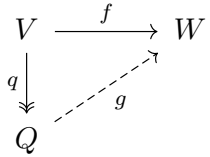
Die weiteren Aussagen sind klar. (Formulieren Sie dies aus!) QED

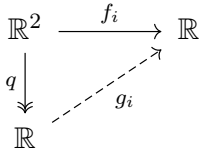
Beispiel: Speziell sei $q : V \to V/U$ ein Quotient. Genau dann faktorisiert
$f : V \to W$ über q zu $g : V/U \to W$, wenn $U \subseteq \ker(f)$ gilt.
In diesem Fall ist g eindeutig und wohldefiniert durch $g(x + U) = f(x)$.

🙂 Der Faktorisierungssatz ist das Universalwerkzeug zur Konstruktion
von R–linearen Abbildungen $g : Q \to W$ auf dem Quotienten $Q = V/U$:
Auf die Elemente $C \in Q$, also Äquivalenzklassen $C = q(x)$, haben wir
meist keinen direkten Zugriff, sondern nur über Repräsentanten $x \in C$.
Wir definieren $g : Q \to W$ mit Hilfe von Repräsentanten gemäß Satz E3J.

Faktorisierung über eine Surjektion

I219





$$f_1 : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto 4x - 5y$$
$$f_2 : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto 4x - 10y$$
$$q : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto 2x - 5y$$

Aufgabe: Finden Sie alle Faktorisierungen $g_1, g_2 : \mathbb{R} \to \mathbb{R}$

1. mit $f_1 = g_1 \circ q$, also $g_1(2x - 5y) = 4x - 5y$ für alle $x, y \in \mathbb{R}$;
2. mit $f_2 = g_2 \circ q$, also $g_2(2x - 5y) = 4x - 10y$ für alle $x, y \in \mathbb{R}$.

Lösung: Wir wenden den Faktorisierungssatz E3J an:

1. Es gibt keine Faktorisierung g_1, denn f_1 ist nicht kompatibel mit q:
   Es gilt $\ker(q) = (5, 2) \cdot \mathbb{R} \not\subseteq \ker(f_1)$, denn $f_1(5, 2) = 10 \neq 0$.
   Es müsste $g_1(0) = 0$ und zugleich $g_1(2 \cdot 5 - 5 \cdot 2) = 10$ gelten.
2. Es gibt genau eine Faktorisierung g_2, denn f_2 ist kompatibel mit q:
   Es gilt $\ker(q) = (5, 2) \cdot \mathbb{R} \subseteq \ker(f_2)$, denn $f_2(5, 2) = 0$.
   Explizit finden wir $g_2(z) = 2z$.

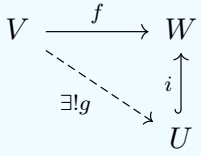
Faktorisierung über eine Injektion

I220
Erläuterung

Dual zur Faktorisierung über eine Surjektion wie in Satz I2E können wir
über eine Injektion faktorisieren. Das ist wesentlich einfacher:

Satz I2F: lineare Faktorisierung über eine Injektion

Sei $i : U \hookrightarrow W$ eine R–lineare Injektion.
Gegeben sei eine R–lineare Abbildung $f : V \to W$.



Zu (f, i) suchen wir eine **Faktorisierung** $g : V \to U$
mit $f = i \circ g$, also $f(x) = i(g(x))$ für alle $x \in V$.

Eindeutigkeit: Je zwei Faktorisierungen $g, g' : V \to U$ sind gleich.
Aus $f(x) = i(g(x)) = i(g'(x))$ folgt $g(x) = g'(x)$ dank Injektivität von i.

Existenz: Genau dann existiert $g : V \to U$ mit $f = i \circ g$, wenn
$f(V) \subseteq i(U)$ gilt. In diesem Falle setzen wir $g(x) = i^{-1}(f(x))$.

Diese Abbildung $g : V \to U$ ist wohldefiniert und R–linear.

Wichtiger Spezialfall: Ist $\iota : U \subseteq W$ eine Inklusion und $f(V) \subseteq U$, so ist
$g = f|_V^U$ die Einschränkung von f auf die Zielmenge U, siehe D306.

Faktorisierung über eine Surjektion

Aufgabe: Gegeben sei eine R–lineare Surjektion $q : V \twoheadrightarrow Q$.
Zu jedem R–linearen Raum W erhalten wir die Abbildung

$$\Phi \;:\; \mathrm{Hom}_R(Q,W) \to \mathrm{Hom}_R(V,W) \;:\; g \mapsto f = g \circ q.$$

(1) Ist Φ injektiv? surjektiv? Bestimmen Sie das Bild von Φ.
(2) Ist die Abbildung Φ additiv? sogar R–linear?

Faktorisierung über eine Surjektion

Lösung: (1) Die R–lineare Surjektion $q : V \twoheadrightarrow Q$ induziert die Injektion

$$\Phi \;:\; \mathrm{Hom}_R(Q,W) \hookrightarrow \mathrm{Hom}_R(V,W) \;:\; g \mapsto f = g \circ q$$

und somit eine Bijektion auf ihr Bild:

$$\Phi \;:\; \mathrm{Hom}_R(Q,W) \xrightarrow{\sim} \{\, f \in \mathrm{Hom}_R(V,W) \mid \ker(q) \subseteq \ker(f) \,\}$$

Dies ist eine Umformulierung des Faktorisierungssatzes I2E.

(2a) Die Mengen $\mathrm{Hom}_R(Q,W)$ und $\mathrm{Hom}_R(V,W)$ sind abelsche Gruppen bezüglich der punktweisen Addition, siehe Satz I1I.
Die Abbildung $\Phi : g \mapsto g \circ q$ ist additiv in g, dank Satz I1J

(2b) Ist R zudem kommutativ, so sind $\mathrm{Hom}_R(Q,W)$ und $\mathrm{Hom}_R(V,W)$ sogar R–lineare Räume und die Abbildung Φ ist R–linear.

Faktorisierung über eine Injektion

Aufgabe: Gegeben sei eine R–lineare Injektion $\iota : U \hookrightarrow W$.
Zu jedem R–linearen Raum V erhalten wir die Abbildung

$$\Psi \;:\; \mathrm{Hom}_R(V,U) \to \mathrm{Hom}_R(V,W) \;:\; g \mapsto f = \iota \circ g.$$

(1) Ist Ψ injektiv? surjektiv? Bestimmen Sie das Bild von Ψ.
(2) Ist die Abbildung Ψ additiv? sogar R–linear?

Faktorisierung über eine Injektion

Lösung: (1) Die R–lineare Injektion $\iota : U \hookrightarrow W$ induziert die Injektion

$$\Psi \;:\; \mathrm{Hom}_R(V,U) \hookrightarrow \mathrm{Hom}_R(V,W) \;:\; g \mapsto f = \iota \circ g.$$

und somit eine Bijektion auf ihr Bild:

$$\Psi \;:\; \mathrm{Hom}_R(V,U) \xrightarrow{\sim} \{\, f \in \mathrm{Hom}_R(V,W) \mid \mathrm{im}(f) \subseteq \mathrm{im}(\iota) \,\}$$

Dies ist eine Umformulierung des Faktorisierungssatzes I2F.

(2a) Die Mengen $\mathrm{Hom}_R(V,U)$ und $\mathrm{Hom}_R(V,W)$ sind abelsche Gruppen bezüglich der punktweisen Addition, siehe Satz I1I.
Die Abbildung $\Psi : g \mapsto \iota \circ g$ ist additiv in g, dank Satz I1J

(2b) Ist R zudem kommutativ, so sind $\mathrm{Hom}_R(V,U)$ und $\mathrm{Hom}_R(V,W)$ sogar R–lineare Räume und die Abbildung Ψ ist R–linear.

Illustration zum Korrespondenzsatz

Aufgabe: Wir betrachten die $\mathbb{Z}$–linearen Räume $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ sowie die Quotientenabbildung $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} : a \mapsto [a] = a + n\mathbb{Z}$.

(0) Warum sind $\mathbb{Z}$–Unterräume dasselbe wie Untergruppen? (I1K)

(1) Zur Erinnerung: Bestimmen Sie alle Unterräume $U \leq \mathbb{Z}$. (G1V)

(2) Korrespondenz: Bestimmen Sie alle Unterräume $V \leq \mathbb{Z}/n\mathbb{Z}$. (I2C)

Lösung: (0) Das folgt aus Existenz und Eindeutigkeit der $\mathbb{Z}$–Operation.

(1) Die Unterräume $U \leq \mathbb{Z}$ sind von der Form $U = u\mathbb{Z}$ mit $u \in \mathbb{N}$. (G1V)

(2a) Ist $V \leq \mathbb{Z}/n\mathbb{Z}$ ein Unterraum, so auch $U := q^{-1}(V) \leq \mathbb{Z}$, und es gilt $\ker(q) = n\mathbb{Z} \leq U$. Dank (1) haben wir $U = u\mathbb{Z}$; aus $n\mathbb{Z} \subseteq u\mathbb{Z}$ folgt $u \mid n$.

(2b) Umgekehrt: Für jede Zahl $u \in \mathbb{N}$ mit $u \mid n$ haben wir $U = u\mathbb{Z} \leq \mathbb{Z}$ mit $\ker(q) = n\mathbb{Z} \leq u\mathbb{Z} = U$ und somit $V = q(u\mathbb{Z}) = u\mathbb{Z}/n\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$.

Dank Korrespondenzsatz I2C erhalten wir: Die Unterräume von $\mathbb{Z}/n\mathbb{Z}$ sind von der Form $u\mathbb{Z}/n\mathbb{Z}$ mit $u \in \mathbb{N}$ und $u \mid n$.

Illustration zum Korrespondenzsatz

Beispiele: (a) Die Unterräume von $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ sind $u\mathbb{Z}/0\mathbb{Z}$ mit $u \in \mathbb{N}$.

(b) Ist $p \in \mathbb{N}_{\geq 2}$ eine Primzahl, so hat $\mathbb{Z}/p\mathbb{Z}$ genau zwei Unterräume, nämlich den trivialen $\{0\} = p\mathbb{Z}/p\mathbb{Z}$ und den gesamten $\mathbb{Z}/p\mathbb{Z} = 1\mathbb{Z}/p\mathbb{Z}$.

(c) Die Unterräume von $\mathbb{Z}/4\mathbb{Z}$ sind neben den extremen Beispielen $\{0\} = 4\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z} = 1\mathbb{Z}/4\mathbb{Z}$ nur noch $2\mathbb{Z}/4\mathbb{Z} = \{[0], [2]\}$.

(d) Die Unterräume von $\mathbb{Z}/8\mathbb{Z}$ sind neben $\{0\} = 8\mathbb{Z}/8\mathbb{Z}$ und $\mathbb{Z}/8\mathbb{Z} = 1\mathbb{Z}/8\mathbb{Z}$ nur $2\mathbb{Z}/8\mathbb{Z} = \{[0], [2], [4], [6]\}$ und $4\mathbb{Z}/8\mathbb{Z} = \{[0], [4]\}$.

(e) Die Unterräume von $\mathbb{Z}/15\mathbb{Z}$ sind neben $\{0\}$ und $\mathbb{Z}/15\mathbb{Z}$ nur $3\mathbb{Z}/15\mathbb{Z} = \{[0], [3], [6], [9], [12]\}$ und $5\mathbb{Z}/15\mathbb{Z} = \{[0], [5], [10]\}$.

🙂 Sie können direkt nachprüfen, dass die angegebenen Beispiele tatsächlich Untergruppen sind, und somit $\mathbb{Z}$–lineare Unterräume.

🙂 Korrespondenz I2C und Klassifikation G1V garantieren zudem, dass diese Beispiele die einzigen Untergruppen / Unterräume sind!

Illustration zum Korrespondenzsatz

Aufgabe: Bestimmen Sie $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ für alle $n \in \mathbb{N}$.

Lösung: Zu jedem $a \in \mathbb{N}$ existiert genau eine $\mathbb{Z}$–lineare Abbildung $f_a : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit $f_a(1) = [a]$, nämlich $f_a(k) = [ak]$. Dabei gilt $f_a = f_b$ genau dann, wenn $a - b \in n\mathbb{Z}$. Somit erhalten wir die Bijektion

$$\mathbb{Z}/n\mathbb{Z} \;\cong\; \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \;:\; [a] \mapsto f_a.$$

Aufgabe: Bestimmen Sie Kern und Bild von $f_a \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.

Lösung: (a) Für $a = 0$ gilt $\ker(f_0) = \mathbb{Z}$. Für $a \neq 0$ gilt

$$\ker(f_a) = \{\, k \in \mathbb{Z} \mid ak \in n\mathbb{Z} \,\} = \frac{\mathrm{kgV}(a,n)}{a}\mathbb{Z}.$$

(b) Wir nutzen die Quotientenabbildung $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$.
Nach Konstruktion von f_a gilt $\mathrm{im}(f_a) = q(a\mathbb{Z})$, also

$$q^{-1}(\mathrm{im}(f_a)) \overset{\text{Def}}{=} q^{-1}(q(a\mathbb{Z})) \overset{\text{I2C}}{=} a\mathbb{Z} + n\mathbb{Z} \overset{\text{I1Y}}{=} \mathrm{ggT}(a,n)\mathbb{Z}.$$

Somit gilt $\mathrm{im}(f_a) = \mathrm{ggT}(a,n)\mathbb{Z}/n\mathbb{Z}$.

Illustration zum Korrespondenzsatz

Beispiel: Wir betrachten die $\mathbb{Z}$–lineare Abbildung

$$f \;:\; \mathbb{Z} \to \mathbb{Z}/60\mathbb{Z} \;:\; k \mapsto 12k.$$

Hier gilt $\ker(f) = 5\mathbb{Z}$ und $\mathrm{im}(f) = 12\mathbb{Z}/60\mathbb{Z}$.

Beispiel: Wir betrachten die $\mathbb{Z}$–lineare Abbildung

$$f \;:\; \mathbb{Z} \to \mathbb{Z}/60\mathbb{Z} \;:\; k \mapsto 27k.$$

Hier gilt $\ker(f) = 15\mathbb{Z}$ und $\mathrm{im}(f) = 3\mathbb{Z}/60\mathbb{Z}$.

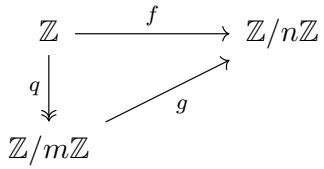
Illustration zur Faktorisierung

Aufgabe: Bestimmen Sie $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ für alle $m, n \in \mathbb{N}$.
Wie viele Elemente hat diese Menge im Fall $m, n \geq 1$?

Lösung: (0) Den Spezialfall $m = 0$ haben wir oben bereits gelöst:

$$\mathbb{Z}/n\mathbb{Z} \;\cong\; \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \;:\; [a] \mapsto f_a.$$

(1) Für den Fall $m \geq 1$ nutzen wir den Spezialfall (0) und
den Quotienten $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/m$ mit dem Faktorisierungssatz I2E.



Sei $g : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ eine beliebige $\mathbb{Z}$–lineare Abbildung.
Es gilt $g([1]) = [a]$ für ein $a \in \mathbb{Z}$, also $g = g_a : [k] \mapsto [ak]$.
Durch den Wert a ist g eindeutig festgelegt.

Illustration zur Faktorisierung

Die $\mathbb{Z}$–lineare Abbildung $g_a : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit $g_a([1]) = [a]$ definiert
eine $\mathbb{Z}$–lineare Abbildung $f_a = g_a \circ q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit $f_a(1) = [a]$ und
der Kompatibilitätsbedingung $m\mathbb{Z} \subseteq \ker(f_a)$, und ebenso umgekehrt.

Für $n = 0$ ist das nur für $a = 0$ möglich; für $a \neq 0$ gilt nämlich
$\ker(f_a) = \{0\} \not\supseteq m\mathbb{Z}$, da wir $m \geq 1$ voraussetzen. Das bedeutet:

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \{0\}$$

Im Falle $n \geq 1$ finden wir dagegen die Bijektion:

$$\frac{n}{\mathrm{ggT}(m,n)}\mathbb{Z}/n\mathbb{Z} \;\cong\; \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \;:\; [a] \mapsto g_a$$

Somit hat die Menge $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ genau $\mathrm{ggT}(m,n)$ Elemente.

Beispiel: Es gilt $\mathrm{Hom}(\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}) \cong \{\,[0]\,\}$.
Es gilt $\mathrm{Hom}(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/15\mathbb{Z}) \cong \{\,[0], [3], [6], [9], [12]\,\}$.

Die hier angegebene Bijektion ist sogar ein Isomorphismus!

Illustration zum Isomorphiesatz

Aufgabe: Illustrieren Sie den Isomorphiesatz I2D für $U, V \leq W = \mathbb{Z}$.

Lösung: Dank G1V gilt $U = u\mathbb{Z}$ und $V = v\mathbb{Z}$ mit $u, v \in \mathbb{N}$.
Dank I1Y gilt $V + U = \mathrm{ggT}(u,v)\mathbb{Z}$ und $V \cap U = \mathrm{kgV}(u,v)\mathbb{Z}$.
(1) Der Isomorphiesatz I2D(1) besagt:

$$\varphi \;:\; V/(V \cap U) \xrightarrow{\sim} (V+U)/U \;:\; x + (V \cap U) \mapsto x + U$$

Wir illustrieren dies für $V = 12\mathbb{Z}$ und $U = 15\mathbb{Z}$:

$$\varphi \;:\; 12\mathbb{Z}/60\mathbb{Z} \xrightarrow{\sim} 3\mathbb{Z}/15\mathbb{Z} \;:\; 12k + 60\mathbb{Z} \mapsto 12k + 15\mathbb{Z}$$

(2) Für $U \leq V \leq W = \mathbb{Z}$ besagt der Isomorphiesatz I2D(2):

$$\psi \;:\; (W/U)/(V/U) \xrightarrow{\sim} W/V \;:\; (x+U) + (V+U) \mapsto x + V$$

Wir illustrieren dies für $U = 6\mathbb{Z}$ und $V = 3\mathbb{Z}$:

$$\psi \;:\; (\mathbb{Z}/6\mathbb{Z})/(3\mathbb{Z}/6\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \;:\; (x + 6\mathbb{Z}) + (3\mathbb{Z} + 6\mathbb{Z}) \mapsto x + 3\mathbb{Z}$$

Illustration zum Isomorphiesatz

Bemerkung: Im Isomorphiesatz I2D(2) schreibe ich $V/U = V + U$
für das Bild des Unterraums $V \leq W$ unter der Quotientenabbildung

$$q \;:\; W \twoheadrightarrow W/U \;:\; x \mapsto x + U.$$

Die Schreibweise $V/U = \{\,[x] = x + U \mid x \in V\,\}$ betont, $V/U \leq W/U$
ein Unterraum ist. Die alternative und bequeme Schreibweise $V + U$
ist suggestiver für die Zuordnungsvorschrift des Isomorphismus

$$\psi \;:\; (W/U)/(V/U) \xrightarrow{\sim} W/V \;:\; (x+U) + (V+U) \mapsto x + V.$$

Formal korrekt sollte ich schreiben:

$$\psi \;:\; (W/U)/(V/U) \xrightarrow{\sim} W/V \;:\; (w+U) + (V/U) \mapsto w + V.$$

Anwendungsbeispiel: Grenzwert von Folgen

Aufgabe: Wir betrachten den $\mathbb{R}$–Vektorraum $\mathbb{R}^{\mathbb{N}}$ der reellen Folgen.

(0) Wiederholen Sie die Definition der Konvergenz $a \to 0$ bzw. $a \to z$ für eine Folge $a \in \mathbb{R}^{\mathbb{N}}$ und eine reelle Zahl $z \in \mathbb{R}$.

In der Grenzwertrechnung erlaubt man sich, eine Folge $a \in \mathbb{R}^{\mathbb{N}}$ an endlich vielen Stellen zu $b \in \mathbb{R}^{\mathbb{N}}$ abzuändern und betrachtet beide Folgen als äquivalent, gesprochen: **schließlich gleich**.

(1) Wie können Sie dies möglichst explizit und elegant als einen Quotienten konstruieren? Ist das Ergebnis ein $\mathbb{R}$–Vektorraum?

(2) Können Sie für eine Äquivalenzklasse schließlich gleicher Folgen immer noch die Begriffe „Konvergenz“ und „Grenzwert“ erklären?

(3) Faktorisiert $\lim : c(\mathbb{N},\mathbb{R}) \to \mathbb{R}$ über diesen Quotienten zu einer linearen Abbildung auf dem Quotientenraum?

Anwendungsbeispiel: Grenzwert von Folgen

(0) Die Folge $a \in \mathbb{R}^{\mathbb{N}}$ **konvergiert gegen** $z \in \mathbb{R}$, falls $a \to z$ gilt:

$$a \to z \quad :\Leftrightarrow \quad \forall \varepsilon \in \mathbb{R}_{>0} \ \exists m \in \mathbb{N} \ \forall n \in \mathbb{N}_{\geq m} \ : \ |a_n - z| < \varepsilon$$

In Worten: Zu jedem noch so kleinen $\varepsilon \in \mathbb{R}_{>0}$ existiert ein Index $m \in \mathbb{N}$, sodass für jeden Index $n \in \mathbb{N}_{\geq m}$ die Ungleichung $|a_n - z| < \varepsilon$ gilt.

In diesem Falle nennen wir die Folge a **konvergent** mit **Grenzwert** z. Wir nennen $a \in \mathbb{R}^{\mathbb{N}}$ eine **Nullfolge**, falls $a \to 0$ gilt.

Bemerkung: Jede Folge $a \in \mathbb{R}^{\mathbb{N}}$ hat höchstens einen Grenzwert in $\mathbb{R}$. Hat sie keinen Grenzwert, so nennen wir die Folge a **divergent**.

Der Begriff der *Konvergenz* ist grundlegend für die gesamte Analysis und ihre Anwendungen. Die Mathematiker des 19. Jahrhunderts vollbrachten die Meisterleistung, ihn rigoros präzise herauszuarbeiten und hierauf eine leistungsfähige Theorie zu errichten, die bis heute trägt und weiter ausgebaut wird. Von ihren Erfolgen legt die Differential- und Integralrechnung beredtes Zeugnis ab, die alle Studenten der Mathematik in ihren ersten Vorlesungen kennenlernen, und die überall in den Natur- und Ingenieurwissenschaften erfolgreich angewendet werden.

Anwendungsbeispiel: Grenzwert von Folgen

(1) Wörtlich übersetzt bedeutet „a schließlich gleich b“ folgendes:

$$a \sim b \quad :\Leftrightarrow \quad \exists m \in \mathbb{N} \ \forall n \in \mathbb{N}_{\geq m} \ : \ a_n = b_n$$

Algebraisch entspricht dies einer sehr vertrauten Bedingung:

$$a - b \ \in \ \mathbb{R}^{(\mathbb{N})}$$

Der gesuchte Quotient ist daher überraschend simpel:

$$F = \mathbb{R}^{\mathbb{N}} / \mathbb{R}^{(\mathbb{N})}$$

Elemente $\alpha \in F$ sind Äquivalenzklassen von Folgen $a \in \mathbb{R}^{\mathbb{N}}$. Die Klasse $[a]$ enthält alle Folgen, die schließlich gleich a sind.

🙂 Wir wissen, dass $\mathbb{R}^{(\mathbb{N})} \leq \mathbb{R}^{\mathbb{N}}$ ein $\mathbb{R}$–Untervektorraum ist (I1Q). Dank Satz I2A ist der Quotient $F = \mathbb{R}^{\mathbb{N}} / \mathbb{R}^{(\mathbb{N})}$ ein $\mathbb{R}$–Vektorraum.

Anwendungsbeispiel: Grenzwert von Folgen

(2) Jede Äquivalenzklasse $\alpha \in F$ können wir repräsentieren durch eine (willkürlich gewählte) Folge $a \in \alpha$. Wir können jedoch nicht mehr vom „$n$ten Folgenterm $\alpha_n \in \mathbb{R}$“ sprechen: denn dies ist nicht wohldefiniert!

Dennoch ist die Konvergenz „$\alpha \to z$“ wohldefiniert durch

$$\alpha \to z \quad :\Leftrightarrow \quad a \to z$$

für ein $a \in \alpha$. Gilt dies für einen Repräsentanten, so gilt es für alle! Konvergenz hängt nicht vom willkürlich gewählten Repräsentanten ab.

(3) Wir haben $\mathbb{R}^{(\mathbb{N})} \leq \ker(\lim) = c_0(\mathbb{N},\mathbb{R})$. Dank Faktorisierungssatz I2E induziert die $\mathbb{R}$–lineare Abbildung $\lim : c(\mathbb{N},\mathbb{R}) \to \mathbb{R}$ somit eine $\mathbb{R}$–lineare Abbildung $\overline{\lim} : c(\mathbb{N},\mathbb{R})/\mathbb{R}^{(\mathbb{N})} \to \mathbb{R}$ auf dem Quotientenraum.

🙂 Diese Überlegungen nutzt man häufig in der Grenzwertrechnung, meist jedoch nicht so explizit, sondern unbewusst oder gar heimlich. Nun wissen Sie genauer, welches Prinzip eigentlich dahinter steckt.

Anwendungsbeispiel: das Integral für Treppenfunktionen

Sei $T \leq \mathbb{R}^{\mathbb{R}}$ der Vektorraum aller Treppenfunktionen $f : \mathbb{R} \to \mathbb{R}$ (I1W).
Dieser wird erzeugt von den Indikatorfunktionen $\mathbf{I}_{[a,b]}$ mit $a \leq b$ in $\mathbb{R}$.
Wir betrachten also die Indexmenge $I = \{\, Q = [a,b] \mid a \leq b \text{ in } \mathbb{R} \,\}$
und die $\mathbb{R}$–lineare Abbildung $\Phi : \mathbb{R}^{(I)} \twoheadrightarrow T : c \mapsto \sum_{Q \in I} c_Q \, \mathbf{I}_Q$.

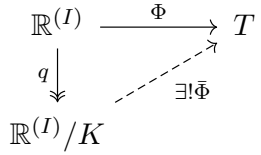
Lemma I2G: Relationen zwischen den Indikatorfunktionen $\mathbf{I}_{[a,b]}$

Es gilt $\ker(\Phi) = K := \{\, e_{[a,c]} - e_{[a,b]} - e_{[b,c]} + e_{[b,b]} \mid a < b < c \text{ in } \mathbb{R} \,\}$.

Beweis: Die Inklusion „$\supseteq$“ ist klar, denn für alle $a < b < c$ in $\mathbb{R}$ gilt

$$\mathbf{I}_{[a,c]} = \mathbf{I}_{[a,b]} + \mathbf{I}_{[b,c]} - \mathbf{I}_{[b,b]} \,.$$

Demnach induziert Φ modulo K die Abbildung $\bar{\Phi} : \mathbb{R}^{(I)}/K \twoheadrightarrow T$:



Die Aussage $\ker(\Phi) = K$ ist somit äquivalent zu Bijektivität von $\bar{\Phi}$.

Anwendungsbeispiel: das Integral für Treppenfunktionen

Für die Umkehrung „$\subseteq$“ konstruieren wir $\bar{\Psi} : T \to \mathbb{R}^{(I)}/K$.
Zu jeder Treppenfunktion $f \in T$ existiert eine Unterteilung
$U = \{x_0 < x_1 < \cdots < x_\ell\} \subset \mathbb{R}$ und Werte $f_1, \ldots, f_\ell \in \mathbb{R}$, sodass

$$f = \textstyle\sum_{k=1}^{\ell} f_k \, \mathbf{I}_{]x_{k-1},x_k[} + \sum_{k=0}^{\ell} f(x_k) \, \mathbf{I}_{[x_k,x_k]} \,.$$

Wir definieren daher $\Psi_U : T_U \to \mathbb{R}^{(I)}$ durch

$$\Psi_U(f) := \textstyle\sum_{k=1}^{\ell} f_k (e_{[x_{k-1},x_k]} - e_{[x_{k-1},x_{k-1}]} - e_{[x_k,x_k]}) + \sum_{k=0}^{\ell} f(x_k) e_{[x_k,x_k]}.$$

Je zwei Unterteilungen $U, V \subset \mathbb{R}$ haben gemeinsame Verfeinerungen,
die kleinstmögliche ist $W = U \cup V$. Schrittweises Verfeinern zeigt nun:

$$\Psi_U(f) \sim \Psi_W(f) \sim \Psi_V(f) \mod K$$

Somit ist $\bar{\Psi}(f) := \Psi_U(f) + K$ unabhängig von der Unterteilung U.
Daher ist $\bar{\Psi} : T \to \mathbb{R}^{(I)}/K : f \mapsto \Psi_U(f) + K$ wohldefiniert und
stiftet den ersehnten Isomorphismus $(\bar{\Phi}, \bar{\Psi}) : \mathbb{R}^{(I)}/K \cong T$. QED

🙂 Die offensichtlichen Relationen $\mathbf{I}_{[a,c]} = \mathbf{I}_{[a,b]} + \mathbf{I}_{[b,c]} - \mathbf{I}_{[b,b]}$ erzeugen demnach bereits alle Relationen. Das ist gut und nützlich zu wissen...

Anwendungsbeispiel: das Integral für Treppenfunktionen

Wir ordnen jedem Intervall $Q = [a,b]$ seine Länge $\lambda([a,b]) = b - a$ zu.
Wir wollen jeder Treppenfunktion $f \in T$ eine Zahl zuordnen gemäß

$$f = \textstyle\sum_{k=1}^{\ell} c_k \, \mathbf{I}_{Q_k} \quad \Longrightarrow \quad \begin{aligned} M(f) &:= \max\{c_1, \ldots, c_\ell\}, \\ N(f) &:= \textstyle\sum_{k=1}^{\ell} c_k^2 \lambda(Q_k), \\ P(f) &:= \textstyle\sum_{k=1}^{\ell} c_k \lambda(Q_k)^2. \end{aligned}$$

Aufgabe: Was ist hieran gefährlich falsch? Sind M, N, P wohldefiniert?
Versuchen Sie, diese Werte für folgende Funktionen zu bestimmen:

$$\begin{aligned} 0 &= 0 \cdot \mathbf{I}_{[0,1]} &&= (+1) \cdot \mathbf{I}_{[0,1]} + (-1) \cdot \mathbf{I}_{[0,1]} \\ f &= 2 \cdot \mathbf{I}_{[0,2]} + 3 \cdot \mathbf{I}_{[1,3]} &&= 2 \cdot \mathbf{I}_{[0,1[} + 5 \cdot \mathbf{I}_{[1,2]} + 3 \cdot \mathbf{I}_{]2,3]} \\ g &= 7 \cdot \mathbf{I}_{[0,1[} - 6 \cdot \mathbf{I}_{[1,3]} &&= 7 \cdot \mathbf{I}_{[0,1[} - 6 \cdot \mathbf{I}_{[1,2]} - 6 \cdot \mathbf{I}_{]2,3]} \end{aligned}$$

Lösung: Die Zuordnungen M, N, P sind nicht wohldefiniert!

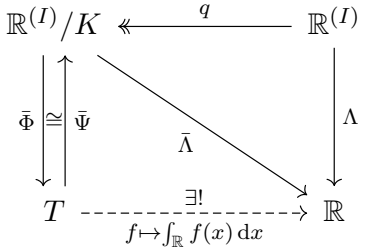
⚠ Verschiedene Darstellungen / Schreibweisen derselben Funktion liefern verschiedene Ergebnisse: Das ergibt überhaupt keinen Sinn!

Anwendungsbeispiel: das Integral für Treppenfunktionen

Wir möchten das Integral definieren durch die naheliegende Formel

$$\int_{\mathbb{R}} \Big[\sum_{Q \in I} c_Q \, \mathbf{I}_Q(x) \Big] \, \mathrm{d}x = \sum_{Q \in I} c_Q \lambda(Q).$$

Die obigen Beispiele mahnen zur Vorsicht: Ist das wohldefiniert?
Wir betrachten daher zunächst $\Lambda : \mathbb{R}^{(I)} \to \mathbb{R} : c \mapsto \sum_{Q \in I} c_Q \lambda(Q)$.
Diese Abbildung ist $\mathbb{R}$–linear und verschwindet auf $K = \ker(\Phi)$.
Wir erhalten so die ersehnte R–lineare Abbildung $\int : T \to \mathbb{R}$:



Jede Konstruktion des Integrals muss dieses Problem irgendwie lösen.
🙂 Nun wissen Sie genauer, was hinter den Kulissen eigentlich vorgeht.

Definition I2H: exakte Sequenz, Bild gleich Kern

Wir betrachten R–lineare Räume und ihre R–lineare Abbildungen.
Eine **Sequenz** $S = (f_i : V_i \to V_{i+1})_{i=0}^{n-1}$ der Länge n hat die Form

$$S: \quad V_0 \xrightarrow{f_0} V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} \dots \longrightarrow V_{n-1} \xrightarrow{f_{n-1}} V_n.$$

Sie heißt **exakt an der Stelle** i mit $0 < i < n$, falls $\operatorname{im}(f_{i-1}) = \ker(f_i)$.
Die Sequenz S heißt **exakt**, falls sie an jeder Stelle exakt ist.

🙂 An jeder Stelle ist das Bild von links gleich dem Kern nach rechts. Zusammengefasst erhalten wir den kurzen Slogan: *Bild gleich Kern!*

Exaktheit ist nichts fundamental Neues, sie hebt lediglich eine wichtige Eigenschaft hervor. Das erweist sich als eine sehr effiziente Sichtweise.

Diese bequeme Schreib- und Sprechweise bündelt eine erstaunliche Vielfalt nützlicher Informationen, wie die folgenden Beispiele zeigen.

Beispiel: Die Exaktheit der Sequenz

$$0 \xrightarrow{0} V \xrightarrow{f} W$$

ist äquivalent zu $\ker(f) \overset{!}{=} \operatorname{im}(0) = \{0\}$, das heißt f ist injektiv (I1R).

Beispiel: Die Exaktheit der Sequenz

$$V \xrightarrow{f} W \xrightarrow{0} 0$$

ist äquivalent zu $\operatorname{im}(f) \overset{!}{=} \ker(0) = W$, das heißt f ist surjektiv (I1R).

Beispiel: Die Exaktheit der Sequenz

$$0 \xrightarrow{0} V \xrightarrow{f} W \xrightarrow{0} 0$$

bedeutet f ist bijektiv, also ein R–Isomorphismus.

Beispiel: Die kanonische Faktorisierung von $f : V \to W$ induziert

$$0 \xrightarrow{0} V/\ker(f) \xrightarrow{\bar{f}} \operatorname{im}(f) \xrightarrow{0} 0.$$

Beispiel: Für jeden Unterraum $U \leq V$ bilden Inklusion $\iota : U \hookrightarrow V$ und Quotient $q : V \twoheadrightarrow V/U$ die kurze exakte Sequenz

$$0 \xrightarrow{0} U \xhookrightarrow{\iota} V \xrightarrow{q} V/U \xrightarrow{0} 0.$$

Das erste Beispiel ist die Restklassenkonstruktion:

$$0 \xrightarrow{0} n\mathbb{Z} \xhookrightarrow{\iota} \mathbb{Z} \xrightarrow{q} \mathbb{Z}/n\mathbb{Z} \xrightarrow{0} 0$$

Beispiel: Der Grenzwert beschert uns die kurze exakte Sequenz

$$0 \xrightarrow{0} c_0(\mathbb{N},\mathbb{R}) \xhookrightarrow{\iota} c(\mathbb{N},\mathbb{R}) \xrightarrow{\lim} \mathbb{R} \xrightarrow{0} 0.$$

Die Ableitung auf $X =]a,b[$ beschert uns die kurze exakte Sequenz

$$0 \xrightarrow{0} \mathbb{R} \xhookrightarrow{\iota} \mathscr{C}^1(X,\mathbb{R}) \xrightarrow{D} \mathscr{C}^0(X,\mathbb{R}) \xrightarrow{0} 0.$$

Hier ist $\iota(a) = \operatorname{const}_X^a$ die Einbettung der reellen Zahlen als Konstanten.

Beispiel: Für jede R–lineare Surjektion $f : V \twoheadrightarrow W$ haben wir

$$0 \xrightarrow{0} \ker(f) \xhookrightarrow{\iota} V \xrightarrow{f} W \xrightarrow{0} 0.$$

Für jede R–lineare Abbildung $f : V \to W$ haben wir entsprechend

$$0 \xrightarrow{0} \ker(f) \xhookrightarrow{\iota} V \xrightarrow{\hat{f}} \operatorname{im}(f) \xrightarrow{0} 0.$$

Wir nennen $\operatorname{coker}(f) := W/\operatorname{im}(f)$ den **Cokern** von f und erhalten so:

$$0 \xrightarrow{0} \ker(f) \xhookrightarrow{\iota} V \xrightarrow{f} W \xrightarrow{q} \operatorname{coker}(f) \xrightarrow{0} 0$$

Dadurch wird die Symmetrie der Begriffe vollständig wiederhergestellt.

🙂 Dies sind jeweils exakte Sequenzen: überall gilt „Bild gleich Kern“. Hier ist ι die Inklusion und q der Quotient. Sequenzen sind sehr flexibel: Auch Varianten sind möglich, wie in obigen Beispielen aus der Analysis.

🙂 Ich wiederhole daher noch einmal Ziel und Zweck dieses Begriffs: Exakte Sequenzen bündeln nützliche Informationen auf effiziente Weise.

Unendlich lange Sequenzen

Sequenzen geringer Länge $2, 3, 4, 5$ wie oben sind besonders häufig. Gelegentlich möchte man auch unendliche Sequenzen betrachten, zum Beispiel $S = (f_i : V_i \to V_{i+1})_{i\in\mathbb{N}}$ oder $S = (f_i : V_i \to V_{i+1})_{i\in\mathbb{Z}}$.

Allgemein betrachten wir daher eine **Sequenz** $S = (f_i : V_i \to V_{i+1})_{i\in I}$, wobei die Indexmenge $I \subseteq \mathbb{Z}$ und das Innere I° folgende Form haben:

$$\begin{aligned} I &= \mathbb{Z}, & I^\circ &= \mathbb{Z}, \\ I &= \mathbb{Z}_{\geq a}, & I^\circ &= \mathbb{Z}_{>a}, \\ I &= \mathbb{Z}_{<b}, & I^\circ &= \mathbb{Z}_{<b}, \\ I &= \{\, i \in \mathbb{Z} \mid a \leq i < b \,\}, & I^\circ &= \{\, i \in \mathbb{Z} \mid a < i < b \,\}. \end{aligned}$$

Die Sequenz S heißt **exakt an der Stelle** $i \in I^\circ$, falls $\operatorname{im}(f_{i-1}) = \ker(f_i)$. Die Sequenz S heißt **exakt**, falls sie an jeder Stelle $i \in I^\circ$ exakt ist.

Bemerkung: Meist lässt sich die Sequenz S auf natürliche Weise nach links und rechts verlängern, so dass wir $I = \mathbb{Z}$ annehmen können.

Notfalls füllen wir durch Nullräume und Nullabbildungen auf; an den Rändern erhalten Kern und Cokern die Exaktheit.

Exakte Sequenzen und Komplexe

Bemerkung: Die Bedingung $\operatorname{im}(f_{i-1}) \subseteq \ker(f_i)$ ist meist recht leicht zu prüfen, denn sie ist äquivalent zu der Gleichung $f_i \circ f_{i-1} = 0$.

Wenn die Abbildungen f_{i-1} und f_i ganz konkret vorliegen, so genügt es, die Komposition zu berechnen und mit der Nullabbildung zu vergleichen.

Eine Sequenz $S = (f_i : V_i \to V_{i+1})_{i\in\mathbb{Z}}$ mit der Eigenschaft $f_i \circ f_{i-1} = 0$ für alle $i \in \mathbb{Z}$ heißt **Kettenkomplex** oder kurz **Komplex**.

In der Linearen Algebra sind Komplexe anfangs noch selten, daher will und werde ich hier nicht genauer darauf eingehen.

Exakte Sequenzen hingegen treten sehr früh und prominent auf, deshalb möchte ich Ihnen diese hilfreiche Sichtweise nahebringen.

Muss das gleich so früh am Anfang geschehen? Ich denke ja! Auch in der Mathematik sieht man nämlich nur, was man weiß.

Man erblickt nur, was man schon weiß und versteht.
Johann Wolfgang von Goethe (1749–1832)

Exakte Sequenzen und Komplexe

Exkurs: Komplexe spielen eine wichtige Rolle in der homologischen Algebra und der algebraischen Topologie und verwandten Gebieten.

Die Vektoranalysis zum Beispiel untersucht glatte Funktionen $f : \Omega \to \mathbb{R}$ und Vektorfelder $g : \Omega \to \mathbb{R}^3$ auf einem Gebiet $\Omega \subseteq \mathbb{R}^3$. Gradient, Rotation und Divergenz bilden darauf einen Komplex:

$$C^\infty(\Omega, \mathbb{R}) \xrightarrow{\text{grad}} C^\infty(\Omega, \mathbb{R}^3) \xrightarrow{\text{rot}} C^\infty(\Omega, \mathbb{R}^3) \xrightarrow{\text{div}} C^\infty(\Omega, \mathbb{R})$$

Ausgeschrieben bedeutet das $\operatorname{rot} \circ \operatorname{grad} = 0$ und $\operatorname{div} \circ \operatorname{rot} = 0$. Diese wunderbaren Rechentechniken lernen Sie in der Analysis und ebenso in der Höheren Mathematik im zweiten und dritten Semester.

Für $\Omega = \mathbb{R}^3$ oder einen Quader $\Omega =]a_1, b_1[\times]a_2, b_2[\times]a_3, b_3[$ ist diese Sequenz tatsächlich exakt. Interessanterweise gilt Exaktheit nicht mehr, wenn das Gebiet Ω Löcher hat.

In diesem Sinne misst der obige Komplex die Löcher des Gebiets Ω. Diese Beobachtung ist der Ausgangspunkt der algebraischen Topologie.

Exakte Sequenzen und Komplexe

Nach diesem Exkurs zu Komplexen komme ich auf Exaktheit zurück, die uns in zahlreichen konkreten Rechnungen noch beschäftigen wird.

Bemerkung: Die Bedingung $\operatorname{im}(f_{i-1}) \subseteq \ker(f_i)$ ist meist leicht; wie oben erklärt genügt es, die Gleichung $f_i \circ f_{i-1} = 0$ zu prüfen.

Die Umkehrung $\operatorname{im}(f_{i-1}) \supseteq \ker(f_i)$ ist naturgemäß schwieriger: Hierzu müssen wir typischerweise den gesamten Kern bestimmen.

In den meisten Beweisen zur Exaktheit wird $\operatorname{im}(f_{i-1}) \subseteq \ker(f_i)$ leicht und routiniert ablaufen, während $\operatorname{im}(f_{i-1}) \supseteq \ker(f_i)$ aufwändiger ist.

Beispiel: Einen ersten (wenn auch noch allzu schwachen) Eindruck vermittelt der folgende Satz und sein Beweis zu direkten Summen.

Beispiel: Eine perfekte Illustration zeigt der Beweis von Lemma I2G zur Exaktheit von $K \to \mathbb{R}^{(I)} \to T \to 0$ für $\Phi : \mathbb{R}^{(I)} \to T : c \mapsto \sum_{Q\in I} c_Q \, \mathbf{I}_Q$.

Die Inklusion $K \subseteq \ker(\Phi)$ ist offensichtlich. Zur Umkehrung $K \supseteq \ker(\Phi)$ konstruieren wir $\bar{\Psi} : T \to \mathbb{R}^{(I)}/K$; das ist schon deutlich raffinierter!

Direkte Summen, extern und intern

Sind $V_1, \dots, V_n$ lineare Räume, so auch ihre **externe direkte Summe**

$$V_1 \times \cdots \times V_n = \{\, (v_1, \dots, v_n) \mid v_1 \in V_1, \dots, v_n \in V_n \,\}.$$

Wie üblich nutzen wir die koordinatenweise Addition und Skalierung.

Satz I2I: interne Summe

Sind $V_1, V_2 \leq W$ lineare Unterräume, so auch $U := V_1 \cap V_2 \leq W$ und $V = V_1 + V_2 \leq W$. Diese fügen sich zur kurzen exakten Sequenz

$$0 \xrightarrow{0} U \xrightarrow[u \mapsto (-u,u)]{f} V_1 \times V_2 \xrightarrow[(v_1,v_2) \mapsto v_1+v_2]{g} V_1 + V_2 \xrightarrow{0} 0.$$

Wichtiger Spezialfall: Gilt $U = \{0\}$, so erhalten wir den Isomorphismus

$$g : V_1 \times V_2 \xrightarrow{\sim} V_1 + V_2 : (v_1, v_2) \mapsto v_1 + v_2.$$

Beweis: Die Abbildungen f und g sind linear, f ist injektiv, g ist surjektiv. Es gilt $g \circ f = 0$, also $\operatorname{im}(f) \subseteq \ker(g)$. Umgekehrt gilt $\operatorname{im}(f) \supseteq \ker(g)$, denn $(v_1, v_2) \in \ker(g)$ bedeutet $v_1 = -v_2 \in V_1 \cap V_2 = U$. QED

Direkte Summen, extern und intern

Das ist ein schönes Beispiel für die ordnende Kraft exakter Sequenzen: Wir können alle relevanten Informationen in einer Zeile bündeln!

🙂 Im wichtigen Spezialfall $V_1 \cap V_2 = \{0\}$ ist g ein Isomorphismus. In Worten bedeutet das: Jeder Vektor $v \in V$ zerlegt sich eindeutig als Summe $v = v_1 + v_2$ mit Komponenten $v_1 \in V_1$ und $v_2 \in V_2$.

Die Summe $V = V_1 + V_2$ nennen wir dann eine **direkte Summe** und schreiben $V = V_1 \oplus V_2$. Wir nennen V_2 ein **direktes Komplement** zu V_1, und umgekehrt. Eine solche Zerlegung ist eine besondere Eigenschaft!

⚠ Nicht jeder Unterraum $V_1 \leq V$ erlaubt ein direktes Komplement V_2.

Beispiel: Im $\mathbb{Z}$–linearen Raum $V = \mathbb{Z}$ ist $V_1 = 2\mathbb{Z}$ ein Unterraum. Es gilt $\mathbb{Z} = 2\mathbb{Z} + \{0, 1\}$, aber es gibt keinen Unterraum $V_2 \leq \mathbb{Z}$ mit $V = V_1 \oplus V_2$.

Beweis: Jeder $\mathbb{Z}$–lineare Unterraum $V_2 \leq \mathbb{Z}$ ist von der Form $V_2 = n\mathbb{Z}$ (G1V). Für $n = 0$ ist $2\mathbb{Z} + 0\mathbb{Z} = 2\mathbb{Z} \neq \mathbb{Z}$. Für $n \geq 1$ ist $2\mathbb{Z} \cap n\mathbb{Z} \neq \{0\}$.

Allgemein ist die interne direkte Summe $V = V_1 \oplus \cdots \oplus V_n$ in W die gewöhnliche Summe $V = V_1 + \cdots + V_n$ mit der zusätzlichen Eigenschaft, dass $V_i \cap \left(\sum_{j \neq i} V_j\right) = \{0\}$ für alle $i = 1, \dots, n$ gilt.

Direkte Summen, extern und intern

Definition I2J: interne direkte Summe

Seien $V_1, \dots, V_n \leq W$ lineare Unterräume mit der Eigenschaft

$$(\star) \qquad V_i \cap \left(\textstyle\sum_{j \neq i} V_j\right) = \{0\} \quad \text{für alle } i = 1, \dots, n.$$

Dann nennen wir $V = V_1 + \cdots + V_n \leq W$ eine **interne direkte Summe**:

$$V = V_1 \oplus \cdots \oplus V_n := V_1 + \cdots + V_n \leq W \qquad \text{mit } (\star)$$

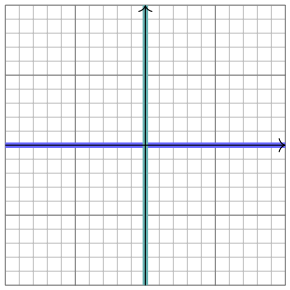
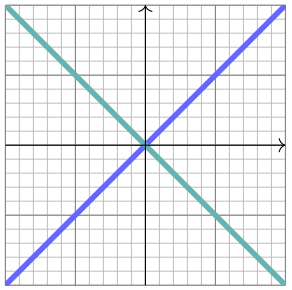
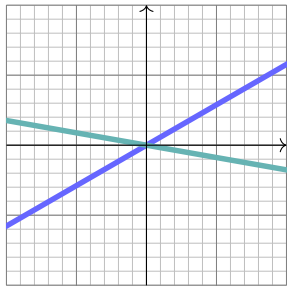
Diese ist isomorph zur **externen direkten Summe** vermöge

$$g : V_1 \times \cdots \times V_n \xrightarrow{\sim} V_1 \oplus \cdots \oplus V_n : (v_1, \dots, v_n) \mapsto v_1 + \cdots + v_n.$$

In Worten bedeutet das: Jeder Vektor $v \in V$ zerlegt sich eindeutig als Summe $v = v_1 + \cdots + v_n$ mit Komponenten $v_1 \in V_1, \dots, v_n \in V_n$.

Beweis: Die Abbildung g ist linear und surjektiv, nach Definition von V. Für $(v_1, \dots, v_n) \in \ker(g)$ gilt $v_i = -(\sum_{j \neq i} v_j) \in V_i \cap \left(\sum_{j \neq i} V_j\right) = \{0\}$, also $v_i = 0$ für alle $i = 1, \dots, n$. Das zeigt $\ker(g) = \{0\}$. QED

Direkte Summen, extern und intern

Beispiele: Die folgenden internen Summen sind direkt:

1. $\mathbb{R}^2 = A_1 \oplus A_2$ mit $A_1 = (1, 0) \cdot \mathbb{R}$ und $A_2 = (0, 1) \cdot \mathbb{R}$,
2. $\mathbb{R}^2 = D_1 \oplus D_2$ mit $D_1 = (1, 1) \cdot \mathbb{R}$ und $D_2 = (1, -1) \cdot \mathbb{R}$,
3. $\mathbb{C} = \mathbb{R} \oplus \mathrm{i}\mathbb{R}$, allgemein $\mathbb{C} = \mathrm{e}^{\mathrm{i}\alpha}\mathbb{R} \oplus \mathrm{e}^{\mathrm{i}\beta}\mathbb{R}$ mit $0 \leq \alpha < \beta < \pi$,
4. $\mathbb{R}^n = e_1\mathbb{R} \oplus \cdots \oplus e_n\mathbb{R} = \langle\, e_1, \dots, e_k \,\rangle \oplus \langle\, e_{k+1}, \dots, e_n \,\rangle$,
5. $\mathbb{R}[X] = \mathbb{R} \oplus X \cdot \mathbb{R}[X] = \mathbb{R} \oplus \{\, F \in \mathbb{R}[X] \mid F(a) = 0 \,\}$ mit $a \in \mathbb{R}$,
6. $\mathbb{R}[X] = \mathbb{R}[X^2] \oplus X \cdot \mathbb{R}[X^2]$, gerade plus ungerade (Beispiel I2M).

Projektion auf direkte Summanden

Satz I2K: Projektion auf direkte Summanden

(1) Gegeben sei eine (interne) direkte Summe $V = V_1 \oplus \cdots \oplus V_n$.
Wir definieren den **Projektor** $p_i : V \to V : \sum_j v_j \mapsto v_i$ für $v_j \in V_j$.
Die Abbildungen $p_1, \ldots, p_n$ sind linear mit der Eigenschaft

$$(\star) \qquad p_1 + \cdots + p_n = \mathrm{id}_V \quad \text{und} \quad p_i \circ p_j = 0 \quad \text{für } i \neq j$$

sowie $p_i^2 = p_i$ mit Bild $\mathrm{im}(p_i) = V_i$ und Kern $\ker(p_i) = \bigoplus_{j \neq i} V_j$.

Hierzu gilt die folgende Umkehrung:
(2) Gegeben seien lineare Abbildungen $p_1, \ldots, p_n : V \to V$ mit $(\star)$.
Dann folgt Idempotenz $p_i^2 = p_i$ für alle i, und für $V_i = \mathrm{im}(p_i) \leq V$ gilt

$$V = V_1 \oplus \cdots \oplus V_n.$$

☺ In diesem Sinne ist jede Summenzerlegung $V = V_1 \oplus \cdots \oplus V_n$ äquivalent zu Projektoren $p_1, \ldots, p_n : V \to V$ mit der Eigenschaft $(\star)$.
Wir rechnen hier im Endomorphismenring $\mathrm{End}_R(V)$, siehe Satz I1J.

Projektion auf direkte Summanden

Beweis: Aussage (1) ist klar nach Konstruktion: Nachrechnen!

(2a) Für jeden Index $i = 1, \ldots, n$ gilt $p_i^2 = p_i$, denn

$$\begin{aligned} p_i &\overset{\text{Ntr}}{=} p_i \circ \mathrm{id}_V \overset{(\star)}{=} p_i \circ (p_1 + \cdots + p_n) \\ &\overset{\text{Dist}}{=} p_i \circ p_1 + \cdots + p_i \circ p_n \overset{(\star)}{=} p_i^2. \end{aligned}$$

(2b) Wir zeigen $V = V_1 + \cdots + V_n$: Die Inklusion „$\supseteq$“ ist klar.
Zur Inklusion „$\subseteq$“ sei $x \in V$. Für $x_i := p_i(x) \in p_i(V) = V_i$ gilt

$$\begin{aligned} x_1 + \cdots + x_n &\overset{\text{Def}}{=} p_1(x) + \cdots + p_n(x) \\ &\overset{\text{Def}}{=} (p_1 + \cdots + p_n)(x) \overset{(\star)}{=} \mathrm{id}_V(x) = x. \end{aligned}$$

(2c) Wir zeigen $V_i \cap (\sum_{j \neq i} V_j) = \{0\}$: Sei $x \in V_i \cap (\sum_{j \neq i} V_j)$.
Zu $x \in V_i = p_i(V)$ existiert $v \in V$ mit $x = p_i(v) = p_i^2(v) = p_i(x)$.
Aus $x \in \sum_{j \neq i} p_j(V)$ folgt durch Anwendung von p_i:

$$x = p_i(x) \in p_i(\textstyle\sum_{j \neq i} p_j(V)) = \sum_{j \neq i} p_i p_j(V) \overset{(\star)}{=} \{0\}$$

Die Aussagen (2b) und (2c) beweisen $V = V_1 \oplus \cdots \oplus V_n$. QED

Projektion auf direkte Summanden

Korollar I2L: Projektor und Idempotenz

(1) Gegeben sei eine (interne) direkte Summe $V = V_1 \oplus V_2$.
Wir definieren den **Projektor auf V_1 parallel zu V_2** durch

$$p : V \to V : v_1 + v_2 \mapsto v_1 \quad \text{für } v_1 \in V_1 \text{ und } v_2 \in V_2.$$

Diese Abbildung ist wohldefiniert, linear, idempotent gemäß $p^2 = p$, mit dem Bild $\mathrm{im}(p) = V_1$ und dem Kern $\ker(p) = V_2$.

(2) Sei $p : V \to V$ eine lineare Abbildung und idempotent, also $p^2 = p$.
Das zugehörige Paar $p_1 = p$ und $p_2 = \mathrm{id}_V - p$ erfüllt $p_1 + p_2 = \mathrm{id}_V$ und $p_1 \circ p_2 = p_2 \circ p_1 = 0$, und induziert somit die Zerlegung

$$V = \mathrm{im}(p) \oplus \ker(p).$$

Beispiel: Zu $a \in \mathbb{R}$ sei $p = p_a : \mathbb{R}[X] \to \mathbb{R}[X] : F \mapsto F(a)$. Wir erhalten:

$$\mathbb{R}[X] = \mathrm{im}(p) \oplus \ker(p) = \mathbb{R} \oplus \{\, F \in \mathbb{R}[X] \mid F(a) = 0 \,\}$$

Für jede Wahl $a \in \mathbb{R}$ erhalten wir einen anderen Summanden $\ker(p_a)$.

Projektion auf direkte Summanden

Beispiel I2M: Zerlegung in gerade und ungerade

Jede Funktion $f : \mathbb{R} \to \mathbb{R}$ schreibt sich eindeutig als Summe $f = g + u$ einer geraden Funktion $g : \mathbb{R} \to \mathbb{R}$, $g(-x) = g(x)$, und einer ungeraden Funktion $u : \mathbb{R} \to \mathbb{R}$, $u(-x) = -u(x)$. Genauer gilt hier:

$$\mathrm{Abb}(\mathbb{R}, \mathbb{R}) = \mathrm{Abb}(\mathbb{R}, \mathbb{R})^+ \oplus \mathrm{Abb}(\mathbb{R}, \mathbb{R})^-$$

Diese Zerlegung folgt aus den $\mathbb{R}$–linearen Projektoren

$$p_1 = p_+ : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}^{\mathbb{R}} : f \mapsto g \quad \text{mit} \quad g(x) = \frac{1}{2}\big[f(x) + f(-x)\big],$$

$$p_2 = p_- : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}^{\mathbb{R}} : f \mapsto u \quad \text{mit} \quad u(x) = \frac{1}{2}\big[f(x) - f(-x)\big].$$

Sie erfüllen $p_1 + p_2 = \mathrm{id}_{\mathbb{R}^{\mathbb{R}}}$ sowie $p_1 \circ p_2 = p_2 \circ p_1 = 0$,
wir können also den vorigen Satz I2K anwenden.

Dieselbe Zerlegung gilt ebenso in $\mathscr{C}^n(\mathbb{R}, \mathbb{R})$ und $\mathrm{Poly}(\mathbb{R}, \mathbb{R})$.
Angewendet auf $\mathbb{R}[X]$ erhalten wir $\mathbb{R}[X] = \mathbb{R}[X^2] \oplus X \cdot \mathbb{R}[X^2]$.

Produkte und Summen: allgemeine Konstruktion

Wir möchten nicht nur endliche direkte Summen nutzen wie

$$\mathbb{R}^n = \bigoplus_{i=1}^{n} \mathbb{R}e_i = \mathbb{R}e_1 \oplus \cdots \oplus \mathbb{R}e_n,$$

sondern auch unendliche direkte Summen wie

$$\mathbb{R}[X] = \bigoplus_{n\in\mathbb{N}} \mathbb{R}X^n = \mathbb{R} \oplus \mathbb{R}X \oplus \mathbb{R}X^2 \oplus \ldots.$$

Das gelingt uns im Prinzip ganz genauso wie im endlichen Fall, aber es gibt einige technische Details, die wir klären müssen.

🙂 Wer sich vor allgemeinen Überlegungen gruselt, kann die folgende Ergänzung getrost ignorieren – und bei Bedarf darauf zurückkommen.

🙂 Wer sich vor unendlichen Indexmengen wie $\mathbb{N}$ nicht fürchtet, den wird die folgende Ergänzung beruhigen, oder gar erfreuen, denn alles verläuft wie im endlichen Fall – mit der nötigen Umsicht.

🙂 Ich denke, man versteht den endlichen Fall dadurch sogar besser: Der allgemeine Kontext erklärt, was „eigentlich“ passiert und macht alle „zufälligen“ Besonderheiten des endlichen Falls klar und verständlich.

Kartesische Produkte: allgemeine Konstruktion

Definition I2N: Produktraum, allgemein

Sei R ein Ring, etwa $\mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \ldots$, und I eine Menge.
Zu jedem Index $i \in I$ sei ein R–linearer Raum V_i gegeben.

Der **Produktraum** der Familie $(V_i)_{i\in I}$ ist das kartesisches Produkt

$$P = \prod_{i\in I} V_i := \{\, u = (u_i)_{i\in I} \mid \forall i \in I : u_i \in V_i \,\}$$

mit koordinatenweiser Addition und Skalarmultiplikation. Damit ist P ein R–linearer Raum. Hierzu gehören die **kanonischen Projektionen**

$$p_i = \mathrm{pr}_i : P \to V_i : u \mapsto u_i.$$

Nach Konstruktion sind dies R–lineare Abbildungen.

Wir nutzen kartesische Produkte wie in D3E erklärt. Alle Konstruktionen, die wir dort für Produkte und Summen von Mengen ausgeführt haben, übertragen wir nun auf Produkte und Summen von linearen Räumen.

Kartesische Produkte: allgemeine Konstruktion

Beispiel: Speziell für $I = \{1, \ldots, n\}$ erhalten wir wie zuvor

$$\prod_{i\in I} V_i = V_1 \times \cdots \times V_n = \{\, u = (u_1, \ldots, u_n) \mid u_1 \in V_1, \ldots, u_n \in V_n \,\}.$$

Beispiel: Das abzählbare Produkt $\prod_{n\in\mathbb{N}} V_n$ besteht aus allen Folgen

$$u = (u_0, u_1, u_2, \ldots) \quad \text{mit } u_n \in V_n \text{ für alle } n \in \mathbb{N}.$$

Beispiel: Gilt $V_i = R$ für alle $i \in I$, so finden wir das vertraute Beispiel

$$\prod_{i\in I} R = R^I = \{\, u : I \to R \,\}.$$

Beispiel: Gilt $V_i = V$ für alle $i \in I$, so finden wir entsprechend

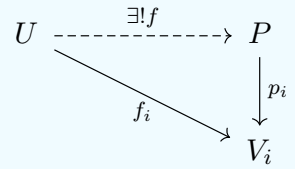
$$\prod_{i\in I} V = V^I = \{\, u : I \to V \,\}.$$

All diese Mengen versehen wir jeweils mit koordinatenweiser Addition und Skalierung; erst dadurch werden sie zu R–linearen Räumen.

Kartesische Produkte: universelle Eigenschaft

Satz I2O: universelle Abbildungseigenschaft (UAE)

Sei $P = \prod_{i\in I} V_i$ der Produktraum der Familie $(V_i)_{i\in I}$.



Zu jeder Familie $(f_i : U \to V_i)_{i\in I}$ von R–linearen Abbildungen existiert genau eine R–lineare Abbildung $f : U \to P$ mit $p_i \circ f = f_i$ für alle $i \in I$, also $f(u) = (f_i(u))_{i\in I}$. Wir haben somit die kanonische Bijektion

$$\Phi : \mathrm{Hom}_R\Big(U, \prod_{i\in I} V_i\Big) \xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_R(U, V_i) : f \mapsto (p_i \circ f)_{i\in I}.$$

Wir schreiben $f = \prod_{i\in I} f_i := \Phi^{-1}((f_i)_{i\in I})$, kurz $f = (f_i : U \to V_i)_{i\in I}$: Die Funktion f besteht aus ihren Koordinatenfunktionen f_i für $i \in I$.

Beweis: Dies folgt aus der Definition I2N des Produkts. QED

Definition I2P: Summenraum, allgemein

Sei R ein Ring, etwa $\mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \ldots$, und I eine Menge.
Zu jedem Index $i \in I$ sei ein R–linearer Raum V_i gegeben.

Der **Summenraum** der Familie $(V_i)_{i\in I}$ ist

$$S = \bigoplus\nolimits_{i\in I} V_i := \left\{ x \in \prod\nolimits_{i\in I} V_i \;\middle|\; \sharp\,\mathrm{supp}(x) < \infty \right\}$$

mit koordinatenweiser Addition und Skalarmultiplikation. Damit ist $S \leq P$ ein R–linearer Raum. Hierzu gehören die **kanonischen Injektionen**

$$\iota_i : V_i \hookrightarrow S : u_i \mapsto u \quad \text{mit } u_j = 0 \text{ für alle } j \neq i.$$

Nach Konstruktion sind dies R–lineare Abbildungen.

Bemerkung: Ist die Indexmenge I endlich, so gilt $\bigoplus_{i\in I} V_i = \prod_{i\in I} V_i$.
Ist die Indexmenge hingegen unendlich, so gilt hier $\bigoplus_{i\in I} V_i < \prod_{i\in I} V_i$.

Beispiel: Speziell für $I = \{1, \ldots, n\}$ erhalten wir wie zuvor

$$\bigoplus\nolimits_{i\in I} V_i = V_1 \oplus \cdots \oplus V_n = \{\, u = (u_1, \ldots, u_n) \mid u_1 \in V_1, \ldots, u_n \in V_n \,\}.$$

Beispiel: Die abzählbare Summe $\prod_{n\in\mathbb{N}} V_n$ besteht aus allen Folgen

$$u = (u_0, u_1, u_2, \ldots) \quad \text{mit } u_n \in V_n \text{ für alle } n \in \mathbb{N}$$

und endlichem Träger: Es existiert ein $m \in \mathbb{N}$ mit $u_n = 0$ für alle $n > m$.

Beispiel: Gilt $V_i = R$ für alle $i \in I$, so finden wir das vertraute Beispiel

$$\bigoplus\nolimits_{i\in I} R \;=\; R^{(I)} = \left\{\, u : I \to R \;\middle|\; \sharp\,\mathrm{supp}(u) < \infty \,\right\} \leq R^I.$$

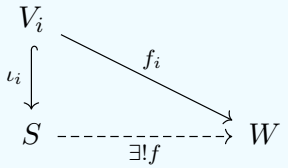
Beispiel: Gilt $V_i = V$ für alle $i \in I$, so finden wir entsprechend

$$\bigoplus\nolimits_{i\in I} V \;=\; V^{(I)} = \left\{\, u : I \to V \;\middle|\; \sharp\,\mathrm{supp}(u) < \infty \,\right\} \leq V^I.$$

All diese Mengen versehen wir jeweils mit koordinatenweiser Addition und Skalierung; erst dadurch werden sie zu R–linearen Räumen.

Satz I2Q: universelle Abbildungseigenschaft (UAE)

Sei $S = \bigoplus_{i\in I} V_i$ die externe direkte Summe der Familie $(V_i)_{i\in I}$.



Zu jeder Familie $(f_i : V_i \to W)_{i\in I}$ von R–linearen Abbildungen existiert genau eine R–lineare Abbildung $f : S \to W$ mit $f \circ \iota_i = f_i$ für alle $i \in I$, also $f(u) = \sum_{i\in I} f_i(u_i)$. Wir haben somit die kanonische Bijektion

$$\Phi : \mathrm{Hom}_R\Big(\bigoplus\nolimits_{i\in I} V_i, W\Big) \to \prod\nolimits_{i\in I} \mathrm{Hom}_R(V_i, W) : f \mapsto (f \circ \iota_i)_{\lambda\in I}.$$

Wir schreiben hierfür kurz $f = \bigoplus_{i\in I} f_i := \Phi^{-1}((f_i)_{i\in I})$.

Beweis: Dies folgt aus der Definition I2P der Summe. QED

🙂 Eigenschaften I2O und I2Q sind dual: Alle Pfeile werden umgedreht.

Beispiel: Wir betrachten $V_i = R$ für alle $i \in I$, also

$$\bigoplus\nolimits_{i\in I} R \;=\; R^{(I)} = \left\{\, u : I \to R \;\middle|\; \sharp\,\mathrm{supp}(u) < \infty \,\right\} \leq R^I$$

Gegeben sei ein R–linearer Raum W und $w_i \in W$ für jedes $i \in I$.
Dazu haben wir die R–lineare Abbildung $f_i : V_i \to W : \lambda_i \mapsto w_i\lambda_i$.
Dank Satz I2Q erhalten wir die vertraute R–lineare Abbildung

$$f = \bigoplus\nolimits_{i\in I} f_i : R^{(I)} \to W : \lambda \mapsto \sum\nolimits_{i\in I} w_i\lambda_i.$$

Diese Abbildung ist wohldefiniert, denn die Summe ist endlich, genauer gesagt: nur endlich viele Summanden sind ungleich Null.

Bemerkung: Der Produktraum $P = \prod_{i\in I} V_i$ hat seine kanonischen Projektionen $p_i : P \twoheadrightarrow V_i$. Der Summenraum $S = \sum_{i\in I} V_i$ hat seine kanonischen Injektion $\iota_i : V_i \hookrightarrow S$. Für diese gilt jeweils die universelle Abbildungseigenschaft I2O bzw. I2Q. Auch der Summenraum S erlaubt Projektionen, als Einschränkung $p_i|_S : S \hookrightarrow P \twoheadrightarrow V_i$. Der Produktraum P erlaubt ebenfalls Injektionen, durch die Inklusion $\mathrm{inc} \circ \iota_i : V_i \hookrightarrow S \hookrightarrow P$. Diese Abbildungen erfüllen jedoch keine besonderen Eigenschaften.

Definition I2R: interne direkte Summe

Zu jedem $i \in I$ sei $V_i \leq W$ ein R–linearer Unterraum. Dabei gelte

$$V_i \cap \left(\sum_{j \neq i} V_j\right) = \{0\} \quad \text{für alle } i \in I.$$

Dann nennen wir ihre Summe in W eine **interne direkte Summe**:

$$V = \bigoplus\nolimits_{i\in I}^{\text{int}} V_i := \sum_{i\in I} V_i \leq W$$

Diese ist isomorph zur **externen direkten Summe** vermöge

$$g : \bigoplus\nolimits_{i\in I}^{\text{ext}} V_i \xrightarrow{\sim} \bigoplus\nolimits_{i\in I}^{\text{int}} V_i : (v_i)_{i\in I} \mapsto \sum_{i\in I} v_i.$$

In Worten bedeutet das: Jeder Vektor $v \in V$ zerlegt sich eindeutig als Summe $v = \sum_{i\in I} v_i$ mit Komponenten $v_i \in V_i$ für jedes $i \in I$.

Beweis: Die Abbildung g ist linear und surjektiv, nach Definition von V. Für $(v_i)_{i\in I} \in \ker(g)$ gilt $v_i = -(\sum_{j\neq i} v_j) \in V_i \cap \left(\sum_{j\neq i} V_j\right) = \{0\}$, also $v_i = 0$ für alle $i \in I$. Das zeigt $\ker(g) = \{0\}$. QED

Bemerkung: Es ist etwas unglücklich, das die externe und die interne direkte Summe beide mit demselben Symbol $\bigoplus$ bezeichnet werden.

Andererseits besteht ein kanonischer Isomorphismus, wie oben erklärt:

$$g : \bigoplus\nolimits_{i\in I}^{\text{ext}} V_i \xrightarrow{\sim} \bigoplus\nolimits_{i\in I}^{\text{int}} V_i : (v_i)_{i\in I} \mapsto \sum_{i\in I} v_i.$$

Zur Klarheit und Betonung habe ich hier „ext“ und „int“ hinzugefügt. In der Praxis lässt man diese durchaus hilfreichen Bezeichnungen meist weg und stellt (hoffentlich) durch den Kontext klar, was gemeint ist.

Im endlichen Falle (Satz I2J) habe ich dieses Problem der Notation gemildert, indem ich $V_1 \times \cdots \times V_n$ für die externe direkte Summe schreibe und $V_1 \oplus \cdots \oplus V_n$ für die interne direkte Summe in W.

Im unendlichen Falle steht dieser Trick nicht zur Verfügung, da wir nicht das Produkt $P = \prod_{i\in I} V_i$ benötigen, sondern die Summe $S = \bigoplus_{i\in I}^{\text{ext}} V_i$, und diese ist ein strikt kleinerer Teilraum $S < P$, wie oben erklärt.

Beispiel: Für den Polynomring über $\mathbb{R}$ gilt

$$\mathbb{R}[X] \;=\; \bigoplus\nolimits_{n\in\mathbb{N}}^{\text{int}} \mathbb{R}X^n \;=\; \mathbb{R} \oplus \mathbb{R}X \oplus \mathbb{R}X^2 \oplus \ldots.$$

Jedes Polynom $P \in \mathbb{R}[X]$ schreibt sich eindeutig als eine Summe

$$P = \sum_{n\in\mathbb{N}} a_n X^n \quad \text{mit} \quad a \in \mathbb{R}^{(\mathbb{N})}.$$

Das war das motivierende Beispiel, das ich eingangs betont habe. Dies ist eine (abzählbar) unendliche direkte Summe von Teilräumen.

Beispiel: Mit den kanonischen Injektionen ι_i (I2P) gilt

$$\bigoplus\nolimits_{i\in I}^{\text{ext}} V_i \;=\; \bigoplus\nolimits_{i\in I}^{\text{int}} \iota_i(V_i) \;\leq\; \prod\nolimits_{i\in I} V_i$$

Hier gilt „<“, falls $V_i \neq \{0\}$ für unendlich viele Indizes $i \in I$ zutrifft, und „=“, falls $V_i \neq \{0\}$ nur für endlich viele Indizes $i \in I$ zutrifft. Eine typische Illustration hierfür ist $\mathbb{R}^{(\mathbb{N})} < \mathbb{R}^{\mathbb{N}}$.

Beispiel: Für $R^{(I)}$ wie in Beispiel I1Q gilt

$$R^{(I)} = \bigoplus\nolimits_{i\in I}^{\text{int}} Re_i \quad \text{bzw.} \quad R^{(I)} = \bigoplus\nolimits_{i\in I}^{\text{int}} e_i R.$$

Jedes Element $u \in R^{(I)}$ schreibt sich eindeutig als Summe $u = \sum_{i\in I} u_i e_i$ (linkslinear) bzw. $u = \sum_{i\in I} e_i u_i$ (rechtslinear).

Hierbei ist Re_i bzw. $e_i R$ das Bild der kanonischen Injektion $\iota_i : R \hookrightarrow R^{(I)}$. Auch dies ist eine (beliebig große) direkte Summe von Teilräumen.

Interne und externe direkte Summe

Aufgabe: Sei $I = A \sqcup B$ eine Zerlegung der Menge I.
Erinnerung: Das bedeutet $I = A \cup B$ und $A \cap B = \emptyset$.

(1) Beweisen Sie die (interne) direkte Summenzerlegung

$$R^{(I)} = \langle\, e_i \mid i \in A \,\rangle \oplus \langle\, e_i \mid i \in B \,\rangle.$$

(2) Konstruieren Sie explizit einen R–Isomorphismus

$$(\varphi, \psi) \,:\, R^{(I)} \cong R^{(A)} \times R^{(B)} \quad \text{bzw.} \quad (\varphi, \psi) \,:\, R^I \cong R^A \times R^B.$$

Allgemein sei $I = \bigsqcup_{\lambda\in\Lambda} A_\lambda$ eine Zerlegung der Menge I.
Das bedeutet $I = \bigcup_{\lambda\in\Lambda} A_\lambda$ und $A_\lambda \cap A_\mu = \emptyset$ für alle $\lambda \neq \mu$.

(3) Beweisen Sie die (interne) direkte Summenzerlegung

$$R^{(I)} = \bigoplus\nolimits^{\text{int}}_{\lambda\in\Lambda} \langle\, e_i \mid i \in A_\lambda \,\rangle.$$

(4) Konstruieren Sie explizit einen R–Isomorphismus

$$(\varphi, \psi) \,:\, R^{(I)} \cong \bigoplus\nolimits^{\text{ext}}_{\lambda\in\Lambda} R^{(A_\lambda)} \quad \text{bzw.} \quad (\varphi, \psi) \,:\, R^I \cong \prod\nolimits_{\lambda\in\Lambda} R^{A_\lambda}.$$

Interne und externe direkte Summe

Lösung: Wir betrachten hier $R^{(I)}$ als rechtslinearen Raum über R; der linkslineare Fall gelingt genauso. Jedes Element $u \in R^{(I)}$ schreibt sich eindeutig als Linearkombination $u = \sum_{i\in I} e_i u_i$, siehe I1Q.

(1a) Wir zeigen zunächst $R^{(I)} = \langle\, e_i \mid i \in A \,\rangle + \langle\, e_i \mid i \in B \,\rangle$.
Die Inklusion „$\supseteq$“ ist klar. Zur Inklusion „$\subseteq$“ sei $u \in R^{(I)}$. Dann gilt
$u = \sum_{i\in I} e_i u_i = \sum_{i\in A} e_i u_i + \sum_{i\in B} e_i u_i \in \langle\, e_i \mid i \in A \,\rangle + \langle\, e_i \mid i \in B \,\rangle$.

(1b) Wir zeigen anschließend $\langle\, e_i \mid i \in A \,\rangle \cap \langle\, e_i \mid i \in B \,\rangle = \{0\}$.
Die Inklusion „$\supseteq$“ ist klar. Zur Inklusion „$\subseteq$“ sei $u : I \to R : i \mapsto u_i$:
Für $u \in \langle\, e_i \mid i \in A \,\rangle$ gilt $\operatorname{supp}(u) \subseteq A$, also $u_i = 0$ für alle $i \in I \smallsetminus A = B$.
Für $u \in \langle\, e_i \mid i \in B \,\rangle$ gilt $\operatorname{supp}(u) \subseteq B$, also $u_i = 0$ für alle $i \in I \smallsetminus B = A$.
Für $u \in \langle\, e_i \mid i \in A \,\rangle \cap \langle\, e_i \mid i \in B \,\rangle$ gilt $u_i = 0$ für alle $i \in A \cup B = I$.
Das bedeutet $u = 0$.

(2) Es genügen $\varphi(u) = (u|_A, u|_B)$ und $\psi(u_A, u_B) = u_A \sqcup u_B$.
Diese beiden Abbildungen sind wohldefiniert und R–linear
und erfüllen $\psi \circ \varphi = \mathrm{id}$ und $\varphi \circ \psi = \mathrm{id}$.

Interne und externe direkte Summe

(3a) Wir zeigen zunächst $R^{(I)} = \sum_{\lambda\in\Lambda} \langle\, e_i \mid i \in A_\lambda \,\rangle$.
Die Inklusion „$\supseteq$“ ist klar. Zur Inklusion „$\subseteq$“ sei $u \in R^{(I)}$.
Dann gilt $u = \sum_{i\in I} e_i u_i = \sum_{\lambda\in\Lambda} \sum_{i\in A_\lambda} e_i u_i \in \sum_{\lambda\in\Lambda} \langle\, e_i \mid i \in A_\lambda \,\rangle$.

(3b) Wir zeigen anschließend

$$\langle\, e_i \mid i \in A_\lambda \,\rangle \cap \textstyle\sum_{\mu\neq\lambda} \langle\, e_i \mid i \in A_\mu \,\rangle = \{0\}.$$

Die Summe können wir zusammenfassen zu

$$\textstyle\sum_{\mu\neq\lambda} \langle\, e_i \mid i \in A_\mu \,\rangle = \langle\, e_i \mid i \in B_\lambda \,\rangle$$

mit $B_\lambda = \bigcup_{\mu\neq\lambda} A_\mu = I \smallsetminus A_\lambda$. Wir können daher (1b) anwenden.

(4) Es genügen $\varphi(u) = (u|_{A_\lambda})_{\lambda\in\Lambda}$ und $\psi((u_\lambda)_{\lambda\in\Lambda}) = \bigsqcup_{\lambda\in\Lambda} u_\lambda$
Diese beiden Abbildungen sind wohldefiniert und R–linear
und erfüllen $\psi \circ \varphi = \mathrm{id}$ und $\varphi \circ \psi = \mathrm{id}$.

Interne und externe direkte Summe

Und die Moral von der Geschicht? Wie bearbeiten wir Anwendungen, in denen endliche Summen und Linearkombinationen nicht genügen?

In der Linearen Algebra arbeiten wir ausschließlich mit endlichen Summen $\sum_{i\in I} v_i$ und endlichen Linearkombinationen $\sum_{i\in I} v_i \lambda_i$.
Oft ist die Indexmenge I zwar unendlich, doch wir stellen auch dann explizit sicher, dass nur endlich viele Summanden ungleich Null sind.

Die Analysis klärt den Begriff der Konvergenz und erntet als Lohn die bewundernswert starken Methoden der Grenzwerte und Reihen.
Beide Sichtweisen vereinen sich später in der Funktionalanalysis, wo Lineare Algebra und Analysis wunderbar zusammenarbeiten.

Die soliden Grundlagen der Linearen Algebra werden sich auch dort, wie überall, für Sie auszahlen.

Kapitel J

Basis und Dimension

Good general theory does not
search for the maximum generality,
but for the right generality.

Saunders Mac Lane (1909–2005)

Inhalt dieses Kapitels J

Motivation und Überblick

In diesem Kapitel erarbeiten wir die Begriffe **Basis** und **Dimension**. Diese schlagen die Brücke von der allgemeinen Theorie der linearen Räume zur Matrizenrechnung, insbesondere zum Gauß–Algorithmus über Divisionsringen (B2C) und seinen zahlreichen Anwendungen.

Damit verbinden wir beides: starke Theorie und effiziente Algorithmen! Das ist der Grund für den anhaltenden Erfolg der Linearen Algebra. Lineare Methoden sind ungemein praktisch und werden überall genutzt, innerhalb der Mathematik und in ihren zahlreichen Anwendungen.

Aller Voraussicht nach wird diese Kombination auch in den nächsten hundert Jahren weiter erfolgreich sein. Gerade aktuell aufstrebende Anwendungen wie Data Science und Quantum Computing benötigen diese Verbindung; aus abstrakter Theorie werden konkrete Methoden.

Motivation und Überblick

☺ Mathematische Abstraktion ist etwas Gutes, Sie sollten sie nicht fürchten, sondern nutzen lernen. Im Idealfall bedeutet sie nicht Anwendungsferne, sondern im Gegenteil vielseitige Anwendbarkeit. (Ich muss dies betonen, weil manchmal das Gegenteil behauptet wird.)

Natürlich sind wir mit unseren bescheidenen Grundlagen noch weit entfernt von hochfliegenden Anwendungen, doch wir bauen darauf zu. Der Weg ist zwar weit, doch wir gehen ihn unbeirrt Schritt um Schritt. Sie sind gerüstet, egal, welchen Abzweig Sie später einschlagen.

Lohnt sich die Sorgfalt und die Mühe der Grundlagen? Ich denke ja. Mathematische Erkenntnis und solide wissenschaftliche Arbeit haben einen extrem langen Nutzen. Die Investition lohnt sich!

Die Frage der Skalare: warum Divisionsringe?

Im letzten Kapitel haben wir die allgemeinen Begriffe zu linearen Räumen über einem Ring R erklärt. Nun wollen wir etwas spezifischer werden und tieferliegende Techniken erarbeiten. Dazu benötigen wir einen **Divisionsring**, und zwar an zwei ganz wesentlichen Stellen:

1. Der Gaußalgorithmus B2C über einem Divisionsring R.
2. Der Existenzsatz J2B für Basen über einem Divisionsring R.

Der allgemeine Kontext ist dennoch ein Vorteil: Sie verfügen über ein reichhaltiges Repertoire an illustrativen und relevanten Beispielen! Daran sehen wir insbesondere, was alles schiefgehen kann, und dass unsere Voraussetzungen tatsächlich benötigt werden.

🙂 Ein typisches Gegenbeispiel ist der Ring $\mathbb{Z}$ der ganzen Zahlen: Dieser ist natürlich überall wichtig, viele Anwendungen fragen nach ganzzahligen Lösungen. Doch $\mathbb{Z}$ ist leider kein Körper, und oft ist es heilsam, sich einfache Gegenbeispiele über $\mathbb{Z}$ vor Augen zu führen.

Die Frage der Skalare: lieber gleich Körper?

🙂 Wenn Sie möchten, können Sie sich in diesem gesamten Kapitel R als einen Divisionsring vorstellen, oder besser noch einen Körper. Die meisten Zahlenbeispiele, die ich hier zur Illustration vorstelle, sind ganz konventionell und arbeiten über den Körpern $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(Ich hatte hie und da auch nicht-kommutative Beispiele im Sinn, etwa Hamiltons Quaternionen, doch diese scheinen bei den Studierenden auf wenig Gegenliebe zu treffen. Es bleibt genug anderes Schönes.)

🙂 Viele Ergebnisse sind wörtlich genauso über jedem Ring gültig, daher gehe ich behutsam vor und sage jeweils dazu, was benötigt wird. Das entspricht einer gewissen Denkökonomie und Nachhaltigkeit: Wir nehmen nur so viel, wie wir wirklich brauchen.

Der einzige Nachteil ist, dass man sich die nötigen Voraussetzungen merken muss. Das gelingt am besten, indem Sie die Beweise kennen! Ich hoffe, der mögliche Nachteil wandelt sich so in einen Vorteil, da nun transparenter wird, was wie wo genutzt wird.

Notation der Skalare: links oder rechts?

Matrizen $A \in R^{m\times n}$ operieren von links auf Spaltenvektoren $R^{n\times 1} \cong R^n$. Skalare $\lambda \in R$ sollten dann von rechts operieren. Durch diese einfache Regel sortieren sich all unsere Formeln und Indexkonventionen von selbst, wie durch Zauberhand fügt sich alles an den rechten Platz.

Diese bessere Buchführung der Indizes halte ich für hilfreich.

Viele Lehrbücher zur Linearen Algebra arbeiten ausschließlich über Körpern. Im kommutativen Fall können wir die Skalare von der einen auf die andere Seite umschreiben, daher stehen dann Skalare meist ebenfalls links. Dagegen ist soweit rein gar nichts einzuwenden.

Die Indexkonventionen sehen dann jedoch recht unnatürlich aus!

Ich mache mir daher die Mühe, beide Sichtweisen zu erklären, sodass Sie für jede Situation die jeweils passende Notation anwenden können.

In diesem Kapitel bedeutet das: Matrizen links, Skalare rechts.

Das Kleingedruckte: der Kampf mit den Indizes

Matrizenrechnung ist nicht nur, aber auch, Buchhaltung der Indizes. Das erfordert anfangs etwas Gewöhnung, ist aber letztlich nur eine Frage der Sorgfalt. Wenn Sie anschließend programmieren wollen, und das wollen Sie, dann geht es gar nicht anders!

Ich formuliere daher die entscheidenden Algorithmen hier explizit aus, sodass sie im Idealfall sofort genutzt und implementiert werden können. Das ist für mich als Autor zwar etwas mühsam, aber es nützt Ihnen zur Klarheit und zur direkten Anwendbarkeit. Sie werden dies in den Übungen merken, wenn Sie selbst erste Rechnungen anstrengen.

Auf den ersten Blick mögen die so gewonnenen Formeln abschrecken, und manche wünschen sich Beispiele ohne theoretische Grundlagen, doch ich bin überzeugt, Sie benötigen *beides* zu Ihrem Lernerfolg. Vorlesung und Übungen ergänzen sich daher weiterhin ganz wesentlich. Lernen Sie beides zu schätzen und zu nutzen: Theorie und Praxis.

Basis, erzeugend und linear unabhängig

Definition J1A: Basis, erzeugend und linear unabhängig

Sei $(V, +, \cdot)$ ein (rechts)linearer Raum über dem Ring $(R, +, \cdot)$.
Gegeben sei eine Familie $\mathcal{B} = (b_i)_{i\in I}$ von Vektoren $b_i \in V$.
Diese Familie $\mathcal{B}$ definiert die R–lineare Abbildung

$$\Phi_{\mathcal{B}} \,:\, R^{(I)} \to V \,:\, \lambda = (\lambda_i)_{i\in I} \mapsto v = \textstyle\sum_{i\in I} b_i\lambda_i.$$

Wir nennen die Familie $\mathcal{B}$ ...

1. eine **Basis** des linearen Raums V über R, wenn $\Phi_{\mathcal{B}}$ bijektiv ist,
2. eine **erzeugende Familie** von V über R, wenn $\Phi_{\mathcal{B}}$ surjektiv ist,
3. und **linear unabhängig** in V über R, wenn $\Phi_{\mathcal{B}}$ injektiv ist.

Der R–lineare Raum V heißt **frei**, wenn eine Basis $\mathcal{B}$ in V existiert;
das Paar $(V, \mathcal{B})$ heißt dann ein **basierter linearer Raum** über R.

Wir schreiben die Skalare hier rechts, alles gilt sinngemäß ebenso links.
Über einem kommutativen Ring ist diese Unterscheidung unnötig.

Basis, erzeugend und linear unabhängig

Eine Familie $\mathcal{B} = (b_i)_{i\in I}$ in V ist eine Abbildung $\mathcal{B} : I \to V : i \mapsto b_i$.
Das bedeutet, jedem Index $i \in I$ wird ein Element $b_i \in V$ zugeordnet.

Im Falle $I = \{1, \dots, n\}$ schreiben wir dies auch bequem als Aufzählung

$$\mathcal{B} = (b_i)_{i=1}^{n} = (b_1, b_2, \dots, b_n).$$

Wir erlauben ebenso unendliche Indexmengen, etwa $I = \mathbb{N}$:

$$\mathcal{B} = (b_i)_{i\in\mathbb{N}} = (b_0, b_1, b_2, \dots).$$

In Definition J1A ist die Indexmenge I zunächst beliebig.
Auch $I = \emptyset$ ist erlaubt; hierbei ist $R^{\emptyset} = \{0\}$ der Nullraum.

Die Elementezahl $\sharp I$ nennen wir die **Länge** der Familie $\mathcal{B}$,
oder auch die **Mächtigkeit** oder **Kardinalität** von I bzw. $\mathcal{B}$.

⚠ Auch wenn die Indexmenge I unendlich ist, so sind doch unsere Linearkombinationen $\sum_{i\in I} b_i\lambda_i$ immer endlich. Dies stellen wir sicher, indem wir nur I–Tupel $\lambda \in R^{(I)}$ mit endlichem Träger zulassen (I1Q).

Erzeugende Familien von V

Das Bild von $\Phi_{\mathcal{B}}$ ist der von $\mathcal{B}$ in V **erzeugte Unterraum** (I1V):

$$\operatorname{im}(\Phi_{\mathcal{B}}) = \langle\, \mathcal{B} \,\rangle_R = \langle\, b_i \mid i \in I \,\rangle_R = \left\{ \textstyle\sum_{i\in I} b_i\lambda_i \;\middle|\; \lambda \in R^{(I)} \right\}$$

Jedes I–Tupel $\lambda \in R^{(I)}$ über R mit endlichem Träger (!) definiert die zugehörige **Linearkombination** $\Phi_{\mathcal{B}}(\lambda) = \sum_{i\in I} b_i\lambda_i$ der Familie $\mathcal{B}$ in V.

Äquivalent sind:

1. Die Familie $\mathcal{B}$ erzeugt den Raum V über R, kurz $\langle\, \mathcal{B} \,\rangle_R = V$.
2. Die Abbildung $\Phi_{\mathcal{B}}$ ist surjektiv: siehe Definition J1A(2).
3. Jeder Vektor $v \in V$ schreibt sich auf **mindestens** eine Weise als eine Linearkombination $v = \sum_{i\in I} b_i\lambda_i$ mit $\lambda \in R^{(I)}$.

Wir nennen $\mathcal{B}$ dann eine **erzeugende Familie** von V über R,
oder ein **R–Erzeugendensystem**, kurz **Erzeugendensystem**.

Erzeugende Familien von V

Die Menge aller Linearkombinationen von $\mathcal{B}$ in V über R
heißt auch das **Erzeugnis** oder der **Aufspann** von $\mathcal{B}$ über R.

Die Schreibweise $\langle\, \mathcal{B} \,\rangle_R$ betont den hier verwendeten Grundring R.
Wenn dieser aus dem Kontext klar ist, so schreiben wir auch kurz $\langle\, \mathcal{B} \,\rangle$.

Im Falle einer endlichen Familie $\mathcal{B} = (b_1, \dots, b_n)$ schreiben wir auch

$$\begin{aligned}\langle\, \mathcal{B} \,\rangle &= \langle\, v_i \mid i = 1, \dots, n \,\rangle = \langle\, b_1, \dots, b_n \,\rangle \\ &= \langle\, b_1, \dots, b_n \,\rangle_R = b_1R + \cdots + b_nR \leq V.\end{aligned}$$

Je nach Situation ist die eine oder die andere Schreibweise bequemer.
All diese Notationen beschreiben das Bild von $\Phi_{\mathcal{B}} : R^{(I)} \to V$.

Es erweist sich im Folgenden meist als besser, nicht nur die Bildmenge $\operatorname{im}(\Phi_{\mathcal{B}}) = \langle\, \mathcal{B} \,\rangle \subseteq V$ zu nutzen, sondern explizit auch die Abbildung $\Phi_{\mathcal{B}}$.

Linear unabhängige Familien in V

Der Kern der Abbildung $\Phi_{\mathcal{B}} : R^{(I)} \to V$ ist

$$\ker(\Phi_{\mathcal{B}}) = \{\, \lambda \in R^{(I)} \mid \textstyle\sum_{i\in I} b_i\lambda_i = 0 \,\}.$$

Jedes Element $\lambda \in \ker(\Phi_{\mathcal{B}})$ heißt eine **Relation** zwischen den Vektoren $(b_i)_{i\in I}$ in V, im Falle $\lambda \neq 0$ nennen wir dies eine **nicht-triviale Relation** und die Familie $\mathcal{B}$ ist **linear abhängig**. Äquivalent sind:

1. Die Familie $\mathcal{B}$ ist linear unabhängig in V über R.
2. Die Abbildung $\Phi_{\mathcal{B}}$ ist injektiv: siehe Definition J1A(3).
3. Jeder Vektor $v \in V$ schreibt sich auf **höchstens** eine Weise als eine R–Linearkombination $v = \sum_{i\in I} b_i\lambda_i$ mit $\lambda \in R^{(I)}$.
4. Es gilt $\ker(\Phi_{\mathcal{B}}) = \{0\}$: Der Kern von $\Phi_{\mathcal{B}}$ ist trivial, siehe I1R.
5. Der Nullvektor $0 \in V$ schreibt sich nur auf **genau** eine Weise als R–Linearkombination: Aus $\lambda \in R^{(I)}$ und $0 = \sum_{i\in I} b_i\lambda_i$ folgt $\lambda = 0$.

Wir nennen $\mathcal{B}$ dann eine **linear unabhängige Familie** in V über R, oder einfach **R–linear unabhängig**, kurz **linear unabhängig**.

Linear unabhängige Familien in V

Das unscheinbare Injektivitätskriterium (4) ist überaus praktisch und wird sich im Folgenden immer wieder als hilfreich erweisen.

Arbeitsersparnis: Für die Injektivität von $\Phi_{\mathcal{B}} : R^{(I)} \to V$ brauchen wir nur eine einzige Faser zu überprüfen, nämlich $\ker(\Phi_{\mathcal{B}}) = \Phi_{\mathcal{B}}^{-1}(\{0\})$.

🙂 Die explizite Umformulierung (5) ist daher meist ein effizienter Ansatz, um lineare Un/Abhängigkeit zu prüfen. Konkret heißt das:

Zum Nachweis der **linearen Abhängigkeit** genügt ein Gegenbeispiel, also eine nicht-triviale Relation $\lambda \in R^{(I)}$, das heißt $\lambda \neq 0$ mit

$$\textstyle\sum_{i\in I} b_i\lambda_i = 0.$$

Zum Nachweis der **linearen Unabhängigkeit** setzen wir umgekehrt die Gleichung $\sum_{i\in I} b_i\lambda_i = 0$ für $\lambda \in R^{(I)}$ an und müssen dann zeigen, dass $\lambda = 0$ die einzige Lösung ist.

⚠ Das klingt zunächst ganz einfach, und das ist es im Prinzip auch, doch diese Technik erfordert einige Übung und vor allem Sorgfalt!

Basen eines linearen Raumes V

Die Lineare Unabhängigkeit und die Erzeugung von V fassen wir zum Begriff der Basis zusammen, wie in Definition J1A vereinbart.

Äquivalent sind:

1. Die Familie $\mathcal{B}$ ist eine Basis des Raums V über R.
2. Die Abbildung $\Phi_{\mathcal{B}} : R^{(I)} \to V$ ist ein Isomorphismus.
3. Es gilt $\ker(\Phi_{\mathcal{B}}) = \{0\}$ und $\operatorname{im}(\Phi_{\mathcal{B}}) = V$.
4. Die Familie $\mathcal{B}$ ist linear unabhängig und erzeugt V über R. Wir schreiben hierfür abkürzend $V = \langle\, \mathcal{B} \,\rangle_R^!$.
5. Jeder Vektor $v \in V$ schreibt sich auf **genau** eine Weise als eine R–Linearkombination $v = \sum_{i\in I} b_i\lambda_i$ mit $\lambda \in R^{(I)}$.

Wir nennen $\Phi_{\mathcal{B}} : R^{(I)} \to V$ das **Koordinatensystem** von V zur Basis $\mathcal{B}$ und $\lambda = (\lambda_i)_{i\in I} = \Phi_{\mathcal{B}}^{-1}(v)$ den **Koordinatenvektor** von v bezüglich $\mathcal{B}$.

Basen eines linearen Raumes V

Zur Notation $V = \langle\, \mathcal{B} \,\rangle_R^!$ sagen wir, V wird **frei erzeugt** von $\mathcal{B}$ über R. Das beinhaltet zwei Aussagen: V wird von $\mathcal{B}$ erzeugt, also $V = \langle\, \mathcal{B} \,\rangle_R$, und $\mathcal{B}$ ist frei, also ohne Relationen, das heißt R–linear unabhängig. Das ist eine bequeme Formel für „$\mathcal{B}$ ist eine Basis von V über R“.

Jede Basis $\mathcal{B} = (b_i)_{i\in I}$ von V über R stiftet einen Isomorphismus

$$\Phi_{\mathcal{B}} \;:\; R^{(I)} \xrightarrow{\sim} V \;:\; \lambda = (\lambda_i)_{i\in I} \mapsto v = \textstyle\sum_{i\in I} b_i\lambda_i.$$

Wir erhalten eine Zerlegung von V als direkte Summe $V = \bigoplus_{i\in I} V_i$ der Teilräume $V_i = b_i R$ mit Isomorphismen $\varphi_i : R \xrightarrow{\sim} V_i : \lambda_i \mapsto b_i\lambda_i$.

Demnach gilt: Ein linearer Raum V über R ist genau dann frei, wenn V die direkte Summe isomorpher Kopien des Raums R ist.

Gilt nämlich umgekehrt $V = \bigoplus_{i\in I} V_i$ mit Isomorphismen $\varphi_i : R \xrightarrow{\sim} V_i$, so erhalten wir daraus die Basis $\mathcal{B} = (b_i)_{i\in I}$ mit $b_i = \varphi_i(1)$.

Erste Beispiele: $\{0\}$ und R über R

Beispiel: Der Nullraum $\{0\}$ ist frei über R mit leerer Basis $\mathcal{B} = ()$.
Ausführlich: Die Indexmenge $I = \emptyset$ ist hier die leere Menge.
Demnach gilt $R^{(\emptyset)} = R^{\emptyset} = \{0\}$ mit $0 : \emptyset \to \mathbb{Z}$, siehe D302.
Somit ist $\Phi_{\mathcal{B}} : R^{\emptyset} \to \{0\}$ tatsächlich ein Isomorphismus.
🙂 Auch dieser „triviale“ Sonderfall fügt sich nahtlos ein.

Beispiel: Der R–lineare Raum R ist frei, die Standardbasis ist 1.
Genau dann ist $b \in R$ eine R–Basis, wenn b in R invertierbar ist:

$$\Phi_b \,:\, R \xrightarrow{\sim} R \,:\, \lambda \mapsto b\lambda \text{ bijektiv} \quad\Longleftrightarrow\quad b \in R^\times \text{ invertierbar}$$

Beweis: Die Implikation „$\Leftarrow$“ ist klar dank $\Phi_b^{-1} = \Phi_{b^{-1}}$. Die Umkehrung „$\Rightarrow$“ ist noch interessanter: Da Φ_b surjektiv ist, existiert $c \in R$ mit $bc = 1$, also ist b rechtsinvertierbar durch c. Zudem ist Φ_b injektiv: Wir haben $b1 = b = 1b = (bc)b = b(cb)$, nach Kürzen also $1 = cb$. QED
🙂 Das entspricht Satz B2D, hier im Spezialfall von 1×1–Matrizen.
Die folgenden Beispiele illustrieren dies für die Ringe $\mathbb{Z}$ und $\mathbb{Z}/n$.

Erste Beispiele: $\mathbb{Z}$ und $\mathbb{Z}/n$ über $\mathbb{Z}$

Beispiel: Der $\mathbb{Z}$–lineare Raum $\mathbb{Z}$ ist frei; mögliche Basen sind 1 und -1.
Jedes $b \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ ist $\mathbb{Z}$–linear unabhängig, erzeugt aber nicht $\mathbb{Z}$.
Ausführlich: Hier ist $\Phi_b : \mathbb{Z} \xrightarrow{\sim} b\mathbb{Z} \lneq \mathbb{Z}$ injektiv, aber nicht surjektiv.

Beispiel: Der $\mathbb{Z}/n$–lineare Raum ist $\mathbb{Z}/n$ frei, die Standardbasis ist 1.
Weitere Basen sind $b \in (\mathbb{Z}/n)^\times = \{\, [a] \mid a \in \mathbb{Z} \wedge \operatorname{ggT}(a,n) = 1 \,\}$;
dies sind die invertierbaren Elemente des Rings $\mathbb{Z}/n$ (A2O).

Beispiel J1B: der Raum $\mathbb{Z}/n\mathbb{Z}$ ist nicht frei über $\mathbb{Z}$.

Der $\mathbb{Z}$–lineare Raum $\mathbb{Z}/n$ mit $n \in \mathbb{N}_{\geq 2}$ ist nicht frei über $\mathbb{Z}$.
Nur für $n \in \{0, 1\}$ sind $\mathbb{Z}/0 \cong \mathbb{Z}$ und $\mathbb{Z}/1 = \{0\}$ frei über $\mathbb{Z}$.

Beweis: Das folgt aus $\mathbb{Z}^{(I)} \ncong \mathbb{Z}/n$ für jede Menge I. Ausführlich:
Jede abelsche Gruppe V ist ein $\mathbb{Z}$–linearer Raum (I1K). Für $1 < \sharp V < \infty$ ist V nicht frei über $\mathbb{Z}$. Zum Beweis sei $\mathcal{B} = (b_i)_{i \in I}$ eine Familie in V.
Im Falle $I = \emptyset$ ist $\mathbb{Z}^{(I)} = \{0\}$ und $\Phi_{\mathcal{B}} : \mathbb{Z}^{(I)} \to V$ nicht surjektiv.
Im Falle $I \neq \emptyset$ ist $\mathbb{Z}^{(I)}$ unendlich, also $\Phi_{\mathcal{B}}$ nicht injektiv. QED

Erste Beispiele: der Koordinatenraum $R^{(I)}$ über R

Beispiel J1C: der Koordinatenraum $R^{(I)}$ über R

Sei R ein Ring und I eine Menge. Der **Koordinatenraum**

$$R^{(I)} = \left\{\, \lambda : I \to R \;\middle|\; \sharp\operatorname{supp}(\lambda) < \infty \,\right\} \leq R^I$$

ist frei bezüglich der **Standardbasis** $\mathcal{E} = (e_i)_{i \in I}$, wobei

$$e_i \,:\, I \to R \,:\, j \mapsto e_i(j) = \begin{cases} 1 & \text{falls } j = i, \\ 0 & \text{falls } j \neq i. \end{cases}$$

Jedes Element $\lambda \in R^{(I)}$ schreibt sich eindeutig als Linearkombination

$$\lambda = \sum_{i \in I} e_i \lambda_i.$$

Hier ist demnach $\Phi_{\mathcal{E}} = \mathrm{id} : R^{(I)} \xrightarrow{\sim} R^{(I)}$ die identische Abbildung.

Erste Beispiele: der Koordinatenraum $R^{(I)}$ über R

Beispiel: Für die Indexmenge $I = \{1, \ldots, m\} \times \{1, \ldots, n\}$ erhalten wir den R–linearen Raum $R^{m \times n}$ der $m \times n$–Matrizen mit der Standardbasis $\mathcal{E} = (E_{ij})_{ij}$. Die Matrix $E_{ij} \in R^{m \times n}$ hat an der Stelle (i, j) den Eintrag 1 und sonst überall 0. Wie gesehen: Diese Matrizen bilden eine Basis!

🙂 Dieser vertraute Koordinatenraum $R^{(I)}$ ist unser Modell, er dient uns als Standardraum. Hierin können wir besonders gut „in Koordinaten“ rechnen, hierzu haben wir insbesondere die Standardbasis $(e_i)_{i \in I}$.

Jede Familie $\mathcal{B} = (b_i)_{i \in I}$ in V definiert die R–lineare Abbildung

$$\Phi_{\mathcal{B}} \,:\, R^{(I)} \to V \,:\, \lambda = (\lambda_i)_{i \in I} \mapsto v = \textstyle\sum_{i \in I} b_i \lambda_i.$$

Dabei gilt $e_i \mapsto b_i$ für jeden Index $i \in I$. Wenn $\mathcal{B}$ zudem eine Basis ist, so ist $\Phi_{\mathcal{B}}$ ein Isomorphismus: Er übersetzt verlustfrei den Modellraum $R^{(I)}$ mit der Standardbasis $(e_i)_{i \in I}$ in den Raum V mit der Basis $(b_i)_{i \in I}$ und zurück. Jeder basierte Raum $(V, (b_i)_{i \in I})$ sieht demnach genau aus wie der Standardraum $(R^{(I)}, (e_i)_{i \in I})$, bis auf den Isomorphismus $\Phi_{\mathcal{B}}$.

Erste Beispiele: $\mathbb{C}$ über $\mathbb{C}$ und über $\mathbb{R}$

J113

Beispiel: Der $\mathbb{C}$–lineare Raum $\mathbb{C}$ ist frei, die Standardbasis ist 1.
Allgemein ist jedes Element $b \in \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ eine $\mathbb{C}$–Basis von $\mathbb{C}$.

Ebenso ist der Raum $\mathbb{C}$ frei über $\mathbb{R} \leq \mathbb{C}$, die Standardbasis ist $(1, \mathrm{i})$:
Jede komplexe Zahl $z \in \mathbb{C}$ schreibt sich eindeutig als Linearkombination

$$z = 1x + \mathrm{i}y \quad \text{mit Koeffizienten} \quad (x, y) \in \mathbb{R}^2.$$

Auch $(1, -\mathrm{i})$ ist eine $\mathbb{R}$–Basis von $\mathbb{C}$. (Es gibt unendlich viele weitere.)

⚠ Die Familie (1) erzeugt den Raum $\mathbb{C}$ über $\mathbb{C}$, aber nicht über $\mathbb{R}$.
Die Familie $(1, \mathrm{i})$ ist linear unabhängig über $\mathbb{R}$, aber abhängig über $\mathbb{C}$.

Beispiel J1D: Basis von $\mathbb{C}^n$, komplex vs reell

Ist $\mathcal{B}_\mathbb{C} = (b_1, \dots, b_n)$ eine Basis der Länge n von $\mathbb{C}^n$ über $\mathbb{C}$, dann
ist $\mathcal{B}_\mathbb{R} = (b_1, b_1\mathrm{i}, \dots, b_n, b_n\mathrm{i})$ eine Basis der Länge $2n$ von $\mathbb{C}^n$ über $\mathbb{R}$.

⚠ Diese Eigenschaften hängen demnach sensibel vom Grundring ab.
Aus dem Kontext muss hervorgehen, über welchem Ring wir arbeiten.

Erste Beispiele: der Raum $\mathbb{C}$ über $\mathbb{C}$ und über $\mathbb{R}$

J114
Erläuterung

Aufgabe: Beweisen Sie die Behauptung dieses Beispiels!

Lösung: (1) Die Familie $\mathcal{B}_\mathbb{R}$ erzeugt $\mathbb{C}^n$ über $\mathbb{R}$: Vorgelegt sei $v \in \mathbb{C}^n$.
Da $\mathcal{B}_\mathbb{C}$ eine Basis über $\mathbb{C}$ ist, existieren Koeffizienten $z \in \mathbb{C}^n$ mit

$$v = \sum_{k=1}^{n} b_k z_k = \sum_{k=1}^{n} b_k \operatorname{Re}(z_k) + b_k \mathrm{i} \operatorname{Im}(z_k).$$

Dies stellt v als $\mathbb{R}$–Linearkombination von $\mathcal{B}_\mathbb{R}$ dar.

(2) Zudem ist $\mathcal{B}_\mathbb{R}$ in $\mathbb{C}^n$ linear unabhängig über $\mathbb{R}$: Vorgelegt seien reelle
Koeffizienten $x_1, y_1, \dots, x_n, y_n \in \mathbb{R}$. Aus der Linearkombination

$$0 = \sum_{k=1}^{n} b_k x_k + b_k \mathrm{i} y_k = \sum_{k=1}^{n} b_k (x_k + \mathrm{i} y_k)$$

folgt $x_k + \mathrm{i}y_k = 0$, da $\mathcal{B}_\mathbb{C}$ linear unabhängig über $\mathbb{C}$ ist.
Das bedeutet $x_k = y_k = 0$ für alle $k = 1, \dots, n$.

Erste Beispiele: der Polynomring $K[X]$ über K

J115

Beispiel: Sei K ein kommutativer Ring und $K[X]$ der Polynomring.
Dann ist $K[X]$ frei über K bezüglich der **Monombasis** $(X^n)_{n \in \mathbb{N}}$.
Das ist geradezu die Definition G3A des Polynomrings $K[X]$ über K.
Daraus folgt insbesondere die Gleichheit durch Koeffizientenvergleich
und daraus anschließend alle weiteren Rechenregeln!
Im Falle $\mathbb{Q} \leq K$ hat $K[X]$ zudem die **faktorielle Basis** $(\frac{1}{n!} X^n)_{n \in \mathbb{N}}$.

Beispiel J1E: gestufte Polynombasis

Sei $(P_n)_{n \in \mathbb{N}}$ eine **gestufte Familie** von Polynomen $P_n \in K[X]$,
mit den Eigenschaften $\deg(P_n) = n$ und $\operatorname{lc}(P_n) \in K^\times$ für alle $n \in \mathbb{N}$.
Dann ist $(P_n)_{n \in \mathbb{N}}$ eine Basis von $K[X]$ über K.

Aufgabe: Ist $K[X]$ ein linearer Raum über dem Ring $K[X^2]$? Ist er frei?
Ist allgemein $K[X]$ frei über $K[X^n]$? Falls ja, nennen Sie eine Basis.
Lösung: Ja, $K[X]$ ist frei über $K[X^2]$ bezüglich der Basis $1, X$. (I2M)
Für $n \in \mathbb{N}_{\geq 1}$ ist $K[X]$ frei über $K[X^n]$ mit Basis $1, X, X^2, \dots, X^{n-1}$.

Erste Beispiele: der Polynomring $K[X]$ über K

J116
Erläuterung

Aufgabe: Beweisen Sie die Behauptung des Beispiels J1E! Genauer:

$$K[X] \quad = \langle\, P_n \mid n \in \mathbb{N} \,\rangle_K^!,$$
$$K[X]_{\leq d} = \langle\, P_n \mid n \leq d \,\rangle_K^!.$$

Lösung: (1) Wir zeigen die Inklusion „$\subseteq$“ per Induktion über d:
Für $K[X]_{<0} = \{0\}$ ist die Aussage klar. Für $P \in K[X]_{\leq d}$ gilt

$$Q = P - \operatorname{lc}(P) \operatorname{lc}(P_n)^{-1} P_n \in K[X]_{<d} = \langle\, P_n \mid n < d \,\rangle.$$

Somit gilt $P \in \langle\, P_n \mid n \leq d \,\rangle$, wie behauptet.

(2) Zudem ist $(P_n)_{n \in \mathbb{N}}$ in $K[X]$ linear unabhängig über K.
Wir betrachten eine K–Linearkombination zu Null:

$$P = \lambda_0 P_0 + \lambda_1 P_1 + \cdots + \lambda_n P_n$$

Im Falle $\lambda_n \neq 0$ gilt $\deg(P) = n$. Aus $P = 0$ folgt also $\lambda_n = 0$.
Per Induktion schließen wir aus $P = 0$ somit $\lambda_k = 0$ für alle k.

Die Standardbasis des linearen Raums R^n über R

J117

Beispiel: Der R–lineare Raum R^n ist frei, die **Standardbasis** ist

$$\mathcal{E}: \quad e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \dots, \quad e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

Beweis: (1) Jeder Vektor $x \in R^n$ schreibt sich als Linearkombination

$$x = \sum_{i=1}^{n} e_i x_i.$$

(2) Eindeutigkeit: Sind zwei solche Darstellungen gegeben,

$$\sum_{i=1}^{n} e_i \lambda_i = \sum_{i=1}^{n} e_i \mu_i,$$

so folgt $\lambda_i = \mu_i$ für alle $i = 1, \dots, n$.

Basen des linearen Raums R^n über R

J118
Erläuterung

Alternativ zu (2): Jede Relation zwischen $e_1, \dots, e_n$ ist trivial, denn aus $\sum_{i=1}^{n} e_i \lambda_i = 0$ folgt $\lambda_i = 0$ für alle $i = 1, \dots, n$.

☺ Die Basiseigenschaft ist für die Familie $\mathcal{E}$ offensichtlich.
Wir haben $R^n = R^I = R^{(I)}$ für $I = \{1, \dots, n\}$, siehe Beispiel J1C.

☺ Dabei stellen wir erfreut fest: Zu jedem Vektor $x \in R^n$ sind die vertrauten kartesischen Koordinaten $(x_1, \dots, x_n)$ zugleich die Koordinaten bezüglich der Standardbasis $\mathcal{E} = (e_1, \dots, e_n)$.

Wir nennen $\mathcal{E}$ die **Standardbasis**, manche Autoren sagen hierzu auch die **kanonische Basis**, die **übliche Basis**, oder ähnliches.

☹ Bitte sagen Sie zu $\mathcal{E}$ nicht „die Basis“ des R^n, das ist verkehrt.

Es gibt zu R^n viele weitere Basen, wie wir gleich sehen werden, die Standardbasis ist besonders einfach. Je nach Problemstellung sind andere Basen eventuell noch nützlicher. Dazu später mehr.

Basen des linearen Raums R^n über R

J119

Für jede Familie $\mathcal{B} = (b_1, \dots, b_k)$ mit $b_1, \dots, b_k \in R^n$ gilt:

$$\Phi_{\mathcal{B}} : R^k \xrightarrow{\sim} R^n : \lambda \mapsto b_1\lambda_1 + \cdots + b_k\lambda_k = B\lambda$$

Wir identifizieren R^n hier mit Spaltenvektoren $R^{n\times 1}$ und betrachten die Vektoren $b_1, \dots, b_k \in R^n$ als die Spalten der Matrix $B \in R^{n\times k}$.

1. Der **Kern** von $\Phi_{\mathcal{B}}$ ist der **Lösungsraum**

$$\ker(\Phi_{\mathcal{B}}) = \ker(B) := \{ \lambda \in R^k \mid B\lambda = 0 \} \leq R^k.$$

   Jede Lösung $\lambda \in R^k$ zu $B\lambda = 0$ ist eine Relation der Familie $\mathcal{B}$. Genau dann ist $\mathcal{B}$ linear unabhängig, wenn $\ker(B) = \{0\}$ gilt.

2. Das **Bild** von $\Phi_{\mathcal{B}}$ ist der **Spaltenraum**

$$\operatorname{im}(\Phi_{\mathcal{B}}) = \operatorname{im}(B) := \langle b_1, \dots, b_k \rangle_R \leq R^n.$$

   Genau dann ist $\mathcal{B}$ erzeugend für R^n, wenn $\operatorname{im}(B) = R^n$ gilt.

3. Genau dann ist die Familie $\mathcal{B}$ eine **Basis** von R^n über R, wenn die Matrix B invertierbar ist, siehe Satz B2D zu $B\lambda = v$.

Gestufte Basen des linearen Raums R^n über R

J120

Beispiel J1F: eine gestufte Basis

Eine **gestufte Basis** des Raums R^n über R ist von der Form

$$b_1 = \begin{bmatrix} \blacksquare \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} * \\ \blacksquare \\ \vdots \\ 0 \end{bmatrix}, \quad \dots, \quad b_n = \begin{bmatrix} * \\ * \\ \vdots \\ \blacksquare \end{bmatrix}$$

mit $b_{ij} = 0$ für alle $j > i$ und invertierbarem Leitkoeffizienten $b_{ii} \in R^\times$.
Jede Teilfamilie ist linear unabhängig, jede Oberfamilie ist erzeugend.

Übung: Erklären Sie, warum $(b_1, \dots, b_n)$ tatsächlich eine Basis ist.
Was können Sie über die zugehörige Matrix B sagen?
Wie bringen Sie B in (reduzierte) Zeilenstufenform?
Wie lösen Sie damit die Gleichgung $B\lambda = v$?

☺ Das ist ein schönes und wichtiges Beispiel. Hier freuen Sie sich, dass Sie bereits seit Satz B2D über passendes Werkzeug verfügen!

Anwendungsbeispiel zur linearen Un/Abhängigkeit

J121
Ausprobieren mit Gaël!

Aufgabe: In $\mathbb{R}^3$ über $\mathbb{R}$ betrachten wir die Familie

$$\mathcal{B}: \quad b_1 = \begin{bmatrix}1\\1\\2\end{bmatrix}, \quad b_2 = \begin{bmatrix}1\\2\\3\end{bmatrix}, \quad b_3 = \begin{bmatrix}3\\4\\7\end{bmatrix}.$$

(1) Ist $\mathcal{B}$ linear unabhängig? Nennen Sie alle Relationen!
(2) Welche Teilfamilien von $\mathcal{B}$ sind linear unabhängig?

Lösung: Wir lösen $B\lambda = v$ mit dem Gauß–Algorithmus (B2C/B2B):

$$B = \begin{bmatrix}1&1&3\\1&2&4\\2&3&7\end{bmatrix} \xrightarrow[SB=B']{\text{RZSF}} B' = \begin{bmatrix}1&0&2\\0&1&1\\0&0&0\end{bmatrix}, \quad \lambda = \begin{bmatrix}2\\1\\-1\end{bmatrix}.$$

(1) Die Familie $\mathcal{B} = (b_1, b_2, b_3)$ ist linear abhängig: Nicht-triviale Relationen sind λ, denn $b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3 = 0$, und alle Vielfachen.

(2) Die Familien (b_1, b_2) und (b_1, b_3) und (b_2, b_3) sind linear unabhängig, zudem offensichtlich auch (b_1) und (b_2) und (b_3) sowie $()$.

Anwendungsbeispiel zur linearen Un/Abhängigkeit

J122
Erläuterung

Die hier betrachtete Familie $\mathcal{B} = (b_1, b_2, b_3)$ ist linear abhängig, doch die Relation λ ist nicht offensichtlich: Wir müssen rechnen.

Dank Gauß finden wir die Zeilenstufenform $B' = SB$. Die invertierbare Matrix $S \in \mathrm{GL}_3\,\mathbb{R}$ codiert die Zeilenoperationen, somit gilt $B = S^{-1}B'$. Daraus folgt insbesondere $\ker(B) = \ker(B')$, denn $B\lambda = 0 \Leftrightarrow B'\lambda = 0$.

In der Matrix B' sieht man sehr leicht, dank reduzierter Zeilenstufenform, dass die Familie der drei Spalten $(B'e_1, B'e_2, B'e_3)$ linear abhängig ist. Dasselbe gilt dann auch für die Familie (Be_1, Be_2, Be_3).

Ebenso sehen wir, dass $(B'e_1, B'e_2)$ und $(B'e_1, B'e_3)$ und $(B'e_2, B'e_3)$ jeweils linear unabhängig sind. Dasselbe gilt dann auch für die Familien (Be_1, Be_2) und (Be_1, Be_3) und (Be_2, Be_3) von Spalten der Matrix B.

🙂 Jede Teilfamilie ist dann ebenfalls linear unabhängig (J1G).

🙂 Satz J1P erklärt Ihnen allgemein einen Algorithmus, mit dem Sie zu jeder Matrix den Bildraum und den Kern bestimmen können.

Anwendungsbeispiel zu erzeugenden Familien

J123
Ausprobieren mit Gaël!

Aufgabe: In $\mathbb{R}^3$ über $\mathbb{R}$ betrachten wir die Familie

$$\mathcal{B}: \quad b_1 = \begin{bmatrix}1\\1\\2\end{bmatrix}, \quad b_2 = \begin{bmatrix}1\\2\\3\end{bmatrix}, \quad b_3 = \begin{bmatrix}3\\4\\7\end{bmatrix}, \quad b_4 = \begin{bmatrix}3\\2\\1\end{bmatrix}.$$

(1) Ist $\mathcal{B}$ erzeugend? linear unabhängig? eine Basis von $\mathbb{R}^3$?
(2) Welche Teilfamilien von $\mathcal{B}$ sind Basen von $\mathbb{R}^3$?

Lösung: Wir lösen $B\lambda = v$ mit dem Gauß–Algorithmus (B2C/B2B):

$$B = \begin{bmatrix}1&1&3&3\\1&2&4&2\\2&3&7&1\end{bmatrix} \xrightarrow[SB=B']{\text{RZSF}} B' = \begin{bmatrix}1&0&2&0\\0&1&1&0\\0&0&0&1\end{bmatrix}, \quad \lambda = \begin{bmatrix}2\\1\\-1\\0\end{bmatrix}.$$

(1) Die Familie $\mathcal{B} = (b_1, b_2, b_3, b_4)$ ist erzeugend, aber linear abhängig: Eine nicht-triviale Relationen ist λ, denn $b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3 + b_4\lambda_4 = 0$.

(2) Die Familien (b_1, b_2, b_4) und (b_1, b_3, b_4) und (b_2, b_3, b_4) sind Basen. Wir sehen dies leicht in B' und übertragen es dann auf B.

Anwendungsbeispiel zu erzeugenden Familien

J124
Erläuterung

Die hier betrachtete Familie $\mathcal{B} = (b_1, b_2, b_3, b_3)$ erzeugt den Raum $\mathbb{R}^3$, doch diese Eigenschaft ist nicht offensichtlich: Wir müssen rechnen.

Dank Gauß finden wir die Zeilenstufenform $B' = SB$. Die invertierbare Matrix $S \in \mathrm{GL}_3\,\mathbb{R}$ codiert die Zeilenoperationen, somit gilt $B = S^{-1}B'$. Daraus folgt insbesondere $\mathrm{im}(B') = S\,\mathrm{im}(B)$ und $\mathrm{im}(B) = S^{-1}\,\mathrm{im}(B')$.

In der Matrix B' sieht man sehr leicht, dank reduzierter Zeilenstufenform, dass die Familie $e_1 = B'e_1$, $e_2 = B'e_2$, $e_3 = B'e_4$ den Raum $\mathbb{R}^3$ erzeugt. Dasselbe gilt dann auch für $S^{-1}e_1 = Be_1$, $S^{-1}e_2 = Be_2$, $S^{-1}e_3 = Be_4$.

Ebenso sehen wir, dass die Familien Be_1, Be_3, Be_4 und Be_2, Be_3, Be_4 Basen sind: Wir sehen dies leicht in B' und übertragen es dann auf B.

🙂 Das ist eine schöne, konkrete Illustration zum Basisauswahlsatz J2B.

🙂 Satz J1P erklärt Ihnen allgemein einen Algorithmus, mit dem Sie zu jeder Matrix den Bildraum und den Kern bestimmen können.

Lineare Un/Abhängigkeit

Aus diesen ersten Zahlenbeispielen extrahieren wir bereits ein paar hilfreiche Bemerkungen, die Ihnen allgemein nützen werden.

Bemerkung: Sei V ein Vektorraum über dem Divisionsring R.
Zwei Vektoren $v_1, v_2 \in V$ sind R–linear abhängig, falls

$$v_1\lambda_1 + v_2\lambda_2 = 0 \quad \text{mit} \quad (\lambda_1, \lambda_2) \neq (0,0).$$

Nach Umnummerierung sei $\lambda_1 \neq 0$. Dann gilt:

$$v_1 = v_2(-\lambda_2\lambda_1^{-1})$$

☺ Einer der beiden Vektoren ist ein Vielfaches des anderen.

⚠ Diese einfache Anschauung gilt nur für zwei Vektoren!

Beispiel: Die drei Vektoren $v_1 = (0,1)$, $v_2 = (1,0)$, $v_3 = (1,1)$ in R^2 sind als Familie linear abhängig, aber doch paarweise unabhängig.

Übung: Nennen Sie $n+1$ Vektoren im linearen Raum R^n über R, die linear abhängig sind, aber je n davon sind linear unabhängig.

Lineare Un/Abhängigkeit

Sei $(v_i)_{i\in I}$ eine Familie von Vektoren im linearen Raum V über R.
Die folgenden **offensichtlichen Kriterien** sind für die lineare Abbhängigkeit zwar nicht notwendig, aber doch hinreichend:

1. Einer der Vektoren ist gleich Null: $v_i = 0$ für ein $i \in I$.
2. Zwei Vektoren sind gleich: $v_i = v_j$ für $i \neq j$ in I.
3. Ein Vektor ist ein Vielfaches eines anderen.

Wenn eines dieser Kriterien erfüllt ist, dann ist die Familie $(v_i)_{i\in I}$ offensichtlich linear abhängig. Die Umkehrung gilt jedoch nicht: Lineare Abhängigkeit ist nicht immer offensichtlich!

⚠ Die oben vereinbarte Definition J1A der linearen Un/Abhängigkeit ist mit Bedacht gewählt. Sie lässt sich nicht weiter vereinfachen!

Alles sollte so einfach wie möglich gemacht werden
— aber nicht noch einfacher.
Albert Einstein (1879–1955)

Lineare Un/Abhängigkeit

Aufgabe: Sei $\mathbb{P} = \{2,3,5,7,\ldots\}$ die Menge der Primzahlen.
Ist die Familie $\mathcal{B} = (\ln p)_{p\in\mathbb{P}}$ in $\mathbb{R}$ linear unabhängig über $\mathbb{Q}$?

Lösung: Wir betrachten eine $\mathbb{Q}$–Linearkombination zu Null:

$$q_1 \ln p_1 + \cdots + q_n \ln p_n = 0$$

mit $p_1 < \ldots < p_n$ in $\mathbb{P}$ und $q_1, \ldots, q_n \in \mathbb{Q}$, also $q_i = a_i/b_i$, $a_i \in \mathbb{Z}$, $b_i \in \mathbb{Z}^*$.

$$\frac{a_1}{b_1} \ln p_1 + \cdots + \frac{a_n}{b_n} \ln p_n = 0$$

Wir multiplizieren mit $b = \mathrm{kgV}(b_1, \ldots, b_n) \in \mathbb{Z}^*$ und erhalten $c_i = q_i b \in \mathbb{Z}$:

$$c_1 \ln p_1 + \cdots + c_n \ln p_n = 0$$

Dank $(\exp, \ln) : (\mathbb{R}, +, 0) \cong (\mathbb{R}_{>0}, \cdot, 1)$ ist dies äquivalent zu:

$$p_1^{c_1} \cdots p_n^{c_n} = 1$$

Dank Fundamentalsatz der Arithmetik A2J folgt $c_1 = \cdots = c_n = 0$, also $q_1 = \cdots = q_n = 0$: Jede rationale Relation zwischen $(\ln p)_{p\in\mathbb{P}}$ ist trivial.

Lineare Un/Abhängigkeit

Das ist ein schönes und konkretes Beispiel, das zur Abwechslung nicht von Vektoren im $\mathbb{R}^n$ handelt und nicht auf Matrizenrechnung beruht.

Bitte versuchen Sie mit der Definition und diesen Illustrationen, Begriff und Technik der linearen Un/Abhängigkeit richtig zu verstehen. Das ist nicht ganz leicht, aber wesentlich für die Lineare Algebra!

Zum Abschluss stelle ich einige einfache Bemerkungen zusammen, die die Logik der Begriffe beleuchten. Bitte nutzen Sie dies als Prüfstein für Ihr Verständnis: Lesen Sie nochmals gründlich die Definition J1A und versuchen Sie, die Umformulierungen sicher nachzuvollziehen.

Mit diesen Bemerkungen können Sie auch die vorigen Beispiele nochmals durchgehen: Sie werden viele der Argumente in den konkreten Rechnungen wiedererkennen. Es lohnt sich also!

Es ist auch für alle folgenden Argumente und Rechnungen hilfreich, diese grundlegenden Beobachtungen parat zu haben.

Teilfamilien und Oberfamilien

Bemerkung J1G: Teilfamilien und Oberfamilien

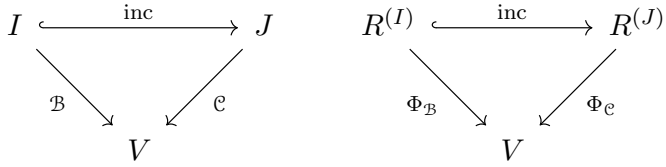
Sei V ein linearer Raum über dem Ring R.

1. Ist die Familie $\mathcal{B} = (v_i)_{i\in I}$ erzeugend für V,
   so auch jede Oberfamilie $\mathcal{C} = (v_i)_{i\in J}$ mit $J \supseteq I$.
2. Ist die Familie $\mathcal{C} = (v_i)_{i\in J}$ nicht erzeugend für V,
   so auch keine Teilfamilie $\mathcal{B} = (v_i)_{i\in I}$ mit $I \subseteq J$.
3. Ist die Familie $\mathcal{B} = (v_i)_{i\in I}$ in V linear abhängig,
   so auch jede Oberfamilie $\mathcal{C} = (v_i)_{i\in J}$ mit $J \supseteq I$.
4. Ist die Familie $\mathcal{C} = (v_i)_{i\in J}$ in V linear unabhängig,
   so auch jede Teilfamilie $\mathcal{B} = (v_i)_{i\in I}$ mit $I \subseteq J$.
5. Genau dann ist $\mathcal{C} = (v_i)_{i\in J}$ linear abhängig,
   wenn eine endliche Teilfamilie $\mathcal{B} = (v_i)_{i\in I}$ linear abhängig ist.
6. Genau dann ist $\mathcal{C} = (v_i)_{i\in J}$ linear unabhängig,
   wenn jede endliche Teilfamilie $\mathcal{B} = (v_i)_{i\in I}$ linear unabhängig ist.

Teilfamilien und Oberfamilien

Beweis: Das ist klar nach Definition. QED

Schreiben Sie es zur Übung und als Wiederholung sorgsam aus!
Aussagen (1) und (3) und (5) sind jeweils klar nach Definition.
Aussagen (2) und (4) und (6) folgen daraus durch Kontraposition.



Für Teilfamilien und Oberfamilien ist folgende Konvention nützlich:

Bemerkung J1H: Ausdehnung / Einschränkung der Indexmenge

Für $I \subseteq J$ betrachten wir $R^I \leq R^J$ und $R^{(I)} \leq R^{(J)}$ als Teilräume.
Ausführlich nutzen wir dazu $(\iota, \rho) : R^I \rightleftarrows R^J$ und $(\iota, \rho) : R^{(I)} \rightleftarrows R^{(J)}$
vermöge $\rho : \mu \mapsto \lambda = \mu|_J$ und $\iota : \lambda \mapsto \mu$ mit $\mu|_I = \lambda$ und $\mu|_{J\smallsetminus I} = 0$.

Familien unter linearen Abbildungen

Bemerkung J1I: Familie unter linearer Abbildung

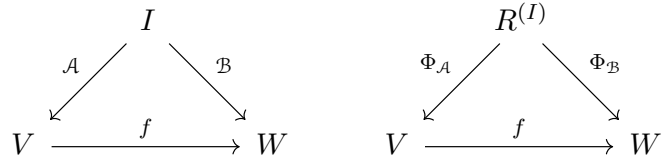
Gegeben sei eine R–lineare Abbildung $f : V \to W$ und eine Familie $\mathcal{A} = (v_i)_{i\in I}$ von Vektoren $v_i \in V$ mit der Bildfamilie $\mathcal{B} = (f(v_i))_{i\in I}$.

1. Ist f bijektiv und die Familie $\mathcal{A} = (v_i)_{i\in I}$ eine Basis von V,
   so ist auch die Bildfamilie $\mathcal{B} = (f(v_i))_{i\in I}$ eine Basis von W.
2. Ist f surjektiv und die Familie $\mathcal{A} = (v_i)_{i\in I}$ erzeugt den Raum V,
   so erzeugt die Bildfamilie $\mathcal{B} = (f(v_i))_{i\in I}$ den Raum W.
3. Ist f injektiv und die Familie $\mathcal{A} = (v_i)_{i\in I}$ in V ist linear unabhängig,
   so ist die Bildfamilie $\mathcal{B} = (f(v_i))_{i\in I}$ in W linear unabhängig.
4. Ist die Familie $\mathcal{A} = (v_i)_{i\in I}$ linear abhängig in V,
   so ist die Bildfamilie $\mathcal{B} = (f(v_i))_{i\in I}$ linear abhängig in W.
5. Ist die Bildfamilie $\mathcal{B} = (f(v_i))_{i\in I}$ linear unabhängig in W,
   so ist die Familie $\mathcal{A} = (v_i)_{i\in I}$ linear unabhängig in V.

Familien und lineare Abbildungen

Beweis: Das ist klar nach Definition. QED

Schreiben Sie es zur Übung und als Wiederholung sorgsam aus!



Die Aussagen (1–3) beruhen auf folgender allgemeinen Überlegung:

1. Die Komposition von zwei Bijektionen ist bijektiv.
2. Die Komposition von zwei Surjektionen ist surjektiv.
3. Die Komposition von zwei Injektionen ist injektiv.

Aussage (4) ist klar: Jede Relation λ der Familie $\mathcal{A}$ besteht weiter für die Bildfamilie $\mathcal{B}$. Daraus folgt (5) durch Kontraposition.

Invarianz der Basislänge

Für jede Familie $\mathcal{B} = (b_1, \dots, b_k)$ mit $b_1, \dots, b_k \in R^n$ gilt:

$$\Phi_{\mathcal{B}} : R^k \xrightarrow{\sim} R^n : \lambda \mapsto b_1\lambda_1 + \cdots + b_k\lambda_k = B\lambda$$

Ist R ein Divisionsring, so können wir B mit dem Gauß–Algorithmus in Zeilenstufenform überführen und den Rang r ablesen. Satz B2D besagt:

1. $\Phi_{\mathcal{B}}$ surjektiv $\iff r = n \leq k$, also Rang gleich Zeilenzahl.
2. $\Phi_{\mathcal{B}}$ injektiv $\iff r = k \leq n$, also Rang gleich Spaltenzahl.
3. $\Phi_{\mathcal{B}}$ bijektiv $\iff r = k = n$, also B quadratisch mit vollem Rang.

Satz J1J: Invarianz der Basislänge

Sei R ein Divisionsring.

1. Ist $\mathcal{B} = (b_1, \dots, b_k)$ ein Erzeugendensystem von R^n, so gilt $k \geq n$.
2. Ist $\mathcal{B} = (b_1, \dots, b_k)$ linear unabhängig in R^n, so gilt $k \leq n$.
3. Ist $\mathcal{B} = (b_1, \dots, b_k)$ eine Basis von R^n, so gilt $k = n$.

Invarianz der Basislänge

Diese Aussagen scheinen zunächst anschaulich recht plausibel, gemessen an unserer geometrisch-physikalischen Erfahrung: Im Raum $\mathbb{R}^3$ genügen zwei Vektoren nicht zum Aufspann von $\mathbb{R}^3$ und je vier Vektoren im $\mathbb{R}^3$ sind zwangsläufig linear abhängig.

So scheint es zumindest … und erweist sich nun als wahr, denn wir können es beweisen wie hier in Satz J1J formuliert.

Schon im Raum $\mathbb{R}^{100}$ ist allein mit „Anschauung“ keineswegs klar, warum jede Familie von 101 Vektoren linear abhängig sein sollte, oder eine Familie von 99 Vektoren nicht zum Aufspann genügt. Man möchte dies zwar gerne glauben, aber das hilft nicht weiter.

🙂 Über Divisionsringen hilft uns wieder einmal der Gauß–Algorithmus! Intuition und Anschauung sind schön und gut, doch wir brauchen mehr: Für eine tragfähige Theorie benötigen wir präzise Definitionen, nachvollziehbare Argumente und effiziente Werkzeuge.

⚠ Diese guten Eigenschaften gelten nicht über jedem Ring! Es gibt mahnende Gegenbeispiele, siehe etwa Beispiel J1O.

Invarianz der Dimension

Als Analogie erinnern wir uns an den Zählsatz E1G:

1. Ist $f : \{1, \dots, k\} \twoheadrightarrow \{1, \dots, n\}$ surjektiv, so gilt $k \geq n$.
2. Ist $f : \{1, \dots, k\} \hookrightarrow \{1, \dots, n\}$ injektiv, so gilt $k \leq n$.
3. Ist $f : \{1, \dots, k\} \xrightarrow{\sim} \{1, \dots, n\}$ bijektiv, so gilt $k = n$.

Satz J1K: Invarianz der Dimension

Sei R ein Divisionsring. Für alle $k, n \in \mathbb{N}$ gilt:

1. Ist $f : R^k \twoheadrightarrow R^n$ eine R–lineare Surjektion, so gilt $k \geq n$.
2. Ist $f : R^k \hookrightarrow R^n$ eine R–lineare Injektion, so gilt $k \leq n$.
3. Ist $f : R^k \xrightarrow{\sim} R^n$ eine R–lineare Bijektion, so gilt $k = n$.

Beweis: Dies folgt aus Satz J1J und Bemerkung J1I: Die Bildfamilie $(f(e_i))_{i=1}^k$ in R^n ist (1) erzeugend, (2) unabhängig, (3) eine Basis. QED

⚠ In diesem Beweis nutzen wir den Gauß–Algorithmus (B2D), deshalb fordern wir als Voraussetzung, dass R ein Divisionsring ist. Der Satz gilt auch über jedem kommutativen Ring $R \neq \{0\}$, siehe L3C. Über beliebigen Ringen gilt der Satz im Allgemeinen nicht, siehe J1O.

Invarianz der Dimension

🙂 Sätze J1J und J1K sind wichtige Ergebnisse über Divisionsringen. Wir bekommen diese Resultate hier gratis aus dem Gauß–Algorithmus, da wir zuvor in Kapitel B schon gut und gründlich gearbeitet haben. Diese anfängliche Investition zahlt sich hier und überall aus.

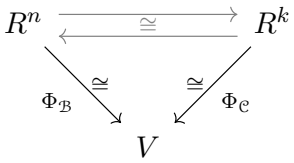
Der Aufbau der Theorie muss insgesamt logisch schlüssig sein, doch innerhalb der logischen Anforderungen bleiben noch viele Freiheiten. Die Vorgehensweise der Darstellung, die Anordnung der Begriffe und Argumente ist eine interessante (und knifflige) didaktische Frage.

Viele Lehrbücher zur Linearen Algebra behandeln die Matrizenrechnung und den Gauß–Algorithmus erst später, nach Vektorräumen und Basen. In diesem Falle müssen die ersten Rechenbeispiele zur Erzeugung und linearen Unabhängigkeit aufgeschoben werden, auch die zugehörigen Beweise müssen anders organisiert werden. Das gelingt ebenso.

Ich finde es eleganter, zwei Fliegen mit einer Klappe zu schlagen: Der Gauß–Algorithmus erlaubt effiziente Rechnungen *und* Beweise!

Wie definieren wir die Dimension eines R–linearen Raumes?

J137



Definition J1L: Dimension eines linearen Raumes

(1) Ein Ring R erfüllt die **Invarianz der Dimension**, falls für alle $k, n \in \mathbb{N}$ gilt: Aus Isomorphie $R^k \cong R^n$ folgt Gleichheit $k = n$.

(2) Unter der Voraussetzung (1) gilt: Ist V ein R–linearer Raum mit Basis $\mathcal{B} = (b_i)_{i \in I}$, so haben alle Basen von V dieselbe Länge $\sharp I$.

In diesem Falle definieren wir die **Dimension** $\dim_R(V) := \sharp I$.

Dies gilt für jeden Divisionsring (J1K), insbesondere für jeden Körper.
Dies gilt auch für jeden endlichen Ring $R \neq \{0\}$ dank Zählsatz E1G.
Es gilt ebenso für jedem kommutativen Ring $R \neq \{0\}$, siehe L3C.

⚠ Über dem Nullring $R = \{0\}$ hingegen gilt $R^1 \cong R^n$ für alle $n \in \mathbb{N}$.
Für ein nicht-triviales, raffiniertes Gegenbeispiel siehe unten J1O

Wie definieren wir die Dimension eines R–linearen Raumes?

J138 Erläuterung

🙂 Damit können wir die „Größe“ des Raums V über R messen.

Bemerkung: Zur Dimension $\dim_R(V)$ benötigen wir zwei Zutaten:

1. Der R–lineare Raum V muss frei sein, also mindestens eine Basis haben; das gilt leider nicht immer, siehe J1B.
   Es gilt für alle Vektorräume, siehe J2B und J2C.
2. Der Ring R muss die Invarianz der Dimension erfüllen:
   Je zwei Basen von V haben dann dieselbe Länge.
   Dies gilt für Divisionsringe dank J1J und J1K.

⚠ Wenn wir im Folgenden von der Dimension $\dim_R(V)$ sprechen, so müssen diese beiden Voraussetzungen erfüllt sein: Wir müssen sie im allgemeinen Fall fordern und im konkreten Fall nachweisen!

🙂 Über jedem Divisionsring sind die Voraussetzungen (1) und (2) immer erfüllt. Das ist die grundlegende Erkenntnis dieses Kapitels.

Über Ringen, die keine Divisionsringe sind, sagen die meisten Autoren vorsichtig **Rang**, ich nenne dies in beiden Fällen einfach **Dimension**.

Wie definieren wir die Dimension eines R–linearen Raumes?

J139 Erläuterung

🙂 Vielleicht halten Sie dieses vorsichtige Vorgehen für hasenfüßig.
Ist das nicht alles klar? Beispiel J1O schützt Sie vor naivem Irrglauben!

Dem Koordinatenraum R^n sieht man die Zahl n direkt an:
Die Menge R^n besteht aus n–Tupel $(x_1, \ldots, x_n)$ über R.

Für einen freien Raum V über R hingegen ist das nicht klar.
Wir können eine Basis $(b_i)_{i \in I}$ wählen, aber es gibt viele Basen,
und die Wahl einer Basis ist daher notgedrungen immer willkürlich.
Es gibt nicht „die“ Basis von V, sondern nur eine Basis von vielen.

Wenn wir also die Dimension von V über R definieren wollen,
so müssen wir zunächst sicherstellen, dass je zwei Basen $(b_i)_{i \in I}$
und $(c_j)_{j \in J}$ von V immer dieselbe Länge haben, also $\sharp I = \sharp J$ gilt.
Genau das sichert die Voraussetzung der Invarianz der Dimension!

🙂 Für viele „vernünftige“ Ringe gilt die Invarianz der Dimension:
zunächst für jeden Divisionsring (J1K) und anschließend für jeden kommutativen Ring (L3C). Sie gilt insbesondere für jeden Körper!

Wie definieren wir die Dimension eines R–linearen Raumes?

J140 Erläuterung

Definition J1L gibt uns eine konkrete Berechnungsmethode an die Hand,
meist tatsächlich einen expliziten Algorithmus (siehe unten, Satz J1P).

🙂 Genau so wird die Dimension $\dim_R(V)$ definiert und in vielen typischen Fällen auch direkt berechnet: Wir finden eine geeignete Familie $(b_i)_{i \in I}$ von V, weisen für $(b_i)_{i \in I}$ lineare Unabhängigkeit und Erzeugung von V nach, und schließen so $\dim_R(V) = \sharp I$.

🙂 Es genügt, dieses Verfahren für *eine* Basis zu durchlaufen:
Jede andere Basis ist genauso gut und liefert dasselbe Ergebnis!
Nach Alexandre Dumas berühmtem Motto: *Eine für alle, alle für eine.*
Das ist nicht nur theoretisch elegant, sondern auch praktisch effizient.

🙂 In unseren vorigen Beispielen haben wir Basen explizit angegeben und die Eigenschaften nachgewiesen: Unabhängigkeit und Erzeugung.
Wir wissen nun auch, dass alle weiteren Basen dieselbe Länge haben.
Zur Wiederholung und Betonung nennen ich die folgenden Beispiele.

Erste Beispiele zur Dimension

J141

Beispiel: Sei R ein Divisionsring oder ein kommutativer Ring. Dann gilt

$$\dim_R(R^n) = n.$$

Dies enthält die Spezialfälle $\dim_R(\{0\}) = 0$ und $\dim_R(R) = 1$.
Siehe hierzu Beispiel J1C: Allgemein gilt $\dim_R(R^{(I)}) = \sharp I$.

Beispiel: Für die komplexen Zahlen $\mathbb{C}$ gilt

$$\dim_{\mathbb{C}}(\mathbb{C}^n) = n \quad \text{und} \quad \dim_{\mathbb{R}}(\mathbb{C}^n) = 2n.$$

Siehe Beispiel J1D: Basis und Dimension hängen vom Grundring ab!
Daher die Schreibweise $\dim_R(V)$, abgekürzt $\dim V$ nur falls R klar ist.

Beispiel: Sei K ein kommutativer Ring und $K[X]$ der Polynomring.
Dann ist $K[X]$ frei über K bezüglich der Monombasis $(X^n)_{n\in\mathbb{N}}$, also

$$\dim_K(K[X]) = \infty.$$

⚠ Der Raum $K[X]$ kann über K nicht endlich erzeugt werden,
denn $\langle P_1, \ldots, P_n \rangle_K \leq K[X]_{\leq m}$ mit $m = \max\{\deg P_1, \ldots, \deg P_n\}$.

Erste Beispiele zur Dimension

J142
Erläuterung

Die Dimension $\dim_{\mathbb{R}}(\mathbb{R}^n) = n$ ist anschaulich plausibel, insbesondere für kleine Werte $n = 1, 2, 3$. Doch schon für einfache Beispiele wie

$$V = \{\, x \in \mathbb{R}^7 \mid \textstyle\sum_{i=1}^7 x_i = \sum_{i=1}^7 i x_i = \sum_{i=1}^7 i^2 x_i = 0 \,\}$$

benötigen wir eine präzise Definition des Dimensionsbegriffs!

Nochmal zur Betonung: Die Berechnung der Dimension $\dim_R(V)$ verläuft immer nach demselben Muster: Wir finden eine geeignete Familie $(b_i)_{i\in I}$ von V, weisen für $(b_i)_{i\in I}$ lineare Unabhängigkeit und Erzeugung von V nach, und schließen so $\dim_R(V) = \sharp I$.

In diesen ersten Beispielen ist diese Berechnung besonders leicht.
Die Komplexität der nötigen Rechnungen hängt von der konkret vorliegenden Anwendung ab, doch das Prinzip ist immer dasselbe.

Im Verlauf dieses Kapitels werden wir mehrere Methoden erarbeiten zur Konstruktion von Basen und zur Berechnung der Dimension.
Zur Dimension von Bild und Kern einer Matrix siehe Satz J1P.

Invarianz der unendlichen Dimension

J143
Erläuterung

Die Invarianz der Dimension J1L besagt: Je zwei endliche Basen von V haben dieselbe Länge. Könnte es sein, dass eine Basis endlich ist und eine andere unendlich? Nein! Diese Klärung reichen wir nun nach:

Lemma J1M: einmal unendlich, immer unendlich

Sei R ein beliebiger Ring mit $0 \neq 1$, also $R \neq \{0\}$.

(1) Ist I unendlich, so ist der Raum $R^{(I)}$ über R nicht endlich erzeugt.

(2) Hat ein linearer Raum V über R eine unendliche Basis $\mathcal{B} = (b_i)_{i\in I}$, so ist jedes Erzeugendensystem $\mathcal{C} = (c_j)_{j\in J}$ ebenfalls unendlich.

Beweis: (1) Für jede endliche Familie $v_1, \ldots, v_n \in R^{(I)}$ ist
$E = \bigcup_{k=1}^n \operatorname{supp}(v_k)$ endlich und $\langle v_1, \ldots, v_n \rangle \leq R^{(E)} \lneq R^{(I)}$.
(Zu dieser Sichtweise $R^{(E)} \leq R^{(I)}$ siehe J1H.)

(2) Wir betrachten die Familie $(v_j)_{j\in J}$ in $R^{(I)}$ mit $v_j = \Phi_{\mathcal{B}}^{-1}(c_j) \in R^{(I)}$.
Dank (1) erzeugt $(v_j)_{j\in J}$ nicht $R^{(I)}$, also erzeugt $\mathcal{C} = (c_j)_{j\in J}$ nicht V.
(Zu dieser Schlussweise siehe Bemerkung J1I.) QED

Invarianz der Dimension, auch unendlich

J144
Erläuterung

Satz J1N: Invarianz der Dimension, auch unendlich

Sei R ein Divisionsring. Für alle Mengen I, J gilt:

1. Ist $f : R^{(I)} \twoheadrightarrow R^{(J)}$ eine lineare Surjektion, so gilt $\sharp I \geq \sharp J$.
2. Ist $f : R^{(I)} \hookrightarrow R^{(J)}$ eine lineare Injektion, so gilt $\sharp I \leq \sharp J$.
3. Ist $f : R^{(I)} \xrightarrow{\sim} R^{(J)}$ eine lineare Bijektion, so gilt $\sharp I = \sharp J$.

Beweis: Dank Bemerkung J1I wissen wir: Die Bildfamilie $(f(e_i))_{i\in I}$ in $R^{(J)}$ ist (1) erzeugend, (2) unabhängig, (3) eine Basis.

(1) Die endlichen Fälle sind geklärt dank J1K.
Ist J unendlich, so auch I dank Lemma J1M.
Ist I unendlich, so ist die Aussage trivial.

(2) Die endlichen Fälle sind geklärt dank J1K.
Ist I unendlich, so auch J, ebenfalls dank J1K.
Ist J unendlich, so ist die Aussage trivial.

(3) Diese Aussage folgt aus (1) und (2). QED

Ein mahnendes Gegenbeispiel

⚠ Über manchen Ringen hat der Begriff „Dimension“ keinen Sinn!
Beispiel: Über dem Nullring $R = \{0\}$ gilt $R^1 \cong R^n$ für alle $n \in \mathbb{N}$.

Beispiel J1o: ein nicht-trivialer Ring mit $R^1 \cong R^2$

Sei K ein Körper, etwa $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$. Hierüber sei $V = K^{(\mathbb{N})} = K[X]$ der Vektorraum der Folgen $x = (x_0, x_1, x_2, \dots)$ mit endlichem Träger.

Im Ring $R = (\mathrm{End}_K(V), +, \circ)$ seien $a, b, c, d : V \to V$ gegeben durch

$$a(x) = (x_0, 0, x_1, 0, x_2, 0, \dots), \qquad c(x) = (x_0, x_2, x_4, x_6, x_8, \dots),$$
$$b(x) = (0, x_0, 0, x_1, 0, x_2, \dots), \qquad d(x) = (x_1, x_3, x_5, x_7, x_9, \dots).$$

(1) Für Matrizen über dem Ring R gelten dann die Gleichungen

$$\begin{pmatrix} c \\ d \end{pmatrix} \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} ca & cb \\ da & db \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = ac + bd = 1.$$

(2) Die Matrizen $\left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} a & b \end{smallmatrix}\right)$ stiften einen Isomorphismus $R^1 \cong R^2$.
(3) Per Induktion folgt $R^1 \cong R^n$ und somit $R^m \cong R^n$ für alle $m, n \in \mathbb{N}_{\geq 1}$.

Ein mahnendes Gegenbeispiel

Beweis: (1) Diese Gleichungen können Sie direkt nachrechnen!

$$\begin{aligned}
c \circ a &: x \mapsto (x_0, 0, x_1, 0, x_2, 0, \dots) \mapsto (x_0, x_1, x_2, \dots) \\
c \circ b &: x \mapsto (0, x_0, 0, x_1, 0, x_2, \dots) \mapsto (0, 0, 0, \dots) \\
d \circ a &: x \mapsto (x_0, 0, x_1, 0, x_2, 0, \dots) \mapsto (0, 0, 0, \dots) \\
d \circ b &: x \mapsto (0, x_0, 0, x_1, 0, x_2, \dots) \mapsto (x_0, x_1, x_2, \dots) \\
a \circ c &: x \mapsto (x_0, x_2, x_4, \dots) \mapsto (x_0, 0, x_2, 0, x_4, 0, \dots) \\
b \circ d &: x \mapsto (x_1, x_3, x_5, \dots) \mapsto (0, x_1, 0, x_3, 0, x_5, 0, \dots)
\end{aligned}$$

Somit gilt $ca = db = \mathrm{id}_V$ und $cb = da = 0$ sowie $ac + bd = \mathrm{id}_V$.
Der Isomorphismus (2) folgt sofort aus (1):

$$f : R^1 \to R^2 : r \mapsto \begin{pmatrix} cr \\ dr \end{pmatrix}, \quad g : R^2 \to R^1 : \begin{pmatrix} s \\ t \end{pmatrix} \mapsto as + bt.$$

(3) Für alle $k \in \mathbb{N}$ gilt demnach $R^{1+k} \cong R^1 \times R^k \cong R^2 \times R^k \cong R^{2+k}$.
Dank Transitivität folgt $R^1 \cong R^n$ und $R^m \cong R^n$ für alle $m, n \in \mathbb{N}_{\geq 1}$. QED

Ein mahnendes Gegenbeispiel

Dieses Gegenbeispiel ist zunächst erschreckend, doch auch heilsam.
Es ist insgesamt nicht so kompliziert wie es auf den ersten Blick scheint, sondern eher sehr konkret und durchsichtig und auch recht natürlich:

🙂 Für Polynome gilt $a : P(X) \mapsto P(X^2)$ und $b : P(X) \mapsto XP(X^2)$ sowie $(c, d) : P \mapsto (P_0, P_1)$ mit $P = P_0(X^2) + XP_1(X^2)$, siehe I2M: Dies entspricht der Zerlegung in geraden und ungeraden Anteil.

🙂 Der Raum $K^{(\mathbb{N})} = K[X]$ der Polynome ist klein und übersichtlich. Die Konstruktion gelingt wörtlich genauso mit dem Folgenraum $K^{\mathbb{N}}$. Alle Formeln und Rechnungen sind für $K^{\mathbb{N}}$ genau dieselben.

Ein mahnendes Gegenbeispiel

Aufgabe: Über einem *kommutativen* Ring R mit $1 \neq 0$ hingegen ist diese Pathologie unmöglich: Hier gilt $R^1 \ncong R^n$ für alle $n \in \mathbb{N}_{\geq 2}$.

Lösung: Je zwei Elemente $a, b \in R^1$ sind R–linear abhängig gemäß

$$a(-b) + ba = 0.$$

In R^n hingegen gibt es R–linear unabhängige Elemente $e_1, e_2, \dots$.

🙂 Wir werden in Kapitel L die Determinante konstruieren und als Werkzeug nutzen lernen. Damit können wir beweisen, dass jeder kommutative Ring $R \neq \{0\}$ die Invarianz der Dimension erfüllt (L3C): Für alle $m \neq n$ in $\mathbb{N}$ gilt $R^m \ncong R^n$. Die obige Aufgabe zu $R^1 \ncong R^n$ für $n \geq 2$ ist eine einfache und erhellende Illustration hierzu.

Bild und Kern einer Matrix in reduzierter Zeilenstufenform

J149

$$\left[\begin{array}{ccccc|c|c} 1 & -2 & 0 & 3 & 0 & -1 & 0 \\ 0 & 0 & 1 & 7 & 0 & 4 & 5 \\ 0 & 0 & 0 & 0 & 1 & 9 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{array}\right] \xrightarrow[\text{Merkregel}]{\text{graphische}} \left[\begin{array}{cc|cc|c|c} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 9 \end{array}\right]$$

A b b' — v_2 v_4 w

Aufgabe: Gegeben ist $A \in \mathbb{R}^{4\times 5}$ in reduzierter Zeilenstufenform.
(1) Explizieren Sie Basen für das Bild $\mathrm{im}(A)$ und den Kern $\ker(A)$.
(2) Bestimmen Sie die Lösungsmenge $L(A,b) = \{\, x \in \mathbb{R}^n \mid Ax = b \,\}$.

Lösung: (1) Aus den obigen Daten lesen wir ab:

$$\mathrm{im}(A) = \langle\, e_1, e_2, e_3 \,\rangle^!_{\mathbb{R}} \leq \mathbb{R}^4 \quad \text{und} \quad \ker(A) = \langle\, v_2, v_4 \,\rangle^!_{\mathbb{R}} \leq \mathbb{R}^5$$

Die Familie (v_2, v_4) ist gestuft, also linear unabhängig in $\mathbb{R}^5$.

(2) Es gilt $b = Aw \in \mathrm{im}(A)$, also $L(A,b) = w + \ker(A) = w + v_2\mathbb{R} + v_4\mathbb{R}$, siehe Satz I1R. Zum Kontrast: Es gilt $b' \notin \mathrm{im}(A)$, also $L(A,b') = \emptyset$,

Bild und Kern einer Matrix in reduzierter Zeilenstufenform

J150

$$s = (\ 2,\ 3,\ 5,\ 8\ ) \qquad A = \begin{bmatrix} 0 & 1 & 0 & * & 0 & * & * & 0 & * & * \\ 0 & 0 & 1 & * & 0 & * & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 1 & * & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Aufgabe: Gegeben sei $A \in R^{m\times n}$ in reduzierter Zeilenstufenform mit Stufen $s = (s_1 < \cdots < s_r)$. Nennen Sie eine Basis für Bild und Kern.

Lösung: (1) Die Pivotspalten sind eine Basis des Bildraums:

$$\mathrm{im}(A) = \big\langle\, Ae_j \;\big|\; j \in J = \{s_1, \ldots, s_r\} \,\big\rangle^!_R = \langle\, e_1, \ldots, e_r \,\rangle^!_R \leq R^m$$

(2) Die verbleibenden freien Spalten induzieren eine Basis des Kerns:

$$\ker(A) = \big\langle\, v_j \;\big|\; j \in K = \{1, \ldots, n\} \smallsetminus \{s_1, \ldots, s_r\} \,\big\rangle^!_R \leq R^n$$

Dabei gilt $v_j := \sum_{i=1}^r e_{s_i} a_{ij} - e_j$, wie im vorigen Beispiel illustriert.
Die Familie $(v_j)_{j\in K}$ ist gestuft, also R–linear unabhängig (J1F).

Bild und Kern einer Matrix in reduzierter Zeilenstufenform

J151
Erläuterung

☺ Das ist ein eleganter und universell einsetzbarer Algorithmus! Über jedem Divisionsring R überführt der Gauß–Algorithmus B2C jede Matrix B in reduzierte Zeilenstufenform A. Daraus lesen wir Basen für Bild $\mathrm{im}(A)$ und Kern $\ker(A)$ ab, wie hier ausgeführt.

Aufgabe: Beweisen Sie, dass die jeweils für Bild und Kern angegebenen Vektoren tatsächlich eine Basis bilden.

Lösung: (1) Die Pivotspalten sind eine Basis des Bildraums:

$$\mathrm{im}(A) = \big\langle\, Ae_j \;\big|\; j \in J = \{s_1, \ldots, s_r\} \,\big\rangle^!_R = \langle\, e_1, \ldots, e_r \,\rangle^!_R \leq R^m$$

(1a) Für jede Zeile $i = 1, \ldots, r$ und die zugehörige Pivotspalte $j = s_i$ gilt $e_i = Ae_j \in \mathrm{im}(A)$ dank RZSF. Daraus folgt $\mathrm{im}(A) \supseteq \langle\, e_1, \ldots, e_r \,\rangle_R$.
(1b) Die umgekehrte Inklusion $\mathrm{im}(A) \subseteq \langle\, e_1, \ldots, e_r \,\rangle_R$ ist klar, denn alle Spaltenvektoren von A haben Träger in $\{1, \ldots, r\}$.
(1c) Die Vektoren $Ae_j = e_i$ in R^m sind R–linear unabhängig (J1F). Somit haben wir tatsächlich eine Basis von $\mathrm{im}(A)$ vorliegen!

Bild und Kern einer Matrix in reduzierter Zeilenstufenform

J152
Erläuterung

(2) Die verbleibenden freien Spalten induzieren eine Basis des Kerns:

$$\ker(A) = \big\langle\, v_j \;\big|\; j \in K = \{1, \ldots, n\} \smallsetminus \{s_1, \ldots, s_r\} \,\big\rangle^!_R \leq R^n$$

(2a) Zunächst liegt jeder Vektor $v_j := \sum_{i=1}^r e_{s_i} a_{ij} - e_j$ im Kern, denn

$$Av_j = \textstyle\sum_{i=1}^r Ae_{s_i} a_{ij} - Ae_j = \sum_{i=1}^r e_i a_{ij} - \sum_{i=1}^r e_i a_{ij} = 0.$$

(2b) Sei umgekehrt $\lambda \in \ker(A)$. Dazu betrachten wir $\mu \in \ker(A)$ mit

$$\mu = \lambda + \textstyle\sum_{j\in K} v_j \lambda_j.$$

Nach Konstruktion gilt $\mu_j = 0$ für alle $j \in K$, also $\mu = \sum_{j\in J} e_j \mu_j$, sowie

$$0 = A\mu = \textstyle\sum_{j\in J} Ae_j \mu_j = \sum_{i=1}^r e_i \mu_{s_i}.$$

Dank linearer Unabhängigkeit von $e_1, \ldots, e_r$ in R^m folgt $\mu_{s_i} = 0$ für alle $i = 1, \ldots, r$, also $\mu = 0$. Das bedeutet $\lambda = -\sum_{j\in K} v_j \lambda_j \in \langle\, v_j \mid j \in K \,\rangle$.
(2c) Die Familie $(v_j)_{j\in K}$ ist gestuft, also R–linear unabhängig (J1F). Somit haben wir tatsächlich eine Basis von $\ker(A)$ vorliegen!

Bild und Kern und Dimensionsformel

Satz J1P: Bild und Kern und Dimensionsformel

Gegeben sei die Matrix $B \in R^{m\times n}$ und eine Transformation $S \in \mathrm{GL}_m R$ in reduzierte Zeilenstufenform $A = SB$ mit Stufen $s = (s_1 < \cdots < s_r)$.

(1) Die Pivotspalten $j = s_1, \ldots, s_r$ sind eine Basis des Bildraums:

$$\mathrm{im}(A) = \langle\, Ae_j \mid j \in J = \{s_1, \ldots, s_r\} \,\rangle^!_R = \langle\, e_1, \ldots, e_r \,\rangle^!_R \qquad \leq R^m$$
$$\mathrm{im}(B) = \langle\, Be_j \mid j \in J = \{s_1, \ldots, s_r\} \,\rangle^!_R = \langle\, S^{-1}e_1, \ldots, S^{-1}e_r \,\rangle^!_R \leq R^m$$

(2) Die verbleibenden freien Spalten induzieren eine Basis des Kerns:

$$\ker(A) = \ker(B) = \langle\, v_j \mid j \in K = \{1, \ldots, n\} \smallsetminus \{s_1, \ldots, s_r\} \,\rangle^!_R \leq R^n$$

Dabei gilt $v_j := \sum_{i=1}^r e_{s_i} a_{ij} - e_j$, wie zuvor erklärt.

(3) Insbesondere gilt $\dim_R \mathrm{im}(B) = r$ und $\dim_R \ker(B) = n - r$.

Unabhängig vom Rang r folgt daraus die Dimensionsformel:

$$\boxed{\dim_R \ker(B) + \dim_R \mathrm{im}(B) = n}$$

Bild und Kern und Dimensionsformel

Aufgabe: Beweisen Sie, dass die jeweils für Bild und Kern angegebenen Vektoren tatsächlich eine Basis bilden.

Lösung: Die Basen für $\mathrm{im}(A)$ und $\ker(A)$ haben wir in der vorigen Aufgabe explizit ausgeführt und alle Behauptungen nachgewiesen.

(1) Wir haben $A = SB$, also $B = S^{-1}A$ und $\mathrm{im}(B) = S^{-1}\,\mathrm{im}(A)$. Dank $\mathrm{im}(A) = \langle\, e_1, \ldots, e_r \,\rangle^!_R$ folgt $\mathrm{im}(B) = \langle\, S^{-1}e_1, \ldots, S^{-1}e_r \,\rangle^!_R$. Wir setzen $e_i = Ae_{s_i}$ ein und erhalten $\mathrm{im}(B) = \langle\, Be_{s_1}, \ldots, Be_{s_r} \,\rangle^!_R$.

(2) Die Matrizen $A = SB$ und $B = S^{-1}A$ haben denselben Kern.

(3) Die Dimensionen folgen aus den expliziten Basen in (1) und (2).

🙂 Da wir in (3) von Dimension sprechen, setzen wir stillschweigend voraus, dass unser Ring R die Invarianz der Dimension erfüllt (J1L). Dies gilt insb. für alle Divisionsringe und alle kommutativen Ringe.

🙂 Über jedem Divisionsring R überführt der Gauß–Algorithmus B2C jede Matrix B in reduzierte Zeilenstufenform A. Daraus lesen wir Basen für Bild $\mathrm{im}(A)$ und Kern $\ker(A)$ ab, wie hier ausgeführt.

Bild und Kern und Dimensionsformel

Aufgabe: Vorgelegt sei eine Matrix $A \in \mathbb{R}^{5\times 9}$ von folgender Gestalt:

$$\begin{bmatrix} * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Was können Sie über die Dimension von Bild und Kern aussagen?

Lösung: Für jede Matrix $A \in \mathbb{R}^{m\times n}$ gilt die Dimensionsformel

$$\dim_{\mathbb{R}} \ker(A) + \dim_{\mathbb{R}} \mathrm{im}(A) = n.$$

Hier haben wir $0 \leq \dim_{\mathbb{R}} \mathrm{im}(A) \leq 4$ und somit $5 \leq \dim_{\mathbb{R}} \ker(A) \leq 9$.

Alle fünf Möglichkeiten $(0,9), (1,8), (2,7), (3,6), (4,5)$ kommen vor:

$$\begin{bmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \end{bmatrix}$$

Bild und Kern und Dimensionsformel

Aufgabe: Vorgelegt sei eine Matrix $A \in \mathbb{R}^{5\times 9}$ von folgender Gestalt:

$$\begin{bmatrix} * & * & * & * & * & * & * & 1 & 0 \\ * & * & * & * & * & * & * & 2 & 0 \\ * & * & * & * & * & * & * & 3 & 3 \\ * & * & * & * & * & * & * & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

Was können Sie über die Dimension von Bild und Kern aussagen?

Lösung: Hier gilt $2 \leq \dim_{\mathbb{R}} \mathrm{im}(A) \leq 5$ und somit $4 \leq \dim_{\mathbb{R}} \ker(A) \leq 7$. Alle vier Möglichkeiten $(2,7), (3,6), (4,5), (5,4)$ treten tatsächlich auf.

Aufgabe: Welche Dimension hat der Kern der $\mathbb{R}$–linearen Abbildung

$$f : \mathbb{R}^{100} \to \mathbb{R} : (x_1, \ldots, x_{100}) \mapsto x_1 + \cdots + x_{100} \ ?$$

Lösung: Es gilt $\dim_{\mathbb{R}} \mathrm{im}(f) = 1$, also $\dim_{\mathbb{R}} \ker(f) = 99$. Explizit ist die Matrix $A = (1, \ldots, 1)$ in RZSF. Eine Basis des Kerns ist $(e_1 - e_j)_{j=2}^{100}$.

Extremale Charakterisierung von Basen

Jeder R–lineare Raum besitzt ein Erzeugendensystem, etwa $(v)_{v\in V}$.
Eine Basis existiert jedoch nicht immer, siehe $\mathbb{Z}/2$ über $\mathbb{Z}$ (J1B).
Wir wollen nun zeigen: Jeder Vektorraum besitzt eine Basis.

Satz J2A: extremale Charakterisierung einer Basis

Sei V ein Vektorraum über dem Divisionsring R.
Sei $(b_i)_{i\in K}$ ein Erzeugendensystem und $I \subseteq K$.

Dann sind äquivalent:

1. Die Familie $\mathcal{B} = (b_i)_{i\in I}$ ist eine Basis von V:
   Sie erzeugt V über R und ist linear unabhängig.
2. $\mathcal{B} = (b_i)_{i\in I}$ erzeugt V und ist dabei minimal:
   Keine echte Teilfamilie $(b_i)_{i\in J}$ mit $J \subsetneq I$ erzeugt V.
3. $\mathcal{B} = (b_i)_{i\in I}$ ist linear unabhängig in V und dabei maximal:
   Jede echte Oberfamilie $(b_i)_{i\in J}$ mit $I \subsetneq J \subseteq K$ ist linear abhängig.

⚠ Minimal / maximal gilt hier bezüglich Inklusion, nicht Elementezahl.
Der Satz ist genau so gemeint, wie er hier sorgsam ausformuliert ist.

Extremale Charakterisierung von Basen

Dieser Satz fordert als Eingabedatum ein Erzeugendensystem von V über R. Meist gibt die konkrete Anwendung ein Erzeugendensystem vor. Wenn uns dazu partout nichts Besseres einfällt, so nehmen wir notfalls die gesamte Menge V als Erzeugendensystem, also die Familie $(v)_{v\in V}$.

🙂 Die Begriffe *minimal* und *maximal* sind hier im Sinne der Inklusion zu verstehen, so wie in geordneten Mengen (Posets) üblich, siehe F1I; genau hierzu haben wir Begriffe und Beispiele in Kapitel F vorbereitet.

⚠ Ich weise vorsorglich auf ein verbreitetes Missverständnis hin:

Damit ist nicht gemeint, dass die Elementezahl minimal / maximal wäre! Das spielt in diesem Satz keine Rolle, es hat genau genommen auch gar keinen rechten Sinn, denn die Mengen dürfen unendlich sein.

Um jedes Missverständnis möglichst auszuschließen, habe ich in der zweiten Zeile jeweils explizit ausformuliert, was *minimal* und *maximal* hier für Teilfamilien und Oberfamilien bedeuten. Möge es nützen!

Basis als maximale linear unabhängige Familie

1. Die Familie $\mathcal{B} = (b_i)_{i\in I}$ ist eine Basis von V:
   Sie erzeugt V über R und ist linear unabhängig.
3. $\mathcal{B} = (b_i)_{i\in I}$ ist linear unabhängig in V und dabei maximal:
   Jede echte Oberfamilie $(b_i)_{i\in J}$ mit $I \subsetneq J \subseteq K$ ist linear abhängig.

Beweis: „(1) ⇒ (3)“: Wir zeigen Maximalität.

Für jeden Index $j \in J \smallsetminus I$ gilt $b_j \in \langle\, b_i \mid i \in I \,\rangle_R$, denn $\mathcal{B}$ ist eine Basis.
Wir haben also $b_j = \sum_{i\in I} b_i\lambda_i$ mit $\lambda \in R^{(I)}$, und somit liefert
$b_j - \sum_{i\in I} b_i\lambda_i = 0$ eine nicht-triviale Relation für $(b_i)_{i\in J}$.

„(3) ⇒ (1)“: Aus (3) und $k \in K$ folgern wir $b_k \in \langle\, b_i \mid i \in I \,\rangle_R$;
daraus folgt sofort $\langle\, b_i \mid i \in I \,\rangle_R \supseteq \langle\, b_k \mid k \in K \,\rangle_R = V$, also gilt (1).

Gäbe es $b_k \in V \smallsetminus \langle\, b_i \mid i \in I \,\rangle_R$, so wäre die Oberfamilie $(b_i)_{i\in J}$ mit
$J = I \sqcup \{k\}$ linear unabhängig: Hierzu sei $\lambda \in R^{(J)}$ und $\sum_{i\in J} b_i\lambda_i = 0$.
Wäre dabei $\lambda_k \neq 0$, so hätten wir $b_k = \sum_{i\in I} b_i(-\lambda_i\lambda_k^{-1}) \in \langle\, b_i \mid i \in I \,\rangle_R$.
Somit muss $\lambda_k = 0$ gelten, und das heißt $\sum_{i\in I} b_i\lambda_i = 0$.
Aber $\mathcal{B} = (b_i)_{i\in I}$ ist linear unabhängig, also $\lambda = 0$.

Basis als minimales Erzeugendensystem

1. Die Familie $\mathcal{B} = (b_i)_{i\in I}$ ist eine Basis von V:
   Sie erzeugt V über R und ist linear unabhängig.
2. $\mathcal{B} = (b_i)_{i\in I}$ erzeugt V und ist dabei minimal:
   Keine echte Teilfamilie $(b_i)_{i\in J}$ mit $J \subsetneq I$ erzeugt V.

Beweis: „(1) ⇒ (2)“: Wir zeigen Minimalität;
für jeden Index $k \in I \smallsetminus J$ gilt $b_k \notin \langle\, b_i \mid i \in J \,\rangle_R$.
Wäre $b_k \in \langle\, b_i \mid i \in J \,\rangle_R$, also $b_k = \sum_{i\in J} b_i\lambda_i$ mit $\lambda \in R^{(J)}$,
dann liefert $b_k - \sum_{i\in J} b_i\lambda_i = 0$ eine nicht-triviale Relation für $(b_i)_{i\in I}$.
Das widerspricht der linearen Unabhängigkeit der Familie $\mathcal{B} = (b_i)_{i\in I}$.

„(2) ⇒ (1)“: Wir zeigen lineare Unabhängigkeit von $\mathcal{B} = (b_i)_{i\in I}$.
Sei $\lambda \in R^{(I)}$ und $\sum_{i\in I} b_i\lambda_i = 0$. Angenommen, $\lambda_k \neq 0$ für ein $k \in I$.
Wir setzen dann $J = I \smallsetminus \{k\}$ und erhalten $b_k = \sum_{i\in J} b_i(-\lambda_i\lambda_k^{-1})$.
In jeder Linearkombination von $(b_i)_{i\in I}$ können wir b_k so ersetzen.
Also erzeugt auch die echte Teilfamilie $(b_i)_{i\in J}$ immer noch V. QED

⚠ Für „(2) ⇒ (1)“ und „(3) ⇒ (1)“ müssen wir $\lambda_k \in R \smallsetminus \{0\}$ invertieren.
Daher gelingt dieser Beweis tatsächlich nur über einem Divisionsring R.

Satz J2B: Existenz von Basen

Sei V ein Vektorraum über dem Divisionsring R und erzeugt von $(v_i)_{i\in K}$.

(1) **Basisergänzungssatz:** Jede linear unabhängige Familie $(v_i)_{i\in I}$ mit $I \subseteq K$ lässt sich zu einer Basis $(v_i)_{i\in J}$ von V ergänzen mit $I \subseteq J \subseteq K$.

(2) **Basisauswahlsatz:** Jedes Erzeugendensystem $(v_i)_{i\in K}$ enthält eine Basis $(v_i)_{i\in J}$ von V als Teilfamilie mit $\emptyset \subseteq J \subseteq K$.

(3) **Existenzsatz:** In jedem Vektorraum V existiert eine Basis $(v_i)_{i\in J}$.

⚠ Wir setzen voraus, dass R ein Divisionsring ist. Ohne geht es nicht:

Beispiel: Im $\mathbb{Z}$–linearen Raum $\mathbb{Z}$ ist $(5, 6)$ erzeugend und minimal, jedoch keine Basis; hieraus lässt sich keine Basis auswählen.

Beispiel: Im $\mathbb{Z}$–linearen Raum $\mathbb{Z}$ ist (5) linear unabhängig und maximal, jedoch keine Basis; (5) lässt sich nicht zu einer Basis ergänzen.

Beispiel: Der $\mathbb{Z}$–lineare Raum $\mathbb{Z}/2\mathbb{Z}$ ist nicht frei (J1B): Es existiert keine $\mathbb{Z}$–Basis von $\mathbb{Z}/2\mathbb{Z}$.

(1) **Basisergänzungssatz:** Jede linear unabhängige Familie $(v_i)_{i\in I}$ mit $I \subseteq K$ lässt sich zu einer Basis $(v_i)_{i\in J}$ von V ergänzen mit $I \subseteq J \subseteq K$.

Beweis: (1a) Zur Vereinfachung sei K endlich, also V endlich erzeugt. Wir wählen J maximal mit $I \subseteq J \subseteq K$ und $(v_i)_{i\in J}$ linear unabhängig. Dank des vorangegangenen Satzes J2A ist $(v_i)_{i\in J}$ eine Basis von V.

(1b) Falls K unendlich ist, so argumentieren wir entsprechend. Wir betrachten das System aller linear unabhängigen Familien:

$$X = \{\, J \mid I \subseteq J \subseteq K \text{ und } (v_i)_{i\in J} \text{ linear unabhängig} \,\}$$

Die geordnete Menge $(X, \subseteq)$ erfüllt die Voraussetzung des Zornschen Lemmas F1V und besitzt somit mindestens ein maximales Element.

(2) Wir setzen $I = \emptyset$ und wählen J wie in (1).

(3) Zu V existiert ein Erzeugendensystem, notfalls $(v)_{v\in V}$. Daraus können wir dank (2) eine Basis auswählen. QED

Die Anwendung des Zornschen Lemmas in (1b) bedarf der Erläuterung. Ganz anschaulich wollen wir linear unabhängige Vektoren hinzufügen, bis wir „schließlich“ eine maximale Familie erreichen. Im endlichen Fall ist das offensichtlich möglich, im unendlichen Fall ist es delikat.

♦ Satz F1V: Lemma von Zorn

Eine geordnete Menge, in der jede Kette eine obere Schranke hat, enthält mindestens ein maximales Element.

Wir wollen dies hier auf die geordnete Menge $(X, \subseteq)$ anwenden. Dazu sei $Y \subseteq X$ eine Kette, das bedeutet, je zwei Elemente $J_1, J_2 \in Y$ sind vergleichbar, es gilt also $J_1 \subseteq J_2$ oder $J_2 \subseteq J_1$. Wir setzen $J := \bigcup Y$. Es gilt $I \subseteq J \subseteq K$ und die Familie $(v_i)_{i\in J}$ ist linear unabhängig:

Hierzu betrachten wir eine Relation, also eine Linearkombination zu Null, $0 = v_{i_1}\lambda_1 + \cdots + v_{i_n}\lambda_n$ mit $i_1, \ldots, i_n \in J$ und $\lambda_1, \ldots, \lambda_n \in R$. Zu jedem Index i_k existiert $J_k \in Y$ mit $i_k \in J_k$ Da Y eine Kette ist, können wir so sortieren, dass $J_1 \subseteq \cdots \subseteq J_n$ gilt. Aber die Familie $(v_i)_{i\in J_n}$ ist linear unabhängig! Also folgt $\lambda_1 = \cdots = \lambda_n = 0$.

In der geordneten Menge $(X, \subseteq)$ hat demnach jede Kette $Y \subseteq X$ eine obere Schranke $J = \bigcup Y$. Dank Zorns Lemma F1V enthält $(X, \subseteq)$ mindestens ein maximales Element. Genau dies wollten wir zeigen.

☹ Zugegeben, diese Rechnung ist einfach, aber nicht erhellend. Wir prüfen die Voraussetzung von Zorns Lemma, das geht leicht, doch die Schlussfolgerung lässt uns etwas enttäuscht zurück.

🙂 Sehen wir es positiv: Dies beweist die Existenz einer Basis, auch wenn die Beweismethode alles andere als konstruktiv ist. Eine schwache Aussage ist besser als gar keine Aussage.

Bemerkung: Meist gibt die Anwendung ein Erzeugendensystem vor, so wie in (1) erklärt. Wenn dabei K endlich ist, so sind wir fein raus. Für Aussage (3) jedoch müssen wir ein Erzeugendensystem wählen. Wenn uns dazu partout nichts Besseres einfällt, so nehmen wir notfalls die gesamte Menge V als Erzeugendensystem, also die Familie $(v)_{v\in V}$.

Anwendung: die Dimension von Vektorräumen

Korollar J2C: die Dimension eines Vektorraumes

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(1) Der Existenzsatz J2B garantiert:
Jeder Vektorraum V über R erlaubt eine Basis $\mathcal{B} = (b_i)_{i \in I}$.

(2) Die Invarianz der Dimension J1K besagt:
Jede weitere Basis von V hat dieselbe Mächtigkeit.

Wir können daher die **Dimension** von V definieren durch

$$\boxed{\dim_R(V) := \sharp I.}$$

Die Dimension ist wohldefiniert: Der Wert existiert und ist eindeutig.

🙂 Die Dimension $\dim_R(V)$ eines linearen Raums V über einem Divisionsring R ist ein wichtiges Hilfsmittel in der Linearen Algebra und all ihren Anwendungen. Es lohnt sich daher, diesen zentralen Begriff und die nötigen Werkzeuge gründlich zu verstehen.

Anwendung: die Dimension von Vektorräumen

Übung: Welche Dimension hat $\mathbb{Q}[\sqrt{2}]$ über $\mathbb{Q}$? Nennen Sie eine Basis!

Lösung: Wir betrachten $\mathbb{Q}[\sqrt{2}]$ als den kleinsten Teilring in $\mathbb{R}$, der $\mathbb{Q}$ und $\sqrt{2}$ enthält. Dies führt zur Menge $\mathbb{Q}[\sqrt{2}] = \{\, x + \sqrt{2}y \mid x, y \in \mathbb{Q} \,\}$.
Somit ist $(1, \sqrt{2})$ ein Erzeugendensystem. Diese Familie ist zudem linear unabhängig: Aus $x, y \in \mathbb{Q}$ und $x + \sqrt{2}y = 0$ folgt $x = y = 0$, dank Irrationalität von $\sqrt{2}$ (A1F). Demnach ist $(1, \sqrt{2})$ linear unabhängig, also eine Basis. Daraus lesen wir die Dimension ab: $\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = 2$.

🙂 Genau so wird die Dimension $\dim_R(V)$ definiert und in vielen typischen Fällen auch direkt berechnet: Wir finden eine geeignete Familie $(b_i)_{i \in I}$ von V, weisen für $(b_i)_{i \in I}$ lineare Unabhängigkeit und Erzeugung von V nach, und schließen so $\dim_R(V) = \sharp I$.

🙂 Es genügt, dieses Verfahren für *eine* Basis zu durchlaufen: Jede andere Basis ist genauso gut und liefert dasselbe Ergebnis!

Basis und Dimension von $\mathbb{R}$ über $\mathbb{Q}$

Beispiel J2D: Basis von $\mathbb{R}$ über $\mathbb{Q}$

Zum Raum $\mathbb{R}$ über $\mathbb{Q}$ existiert dank Satz J2B eine Basis $\mathcal{B} = (b_i)_{i \in I}$.

Wir erhalten so die $\mathbb{Q}$–lineare Bijektion

$$\Phi_{\mathcal{B}} : \mathbb{Q}^{(I)} \xrightarrow{\sim} \mathbb{R}.$$

Dabei ist I überabzählbar, denn $\mathbb{Q}^{(\mathbb{N})}$ ist abzählbar (F2P).

Insbesondere gilt

$$\boxed{\dim_{\mathbb{Q}}(\mathbb{R}) = \infty.}$$

Basis und Dimension von $\mathbb{R}$ über $\mathbb{Q}$

☹ Der Beweis des Existenzsatzes J2B nutzt das Zornsche Lemma und ist daher nicht konstruktiv. Er sichert allein die Existenz, mehr nicht.

Niemand hat je eine Basis von $\mathbb{R}$ über $\mathbb{Q}$ gesehen.

🙂 Wir können immerhin eine unendliche, linear unabhängige Familie angeben (J127): Die Familie $(\ln p)_{p \in \mathbb{P}}$ in $\mathbb{R}$ linear unabhängig über $\mathbb{Q}$.

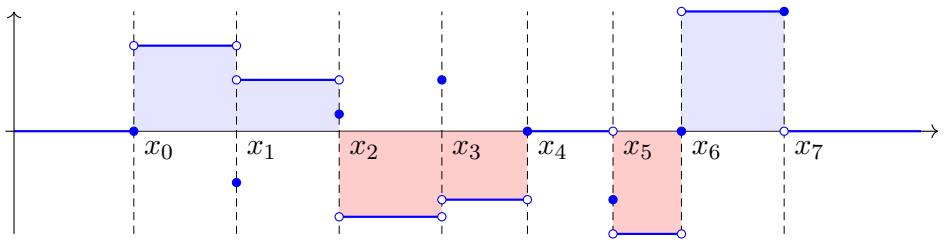
Das ist sehr konkret und der Beweis ist lehrreich!

🙂 Genau genommen ist $\mathbb{R}$ über $\mathbb{Q}$ nicht nur unendlich-dimensional, die Dimension ist wie hier zu sehen sogar überabzählbar unendlich.

Auf diese genauere Sichtweise gehe ich hier nicht näher ein.

Illustration: Treppenfunktionen

J213



♦ Satz I1W: eindimensionale Treppenfunktionen

Die Treppenfunktionen $T(\mathbb{R},\mathbb{R}) \leq \mathbb{R}^{\mathbb{R}}$ bilden einen $\mathbb{R}$–Untervektorraum. Dieser wird erzeugt von den Indikatorfunktionen $\mathbf{I}_{[a,b]}$ mit $a \leq b$ in $\mathbb{R}$.

Aufgabe: (1) Ist die Familie $(\mathbf{I}_{[a,b]})_{a\leq b}$ eine Basis von $T(\mathbb{R},\mathbb{R})$?
(2) Können Sie aus $(\mathbf{I}_{[a,b]})_{a\leq b}$ eine Basis auswählen? (3) explizit?

Lösung:
(1) Es gelten die Relationen $\mathbf{I}_{[a,c]} = \mathbf{I}_{[a,b]} + \mathbf{I}_{[b,c]} - \mathbf{I}_{[b,b]}$ für $a < b < c$.
Somit ist $(\mathbf{I}_{[a,b]})_{a\leq b}$ ein Erzeugendensystem, aber linear abhängig.

(2) Ja, dank Auswahlsatz J2B. (3) Hier muss man kreativ sein!

Illustration: Treppenfunktionen

J214
Erläuterung

☺ Dies ist eine unendlich-dimensionale, doch konkrete Illustration zu **Erzeugendensystemen** und **linearer Unabhängigkeit** und **Basen**:
Die Familie der Indikatorfunktionen $\mathbf{I}_{[a,b]}$ mit $a \leq b$ in $\mathbb{R}$ erzeugt $T(\mathbb{R},\mathbb{R})$, aber sie ist, wie hier zu sehen, linear abhängig und somit keine Basis.

☺ Dieses Beispiel ist vollkommen realistisch und naturgemäß vertrackt, aber zugleich noch einfach genug, um elementar gelöst zu werden.
Wenn Sie möchten, versuchen Sie es! Sie können daran viel lernen.
Alternativ können Sie später einmal darauf zurückkommen...

☺ In der Analysis sind Treppenfunktionen ein erster wichtiger Schritt zur Integration von Funktionen $f : \mathbb{R} \to \mathbb{R}$ und allgemein $f : \mathbb{R}^n \to \mathbb{R}$.
Treppenfunktionen werden dort nur als Werkzeug eingesetzt, aber darüber hinaus nicht weiter betrachtet. Sie sind jedoch auch eine schöne Illustration und hier sogar selbst Untersuchungsgegenstand.

Illustration: Treppenfunktionen

J215
Erläuterung

Beispiel J2E: eine Basis des Raums der Treppenfunktionen

Aus dem Erzeugendensystem $(\mathbf{I}_{[a,b]})_{a\leq b}$ wählen wir (etwas willkürlich, aber geschickt) die Teilfamilie $(\mathbf{I}_Q)_{Q\in I}$ wobei $I = I_0 \sqcup I_+ \sqcup I_-$ mit $I_0 = \{\, [a,a] \mid a \in \mathbb{R} \,\}$, $I_+ = \{\, [0,a] \mid a \in \mathbb{R}_{>0} \,\}$, $I_- = \{\, [a,0] \mid a \in \mathbb{R}_{<0} \,\}$.

Diese Familie $(\mathbf{I}_Q)_{Q\in I}$ ist eine Basis des Vektorraums $T(\mathbb{R},\mathbb{R}) \leq \mathbb{R}^{\mathbb{R}}$.

Aufgabe: (Wenn Sie gerne knobeln...) Beweisen Sie dies!

Lösung: (1) Die Familie $(\mathbf{I}_Q)_{Q\in I}$ erzeugt $T(\mathbb{R},\mathbb{R})$.
Hierzu genügt es, die Funktionen $\mathbf{I}_{[a,b]}$ für $a \leq b$ in $\mathbb{R}$ zu erzeugen.
Die fehlenden Fälle $0 < a < b$ und $a < 0 < b$ und $a < b < 0$ sind klar:

$$0 < a < b : \quad \mathbf{I}_{[a,b]} = \mathbf{I}_{[0,b]} - \mathbf{I}_{[0,a]} + \mathbf{I}_{[a,a]}$$
$$a < 0 < b : \quad \mathbf{I}_{[a,b]} = \mathbf{I}_{[a,0]} + \mathbf{I}_{[0,b]} - \mathbf{I}_{[0,0]}$$
$$a < b < 0 : \quad \mathbf{I}_{[a,b]} = \mathbf{I}_{[a,0]} - \mathbf{I}_{[b,0]} + \mathbf{I}_{[b,b]}$$

Illustration: Treppenfunktionen

J216
Erläuterung

(2) Die Familie $(\mathbf{I}_Q)_{Q\in I}$ ist linear unabhängig in $T(\mathbb{R},\mathbb{R})$.
Zu jedem $P \in I$ betrachten wir die $\mathbb{R}$–lineare Abbildung φ_P:

$$\varphi_{[0,a]} : T(\mathbb{R},\mathbb{R}) \to \mathbb{R} : f \mapsto \lim_{x\nearrow a} f(x) - \lim_{x\searrow a} f(x)$$
$$\varphi_{[0,0]} : T(\mathbb{R},\mathbb{R}) \to \mathbb{R} : f \mapsto \lim_{x\searrow a} f(x) - \lim_{x\nearrow a} f(x)$$
$$\varphi_{[a,a]} : T(\mathbb{R},\mathbb{R}) \to \mathbb{R} : f \mapsto \begin{cases} f(a) - \varphi_{[a,0]}(f) & \text{falls } a < 0 \text{ und} \\ f(a) - \varphi_{[0,a]}(f) & \text{falls } a > 0, \text{ sonst} \\ f(0) - \sum_{s<0} \varphi_{[s,0]}(f) - \sum_{s>0} \varphi_{[0,s]}(f) \end{cases}$$

Für alle $P, Q \in I$ prüft man nun geduldig nach, dass folgendes gilt:

$$\varphi_P(\mathbf{I}_Q) = \begin{cases} 1 & \text{falls } P = Q, \\ 0 & \text{falls } P \neq Q. \end{cases}$$

Daraus folgt die lineare Unabhängigkeit der Familie $(\mathbf{I}_Q)_{Q\in I}$:
Hierzu sei $\lambda \in \mathbb{R}^{(I)}$ und $0 = \sum_{Q\in I} \lambda_Q \mathbf{I}_Q$. Für jedes $P \in I$ folgt $0 = \varphi_P(\sum_{Q\in I} \lambda_Q \mathbf{I}_Q) = \lambda_P$. Das zeigt $\lambda = 0$.

Ordnung endlicher Vektorräume und endlicher Körper

Satz J2F: Ordnung endlicher Vektorräume

Sei V ein Vektorraum über dem Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
Dann gilt entweder $\sharp V = \infty$ oder $\sharp V = p^d$ mit $d \in \mathbb{N}$.

Beispiel: Es gibt Vektorräume der Ordnung $1, 2, 3, 4, 5$, aber nicht 6.

Beweis: Nach Wahl einer Basis $\mathcal{B} = (b_i)_{i\in I}$ gilt $\Phi_{\mathcal{B}} : \mathbb{F}_p^{(I)} \xrightarrow{\sim} V$.
Im endlichen Falle gilt $\sharp I = d \in \mathbb{N}$ und somit $\sharp V = \sharp \mathbb{F}_p^d = p^d$. QED

Satz J2G: Ordnung endlicher Körper

Sei K ein endlicher Körper (oder Divisionsring).
Dann gilt $\sharp K = p^d$ mit $p \in \mathbb{N}_{\geq 2}$ prim und $d \in \mathbb{N}_{\geq 1}$.

Beispiel: Es gibt Körper der Ordnung $2, 3, 4, 5$, aber nicht 6.

Beweis: Der Körper K enthält seinen charakteristischen Unterkörper $\mathrm{Char}(K) \cong \mathbb{F}_p$ mit $p \in \mathbb{N}_{\geq 2}$ prim (G2H). Hierüber ist K ein Vektorraum.
Dank J2F folgt $\mathbb{F}_p^d \xrightarrow{\sim} K$ und $\sharp K = \sharp \mathbb{F}_p^d = p^d$ mit $d \in \mathbb{N}_{\geq 1}$. QED

Ordnung der Gruppe $\mathrm{GL}_3 \mathbb{F}_2$

☺ Es ist oft lehrreich, neu definierte Objekte zu zählen. Dies zwingt, die Definition genau zu verstehen und klärt so Missverständnisse auf.
Eine weitere schöne Zählaufgabe ist die folgende:

Aufgabe: Wie viele Elemente hat der Ring $\mathbb{F}_2^{3\times 3}$? die Gruppe $\mathrm{GL}_3 \mathbb{F}_2$?

Wenn Sie zufällig eine 3×3–Matrix A mit Nullen und Einsen befüllen, mit welcher Wahrscheinlichkeit ist dann A in $\mathbb{F}_2^{3\times 3}$ invertierbar?

Lösung: (1) Der Matrixring $\mathbb{F}_2^{3\times 3}$ hat genau $2^9 = 512$ Elemente.

(2) In $(\mathbb{F}_2^{3\times 3}, \cdot)$ ist eine Matrix $A \in \mathbb{F}_2^{3\times 3}$ genau dann invertierbar, wenn ihre Spalten a_1, a_2, a_3 eine Basis von $\mathbb{F}_2^3$ über $\mathbb{F}_2$ bilden (B2D).

1. Für $a_1 \in \mathbb{F}_2^3 \smallsetminus \{0\}$ haben wir zunächst $2^3 - 1 = 7$ Möglichkeiten.
2. Für $a_2 \in \mathbb{F}_2^3 \smallsetminus \langle\, a_1 \,\rangle$ bleiben dann $2^3 - 2 = 6$ Möglichkeiten.
3. Für $a_3 \in \mathbb{F}_2^3 \smallsetminus \langle\, a_1, a_2 \,\rangle$ bleiben $2^3 - 2^2 = 4$ Möglichkeiten.

Demnach hat die Gruppe $\mathrm{GL}_3 \mathbb{F}_2$ genau $7 \cdot 6 \cdot 4 = 168$ Elemente.

(3) Die gesuchte Wahrscheinlichkeit ist $168/512 = 0.328125$.

Ordnung der Gruppe $\mathrm{GL}_n \mathbb{F}_q$

Satz J2H: Ordnung der Gruppe $\mathrm{GL}_n \mathbb{F}_q$

(1) Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen. Für alle $n \in \mathbb{N}$ gilt

$$\sharp\, \mathrm{GL}_n \mathbb{F}_q = \prod_{k=0}^{n-1} (q^n - q^k) = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

(2) Die Anzahl der linear unabhängigen Familien $(a_1, \ldots, a_\ell)$ in $\mathbb{F}_q^n$ ist

$$b_q(n, \ell) = \prod_{k=0}^{\ell-1} (q^n - q^k) = (q^n - 1)(q^n - q) \cdots (q^n - q^{\ell-1}).$$

(3) Die Anzahl der ℓ–dimensionalen Unterräume $U \leq \mathbb{F}_q^n$ ist

$$\frac{b_q(n,\ell)}{b_q(\ell,\ell)} = \prod_{k=0}^{\ell-1} \frac{q^n - q^k}{q^\ell - q^k} = \prod_{k=0}^{\ell-1} \frac{q^{n-k} - 1}{q^{\ell-k} - 1} =: \binom{n}{\ell}_q$$

☺ Formel (3) ist eine schöne Anwendung der Klassengleichung E3C.

Ordnung der Gruppe $\mathrm{GL}_n \mathbb{F}_q$

Beweis: (1) Eine Matrix $A \in \mathbb{F}_q^{n\times n}$ ist genau dann invertierbar, wenn ihre Spalten $a_1, \ldots, a_n \in \mathbb{F}_q^n$ eine Basis von $\mathbb{F}_q^n$ über $\mathbb{F}_q$ bilden (B2D).
Somit ist die Formel (1) ein Spezialfall der allgemeinen Formel (2).

(2) Für $B_q(n, \ell) = \{\, (a_1, \ldots, a_\ell) \in (\mathbb{F}_q^n)^\ell \text{ linear unabhängig} \,\}$ zeigen wir:

$$\sharp B_q(n, \ell) = b_q(n, \ell)$$

Wir führen Induktion über ℓ: Die Formel gilt für $\ell = 0$.
Sei nun $\ell \geq 1$ und $(a_1, \ldots, a_{\ell-1})$ in $\mathbb{F}_q^n$ linear unabhängig.
Die möglichen linear unabhängigen Ergänzungen sind

$$a_\ell \in \mathbb{F}_q^n \smallsetminus \langle\, a_1, \ldots, a_{\ell-1} \,\rangle_{\mathbb{F}_q}^{!}.$$

Mit der Induktionsvoraussetzung folgt daraus die behauptete Formel:

$$\sharp B_q(n, \ell) = \sharp B_q(n, \ell-1)(q^n - q^{\ell-1}) = b_q(n, \ell-1)(q^n - q^{\ell-1}) = b_q(n, \ell)$$

(3) Die Anzahl der linear unabhängigen Familien $(a_1, \ldots, a_\ell)$ ist $b_q(n, \ell)$.
Jede erzeugt einen Unterraum $U = \langle\, a_1, \ldots, a_\ell \,\rangle_{\mathbb{F}_q}^{!}$ der Dimension ℓ.
Jeweils $b_q(\ell, \ell)$ davon erzeugen denselben Unterraum U. QED

Wie wahrscheinlich ist Invertierbarkeit?

J221
Ergänzung

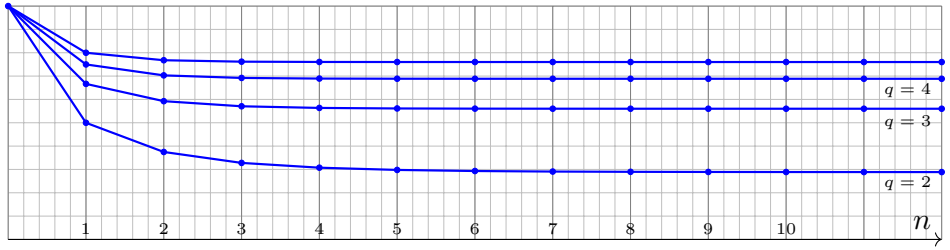
Aufgabe: Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen und $n \in \mathbb{N}$. Sie wählen zufällig (gleichverteilt) eine Matrix $A \in \mathbb{F}_q^{n\times n}$. Mit welcher Wahrscheinlichkeit ist A invertierbar? Für große q? Für große n?

Lösung: (1) Es gibt q^{n^2} Matrizen, die invertierbaren bilden den Anteil

$$\varphi(q,n) = \frac{\sharp\,\mathrm{GL}_n\,\mathbb{F}_q}{\sharp\,\mathbb{F}_q^{n\times n}} = \prod_{k=0}^{n-1} \frac{q^n - q^k}{q^n} = (1-q^{-1})(1-q^{-2})\dots(1-q^{-n}).$$

(2) Für $q \to \infty$ erhalten wir $\varphi(q,n) \to 1$. Über einem großen endlichen Körper $\mathbb{F}_q$ ist eine zufällige Matrix also „nahezu sicher“ invertierbar.

(3) Bei festem q konvergiert $\varphi(q,n)$ für $n \to \infty$ sehr schnell:



Wie wahrscheinlich ist Invertierbarkeit?

J222
Ergänzung

🙂 Solche Zahlen(bei)spiele geben uns eine hilfreiche Anschauung, wie häufig invertierbare Matrizen sind. Ebenso können wir fragen, mit welcher Wkt k Vektoren linear unabhängig sind, oder ähnliches.

Wir stellen erstaunt fest, dass die invertierbaren Matrizen gar nicht selten sind, wie man vielleicht vermuten könnte, sondern die Mehrheit.

Anschauliche Überschlagsrechnung: Für große q vernachlässigen wir die Faktoren $(1-q^{-2}),\dots,(1-q^{-n})$, denn sie liegen recht nahe bei 1.

Der Anteil der invertierbaren Matrizen ist dann

$$\frac{\sharp\,\mathrm{GL}_n\,\mathbb{F}_q}{\sharp\,\mathbb{F}_q^{n\times n}} = (1-q^{-1})(1-q^{-2})\dots(1-q^{-n}) \lessapprox (1-q^{-1}).$$

Im Beispiel $q = 11$ finden wir $0.900832 < \varphi(q,n) \le 10/11 < 0.909091$. Die Schätzung ist bereits auf 1% genau, was uns hier genügen soll.

🙂 Der Anteil der invertierbaren Matrizen in $\mathbb{F}_q^{n\times n}$ ist kaum geringer als der Anteil der invertierbaren Skalare in $\mathbb{F}_q$, also $1 - 1/q$.

Der kuriose Grenzwert $q \searrow 1$

J223
Ergänzung

Aufgabe: (0) Zu $q \in \mathbb{R}_{>1}$ und $n,k \in \mathbb{N}$ setzen wir

$$[n]_q := \frac{q^n - 1}{q-1} = 1 + q + \dots + q^{n-1},$$
$$[n]_q! := [n]_q \cdot [n-1]_q \cdots [3]_q \cdot [2]_q \cdot [1]_q.$$

(1) Damit erhalten wir die Darstellung:

$$\binom{n}{k}_q := \frac{[n]_q!}{[n-k]_q!\,[k]_q!} = \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1} = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}.$$

(2) Ist $\mathbb{F}_q$ ein endlicher Körper mit q Elementen, so ist $\binom{n}{k}_q$ die Anzahl der k–dimensionalen Unterräume $U \le \mathbb{F}_q^n$. Was erhalten Sie für $q \searrow 1$?

Lösung: (1) Wir setzen (0) ein und formen dies sorgsam um.
(2) Im Grenzwert $q \to 1$ finden wir $[n]_q \to n$ und $[n]_q! \to n!$, also

$$\binom{n}{k}_q = \frac{[n]_q!}{[n-k]_q!\,[k]_q!} \;\to\; \frac{n!}{(n-k)!\,k!} = \binom{n}{k}.$$

Der kuriose Grenzwert $q \searrow 1$

J224
Ergänzung

🙂 Die linke Seite ist die Anzahl k–dimensionaler Unterräume $U \le \mathbb{F}_q^n$. Die rechte Seite ist der übliche Binomialkoeffizient! Er gibt die Anzahl der k–elementigen Teilmengen in einer Menge von n Elementen (E2I).

Natürlich ist der Grenzwert für $q \searrow 1$ zunächst nur numerisch.
Die geometrische Interpretation als Anzahl der k–dimensionalen Teilräume in $\mathbb{F}_q^n$ gilt ja nur für $q = 2,3,4,5,7,8,9,11,13,16,\dots$.
Dennoch ist es bemerkenswert, dass wir für den Grenzwert $\binom{n}{k}$ eine ganz ähnliche Interpretation bereits aus einem anderen Kontext kennen!

Es gibt zahlreiche weitere solcher kombinatorisch-numerischer Zufälle. Diese Phänomene fasst man provokativ unter dem Schlagwort „der Körper mit einem Element“ zusammen: Natürlich hat jeder Körper $\mathbb{F}_q$ mindestens zwei Elemente, da $0 \neq 1$, aber der Grenzwert $q \searrow 1$ ist dennoch faszinierend und lädt zu interessanten Spekulationen ein.

🙂 Für uns ist es vor allem eine schöne numerische Illustration. Das konkrete Abzählen hilft dem Verständnis und der Intuition.

Invarianz der Dimension

☺ Analog zur Invarianz der Elementezahl E1H gilt für die Dimension:

Korollar J2I: Invarianz der Dimension

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Vorgelegt sei eine lineare Abbildung $f : U \to V$ zwischen Vektorräumen über R.

1. Ist $f : U \xrightarrow{\sim} V$ bijektiv, so folgt $\dim U = \dim V$.
2. Ist $f : U \twoheadrightarrow V$ surjektiv, so folgt $\dim U \geq \dim V$.
   Gilt zudem $\dim U \leq \dim V < \infty$, so ist f bijektiv.
3. Ist $f : U \hookrightarrow V$ injektiv, so folgt $\dim U \leq \dim V$.
   Gilt zudem $\infty > \dim U \geq \dim V$, so ist f bijektiv.

$$\begin{array}{ccc} U & \xrightarrow{f} & V \\ {\scriptstyle\cong}\uparrow{\scriptstyle\Phi_{\mathcal{U}}} & & {\scriptstyle\cong}\uparrow{\scriptstyle\Phi_{\mathcal{V}}} \\ R^n & \xrightarrow{g} & R^m \end{array}$$

Per Kontraposition folgt aus (3) analog zum Schubfachprinzip E1I:

4. Gilt $\dim U > \dim V$, so ist $f : U \to V$ nicht injektiv:
   Es existiert $u \neq 0$ in U mit $f(u) = 0$ in V.

Beispiel: Für $A \in R^{m \times n}$ mit $m < n$ hat $Ax = 0$ nicht-triviale Lösungen.

Invarianz der Dimension

☺ Als lineares Gleichungssystem $Ax = 0$ gelesen: Gibt es mehr Variablen als Gleichungen, so existieren nicht-triviale Lösungen.

☺ Gibt es umgekehrt mehr Gleichungen als Variablen, so ist die Gleichung $Ax = b$ für manche rechte Seiten b nicht lösbar.

☺ Dies wissen Sie bereits vor und unabhängig von jeder Rechnung! Das ist oft nützlich, zur Prognose oder Prüfung konkreter Rechnungen.

Beweis: Zu U und V existieren Basen $\mathcal{U}$ und $\mathcal{V}$ dank Satz J2B.
So erhalten wir Isomorphismen $\Phi_{\mathcal{U}} : R^{(I)} \xrightarrow{\sim} U$ und $\Phi_{\mathcal{V}} : R^{(J)} \xrightarrow{\sim} V$ sowie die Dimensionen $\dim_R(U) = \sharp I$ und $\dim_R(V) = \sharp J$.

Jede lineare Abbildung $f : U \to V$ definiert $g = \Phi_{\mathcal{V}} \circ f \circ \Phi_{\mathcal{U}}^{-1}$.
Genau dann ist $g : R^{(I)} \to R^{(J)}$ sur/in/bijektiv, wenn $f : U \to V$ dies ist.

Für $g : R^{(I)} \to R^{(J)}$ nutzen wir nun die Invarianz der Dimension (J1N).

Im endlichen Fall können wir g zudem als Matrix $A \in R^{m \times n}$ darstellen, den Gauß–Algorithmus anwenden und den Rang nutzen (B2D). QED

Klassifikation endlich-dimensionaler Vektorräume

Satz J2J: Klassifikation endlich-dimensionaler Vektorräume

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Zwei endlich-dimensionale Vektorräume U und V über R sind genau dann isomorph, wenn sie dieselbe Dimension haben.

Beweis: Nach Wahl von Basen (J2B) haben wir:

$$\begin{array}{ccc} U & \dashrightarrow^{f} & V \\ {\scriptstyle\cong}\uparrow{\scriptstyle\Phi_{\mathcal{U}}} & & {\scriptstyle\cong}\uparrow{\scriptstyle\Phi_{\mathcal{V}}} \\ R^n & \dashrightarrow^{g} & R^m \end{array}$$

☺ Die Lineare Algebra mag Ihnen zwar anfangs abstrakt erscheinen, doch die betrachteten Objekte sind schließlich einfach und übersichtlich! Das Isomorphieproblem für Vektorräume über R wird durch eine einzige Zahl gelöst: die Dimension (als Kardinalität einer / jeder Basis).

Klassifikation endlich-dimensionaler Vektorräume

Aus Satz E1H kennen wir die wichtigste Invariante der Mathematik: Die Elementezahl ändert sich nicht unter Anwendung von Bijektionen!

Hier bestaunen wir nun die wichtigste Invariante der Linearen Algebra: Die R–Dimension ändert sich nicht unter R–linearen Bijektionen!

Wir nutzen dazu insb. alle Techniken zur Elementezahl aus Kapitel E, denn die Dimension ist nichts anderes als die Elementezahl einer Basis.

Allgemein versteht die Mathematik unter einer **Invariante** folgendes: Jedem der betrachteten Objekte (hier: R–Vektorräume) wird eine Größe zugeordnet (hier: ihre R–Dimension); diese Größe ändert sich nicht unter den betrachteten Umformungen (hier: R–Isomorphismen).

Invarianten sind ein wichtiges Hilfsmittel bei Klassifikationsproblemen: Objekte mit unterschiedlichen Invarianten sind wesentlich verschieden. Manchmal gilt sogar die Umkehrung, und Objekte mit gleichen Werten unter der Invariante lassen sich ineinander umformen. Wir sprechen dann von einer **vollständigen Invarianten**. Genau das liegt hier vor!

Dimension von Unterräumen

☺ Auch folgende Eigenschaft ist erfreulich, beruhigend und nützlich.
Aussage und Beweis entsprechen dem Abzählen von Mengen (E2B).

Satz J2K: Dimension von Unterräumen

Sei V ein Vektorraum über dem Divisionsring R.

(1) Für jeden Unterraum $U \leq V$ gilt $\dim_R(U) \leq \dim_R(V)$.

(2) Gilt zudem $\dim_R(U) = \dim_R(V) < \infty$, so folgt $U = V$.

Beweis: Vermöge Satz J2B wählen wir eine Basis $(v_i)_{i\in I}$ von U und ergänzen diese zu einer Basis $(v_j)_{j\in J}$ von V, wobei $I \subseteq J$.

(1) Daraus folgt $\dim_R(U) = \sharp I \leq \sharp J = \dim_R(V)$. (E2B)

(2) Im Falle $\dim_R(U) = \dim_R(V) < \infty$ gilt $I = J$. (E2B) QED

⚠ Für (2) ist $\dim_R(V) < \infty$ wesentlich: In $V = \mathbb{R}[X]$ ist $U = X\mathbb{R}[X]$ ein echter Teilraum, dennoch gilt $\dim_{\mathbb{R}}(U) = \dim_{\mathbb{R}}(V) = \infty$.

Dimension von Unterräumen

⚠ Es gibt Situationen in der Mathematik (und auch sonst im Leben), wo das Unterobjekt U komplizierter sein kann als das Gesamtobjekt V. Für Vektorräume kann dieses Problem zum Glück nicht auftreten. Das ist nicht selbstverständlich, sondern muss bewiesen werden.

Beispiel: Sei K ein Körper und $R = K^{\mathbb{N}}$ der Ring aller Folgen mit punktweiser Addition und Multiplikation (G2N). Dann ist $V = R = K^{\mathbb{N}}$ ein R–linearer Raum. Er ist frei, mit dem Einselement 1 als Basis. Hierin liegt der Unterraum $U = K^{(\mathbb{N})}$ der Folgen mit endlichem Träger. Anders als V über R ist der Unterraum $U \leq V$ nicht endlich erzeugt!

Beispiel: Sei $M = \{X, Y\}^* = \{1, X, Y, XX, XY, YX, YY, XXX, \ldots\}$ die Menge aller endlichen Wörter über den Buchstaben X, Y. Diese Wörter betrachten wir nun als „Monome“ und $\mathbb{R}[M]$ als „Polynomring“ in den nicht-kommutierenden Variablen X, Y. Der Ring $\mathbb{R}[M]$ enthält den Teilkörper $\mathbb{R}$ im Zentrum und hat die Menge M als Basis über $\mathbb{R}$. Dann ist $V = \mathbb{R}[M]$ frei über $\mathbb{R}[M]$, mit dem Einselement 1 als Basis. Hierin ist $U = X\mathbb{R}[M] \oplus Y\mathbb{R}[M]$ ein Unterraum mit Basis (X, Y).

Dimensionskriterium für Basen

Korollar J2L: Dimensionskriterium für Basen

Sei V ein Vektorraum über dem Divisionsring R.
Ist die Dimension $\dim_R(V) = n$ endlich, so gilt:

1. Jedes Erzeugendensystem $v_1, \ldots, v_n \in V$ der Länge n ist minimal, also eine Basis.
2. Jede linear unabhängige Familie $v_1, \ldots, v_n \in V$ der Länge n ist maximal, also eine Basis.

Beweis: Dies folgt dank Basisauswahl / Basisergänzung (J2B) und der Invarianz der Dimension (J1K): Wir können die Familie $v_1, \ldots, v_n$ verkürzen / ergänzen zu einer Basis – derselben Länge! QED

☺ Dieses Kriterium erspart Ihnen jeweils die eine Hälfte der Arbeit!

Eigentlich müssten Sie in (1) noch lineare Unabhängigkeit nachweisen, ebenso müssten Sie in (2) noch Erzeugung nachweisen. Den zweiten Teil der Arbeit können Sie sich sparen, wenn die Dimension passt.

Dimensionskriterium für Basen

Das klingt intuitiv recht plausibel, doch auch hier ist es heilsam, sich nocheinmal mögliche Gegenbeispiele vor Augen zu führen.

Beispiel: Ist R ein Ring mit $R^4 \cong R^7$ wie in J1O, so gibt es im Raum R^7 über R Erzeugendensysteme $v_1, \ldots, v_7$, die sich noch verkürzen lassen. Ebenso gibt es im Raum R^4 linear unabhängige Familien $u_1, \ldots, u_4$, die sich noch ergänzen lassen. Wer hätte das gedacht?

Warum erzähle ich Ihnen das so ausführlich?

☺ Die illustrativen Gegen/Beispiele zeigen Ihnen, dass präzise Sätze hier tatsächlich nötig sind.

☺ Unsere gründlichen Beweise garantieren Ihnen, dass am Ende alles gut ausgeht, so wie erhofft.

Die Mühe ist also notwendig, und sie lohnt sich!

Zusammensetzen von Basen

Satz J2M: exakte Sequenz und Dimensionsformel

Sei R ein Ring. Gegeben sei eine kurze exakte Sequenz:

$$0 \xrightarrow{0} U \xrightarrow{f} V \xrightarrow{g} W \xrightarrow{0} 0$$

$$u_i \longmapsto v_i \qquad \text{Basis} \qquad v_j \longmapsto w_j \qquad \text{Basis}$$

Sei $(u_i)_{i\in I}$ eine Basis von U und $(w_j)_{j\in J}$ eine Basis von W.
Wir können $I \cap J = \emptyset$ annehmen und setzen $K = I \sqcup J$.

(1) Für $i \in I$ sei $v_i := f(u_i) \in V$. Für $j \in J$ wählen wir ein Urbild $v_j \in V$ mit $g(v_j) = w_j$ dank Surjektivität. Dann ist $(v_k)_{k\in K}$ eine Basis von V.

(2) Daher gilt $V = V_1 \oplus V_2$ mit $V_1 = \operatorname{im}(f) = \ker(g) = \langle\, v_i \mid i \in I \,\rangle_R^!$ und $V_2 = \langle\, v_j \mid j \in J \,\rangle_R^!$. Dabei gilt $f|^{V_1} : U \xrightarrow{\sim} V_1$ und $g|_{V_2} : V_2 \xrightarrow{\sim} W$.

(3) Für die Dimensionen folgt $\dim_R(V) = \dim_R(U) + \dim_R(W)$.

Für (3) setzen wir voraus, dass R die Invarianz der Dimension erfüllt.

Zusammensetzen von Basen

$$0 \xrightarrow{0} U \xrightarrow{f} V \xrightarrow{g} W \xrightarrow{0} 0$$

$$u_i \longmapsto v_i \qquad \text{Basis} \qquad v_j \longmapsto w_j \qquad \text{Basis}$$

Beweis: (1) Wir zeigen, dass $(v_k)_{k\in K}$ eine Basis von V ist.

Lineare Unabhängigkeit: Sei $0 = \sum_{k\in K} v_k\lambda_k$ mit $\lambda \in R^{(K)}$.
Dann gilt $0 = g(\sum_{k\in K} v_k\lambda_k) = \sum_{j\in J} w_j\lambda_j$, also $\lambda|_J = 0$.
Es gilt $0 = \sum_{i\in I} v_i\lambda_i = f(\sum_{i\in I} u_i\lambda_i)$, also $\sum_{i\in I} u_i\lambda_i = 0$.
Daraus folgt $\lambda|_I = 0$, insgesamt also $\lambda = 0$.

Erzeugendensystem: Vorgelegt sei $v \in V$.
Wir haben $g(v) = w = \sum_{j\in J} w_j\lambda_j$ für ein $\lambda|_J \in R^{(J)}$.
Für $v_2 = \sum_{j\in J} v_j\lambda_j$ in V gilt ebenfalls $g(v_2) = w$ in W.
Für $v_1 = v - v_2$ folgt $g(v_1) = 0$, also $v_1 \in \ker(g) = \operatorname{im}(f)$.
Das bedeutet $v_1 = f(u)$ mit $u = \sum_{i\in I} u_i\lambda_i$ in U und $\lambda|_I \in R^{(I)}$.
Daraus folgt $v = v_1 + v_2 = \sum_{i\in I} v_i\lambda_i + \sum_{j\in J} v_j\lambda_j = \sum_{k\in K} v_k\lambda_k$. QED

Die Dimensionsformel für lineare Abbildungen

🙂 Ich betone noch einmal Ziel und Zweck exakter Sequenzen:
Diese Technik bündelt nützliche Informationen auf effiziente Weise.
Die nachstehenden Folgerungen illustrieren dies eindrücklich.

Satz J2N: die Dimensionsformel für lineare Abbildungen

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Für jede R–lineare Abbildung $f : V \to W$ gilt die Dimensionsformel:

$$\dim_R(V) = \dim_R \ker(f) + \dim_R \operatorname{im}(f)$$

Beweis: Dies folgt dank Satz J2M aus der kurzen exakten Sequenz

$$0 \xrightarrow{0} \ker(f) \xhookrightarrow{\iota} V \xrightarrow{\hat{f}} \operatorname{im}(f) \xrightarrow{0} 0.$$

Hierbei ist $\iota : \ker(f) \hookrightarrow V : v \mapsto v$ die Inklusion des Kerns
und $\hat{f} : V \twoheadrightarrow \operatorname{im}(f) : v \mapsto f(v)$ die Surjektion auf das Bild. QED

🙂 Wir können Basen wie in Satz J2M zusammensetzen.

Die Dimensionsformel für lineare Abbildungen

🙂 Für die Dimensionsformel J2N setzen wir einen Divisionsring voraus; damit sichern wir sowohl die Eindeutigkeit der Dimension (J1K) als auch die Existenz von Basen (J2B), hier angewendet auf $\ker(f)$ und $\operatorname{im}(f)$.

🙂 Im vorangegangenen Satz J2M hingegen ist R ein beliebiger Ring. Die benötigten Basen von U und V werden als Eingabedaten geliefert, der Satz fügt diese dann wie gezeigt zu einer Basis von V zusammen.

🙂 Auch die Dimensionsformel J2N können wir genauso formulieren: Ist $f : V \to W$ eine R–lineare Abbildung und sind $\ker(f)$ und $\operatorname{im}(f)$ frei, so ist auch V frei, und es gilt die Dimensionsformel

$$\dim_R(V) = \dim_R \ker(f) + \dim_R \operatorname{im}(f).$$

Diese Formulierung ist allgemeiner, doch leider auch etwas technisch.
Ich präsentiere daher die vereinfachte Version J2N über Divisionsringen.

Beispiel: Über $\mathbb{Z}$ ist die Sequenz $0 \to \mathbb{Z} \hookrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} \to 0$ exakt, aber die Dimensionsformel lässt sich nicht anwenden.

Die Dimensionsformel für direkte Summen

Satz J2O: die Dimensionsformel für direkte Summen

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(1) Für jede direkte Summe von R–Vektorräumen $V_1, \dots, V_n \leq W$ gilt

$$\dim_R(V_1 \oplus \cdots \oplus V_n) = \dim_R(V_1) + \cdots + \dim_R(V_n)$$

Genauer: Ist eine Basis $(v_i)_{i \in I_k}$ von V_k gegeben für jedes k,
so erhalten wir zu $V = \bigoplus_k V_k$ die Basis $(v_i)_{i \in I}$ mit $I = \bigsqcup_k I_k$.

(2) Dank $V_1 \times \cdots \times V_n \cong V_1 \oplus \cdots \oplus V_n$ folgt insbesondere

$$\dim_R(V_1 \times \cdots \times V_n) = \dim_R(V_1) + \cdots + \dim_R(V_n).$$

Beweis: Der Fall $n = 2$ folgt dank Satz J2M aus der exakten Sequenz

$$0 \xrightarrow{0} V_1 \xrightarrow[v_1 \mapsto v_1 + 0]{f} V_1 \oplus V_2 \xrightarrow[v_1 + v_2 \mapsto v_2]{g} V_2 \xrightarrow{0} 0.$$

Der allgemeine Fall $n \in \mathbb{N}$ folgt daraus per Induktion. QED

Die Dimensionsformel für direkte Summen

Aussagen und Beweise zu Dimensionen entsprechen dem Abzählen von Basen, hier also der Mächtigkeit einer disjunkten Vereinigung:

$$\sharp(I_1 \sqcup I_2 \sqcup \cdots \sqcup I_n) = (\sharp I_1) + (\sharp I_2) + \cdots + (\sharp I_n)$$

Dies folgt per Induktion aus dem Fall $n = 2$ (Satz E2A):

$$\sharp(I_1 \sqcup I_2) = \sharp I_1 + \sharp I_2$$

Im Falle eines nicht-leeren Schnitts haben wir (Satz E2B):

$$\sharp(I_1 \cup I_2) = \sharp I_1 + \sharp I_2 - \sharp(I_1 \cap I_2)$$

Dieselbe Eigenschaft finden wir für die Dimension von Vektorräumen!
Dazu müssen wir nur geeignete Basen konstruieren, etwa mit Satz J2M.

🙂 Das sind zwei der guten Gründe, warum ich Abzählungen von Mengen in Kapitel E so ausführlich diskutiert, ja zelebriert habe:

- Sie bieten gutes Anschauungs- und Lernmaterial für den Einstieg.
- Sätze und Techniken übertragen sich auf Basen von Vektorräumen.

Die Dimensionsformel für beliebige Summen

Satz J2P: die Dimensionsformel für beliebige Summen

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(1) Für je zwei Unterräume $V_1, V_2 \leq W$ gilt:

$$\dim_R(V_1 + V_2) + \dim_R(V_1 \cap V_2) = \dim_R(V_1) + \dim_R(V_2)$$

(2) Sind alle Dimensionen endlich, so folgt:

$$\dim_R(V_1 + V_2) = \dim_R(V_1) + \dim_R(V_2) - \dim_R(V_1 \cap V_2)$$

Dieser allgemeine, aber einfache Zusammenhang ist bemerkenswert.
Die Gleichung folgt leicht aus… der zugehörigen exakten Sequenz!

Beweis: (1) Dies folgt aus Satz J2M und der exakten Sequenz I2I:

$$0 \xrightarrow{0} V_1 \cap V_2 \xrightarrow[u \mapsto (-u,u)]{f} V_1 \times V_2 \xrightarrow[(v_1,v_2) \mapsto v_1 + v_2]{g} V_1 + V_2 \xrightarrow{0} 0$$

(2) Dies folgt aus (1) durch Umstellung in $\mathbb{N}$. QED

Die Dimensionsformel für beliebige Summen

🙂 Damit kennen wir die Dimension, hierzu existieren Basen:

Satz J2P: angepasste Basis zu $U = V_1 \cap V_2$ und $V = V_1 + V_2$

(3) Wir wählen zunächst eine Basis $(v_i)_{i \in I_0}$ von U, dank J2B.
Wir ergänzen $(v_i)_{i \in I_0}$ zu einer Basis $(v_i)_{i \in I_1}$ von V_1, dank J2B.
Wir ergänzen $(v_i)_{i \in I_0}$ zu einer Basis $(v_i)_{i \in I_2}$ von V_2, dank J2B.
Dabei vergeben wir keinen Index doppelt, also $I_1 \cap I_2 = I_0$.
Dann ist $(v_i)_{i \in I}$ mit $I = I_1 \cup I_2$ eine Basis von $V = V_1 + V_2$.

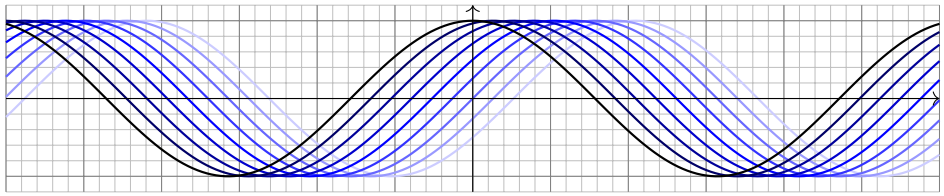
Beweis im endlichen Fall: Die Familie $(v_i)_{i \in I}$ erzeugt V.
Zudem gilt $\dim_R(V) = \sharp I_1 + \sharp I_2 - \sharp I_0 = \sharp I$, dank J2P.
Also ist $(v_i)_{i \in I}$ eine Basis von V, dank J2L. QED

Der **Zassenhaus–Algorithmus** führt die Konstruktion für $V_1, V_2 \leq R^n$ explizit aus: Eingabe sind Erzeugendensysteme von V_1 und V_2 in R^n.
Ausgabe ist eine angepasste Basis von $U = V_1 \cap V_2$ und $V = V_1 + V_2$.
So wird das Problem in Computer-Algebra-Systemen effizient gelöst.

📖 Literatur: Das Lernbuch von Fischer stellt dies ausführlich dar.

Dimension eines Untervektorraums über $\mathbb{R}$

J301
Übung



Über dem Körper $\mathbb{R}$ betrachten wir den Funktionenraum $V = \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ aller reellen Abbildungen $f : \mathbb{R} \to \mathbb{R}$ und darin speziell den Unterraum

$$U := \langle\, f_\alpha \mid \alpha \in \mathbb{R} \,\rangle_{\mathbb{R}}$$

erzeugt von den Funktionen $f_\alpha : \mathbb{R} \to \mathbb{R} : t \mapsto \cos(t - \alpha)$.

Aufgabe: Welche Dimension hat dieser Vektorraum U über $\mathbb{R}$?

⚠ Das angegebene Erzeugendensystem $(f_\alpha)_{\alpha\in\mathbb{R}}$ ist überabzählbar, und auch der Raum U sieht zunächst riesig aus. Doch das täuscht!

🙂 Es gibt letztlich nur einen Weg, die Dimension zu bestimmen:
Wir müssen eine Basis von U finden! Bitte schauen Sie genau hin.

Dimension eines Untervektorraums über $\mathbb{R}$

J302
Übung

Lösung: Die Euler–Formel $\mathrm{e}^{\mathrm{i}t} = \cos t + \mathrm{i} \sin t$ und die Homomorphie $\mathrm{e}^{x+y} = \mathrm{e}^x\, \mathrm{e}^y$ führen zu den bekannten Additionstheoremen:

$$\begin{aligned} \cos(u \pm v) &= \cos u \cdot \cos v \mp \sin u \cdot \sin v \\ \sin(u \pm v) &= \sin u \cdot \cos v \pm \cos u \cdot \sin v \end{aligned}$$

Für unsere Funktionenschar $(f_\alpha)_{\alpha\in\mathbb{R}}$ bedeutet das

$$f_\alpha \,:\, \mathbb{R} \to \mathbb{R} \,:\, t \mapsto \cos(t - \alpha) = \cos t \cdot \cos\alpha + \sin t \cdot \sin\alpha.$$

Somit wird unser Raum U bereits erzeugt von $\cos = f_0$ und $\sin = f_{\pi/2}$.
Diese beiden Funktionen sind linear unabhängig, denn die Auswertung

$$\Psi \,:\, U \to \mathbb{R}^2 \,:\, f \mapsto \big(\, f(0),\, f(\pi/2) \,\big)$$

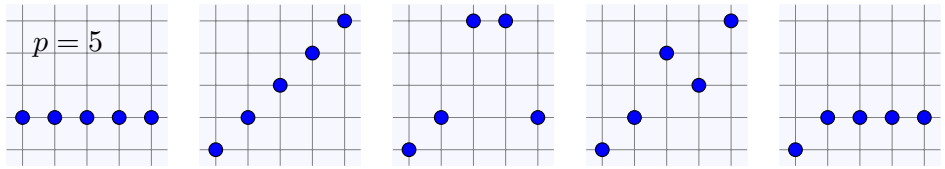
ist linear und erfüllt $\Psi(\cos) = (1, 0)$ und $\Psi(\sin) = (0, 1)$, siehe J1I.
Wir erhalten damit schließlich eine sehr übersichtliche Basis:

$$U := \langle\, \cos,\, \sin \,\rangle_{\mathbb{R}}^{!} \quad \text{und} \quad \Psi : U \xrightarrow{\sim} \mathbb{R}^2$$

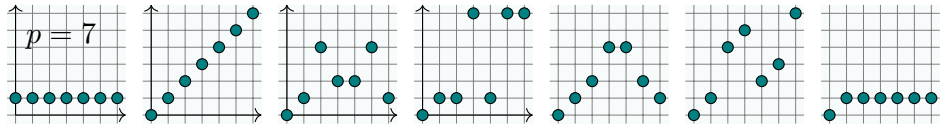
Insbesondere finden wir so die Dimension $\dim_{\mathbb{R}}(U) = 2$.

Dimension eines Untervektorraums über $\mathbb{F}_p$

J303
Übung



Über dem endlichen Körper $\mathbb{F}_p$ betrachten wir den Funktionenraum $V = \mathrm{Abb}(\mathbb{F}_p, \mathbb{F}_p)$ und darin speziell den Unterraum $U := \langle\, f_k \mid k \in \mathbb{N} \,\rangle_{\mathbb{F}_p}$ erzeugt von den Potenzfunktionen $f_k : \mathbb{F}_p \to \mathbb{F}_p : x \mapsto x^k$ für alle $k \in \mathbb{N}$.



Aufgabe: Welche Dimension haben die Vektorräume U und V über $\mathbb{F}_p$?

🙂 Die Funktionen f_k sehen zunächst verwirrend unstrukturiert aus.
Welche algebraische Struktur steckt dahinter? Schauen Sie genau hin.

Dimension eines Untervektorraums über $\mathbb{F}_p$

J304
Übung

Lösung: Jedes Polynom $A = \sum_{i=0}^{n} a_i X^i \in \mathbb{F}_p[X]$ definiert seine zugehörige Polynomfunktion $f_A : \mathbb{F}_p \to \mathbb{F}_p : x \mapsto A(x) = \sum_{i=0}^{n} a_i x^i$.
Wir erhalten so den Ringhomomorphismus $\Phi : \mathbb{F}_p[X] \to \mathrm{Abb}(\mathbb{F}_p, \mathbb{F}_p)$.
Wegen $X^k \mapsto f_k$ gilt $\mathrm{im}(\Phi) = U$. Dank G3M haben wir die Bijektion

$$\Psi \,:\, \mathbb{F}_p[X]_{<p} \xrightarrow{\sim} \mathrm{Abb}(\mathbb{F}_p, \mathbb{F}_p) \,:\, A \mapsto f_A.$$

In Worten: Zu beliebig vorgegebenen Werten $y_0, y_1, \ldots, y_{p-1} \in \mathbb{F}_p$ existiert genau ein interpolierendes Polynom $A \in \mathbb{F}_p[X]_{<p}$ mit

$$A(0) = y_0,\ A(1) = y_1,\ \ldots,\ A(p-1) = y_{p-1}.$$

Somit schließen wir $\dim_{\mathbb{F}_p}(U) = p$ und $U = V$, genauer:

$$U = V = \langle\, f_0, f_1, \ldots, f_{p-1} \,\rangle_{\mathbb{F}_p}^{!}$$

🙂 Das sieht man obigen Graphen der Funktionen f_k wohl kaum an.
Die Arithmetik des Polynomrings hilft, damit erkennen wir die Struktur.

Kapitel K

Darstellung linearer Abbildungen durch Matrizen

We share a philosophy about linear algebra:
we think basis-free, we write basis-free,
but when the chips are down
we close the office door and
compute with matrices like fury.

Irving Kaplansky (1917–2006), über sich und Paul Halmos

Inhalt dieses Kapitels K

Motivation und Überblick

In diesem Kapitel geht es vorrangig darum, eine R–lineare Abbildung $f : V \to W$ geeignet darzustellen durch eine Matrix $A \in R^{m\times n}$.

Dies gelingt, sobald eine Basis $\mathcal{B} = (b_1, \dots, b_n)$ des Startraums V und eine Basis $\mathcal{C} = (c_1, \dots, c_m)$ des Zielraums W gegeben ist. Wir erhalten dann eine Bijektion zwischen Matrizen und linearen Abbildungen:

$$(\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}) \;:\; R^{m\times n} \;\cong\; \mathrm{Hom}_R(V, W).$$

Das ist Gegenstand des Darstellungssatzes K1F. Diese Bijektion respektiert die Addition (K1I) sowie Multiplikation und Komposition (K1J). Wir erhalten so den Isomorphismus von Ringen bzw. Gruppen:

$$(\mathrm{L}_{\mathcal{B}}^{\mathcal{B}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}) \;:\; (R^{n\times n}, +, \cdot) \;\cong\; (\mathrm{End}_R(V), +, \circ)$$
$$(\mathrm{L}_{\mathcal{B}}^{\mathcal{B}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}) \;:\; (\mathrm{GL}_n R, \cdot) \;\cong\; (\mathrm{Aut}_R(V), \circ).$$

Als Matrizen werden diese Objekte leichter fasslich!

Motivation und Überblick

Diese Übersetzung von Matrizen zu linearen Abbildungen und zurück ist überaus nützlich! Eigentlich interessiert uns die lineare Abbildung f, doch mit der Matrix A können wir besonders gut und effizient rechnen. Das Bijektionspaar $(\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{C}})$ übersetzt verlustfrei zwischen beiden.

Dazu muss allerdings eine Basis $\mathcal{B}$ des Startraums und eine Basis $\mathcal{C}$ des Zielraums W vorliegen! Das ist einerseits eine Bürde, denn wir müssen Basen konstruieren und dabei willkürliche Wahlen treffen, andererseits bietet uns diese Wahl auch gewisse Freiheiten.

Diese Freiheit können wir nutzen, etwa zur kanonischen Darstellung von $f : V \to W$ durch eine besonders einfache Modellmatrix (K2C).

Es ist ein wichtiges und interessantes Problem, zu $f : V \to V$ eine angepasste Basis $\mathcal{B}$ von V zu wählen, sodass die darstellende Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f)$ möglichst einfach wird, am besten diagonal. Hierzu werden wir in den nächsten Kapiteln die nötigen Techniken entwickeln. Schon jetzt können wir relevante Beispiele bearbeiten zur Illustration und Motivation.

Motivation und Überblick

Ich zeige in diesem Kapitel (wie gelegentlich auch bereits zuvor) mit Begeisterung schöne und relevante Beispiele aus der Analysis. Diese Querbezüge sollten Sie nicht schrecken, sondern freuen: Bitte denken Sie nicht in Schubladen, sondern lernen Sie vernetzt, das hilft!

Die Methoden der Linearen Algebra lassen sich überall gewinnbringend nutzen, auch und gerade in der Analysis, zum Beispiel bei der Lösung von gewöhnlichen Differentialgleichungen und linearen Systemen. Wir machen uns daher früh mit konkreten Beispielen vertraut.

Motivation und Überblick

Natürlich sollten Sie zur Übung auch willkürliche Zahlenbeispiele routiniert rechnen (können), ohne jede Anschauung und Bedeutung. Das erfordert wie immer Übung und gelingt nur durch die eigene Hand, diese Mühe kann und diese Freude will ich Ihnen nicht nehmen.

Ich empfehle hierzu unser didaktische Online-Tool Gaël. Damit können Sie leicht experimentieren und Erfahrungen sammeln. Kleine Beispiele gelingen Ihnen von Hand, große Beispiele übergeben Sie vollständig dem Computer, Gaël ist ideal für den Übergang.

Auch solche numerischen Beispiele sind wichtig und sehr hilfreich. Die knappe Zeit der Vorlesung investiere ich lieber in schöne, relevante Beispiele mit Bedeutung und Anschauung!

Motivation und Überblick

Motivation und Überblick

Vergleich von Homomorphismen auf Erzeugern

K101

Wie testen wir effizient die Gleichheit von zwei linearen Abbildungen?

Lemma K1A: Vergleich von Homomorphismen auf Erzeugern

Wir vergleichen lineare Abbildungen $f, g : V \to W$ über dem Ring R.
Hierzu sei $(v_i)_{i\in I}$ eine Familie in V mit $f(v_i) = g(v_i)$ für alle $i \in I$.
(1) Daraus folgt $f(v) = g(v)$ für alle $v \in U = \langle\, v_i \mid i \in I \,\rangle_R$.
(2) Erzeugt $(v_i)_{i\in I}$ den gesamten Raum V, so folgt $f = g$.

☺ Es genügt, f und g auf einem Erzeugendensystem zu vergleichen.

Beweis: (1) Jedes Element $v \in U$ schreibt sich als Linearkombination

$$v = \textstyle\sum_{i\in I} v_i\lambda_i \quad \text{mit} \quad \lambda \in R^{(I)}.$$

Dank Linearität von f und g folgt daraus:

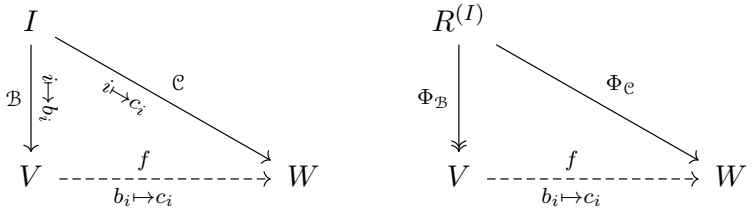
$$\begin{aligned} f(v) \;=\; f\big(\textstyle\sum_{i\in I} v_i\lambda_i\big) &\overset{\text{Lin}}{=} \textstyle\sum_{i\in I} f(v_i)\lambda_i \\ &\overset{\text{Vor}}{=} \textstyle\sum_{i\in I} g(v_i)\lambda_i \overset{\text{Lin}}{=} g\big(\textstyle\sum_{i\in I} v_i\lambda_i\big) \;=\; g(v) \end{aligned}$$

(2) Im Falle $U = V$ bedeutet das $f = g$. QED

Vergleich von Homomorphismen auf Erzeugern

K102
Erläuterung

☺ Dieses Lemma hilft beim **Vergleich** von linearen Abbildungen.
⚠ Es ist jedoch ungeeignet zur **Konstruktion** linearer Abbildungen.
☺ Zur Konstruktion von f nutzen wir den Faktorisierungssatz I2E:



Genau dann existiert die lineare Abbildung $f : V \to W$ mit $f \circ \Phi_{\mathcal{B}} = \Phi_{\mathcal{C}}$, wenn $\ker(\Phi_{\mathcal{B}}) \subseteq \ker(\Phi_{\mathcal{C}})$ gilt. Diese Bedingung ist trivialerweise erfüllt, falls $\ker(\Phi_{\mathcal{B}}) = \{0\}$, wenn also $\Phi_{\mathcal{B}}$ bijektiv und somit $\mathcal{B}$ eine Basis ist.

☺ Dieser wichtige Spezialfall ist die Aussage des folgenden Satzes.
Er ist ein universelles Werkzeug zur Konstruktion linearer Abbildungen $f : V \to W$, falls der Startraum V mit einer Basis $\mathcal{B}$ ausgestattet ist.

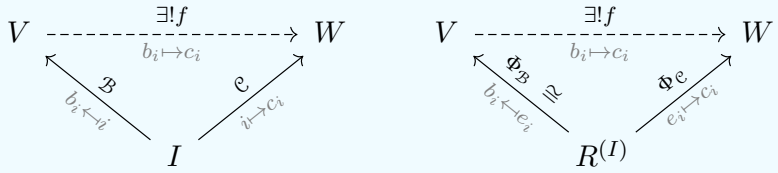
Prinzip der linearen Fortsetzung

K103

Wie konstruieren wir effizient eine lineare Abbildung $f : V \to W$?

Satz K1B: das Prinzip der linearen Fortsetzung, PLF

Gegeben sei ein R–linearer Raum V mit einer Basis $\mathcal{B} = (b_i)_{i\in I}$ und ein R–linearer Raum W mit einer beliebigen Familie $\mathcal{C} = (c_i)_{i\in I}$.



Dann existiert genau eine R–lineare Abbildung $f : V \to W$ mit $f(b_i) = c_i$ für alle $i \in I$, nämlich $f = \Phi_{\mathcal{C}} \circ \Phi_{\mathcal{B}}^{-1}$. Ausgeschrieben bedeutet das:

$$\boxed{f\big(\textstyle\sum_{i\in I} b_i\lambda_i\big) = \textstyle\sum_{i\in I} c_i\lambda_i \quad \text{für alle } (\lambda_i)_{i\in I} \in R^{(I)}.}$$

☺ Es genügt die Bilder einer Basis vorzugeben und linear fortzusetzen.

Prinzip der linearen Fortsetzung

K104
Erläuterung

Aufgabe: Beweisen Sie diesen Satz! Was ist hier zu zeigen?
Die Formulierung ist vollkommen explizit. Rechnen Sie es nach!

Lösung: Wir müssen Existenz und Eindeutigkeit der Lösung f zeigen.

Existenz: Die Komposition $f = \Phi_{\mathcal{C}} \circ \Phi_{\mathcal{B}}^{-1} : V \to W$ ist R–linear (I1G).
Gemäß dieser Konstruktion gilt für jeden Index $i \in I$ wie gewünscht

$$f(b_i) = \Phi_{\mathcal{C}}(\Phi_{\mathcal{B}}^{-1}(b_i)) = \Phi_{\mathcal{C}}(e_i) = c_i.$$

Somit erfüllt f die beiden im Satz geforderten Eigenschaften.

Eindeutigkeit: Die Eindeutigkeit folgt aus dem vorigen Lemma K1A:
Sind $f, g : V \to W$ zwei Lösungen, so gilt $f = g$.

Bemerkung: Die Basis $\mathcal{B} : I \to V$ von V stiftet demnach die Bijektion

$$\mathrm{Hom}_R(V, W) \xrightarrow{\sim} \mathrm{Abb}(I, W) \;:\; f \mapsto \mathcal{C} = f \circ \mathcal{B}.$$

Die Umkehrung ist die lineare Fortsetzung $\mathcal{C} \mapsto f = \Phi_{\mathcal{C}} \circ \Phi_{\mathcal{B}}^{-1}$.
Das ist eine universelle Abbildungseigenschaft für $(V, \mathcal{B})$.

Anwendungsbeispiel: formale Ableitung von Polynomen

Beispiel K1C: formale Ableitung von Polynomen

Sei K ein kommutativer Ring und $K[X]$ der Polynomring über K.
Wir definieren die (formale) **Ableitung** als die K–lineare Abbildung

$$D = \partial \,:\, K[X] \to K[X] \,:\, X^n \mapsto nX^{n-1} \quad \text{für alle } n \in \mathbb{N}.$$

Dies gelingt dank Prinzip der linearen Fortsetzung K1B. Wir erhalten

$$D = \partial \,:\, K[X] \to K[X] \,:\, F = \textstyle\sum_n a_n X^n \mapsto f = \sum_n n a_n X^{n-1}.$$

Im Falle $\mathbb{Q} \leq K$ definieren wir ebenso das (unbestimmte) **Integral**:

$$I = \textstyle\int \,:\, K[X] \to K[X] \,:\, X^n \mapsto \frac{1}{n+1} X^{n+1}$$

Dank dem Prinzip der linearen Fortsetzung K1B erhalten wir hier:

$$I = \textstyle\int \,:\, K[X] \to K[X] \,:\, f = \sum_n a_n X^n \mapsto F = \sum_n \frac{a_n}{n+1} X^{n+1}$$

Damit gilt der **HDI** für Polynome: $DI(f) = f$ und $ID(F) = F - F(0)$.
Dank Lemma K1A genügt es, dies auf der Monombasis zu prüfen.

Anwendungsbeispiel: formale Ableitung von Polynomen

Das ist die „formale“ Definition der Ableitung $D : K[X] \to K[X]$
auf dem Polynomring $K[X]$ über einem beliebigen Grundring K.

🙂 In der Analysis lernen Sie die Ableitung über $K = \mathbb{R}$ (später $\mathbb{C}$)
als Grenzwert des Differenzenquotienten kennen, ausgeschrieben

$$D \,:\, \mathscr{C}^1(\mathbb{R},\mathbb{R}) \to \mathscr{C}^0(\mathbb{R},\mathbb{R}) \,:\, F \mapsto f, \qquad f(x) = \lim_{t \to x} \frac{F(t) - F(x)}{t - x}.$$

Für die Polynomfunktion $F(x) = x^n$ berechnen Sie damit $f(x) = nx^{n-1}$.
Die Ableitung ist linear, für $F(x) = \sum_n a_n x^n$ folgt $f(x) = \sum_n n a_n x^{n-1}$.

🙂 Die Formel $X^n \mapsto nX^{n-1}$ nehmen wir uns nun zum Vorbild
und definieren $D : K[X] \to K[X]$ formal wie oben erklärt.
Diese Konstruktion gelingt ganz ohne Grenzwerte.

🙂 Polynome sind ein sehr übersichtliches und einfaches Beispiel,
alle Formeln lassen sich wie hier gesehen explizit ausschreiben.
Das Prinzip der linearen Fortsetzung besagt dasselbe nun allgemein:
Sobald eine Basis gegeben ist, können wir f direkt hinschreiben.

Anwendungsbeispiel: die Leibniz–Produktregel

Satz K1C: Leibniz–Produktregel für die formale Ableitung

Sei K ein kommutativer Ring und $K[X]$ der Polynomring über K.
Hierauf sei $\partial : K[X] \to K[X]$ die (formale) Ableitung, wie oben erklärt.
Für alle Polynome $P, Q \in K[X]$ gilt dann

$$\boxed{\partial(P \cdot Q) = (\partial P) \cdot Q + P \cdot (\partial Q).}$$

Diese Eigenschaft heißt **Produktregel** oder auch **Leibniz–Regel**.

Aufgabe: Beweisen Sie dies (1) für Monome $P = X^m$ und $Q = X^n$ und
(2) für beliebige Polynome $P, Q \in K[X]$ durch lineare Fortsetzung.

Lösung: (1) Für Monome ist die explizite Rechnung leicht:

$$\begin{aligned} \partial(X^m \cdot X^n) &\overset{K[X]}{=} \partial(X^{m+n}) \\ &\overset{\text{Def}}{=} (m+n)X^{m+n-1} \\ (\partial X^m) \cdot X^n + X^m \cdot (\partial X^n) &\overset{\text{Def}}{=} mX^{m-1} \cdot X^n + X^m \cdot nX^{n-1} \\ &\overset{K[X]}{=} (m+n)X^{m+n-1} \end{aligned}$$

Anwendungsbeispiel: die Leibniz–Produktregel

(2) Wir zeigen nun die Leibniz–Regel $\partial(P \cdot Q) = (\partial P) \cdot Q + P \cdot (\partial Q)$
für alle Polynome $P, Q \in K[X]$. Dank (1) gilt sie für alle Monome.
Wir nutzen nun geschickt das Eindeutigkeitslemma K1A:

(2a) Wir fixieren $Q = X^n$ und betrachten die Fehlerabbildung

$$\varepsilon \,:\, K[X] \to K[X] \,:\, P \mapsto (\partial P) \cdot Q + P \cdot (\partial Q) - \partial(P \cdot Q).$$

Jedes Monom $P = X^m$ erfüllt $\varepsilon(X^m) = 0$ dank (1).
Die Abbildung ε ist linear. Also folgt $\varepsilon = 0$ dank K1A.

(2b) Wir fixieren $P \in K[X]$ und betrachten die Fehlerabbildung

$$\varepsilon \,:\, K[X] \to K[X] \,:\, Q \mapsto (\partial P) \cdot Q + P \cdot (\partial Q) - \partial(P \cdot Q).$$

Jedes Monom $Q = X^n$ erfüllt $\varepsilon(X^n) = 0$ dank (2a).
Die Abbildung ε ist linear. Also folgt $\varepsilon = 0$ Dank K1A.

🙂 Das Prinzip der linearen Fortsetzung K1B dient zur Konstruktion, das
Eindeutigkeitslemma K1A zum Vergleich von linearen Abbildungen.
Diese Werkzeuge trivialisieren viele Rechnungen, so wie hier zu sehen.

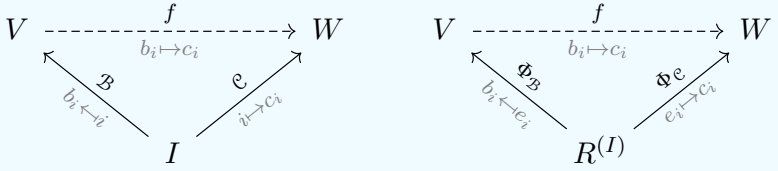
Das starke Prinzip der linearen Fortsetzung

☺ Über jedem Divisionsring R können wir das Prinzip der linearen Fortsetzung K1B kombinieren mit dem Basisergänzungssatz J2B:

Satz K1D: starkes Prinzip der linearen Fortsetzung, SPLF

Seien V und W Vektorräume über dem Divisionsring R.

(1) Gegeben seien Familien $\mathcal{B} = (b_i)_{i\in I}$ in V und $\mathcal{C} = (c_i)_{i\in I}$ in W.
Wir suchen R–lineare Abbildungen $f : V \to W$ mit $f(b_i) = c_i$ für $i \in I$.



Ist $\mathcal{B} = (b_i)_{i\in I}$ erzeugend / unabhängig / eine Basis von V,
so existiert höchstens / mindestens / genau eine Lösung f.

Das starke Prinzip der linearen Fortsetzung

☺ Wir nennen dies das *starke* Prinzip der linearen Fortsetzung, da es nicht nur Basen behandelt, sondern beliebige Familien. Dafür benötigen wir auch stärkere Voraussetzungen, nämlich einen Divisionsring R, da wir im Fall (b) den Basisergänzungssatz J2B einsetzen.

Aufgabe: Beweisen Sie diese drei Aussagen!
Nutzen Sie dazu die zuvor bewiesenen Ergebnisse.

Lösung: Zwei der drei Fälle haben wir bereits geklärt:

(1a) Ist die Familie $\mathcal{B} = (b_i)_{i\in I}$ erzeugend, so nutzen wir das Eindeutigkeitslemma K1A: Es existiert höchstens eine Lösung f.

(1c) Ist $\mathcal{B} = (b_i)_{i\in I}$ eine Basis von V, so nutzen wir das Prinzip der linearen Fortsetzung K1B: Es existiert genau eine Lösung f.

(1b) Ist $\mathcal{B} = (b_i)_{i\in I}$ linear unabhängig in V, so können wir zu einer Basis $(b_j)_{j\in J}$ mit $I \subseteq J$ ergänzen (J2B). Für $j \in J \smallsetminus I$ wählen wir $c_j \in W$ beliebig, etwa $c_j = 0$. Anschließend können wir (1c) anwenden.

Das starke Prinzip der linearen Fortsetzung

☺ Wie charakterisieren wir Basen durch eine Abbildungseigenschaft?

Satz K1D: starkes Prinzip der linearen Fortsetzung, SPLF

Seien V und $W \neq 0$ Vektorräume über dem Divisionsring R.

(2) Gegeben sei eine Familie $\mathcal{B} = (b_i)_{i\in I}$ in V. Die Auswertung ergibt

$$\mathrm{ev}_{\mathcal{B}} \;:\; \mathrm{Hom}_R(V,W) \to \mathrm{Abb}(I,W) \;:\; f \mapsto (f(b_i))_{i\in I}.$$

Genau dann ist $\mathcal{B} = (b_i)_{i\in I}$ erzeugend / unabhängig / eine Basis von V,
wenn die Auswertungsabbildung $\mathrm{ev}_{\mathcal{B}}$ injektiv / surjektiv / bijektiv ist.

☺ Das ist eine bemerkenswerte Charakterisierung dieser „internen“ Eigenschaften einer Familie $\mathcal{B} = (v_i)_{i\in I}$ in V durch die „externen“ Abbildungseigenschaften von Homomorphismen $f : V \to W$.

Aufgabe: Beweisen Sie diese drei Äquivalenzen!
Nutzen Sie dazu die zuvor bewiesenen Ergebnisse.

Das starke Prinzip der linearen Fortsetzung

Lösung: Die drei Implikationen „⇒“ haben wir in (1) bereits gezeigt.
Wir beweisen nun die drei Umkehrungen „⇐“ durch Kontraposition:

(2a) Die Familie $\mathcal{B}$ erzeugt den Unterraum $U = \langle\, b_i \mid i \in I \,\rangle_R \leq V$.
Angenommen, es gilt $U \neq V$. Wir wählen eine Basis $(b_i)_{i\in J}$ von U mit $J \subseteq I$ (J2B) und ergänzen diese zu einer Basis $(b_i)_{i\in J\sqcup K}$ von V (J2B).
Wegen $K \neq \emptyset$ ist die Auswertung $\mathrm{ev}_{\mathcal{B}} : f \mapsto (f(b_i))_{i\in I}$ nicht injektiv:
Auf $(b_i)_{i\in J\sqcup K}$ können wir die Werte beliebig vorgeben (dank K1B),
doch $\mathrm{ev}_{\mathcal{B}}$ ignoriert den Teil auf K, also alle Werte $(b_i)_{i\in K}$.

(2b) Angenommen, die Familie $\mathcal{B} = (b_i)_{i\in I}$ ist linear abhängig in V,
das heißt, es gilt eine Relation $\sum_{i\in I} b_i\lambda_i$ mit $\lambda_j \neq 0$ für ein $j \in I$.
Nach Division in R gilt $v_j = \sum_{i\in I\smallsetminus\{j\}} b_i\mu_i$ mit $\mu_i = -\lambda_i/\lambda_j$.
Dann gilt $f(v_j) = \sum_{i\in I\smallsetminus\{j\}} f(b_i)\mu_i$ auch für die Bilder.
Somit ist die Auswertung $\mathrm{ev}_{\mathcal{B}}$ nicht surjektiv.

(2c) Ist die Auswertung $\mathrm{ev}_{\mathcal{B}}$ bijektiv, also injektiv und surjektiv,
so ist $\mathcal{B}$ erzeugend dank (2a) und linear unabhängig dank (2b),
also eine Basis von V.

Darstellung einer linearen Abbildung durch eine Matrix

Zu jeder Matrix $A \in R^{m\times n}$ gehört ihre R–lineare Abbildung (I1H):

$$A = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix} \quad \Longrightarrow \quad f_A : R^n \to R^m : x \mapsto Ax = \sum_{j=1}^{n} v_j x_j$$

Die $j$te Spalte von A sind die Koordinaten des $j$ten Bildvektors $v_j = Ae_j$.

Satz K1E: Bijektion zwischen Matrizen und linearen Abbildungen

Diese Zuordnung $A \mapsto f_A$ ist eine Bijektion:

$$\mathrm{L} : R^{m\times n} \xrightarrow{\sim} \mathrm{Hom}_R(R^n, R^m) : A \mapsto f_A$$

Zu jeder R–linearen Abbildung $f : R^n \to R^m$ existiert genau eine Matrix $A = \mathrm{M}(f) \in R^{m\times n}$, sodass $f = f_A$ gilt, also $f(x) = Ax$ für alle $x \in R^n$.

Wir erhalten so das Bijektionspaar $A \mapsto f = \mathrm{L}(A)$ und $f \mapsto A = \mathrm{M}(f)$:

$$(\mathrm{L}, \mathrm{M}) : R^{m\times n} \cong \mathrm{Hom}_R(R^n, R^m).$$

Darstellung einer linearen Abbildung durch eine Matrix

Beweis: Gegeben sei eine R–lineare Abbildung $f : R^n \to R^m$.
Gesucht ist eine darstellende Matrix $A \in R^{m\times n}$ mit $f_A = f$.

(1) Existenz: Wir lesen die obige Konstruktion rückwärts:

Die $j$te Spalte von A sind die Koordinaten des $j$ten Bildvektors $f(e_j)$.

Wir stellen jeden Bildvektor $f(e_j)$ in der Basis $(e_i)_{i=1}^m$ des Zielraums dar:

$$e_j \mapsto f(e_j) = \textstyle\sum_{i=1}^m e_i a_{ij} \text{ mit } a_{ij} \in R \quad \Longrightarrow \quad A = (a_{ij})$$

Die Koeffizienten a_{ij} definieren die Matrix $\mathrm{M}(f) = A := (a_{ij}) \in R^{m\times n}$.
Nach Konstruktion gilt $f(e_j) = f_A(e_j)$ für alle $j = 1, \ldots, n$.
Dank Eindeutigkeitslemma K1A folgt $f = f_A$.

(2) Eindeutigkeit: Seien $A, A' \in R^{m\times n}$ zwei Matrizen mit $f = f_A = f_{A'}$.
Für alle $j = 1, \ldots, n$ ist $f_A(e_j) = \sum_{i=1}^m e_i a_{ij}$ gleich $f_{A'}(e_j) = \sum_{i=1}^m e_i a'_{ij}$.
Dank linearer Unabhängigkeit folgt $a_{ij} = a'_{ij}$ für alle $i = 1, \ldots, m$. QED

Darstellung einer linearen Abbildung durch eine Matrix

Aufgabe: Wir betrachten die $\mathbb{R}$–lineare Abbildung

$$f : \mathbb{R}^3 \to \mathbb{R}^2 : \begin{bmatrix} x \\ y \\ z \end{bmatrix} \mapsto \begin{bmatrix} 4z - 2y \\ 5x + 2z \end{bmatrix}.$$

Schreiben Sie diese Abbildung als Matrix A, sodass $f = f_A$ gilt.

Lösung: Wir schreiben jeden Bildvektor $f(e_j)_{j=1}^3$ in der Basis $(e_i)_{i=1}^2$:

$$f(e_1) = \begin{bmatrix} 0 \\ 5 \end{bmatrix} = \begin{cases} +0e_1 \\ +5e_2 \end{cases}, \quad f(e_2) = \begin{bmatrix} -2 \\ 0 \end{bmatrix} = \begin{cases} -2e_1 \\ +0e_2 \end{cases}, \quad f(e_3) = \begin{bmatrix} 4 \\ 2 \end{bmatrix} = \begin{cases} +4e_1 \\ +2e_2 \end{cases}.$$

Wir erhalten:

$$A = \begin{bmatrix} 0 & -2 & 4 \\ 5 & 0 & 2 \end{bmatrix} = \mathrm{M}(f) \in \mathbb{R}^{2\times 3}$$

Probe: Wir schreiben $f_A : x \mapsto Ax$ explizit aus:

$$f_A : \begin{bmatrix} x \\ y \\ z \end{bmatrix} \mapsto \begin{bmatrix} 0 & -2 & 4 \\ 5 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0x - 2y + 4z \\ 5x + 0y + 2z \end{bmatrix}.$$

☺ Somit gilt die Gleichheit $f = f_A$ wie gewünscht.

Darstellung einer linearen Abbildung durch eine Matrix

☺ Im Nachgang denken Sie vermutlich: Das ist ja simpel!
In diesem Falle kann ich Ihnen nur zustimmen: Ja, das ist es.

- Der obige Satz erklärt Ihnen genau, wie die Matrix A zu bilden ist.
- Sie müssen nicht kreativ werden, nur gewissenhaft rechnen.
- Beachten Sie die Indexkonventionen. Das war's schon.

Auch wenn die Idee klar ist, so brauchen die konkreten Rechnungen wie immer etwas Gewöhnung und Übung. Bitte rechnen Sie Beispiele und Übungen sorgfältig durch, dann geht es Ihnen leicht von der Hand.

⚠ Für größere Matrizen können die Rechnungen umfangreich werden. Vermutlich möchten Sie später diese Arbeit dem Computer übertragen.

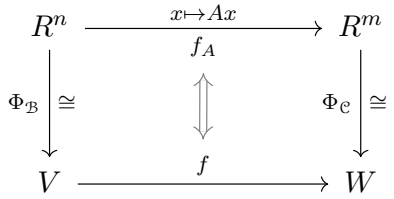
☺ Sie können die Matrizenrechnung sofort auf dem Computer nutzen, und genau dazu müssen Sie diese simplen Rechenregeln beherrschen, damit Sie wissen, was Sie tun bzw. was Sie delegieren.

⚠ Oft identifiziert man die Matrix A mit der Abbildung f_A. Es sind aber verschiedene Objekte, daher will ich zunächst den Unterschied betonen.

Darstellung einer linearen Abbildung durch eine Matrix

Jede Matrix $A \in R^{m\times n}$ definiert eine lineare Abbildung $f_A : R^n \to R^m$.
Jede lineare Abbildung $f : R^n \to R^m$ entspricht einer Matrix $A \in R^{m\times n}$.

Wir können dies auf beliebige R–lineare Räume V und W übertragen, sobald eine Basis $\mathcal{B} = (b_j)_{j=1}^n$ von V und $\mathcal{C} = (c_i)_{i=1}^m$ von W vorliegt:



🙂 Dieses übersichtliche Diagramm fasst die Konstruktion zusammen:
Wir erhalten $f = \Phi_{\mathcal{C}} \circ f_A \circ \Phi_{\mathcal{B}}^{-1}$ und umgekehrt $f_A = \Phi_{\mathcal{C}}^{-1} \circ f \circ \Phi_{\mathcal{B}}$.

🙂 Der folgende Satz schreibt die zugehörigen Formeln explizit aus.
Beides ist nützlich und wichtig: Übersicht und Details.

Darstellung einer linearen Abbildung durch eine Matrix

Satz K1F: Bijektion zwischen Matrizen und linearen Abbildungen

Sei R ein Ring sowie V und W (rechts)lineare Räume über R.
Gegeben sei eine Basis $\mathcal{B} = (b_j)_{j=1}^n$ von V und $\mathcal{C} = (c_i)_{i=1}^m$ von W.
(1) Jede Matrix $A \in R^{m\times n}$ definiert die zugehörige R–lineare Abbildung

$$f = \mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A) \,:\, V \to W \,:\, v = \sum_{j=1}^n b_j\lambda_j \mapsto w = \sum_{i=1}^m c_i\mu_i, \;\; \mu_i = \sum_{j=1}^n a_{ij}\lambda_j.$$

Die Koordinaten $\lambda \in R^n$ bezüglich $\mathcal{B}$ werden zu $\mu = A\lambda$ bezüglich $\mathcal{C}$.
(2) Die $j$te Spalte von A sind die Koordinaten des $j$ten Bildvektors $f(b_j)$:

$$f \,:\, b_j \mapsto f(b_j) = \textstyle\sum_{i=1}^m c_i a_{ij} \quad \text{mit } a_{ij} \in R$$

(3) Jede R–lineare Abbildung $f : V \to W$ lässt sich so eindeutig durch eine Matrix $A = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f) \in R^{m\times n}$ darstellen. Wir erhalten die Bijektion

$$(\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}) \,:\, R^{m\times n} \;\cong\; \mathrm{Hom}_R(V, W).$$

Darstellung einer linearen Abbildung durch eine Matrix

Aufgabe: Das folgt aus dem vorigen Satz K1E. Führen Sie dies aus!

Lösung: Die Formeln des Satzes übersetzen das obige Diagramm.
(1) Gegeben sei eine beliebige Matrix $A \in R^{m\times n}$. Die hier definierte Abbildung $f = \mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A) : V \to W$ ist wohldefiniert und linear, siehe I1H.
(2) Speziell für $\lambda = e_j$ erhalten wir die Bilder der Basisvektoren:

$$f \,:\, b_j \mapsto f(b_j) = \sum_{i=1}^m c_i a_{ij}$$

Bereits diese Eigenschaft definiert f dank linearer Fortsetzung K1B; diese rekonstruiert die explizite Formel wie in (1) angegeben.
(3) Gegeben sei nun umgekehrt eine R–lineare Abbildung $f : V \to W$. Wie in (2) schreiben wir jeden Bildvektor $f(b_j)$ in der Basis $\mathcal{C} = (c_i)_{i=1}^m$.
Die so gefundenen Koeffizienten a_{ij} definieren die zur Abbildung f gehörige darstellende Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f) := A = (a_{ij}) \in R^{m\times n}$.
Dank Eindeutigkeitslemma K1A gilt $f = \mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A)$

Darstellung einer linearen Abbildung durch eine Matrix

Alternative: Dank Satz K1E haben wir bereits das Bijektionspaar

$$(\mathrm{L}, \mathrm{M}) \,:\, R^{m\times n} \;\cong\; \mathrm{Hom}_R(R^n, R^m).$$

(4) Wie im obigen Diagramm dargestellt gilt

$$\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A) = \Phi_{\mathcal{C}} \circ \mathrm{L}(A) \circ \Phi_{\mathcal{B}}^{-1},$$
$$\mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f) = \mathrm{M}(\Phi_{\mathcal{C}}^{-1} \circ f \circ \Phi_{\mathcal{B}}).$$

Dies definiert das Bijektionspaar $(\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}) : R^{m\times n} \cong \mathrm{Hom}_R(V, W)$:
(4a) Für jede Matrix $A \in R^{m\times n}$ und $f := \mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A)$ gilt $A = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f)$, denn

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A)) = \mathrm{M}(\Phi_{\mathcal{C}}^{-1} \circ \Phi_{\mathcal{C}} \circ \mathrm{L}(A) \circ \Phi_{\mathcal{B}}^{-1} \circ \Phi_{\mathcal{B}}) = A.$$

(4b) Für $f \in \mathrm{Hom}_R(V, W)$ und $A := \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f)$ gilt $f = \mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A)$, denn

$$\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(\mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f)) = \Phi_{\mathcal{C}} \circ \mathrm{L}(\mathrm{M}(\Phi_{\mathcal{C}}^{-1} \circ f \circ \Phi_{\mathcal{B}})) \circ \Phi_{\mathcal{B}}^{-1} = f.$$

Darstellung einer linearen Abbildung durch eine Matrix

K125

Aufgabe: Stellen Sie die Ableitung $\partial\colon \mathbb{R}[X]_{\leq 3} \to \mathbb{R}[X]_{\leq 2}$ als Matrix $A := \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\partial)$ bezüglich der Monombasen dar. Wir betrachten hier

den Raum $V = \mathbb{R}[X]_{\leq 3}$ mit der Basis $\mathcal{B} = (X^j)_{j=0}^3$,
den Raum $W = \mathbb{R}[X]_{\leq 2}$ mit der Basis $\mathcal{C} = (X^i)_{i=0}^2$.

Lösung: Wir schreiben $\partial(X^j) = \sum_{i=0}^2 X^i a_{ij}$ in Koordinaten aus:

$$\begin{aligned}
X^0 &\mapsto \partial X^0 = 0 &&= 0\cdot X^0 + 0\cdot X^1 + 0\cdot X^2,\\
X^1 &\mapsto \partial X^1 = 1 &&= 1\cdot X^0 + 0\cdot X^1 + 0\cdot X^2,\\
X^2 &\mapsto \partial X^2 = 2X &&= 0\cdot X^0 + 2\cdot X^1 + 0\cdot X^2,\\
X^3 &\mapsto \partial X^3 = 3X^2 &&= 0\cdot X^0 + 0\cdot X^1 + 3\cdot X^2.
\end{aligned}$$

In der $j$ten Spalten von A stehen die Koordinaten des $j$ten Bildvektors:

$$A = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\partial) = \begin{bmatrix} 0 & 1 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 3 \end{bmatrix}$$

Darstellung einer linearen Abbildung durch eine Matrix

K126
Erläuterung

🙂 Wir folgen dem expliziten Verfahren des Darstellungssatzes K1F: Wir bestimmen die Koeffizienten $a_{ij} \in R$ in der eindeutigen Darstellung

$$f(b_j) = \textstyle\sum_{i=1}^m c_i a_{ij}.$$

Diese Koeffizienten fassen wir *spaltenweise* zur Matrix A zusammen: Die $j$te Spalte von A sind die Koordinaten des $j$ten Bildvektors $f(b_j)$.

Für diese ersten Beispiele habe ich nicht-quadratische Matrizen gewählt, damit die spaltenweise Konstruktion besonders augenfällig wird.

⚠ Oft betrachten wir quadratische Matrizen, und dort besteht eine gewisse Verwechslungsgefahr da Spalten und Zeilen gleich lang sind. Bis dahin ist Ihnen die Spaltenkonvention hoffentlich in Fleisch und Blut übergegangen. Zur Betonung sind unsere ersten Beispiele rechteckig, nicht quadratisch, das verhindert weitgehend alle Missverständnisse.

⚠ Die Spaltenkonvention kommt daher, dass wie Matrizen gemäß Ax von links auf Vektoren wirken lassen. Manche Autoren bevorzugen xA, das geht ebenfalls, und dann ist alles entsprechend umgekehrt.

Darstellung einer linearen Abbildung durch eine Matrix

K127

Aufgabe: Stellen Sie die Ableitung $\partial\colon \mathbb{R}[X]_{\leq 3} \to \mathbb{R}[X]_{\leq 2}$ als Matrix $A' := \mathrm{M}_{\mathcal{B}'}^{\mathcal{C}'}(\partial)$ bezüglich der faktoriellen Basen dar. Wir betrachten hier

den Raum $V = \mathbb{R}[X]_{\leq 3}$ mit der Basis $\mathcal{B}' = (\frac{1}{j!}X^j)_{j=0}^3$,
den Raum $W = \mathbb{R}[X]_{\leq 2}$ mit der Basis $\mathcal{C}' = (\frac{1}{i!}X^i)_{i=0}^2$.

Lösung: Wir schreiben $\partial(\frac{1}{j!}X^j) = \sum_{i=0}^2 \frac{1}{i!}X^i a'_{ij}$ in Koordinaten aus:

$$\begin{aligned}
\tfrac{1}{0!}X^0 &\mapsto 0 &&= 0\cdot\tfrac{1}{0!}X^0 + 0\cdot\tfrac{1}{1!}X^1 + 0\cdot\tfrac{1}{2!}X^2,\\
\tfrac{1}{1!}X^1 &\mapsto \tfrac{1}{0!}X^0 &&= 1\cdot\tfrac{1}{0!}X^0 + 0\cdot\tfrac{1}{1!}X^1 + 0\cdot\tfrac{1}{2!}X^2,\\
\tfrac{1}{2!}X^2 &\mapsto \tfrac{1}{1!}X^1 &&= 0\cdot\tfrac{1}{0!}X^0 + 1\cdot\tfrac{1}{1!}X^1 + 0\cdot\tfrac{1}{2!}X^2,\\
\tfrac{1}{3!}X^3 &\mapsto \tfrac{1}{2!}X^2 &&= 0\cdot\tfrac{1}{0!}X^0 + 0\cdot\tfrac{1}{1!}X^1 + 1\cdot\tfrac{1}{2!}X^2.
\end{aligned}$$

In der $j$ten Spalten von A' stehen die Koordinaten des $j$ten Bildvektors:

$$A' = \mathrm{M}_{\mathcal{B}'}^{\mathcal{C}'}(\partial) = \begin{bmatrix} 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Darstellung einer linearen Abbildung durch eine Matrix

K128
Erläuterung

🙂 Sie sehen an diesem Beispiel sehr eindrücklich, dass die darstellende Matrix sensibel von den gewählten Basen abhängt.

🙂 Die Form dieser Matrix ist interessant, siehe K1H, insbesondere wenn wir $\partial\colon \mathbb{R}[X]_{\leq n} \to \mathbb{R}[X]_{\leq n}$ als Endomorphismus betrachten.

Darstellung einer linearen Abbildung durch eine Matrix

Aufgabe: Stellen Sie das Integral $\int : \mathbb{R}[X]_{\leq 2} \to \mathbb{R}[X]_{\leq 3}$ als Matrix $B := \mathrm{M}_{\mathcal{C}}^{\mathcal{B}}(\int)$ bezüglich der Monombasen dar.

$$\int : P \mapsto Q \quad \text{sodass } \partial Q = P \text{ und } Q(0) = 0$$

Lösung: Zu jedem Basisvektor X^i der Basis $\mathcal{C} = (X^i)_{i=0}^2$ schreiben wir den Bildvektor $\int(X^i) = \sum_{j=0}^3 X^j b_{ji}$ in der Basis $\mathcal{B} = (X^j)_{j=0}^3$.

$$\begin{aligned}
X^0 \mapsto \int X^0 = X &= 0 \cdot X^0 + 1 \cdot X^1 + 0 \cdot X^2 + 0 \cdot X^3, \\
X^1 \mapsto \int X^1 = \tfrac{1}{2}X^2 &= 0 \cdot X^0 + 0 \cdot X^1 + \tfrac{1}{2} \cdot X^2 + 0 \cdot X^3, \\
X^2 \mapsto \int X^2 = \tfrac{1}{3}X^3 &= 0 \cdot X^0 + 0 \cdot X^1 + 0 \cdot X^2 + \tfrac{1}{3} \cdot X^3.
\end{aligned}$$

In der $i$ten Spalte von B steht das Bild des $i$ten Basisvektors:

$$B = \mathrm{M}_{\mathcal{C}}^{\mathcal{B}}(\int) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{3} \end{bmatrix}$$

Darstellung einer linearen Abbildung durch eine Matrix

Darstellung einer linearen Abbildung durch eine Matrix

Aufgabe: Stellen Sie das Integral $\int : \mathbb{R}[X]_{\leq 2} \to \mathbb{R}[X]_{\leq 3}$ als Matrix $B' := \mathrm{M}_{\mathcal{C}}^{\mathcal{B}}(\int)$ bezüglich der faktoriellen Basen dar.

$$\int : P \mapsto Q \quad \text{sodass } \partial Q = P \text{ und } Q(0) = 0$$

Lösung: Zu jedem Basisvektor $\frac{1}{i!}X^i$ der Basis $\mathcal{C}' = (\frac{1}{i!}X^i)_{i=0}^2$ schreiben wir den Bildvektor $\int(\frac{1}{i!}X^i) = \sum_{j=0}^3 \frac{1}{j!}X^j b'_{ji}$ in der Basis $\mathcal{B}' = (\frac{1}{j!}X^j)_{j=0}^3$.

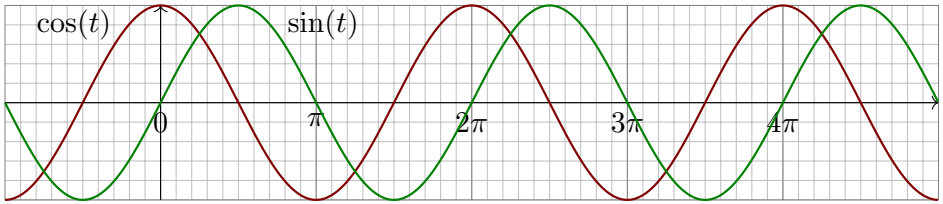
$$\begin{aligned}
\tfrac{1}{0!}X^0 \mapsto \tfrac{1}{1!}X^1 &= 0 \cdot \tfrac{1}{0!}X^0 + 1 \cdot \tfrac{1}{1!}X^1 + 0 \cdot \tfrac{1}{2!}X^2 + 0 \cdot \tfrac{1}{3!}X^3, \\
\tfrac{1}{1!}X^1 \mapsto \tfrac{1}{2!}X^2 &= 0 \cdot \tfrac{1}{0!}X^0 + 0 \cdot \tfrac{1}{1!}X^1 + 1 \cdot \tfrac{1}{2!}X^2 + 0 \cdot \tfrac{1}{3!}X^3, \\
\tfrac{1}{2!}X^2 \mapsto \tfrac{1}{3!}X^3 &= 0 \cdot \tfrac{1}{0!}X^0 + 1 \cdot \tfrac{1}{1!}X^1 + 0 \cdot \tfrac{1}{2!}X^2 + 1 \cdot \tfrac{1}{3!}X^3.
\end{aligned}$$

In der $i$ten Spalte von B' steht das Bild des $i$ten Basisvektors:

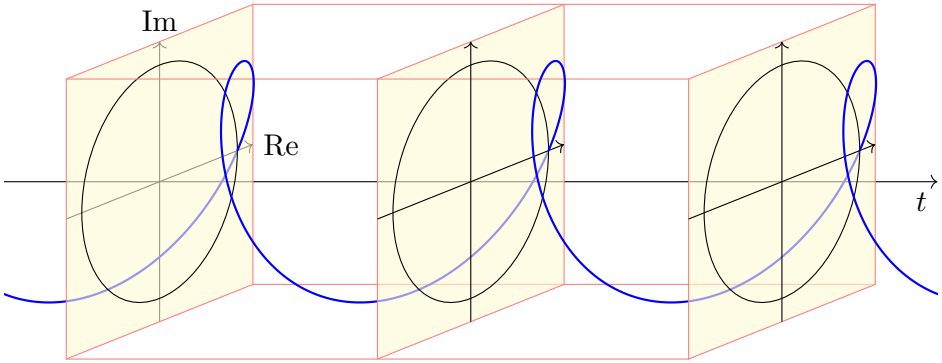
$$B' = \mathrm{M}_{\mathcal{C}'}^{\mathcal{B}'}(\int) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Darstellung einer linearen Abbildung durch eine Matrix

Erinnerung: die komplexe Exponentialfunktion



Die komplexe Exponentialfunktion $\mathbb{R} \to \mathbb{C} : t \mapsto \mathrm{e}^{\mathrm{i}t} = \cos(t) + \mathrm{i}\sin(t)$:



Erinnerung: die komplexe Exponentialfunktion

Sie kennen die reellen Funktionen Sinus und Cosinus, $\sin, \cos : \mathbb{R} \to \mathbb{R}$.
Diese fassen wir in der komplexen Exponentialfunktion zusammen:

$$g \,:\, \mathbb{R} \to \mathbb{C} \,:\, t \mapsto \mathrm{e}^{\mathrm{i}t} = \cos t + \mathrm{i}\sin t.$$

Die obige Graphik macht dies dreidimensional anschaulich.
In der komplexen Ebene $\mathbb{C} = \mathbb{R}^2$ beschreibt g die Kreislinie.
Wenn wir gleichzeitig die Zeitachse nach rechts abtragen,
so erhalten wir die gezeigte rechtshändige Schraubenlinie.

Die komplex-konjugierte Funktion

$$\overline{g} \,:\, \mathbb{R} \to \mathbb{C} \,:\, t \mapsto \mathrm{e}^{-\mathrm{i}t} = \cos t - \mathrm{i}\sin t$$

beschreibt entsprechend eine linkshändige Schraubenlinie.

Erinnerung: die komplexe Exponentialfunktion

Aufgabe: Zeigen Sie $g' = \mathrm{i}g$ durch (1) Ableiten und (2) geometrisch.

Lösung: (1) Wir leiten g termweise ab und vergleichen:

$$\begin{aligned} g(t) &= \cos t + \mathrm{i}\sin t \\ g'(t) &= -\sin t + \mathrm{i}\cos t \\ \mathrm{i}g(t) &= \mathrm{i}\cos t - \sin t \end{aligned}$$

(2) Wir können alle Ableitungen auch geometrisch bestimmen!
Wir benötigen dazu nur eine Information (die ich voraussetze):
g durchläuft die Kreislinie mit konstanter Geschwindigkeit 1.

Die Tangente an den Kreis steht senkrecht auf den Radius, hier $g(t)$.
Also ist der Geschwindigkeitsvektor $g'(t)$ ein reelles Vielfaches von $\mathrm{i}g(t)$.
Da wir zudem $|g'(t)| = 1$ und die Richtung kennen, folgt $g'(t) = \mathrm{i}g(t)$.

Erinnerung: die komplexe Exponentialfunktion

Das obige Bild hilft der Anschauung, für unsere nächsten Rechnungen benötigen wir zudem die Ableitungen. Den „Ableitungsoperator“ wollen wir in den folgenden Beispielen als lineare Abbildung betrachten und bezüglich geeigneter Basen als Matrix darstellen.

Darstellung einer linearen Abbildung durch eine Matrix

K137

Aufgabe: Wir arbeiten über dem Körper $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$.
Wir betrachten den Funktionenraum $\mathbb{K}^{\mathbb{R}} = \mathrm{Abb}(\mathbb{R}, \mathbb{K})$ über $\mathbb{K}$ und darin

$$V := \langle \cos, \sin \rangle_{\mathbb{K}} = \{ f : \mathbb{R} \to \mathbb{K} : t \mapsto a\cos(t) + b\sin(t) \mid a, b \in \mathbb{K} \}.$$

(1) Zeigen Sie, dass $\mathcal{A} = (\cos, \sin)$ eine Basis von V über $\mathbb{K}$ ist.
(2) Stellen Sie die Ableitung $\partial : V \to V$ als Matrix bezüglich $\mathcal{A}$ dar.

Lösung: (1) Die Familie $\mathcal{A} = (\cos, \sin)$ erzeugt V, nach Konstruktion.
Zur Unabhängigkeit nutzen wir die $\mathbb{K}$–lineare Abbildung $\Psi : V \to \mathbb{K}^2$ mit

$$\Psi(f) = \begin{bmatrix} f(0) \\ f(\pi/2) \end{bmatrix}, \quad M = \big(\Psi(\cos), \Psi(\sin)\big) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Die Matrix M ist invertierbar, ihre Spalten sind also linear unabhängig.
Folglich ist auch $\mathcal{A} = (\cos, \sin)$ linear unabhängig über $\mathbb{K}$, dank J1I.
(2) Wir finden $\cos' = -\sin$ und $\sin' = \cos$. Die darstellende Matrix ist

$$\mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Darstellung einer linearen Abbildung durch eine Matrix

K138
Erläuterung

☺ Die lineare Unabhängigkeit lässt sich in diesem Beispiel nicht direkt mit dem Gauß–Algorithmus berechnen. Doch wir können linear abbilden in einen Koordinatenraum $\mathbb{K}^n$ und dann Bemerkung J1I anwenden.

Bemerkung: Alternativ nutzen wir die Abbildung $\Psi : V \to \mathbb{K}^2$ mit

$$\Psi(f) = \begin{bmatrix} f(0) \\ f'(0) \end{bmatrix}, \quad M = \big(\Psi(\cos), \Psi(\sin)\big) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Die Matrix M ist invertierbar, ihre Spalten sind also linear unabhängig.
Folglich ist auch $\mathcal{A} = (\cos, \sin)$ linear unabhängig über $\mathbb{K}$, dank J1I.

☺ Der Raum $V = \langle \cos, \sin \rangle_{\mathbb{K}} \leq \mathbb{K}^{\mathbb{R}}$ hat zunächst keine Koordinaten:
Es gibt kein „kanonisches“ oder „naturgegebenes“ Koordinatensystem.

Für konkrete Rechnungen können wir jedoch Koordinaten einführen,
und die naheliegende Wahl hierzu ist die Basis $\mathcal{A} = (\cos, \sin)$

Die folgende Aufgabe zeigt eine weitere mögliche Basiswahl.
Die darstellende Matrix wird dann sogar diagonal!

Darstellung einer linearen Abbildung durch eine Matrix

K139

Aufgabe: Im Funktionenraum $\mathbb{C}^{\mathbb{R}} = \mathrm{Abb}(\mathbb{R}, \mathbb{C})$ über $\mathbb{C}$ betrachten wir $g(t) = \mathrm{e}^{\mathrm{i}t} = \cos t + \mathrm{i}\sin t$ und $\overline{g}(t) = \mathrm{e}^{-\mathrm{i}t} = \cos t - \mathrm{i}\sin t$, sowie

$$\begin{aligned} V &:= \langle \cos, \sin \rangle_{\mathbb{C}}^{!} \geq \langle g, \overline{g} \rangle_{\mathbb{C}} \\ &= \{ f : \mathbb{R} \to \mathbb{C} : t \mapsto c_1 \mathrm{e}^{\mathrm{i}t} + c_2 \mathrm{e}^{-\mathrm{i}t} \mid c_1, c_2 \in \mathbb{C} \}. \end{aligned}$$

(1) Zeigen Sie, dass auch $\mathcal{B} = (g, \overline{g})$ eine Basis von V über $\mathbb{C}$ ist.
(2) Stellen Sie die Ableitung $\partial : V \to V$ als Matrix bezüglich $\mathcal{B}$ dar.

Lösung: (1) Die Familie $\mathcal{B} = (g, \overline{g})$ erzeugt $V = \langle \cos, \sin \rangle_{\mathbb{C}}^{!}$, denn

$$\begin{aligned} \cos(t) &= \mathrm{Re}\, g(t) = \tfrac{1}{2}[g(t) + \overline{g}(t)] \ \in \langle g, \overline{g} \rangle_{\mathbb{C}}, \\ \sin(t) &= \mathrm{Im}\, g(t) = \tfrac{1}{2\mathrm{i}}[g(t) - \overline{g}(t)] \in \langle g, \overline{g} \rangle_{\mathbb{C}}. \end{aligned}$$

Wegen $\dim_{\mathbb{C}}(V) = 2$ ist $\mathcal{B}$ minimal, also eine Basis von V, dank J2L.
(2) Wir finden $g' = \mathrm{i}g$ und $\overline{g}' = -\mathrm{i}\overline{g}$. Die darstellende Matrix ist also

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix}.$$

Darstellung einer linearen Abbildung durch eine Matrix

K140
Erläuterung

☺ Funktionenräume sind besonders lehrreiche Beispiele:

1. Sie sind relevant in der Analysis und vielen Anwendungen.
2. Wir rechnen nicht unmittelbar in einem Koordinatenraum.
3. Wir können jedoch hilfreiche Koordinaten einführen, ...
4. und dazu müssen wir die Definitionen ernst nehmen!

☺ Das vorliegende Beispiel zeigt, warum die komplexen Zahlen $\mathbb{C}$ hier nützlicher und somit „natürlicher“ sind als die reellen Zahlen $\mathbb{R}$:
In der Basis $\mathcal{B} = (g, \overline{g})$ wird die darstellende Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial)$ diagonal!
Das ist für viele Rechnungen einfacher und daher vorteilhaft.

☺ Außerdem ist die Exponentialfunktion (zuerst reell, dann komplex) die wichtigste Funktion der Analysis, daher kann es nicht schaden, sie hier als Beispiel zu untersuchen. Nutzen Sie die Querbezüge, denken Sie nicht in Schubladen, sondern lernen Sie vernetzt!

Darstellung einer linearen Abbildung durch eine Matrix

Beispiel K1G: Exponentialfunktionen und Diagonalmatrix

Wir arbeiten über $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$. Gegeben seien Konstanten $\lambda_0, \dots, \lambda_n$ in $\mathbb{K}$ mit $\lambda_i \neq \lambda_j$ für $i \neq j$. Wir betrachten die Funktionen

$$f_k : \mathbb{R} \to \mathbb{K} : t \mapsto \mathrm{e}^{\lambda_k t}.$$

Die Familie $\mathcal{B} = (f_0, \dots, f_n)$ ist linear unabhängig über $\mathbb{K}$. (Übung!)

$$\begin{aligned} V &:= \langle\, f_0, \dots, f_n \,\rangle_{\mathbb{K}}^{!} \\ &= \left\{\, f : \mathbb{R} \to \mathbb{K} : t \mapsto c_0\, \mathrm{e}^{\lambda_0 t} + \dots + c_n\, \mathrm{e}^{\lambda_n t} \;\middle|\; c_0, \dots, c_n \in \mathbb{K} \,\right\} \end{aligned}$$

Für die Ableitung finden wir $\partial f_k = \lambda_k f_k$. Die darstellende Matrix von $\partial : V \to V$ bezüglich der Basis $\mathcal{B}$ ist demnach eine **Diagonalmatrix**:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \operatorname{diag}(\lambda_0, \dots, \lambda_n) = \begin{bmatrix} \lambda_0 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}.$$

Darstellung einer linearen Abbildung durch eine Matrix

☺ Wenn Sie möchten, lesen Sie dieses Beispiel zunächst für $\mathbb{K} = \mathbb{R}$, sodass Sie vereinfachend nur reelle Funktionen $f : \mathbb{R} \to \mathbb{R}$ betrachten. Die Rechnung über $\mathbb{C}$ verläuft wörtlich genauso. Es ist daher günstig, beide Fälle $\mathbb{K} = \mathbb{R}, \mathbb{C}$ gleich zusammenfassend zu behandeln.

☺ Das ist ein schönes Beispiel für eine gelungene **Diagonalisierung**.
Die allgemeine Problemstellung lautet entsprechend: Gegeben ist eine lineare Abbildung $f : V \to V$. Hierzu wollen wir eine Basis $\mathcal{B}$ von V finden, sodass die darstellende Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f)$ möglichst einfache Gestalt hat, idealerweise sogar diagonal. Hier gelingt genau dies!

Die allgemeine Problemstellung der Diagonalisierung werden wir in Definition K2M gegen Ende des Kapitels zusammenfassen. Diagonalisierung ist ein zentrales Anliegen der Linearen Algebra; wir werden es in den nächsten Kapiteln genauer untersuchen.

Darstellung einer linearen Abbildung durch eine Matrix

Aufgabe: (1) Beweisen Sie, dass $f_0, \dots, f_n$ linear unabhängig sind. Untersuchen Sie hierzu die $\mathbb{K}$–lineare Abbildung $\Psi : V \to \mathbb{K}^{n+1}$ mit

$$\Psi(f) = \big(f(0), f'(0), \dots, f^{(n)}(0)\big)^{\mathsf{T}}.$$

Das entspricht dem Beginn der Taylor–Entwicklung im Punkt 0.

(2) Überprüfen Sie die behaupteten Ableitungen $\partial f_k = \lambda_k f_k$ und so die darstellende Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial)$ wie angegeben.

Lösung: (2) Reell ist dies klar, es gilt ebenso komplex.
Für jede komplexe Zahl $\lambda = \sigma + \mathrm{i}\tau$ mit $\sigma, \tau \in \mathbb{R}$ haben wir:

$$f(t) = \mathrm{e}^{\lambda t} = \mathrm{e}^{\sigma t} \cdot \mathrm{e}^{\mathrm{i}\tau t} = \mathrm{e}^{\sigma t}\big[\cos(\tau t) + \mathrm{i}\sin(\tau t)\big]$$

Nach den reellen Ableitungsregeln finden wir:

$$f'(t) = \sigma\, \mathrm{e}^{\sigma t} \cdot \mathrm{e}^{\mathrm{i}\tau t} + \mathrm{e}^{\sigma t} \cdot \mathrm{i}\tau\, \mathrm{e}^{\mathrm{i}\tau t} = \lambda\, \mathrm{e}^{\lambda t}.$$

Darstellung einer linearen Abbildung durch eine Matrix

Lösung: (1) Wir fassen die Bildvektoren als Matrix zusammen:

$$\Psi(f) = \begin{bmatrix} f(0) \\ f'(0) \\ \vdots \\ f^{(n)}(0) \end{bmatrix}, \quad M = \big(\Psi(f_0), \dots, \Psi(f_n)\big) = \begin{bmatrix} \lambda_0^0 & \lambda_1^0 & \dots & \lambda_n^0 \\ \lambda_0^1 & \lambda_1^1 & \dots & \lambda_n^1 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_0^n & \lambda_1^n & \dots & \lambda_n^n \end{bmatrix}.$$

Dies ist die Vandermonde–Matrix bzw. ihre Transponierte (Satz B3A). Die Matrix M ist invertierbar, ihre Spalten sind also linear unabhängig. Folglich sind auch $f_0, \dots, f_n$ linear unabhängig, dank J1I.

Bemerkung: Die darstellende Matrix von Ψ bezüglich der Basen $\mathcal{B} = (f_0, \dots, f_n)$ und $\mathcal{E} = (e_0, \dots, e_n)$ ist demnach $\mathrm{M}_{\mathcal{B}}^{\mathcal{E}}(\Psi) = M$.

Bemerkung: Alternativ können wir als Abbildung $\Psi : V \to \mathbb{K}^{n+1}$ auch die Auswertung an den Stellen $t = 0, 1, \dots, n$ betrachten. Wir erhalten dann die Vandermonde–Matrix zu $\mu_k = \mathrm{e}^{\lambda_k}$.

Darstellung einer linearen Abbildung durch eine Matrix

K145

Beispiel K1H: Exponentialfunktionen und Jordan–Block

Sei $\mathbb{K} = \mathbb{R}, \mathbb{C}$ und $\lambda \in \mathbb{K}$. Zu $k \in \mathbb{N}$ betrachten wir die Funktion

$$f_k : \mathbb{R} \to \mathbb{K} : t \mapsto \frac{t^k}{k!} \mathrm{e}^{\lambda t}.$$

Die Familie $\mathcal{B} = (f_0, \dots, f_n)$ ist linear unabhängig über $\mathbb{K}$. (Übung!)

$$\begin{aligned} V &:= \langle\, f_0, \dots, f_n \,\rangle_{\mathbb{K}}^{!} \\ &= \left\{\, f : \mathbb{R} \to \mathbb{K} : t \mapsto \left(c_0 + c_1 t + \cdots + c_n t^n\right) \mathrm{e}^{\lambda t} \;\middle|\; c_0, c_1, \dots, c_n \in \mathbb{K} \,\right\} \end{aligned}$$

Wir finden $\partial f_0 = \lambda f_0$ und $\partial f_k = \lambda f_k + f_{k-1}$ für $k \geq 1$. Die darstellende Matrix von $\partial : V \to V$ bezüglich der Basis $\mathcal{B}$ ist ein **Jordan–Block**:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix}$$

Darstellung einer linearen Abbildung durch eine Matrix

K146
Erläuterung

🙂 Wenn Sie möchten, lesen Sie dieses Beispiel zunächst für $\mathbb{K} = \mathbb{R}$, sodass Sie vereinfachend nur reelle Funktionen $f : \mathbb{R} \to \mathbb{R}$ betrachten. Die Rechnung über $\mathbb{C}$ verläuft wörtlich genauso. Es ist daher günstig, beide Fälle $\mathbb{K} = \mathbb{R}, \mathbb{C}$ gleich zusammenfassend zu behandeln.

🙂 Das ist ein schönes Beispiel für eine gelungene **Jordanisierung**.
Zu einer linearen Abbildung $f : V \to V$ wollen wir eine Basis $\mathcal{B}$ von V finden, sodass die darstellende Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f)$ möglichst einfache Gestalt hat. Diagonalisierung ist in diesem Beispiel nicht möglich, aber die gezeigte Jordan–Matrix ist die nächstbeste Lösung.

Darstellung einer linearen Abbildung durch eine Matrix

K147
Erläuterung

Aufgabe: (1) Beweisen Sie, dass $f_0, \dots, f_n$ linear unabhängig sind.
(2) Überprüfen Sie die behaupteten Ableitungen $\partial f_k = \lambda_k f_k + f_{k-1}$ und so die darstellende Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial)$ wie angegeben.

Lösung: (2a) Für $f_0(t) = \mathrm{e}^{\lambda t}$ wissen wir bereits $f_0'(t) = \lambda\, \mathrm{e}^{\lambda t}$.
Für $f_k(t) = \mathrm{e}^{\lambda t} t^k / k!$ mit $k \geq 1$ finden wir dank Produktregel:

$$f_k'(t) = \lambda\, \mathrm{e}^{\lambda t} t^k / k! + \mathrm{e}^{\lambda t} t^{k-1} / (k-1)! = \lambda f_k(t) + f_{k-1}(t)$$

(2b) Zur Aufstellung der Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial)$ setzen wir wie in (1) voraus, dass die Familie $\mathcal{B} = (f_0, \dots, f_n)$ tatsächlich eine Basis von V ist.
Die $k$te Spalte der Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial)$ besteht aus den Koeffizienten des Bildes $\partial f_k = \lambda_k f_k + f_{k-1}$. Wir erhalten die oben angegebene Matrix.

Darstellung einer linearen Abbildung durch eine Matrix

K148
Erläuterung

Lösung: (1a) Aus $f = \sum_{k=0}^{n} \alpha_k f_k$ mit $\alpha_0, \dots, \alpha_n \in \mathbb{K}$ folgt

$$f(t) = \mathrm{e}^{\lambda t} \sum_{k=0}^{n} \frac{\alpha_k}{k!} t^k.$$

für alle $t \in \mathbb{R}$. Somit gilt $f = 0$ nur, falls $\alpha_k = 0$ für alle k. (B3A, G3M).
(1b) Wir nutzen die lineare Abbildung $\Psi : V \to \mathbb{R}^n$ mit

$$\Psi(f) = \begin{bmatrix} f(0) \\ f'(0) \\ \vdots \\ f^{(n)}(0) \end{bmatrix}, \quad M = \big(\Psi(f_0), \dots, \Psi(f_n)\big) = \begin{bmatrix} 1 & 0 & \dots & 0 \\ * & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \dots & 1 \end{bmatrix}.$$

Die Matrix M ist invertierbar, ihre Spalten sind also linear unabhängig. Folglich sind auch $f_0, \dots, f_n$ linear unabhängig, dank J1I.

Bemerkung: Die darstellende Matrix von Ψ bezüglich der Basen $\mathcal{B} = (f_0, \dots, f_n)$ und $\mathcal{E} = (e_0, \dots, e_n)$ ist demnach $\mathrm{M}_{\mathcal{B}}^{\mathcal{E}}(\Psi) = M$.

Satz K1ı: Verträglichkeit mit Addition und Skalierung

Sei R ein Ring sowie V und W (rechts)lineare Räume über R. Gegeben sei eine Basis $\mathcal{V} = (v_i)_{i=1}^n$ von V und $\mathcal{W} = (w_i)_{i=1}^m$ von W.

(1) Die Menge $\mathrm{Hom}_R(V,W)$ ist eine Gruppe bezüglich punktweiser Addition, dank Satz I1ı. Das oben konstruierte Bijektionspaar

$$(\mathrm{L}_{\mathcal{V}}^{\mathcal{W}}, \mathrm{M}_{\mathcal{V}}^{\mathcal{W}}) \;:\; (R^{m\times n}, +) \;\cong\; (\mathrm{Hom}_R(V,W), +)$$

ist ein Isomorphismus abelscher Gruppen.

(2) Ist R zudem kommutativ, so ist auch $\mathrm{Hom}_R(V,W)$ ein R–linearer Raum bezüglich punktweiser Skalierung, dank Satz I1ı. Damit ist

$$(\mathrm{L}_{\mathcal{V}}^{\mathcal{W}}, \mathrm{M}_{\mathcal{V}}^{\mathcal{W}}) \;:\; (R^{m\times n}, +, \cdot) \;\cong\; (\mathrm{Hom}_R(V,W), +, \cdot)$$

sogar ein Isomorphismus R–linearer Räume. Insbesondere gilt

$$\dim_R \mathrm{Hom}_R(V,W) = \dim_R(R^{m\times n}) = mn.$$

Anschaulich gesagt:

1. Wenn Sie Matrizen A und A' in $R^{m\times n}$ addieren, dann addieren sich die zugehörigen linearen Abbildungen f und f' in $\mathrm{Hom}_R(V,W)$.
2. Wenn Sie eine Matrix A in $R^{m\times n}$ skalieren zu λA, dann skaliert auch die zugehörige lineare Abbildung f in $\mathrm{Hom}_R(V,W)$ zu λf.

Gerade diese grundlegenden Rechenregeln werden wir später oft und gerne nutzen, meist sogar ohne es weiter zu bemerken. Es ist daher hilfreich, sie hier explizit zu formulieren… und auch zu beweisen.

Aufgabe: Rechnen Sie diese beiden Aussagen nach!

Lösung: (1) Gegeben seien Matrizen A und A' in $R^{m\times n}$ mit ihren linearen Abbildungen $f = \mathrm{L}_{\mathcal{V}}^{\mathcal{W}}(A)$ und $f' = \mathrm{L}_{\mathcal{V}}^{\mathcal{W}}(A')$. Wir finden:

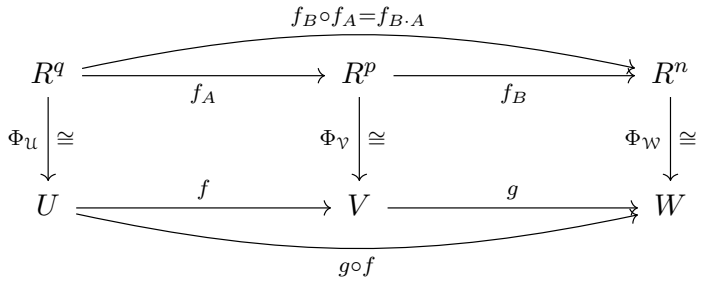
$$\begin{aligned}\mathrm{L}_{\mathcal{V}}^{\mathcal{W}}(A+A') \;:\; v = \sum_{j=1}^n v_j\lambda_j &\mapsto \sum_{i=1}^m w_i \sum_{j=1}^n (a_{ij}+a'_{ij})\lambda_j \\ &= \sum_{i=1}^m w_i \sum_{j=1}^n a_{ij}\lambda_j + \sum_{i=1}^m w_i \sum_{j=1}^n a'_{ij}\lambda_j = f(v) + f'(v)\end{aligned}$$

(2) Für jeden Skalar $\mu \in R$ gilt dann entsprechend dank Kommutativität:

$$\begin{aligned}\mathrm{L}_{\mathcal{V}}^{\mathcal{W}}(A\mu) \;:\; v = \sum_{j=1}^n v_j\lambda_j &\mapsto \sum_{i=1}^m w_i \sum_{j=1}^n a_{ij}\mu\lambda_j \\ &= \sum_{i=1}^m w_i \sum_{j=1}^n a_{ij}\lambda_j\mu = f(v)\mu\end{aligned}$$

🙂 Alternativ genügt es jeweils, die Bilder der Basis $\mathcal{V}$ zu vergleichen.

Darstellung linearer Abbildungen durch Matrizen



Satz K1J: Matrixmultiplikation und Komposition

Sei R ein Ring sowie U, V, W (rechts)lineare Räume über R mit Basen $\mathcal{U} = (u_i)_{i=1}^q$ von U und $\mathcal{V} = (v_j)_{j=1}^p$ von V und $\mathcal{W} = (w_k)_{k=1}^n$ von W.

(1) Für je zwei Matrizen $A \in R^{p\times q}$ und $B \in R^{n\times p}$ gilt:

$$\mathrm{L}_{\mathcal{U}}^{\mathcal{W}}(B \cdot A) = \mathrm{L}_{\mathcal{V}}^{\mathcal{W}}(B) \circ \mathrm{L}_{\mathcal{U}}^{\mathcal{V}}(A)$$

(2) Für je zwei R–lineare Abbildungen $f : U \to V$ und $g : V \to W$ folgt:

$$\mathrm{M}_{\mathcal{U}}^{\mathcal{W}}(g \circ f) = \mathrm{M}_{\mathcal{V}}^{\mathcal{W}}(g) \cdot \mathrm{M}_{\mathcal{U}}^{\mathcal{V}}(f)$$

Darstellung linearer Abbildungen durch Matrizen

Die Grundidee des Beweises ist im obigen Diagramm dargestellt!

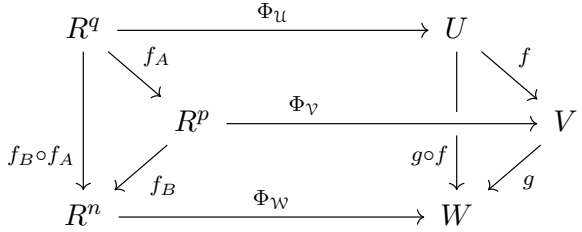
Für je zwei Matrizen $A \in R^{p\times q}$ und $B \in R^{n\times p}$ haben wir die linearen Abbildungen $f_A : R^q \to \mathbb{R}^p : x \mapsto y = Ax$ und $f_B : R^p \to R^q : y \mapsto z = Ay$. Die Komposition ist dann $f_B \circ f_A = f_{B\cdot A}$, denn für alle $x \in R^q$ gilt:

$$(f_B \circ f_A)(x) = f_B(f_A(x)) = B(Ax) = (BA)x = f_{BA}(x)$$

Diese Eigenschaft überträgt sich nun allgemein durch das Bijektionspaar (L, M) wie im Satz ausformuliert.

Darstellung linearer Abbildungen durch Matrizen

Hier noch einmal dasselbe Diagramm in anderer Darstellung:



Aufgabe: Beweisen Sie den Satz nach Vorbild der obigen Diagramme.

Darstellung linearer Abbildungen durch Matrizen

Lösung: (1) Zu $A \in R^{p\times q}$ und $B \in R^{n\times p}$ gilt:

$$\begin{aligned} \mathrm{L}_{\mathcal{V}}^{\mathcal{W}}(B) \circ \mathrm{L}_{\mathcal{U}}^{\mathcal{V}}(A) &\overset{\text{Def}}{=} \Phi_{\mathcal{W}} f_B \Phi_{\mathcal{V}}^{-1} \circ \Phi_{\mathcal{V}} f_A \Phi_{\mathcal{U}}^{-1} \\ &\overset{\text{Ass}}{=} \Phi_{\mathcal{W}} f_{B\cdot A} \Phi_{\mathcal{U}}^{-1} \overset{\text{Def}}{=} \mathrm{L}_{\mathcal{U}}^{\mathcal{W}}(B \cdot A) \end{aligned}$$

(2) Zu $f : U \to V$ und $g : V \to W$ sowie $A = \mathrm{M}_{\mathcal{U}}^{\mathcal{V}}(f)$ und $B = \mathrm{M}_{\mathcal{V}}^{\mathcal{W}}(g)$ gilt:

$$\begin{aligned} \mathrm{M}_{\mathcal{U}}^{\mathcal{W}}(g \circ f) &\overset{\text{K1F}}{=} \mathrm{M}_{\mathcal{U}}^{\mathcal{W}}(\mathrm{L}_{\mathcal{V}}^{\mathcal{W}}(B) \circ \mathrm{L}_{\mathcal{U}}^{\mathcal{V}}(A)) \\ &\overset{(1)}{=} \mathrm{M}_{\mathcal{U}}^{\mathcal{W}}(\mathrm{L}_{\mathcal{U}}^{\mathcal{W}}(B \cdot A)) \overset{\text{K1F}}{=} B \cdot A \overset{\text{Def}}{=} \mathrm{M}_{\mathcal{V}}^{\mathcal{W}}(g) \cdot \mathrm{M}_{\mathcal{U}}^{\mathcal{V}}(f) \end{aligned}$$

☺ Der Beweis übersetzt das Diagramm in explizite Formeln.

Matrixdarstellung von Homomorphismen und Komposition

Aufgabe: Stellen Sie die Ableitung $\partial : \mathbb{R}[X]_{\leq 3} \to \mathbb{R}[X]_{\leq 2}$ als Matrix $A := \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\partial)$ bezüglich der Monombasen $\mathcal{B} = (X^j)_{j=0}^3$ und $\mathcal{C} = (X^i)_{i=0}^2$ dar, ebenso das Integral $\int : \mathbb{R}[X]_{\leq 2} \to \mathbb{R}[X]_{\leq 3}$ als Matrix B.

Was erwarten Sie für die Produkte $A \cdot B$ und $B \cdot A$?

Lösung: Wir finden

$$A = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\partial) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \quad B = \mathrm{M}_{\mathcal{C}}^{\mathcal{B}}(\textstyle\int) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/3 \end{bmatrix}.$$

Für die Produkte gilt

$$A \cdot B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad B \cdot A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

☺ Das entspricht dem HDI (I1S, K1C), hier durch Matrizen formuliert.

Matrixdarstellung von Homomorphismen und Komposition

Matrixdarstellung von Endomorphismen und Komposition

Aufgabe: Stellen Sie die Ableitung $\partial : \mathbb{R}[X]_{\leq 3} \to \mathbb{R}[X]_{\leq 3}$ als Matrix A bezüglich der Monombasis $\mathcal{B}$ dar, ebenso $\partial^2 = \partial \circ \partial$ als Matrix B. Vergleichen Sie die Matrix B mit dem Produkt $A \cdot A$. Was erwarten Sie?

Lösung: Wir finden

$$A = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad B = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial^2) = \begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

☺ Tatsächlich gilt $A \cdot A = B$, wie vom Kompositionssatz K1K garantiert.

Bemerkung: In der faktoriellen Basis $\mathcal{B}'$ finden wir

$$A' = \mathrm{M}_{\mathcal{B}'}^{\mathcal{B}'}(\partial) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad B' = \mathrm{M}_{\mathcal{B}'}^{\mathcal{B}'}(\partial^2) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

☺ Auch hier gilt $A' \cdot A' = B'$, wie vom Kompositionssatz K1K garantiert.

Matrixdarstellung von Endomorphismen und Komposition

Darstellung von Endomorphismen und Automorphismen

$$\begin{array}{ccc} R^n & \xrightarrow{f_A} & R^n \\ {\scriptstyle \Phi_{\mathcal{B}}}\downarrow{\scriptstyle \cong} & & {\scriptstyle \Phi_{\mathcal{B}}}\downarrow{\scriptstyle \cong} \\ V & \xrightarrow{f} & V \end{array}$$

Korollar K1K: Endomorphismenring und Automorphismengruppe

Sei V ein (rechts)linearer Raum über R mit Basis $\mathcal{B} = (b_i)_{i=1}^n$.
Das oben konstruierte Bijektionspaar

$$(\mathrm{L}_{\mathcal{B}}^{\mathcal{B}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}) \,:\, (R^{n\times n}, +, \cdot) \;\cong\; (\mathrm{End}_R(V), +, \circ)$$

ist ein Isomorphismus von Ringen. Insbesondere ist

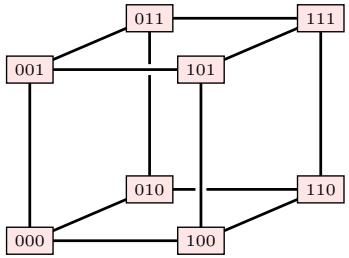
$$(\mathrm{L}_{\mathcal{B}}^{\mathcal{B}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}) \,:\, (\mathrm{GL}_n\, R, \cdot) \;\cong\; (\mathrm{Aut}_R(V), \circ)$$

ein Isomorphismus von Gruppen.

Darstellung von Endomorphismen und Automorphismen

Beweis: Die Verträglichkeit mit der Addition haben wir in Satz K1I bewiesen. Die Verträglichkeit mit Multiplikation und Komposition ist der Spezialfall $U = V = W$ in Satz K1J. QED

Darstellung von Endomorphismen und Automorphismen



Aufgabe: Wir betrachten die abelsche Gruppe $(V, +) = (\mathbb{F}_2^3, +)$.
Wie viele Elemente haben $\mathrm{End}(V, +)$ und $\mathrm{Aut}(V, +)$?

Lösung: Die Gruppe $(V, +)$ ist ein Vektorraum über $K = \mathbb{F}_2$. (I1L)
Jeder Gruppenhomomorphismus $f : (V, +) \to (V, +)$ ist K–linear.

☺ Damit greifen unsere Werkzeuge der Linearen Algebra!

Dank K1K haben wir $\mathrm{End}_K(V) \cong \mathbb{F}_2^{3\times 3}$, also $\sharp\,\mathrm{End}_K(V) = 2^9 = 512$.
Aus $\mathrm{Aut}_K(V) \cong \mathrm{GL}_3\,\mathbb{F}_2$ folgt $\sharp\,\mathrm{Aut}_K(V) = 7 \cdot 6 \cdot 4 = 168$, siehe J218.

Darstellung von Endomorphismen und Automorphismen

☺ Eine Automorphismengruppe zu bestimmen ist meist schwierig.
Warum ist es hier nun so leicht? Wir haben die starken Werkzeuge der Linearen Algebra, hier Vektorräume und Basen und Matrixdarstellung!

Die Modellmatrix $D^r_{m\times n}$ vom Rang r

K201

Definition K2A: die Modellmatrix $D^r_{m\times n}$ vom Rang r

Sei R ein Ring und $m,n,r\in\mathbb{N}$ mit $r\le\min\{m,n\}$. Wir definieren

$$D=D^r_{m\times n}:=\begin{bmatrix}1&\cdots&0&0&\cdots&0\\ \vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\ 0&\cdots&1&0&\cdots&0\\ 0&\cdots&0&0&\cdots&0\\ \vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\ 0&\cdots&0&0&\cdots&0\end{bmatrix}=\begin{bmatrix}1_{r\times r}&0_{r\times n'}\\ 0_{m'\times r}&0_{m'\times n'}\end{bmatrix}.$$

Dies nennen wir die **Modellmatrix** der Größe $m\times n$ vom Rang r und

$$f_D\,:\,R^n\to R^m\,:\,(x_1,\dots,x_r,\dots,x_n)\mapsto(x_1,\dots,x_r,0,\dots,0)$$

die zugehörige R–lineare **Modellabbildung**. Daran lesen wir ab:

$$\begin{aligned}\operatorname{im}(f_D)&=\operatorname{im}(D^r_{m\times n})=\langle\,e_1,\dots,e_r\,\rangle^!_R\le R^m,\\ \ker(f_D)&=\ker(D^r_{m\times n})=\langle\,e_{r+1},\dots,e_n\,\rangle^!_R\le R^n.\end{aligned}$$

Die Modellmatrix $D^r_{m\times n}$ vom Rang r

K202

☺ Die Modellabbildung f_D ist besonders einfach und übersichtlich.
Erstaunlicherweise lässt sich *jede* lineare Abbildung so darstellen!

Definition K2B: Rang und Defekt

Sei $f:V\to W$ eine lineare Abbildung über einem Divisionsring R.

Wir definieren den **Rang** und den **Defekt** von $f:V\to W$ durch

$$\operatorname{rang}_R(f):=\dim_R\operatorname{im}(f)\quad\text{und}\quad\operatorname{def}_R(f):=\dim_R\ker(f).$$

Erinnerung: Dank Dimensionsformel J2N gilt

$$\operatorname{rang}(f)+\operatorname{def}(f)=\dim(V).$$

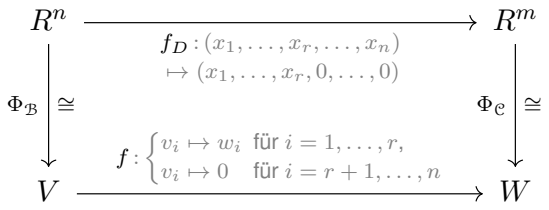
Typisches Beispiel:: Wir betrachten die obige Modellabbildung:

$$f\,:\,R^n\to R^m\,:\,(x_1,\dots,x_r,\dots,x_n)\mapsto(x_1,\dots,x_r,0,\dots,0)$$

Hier gilt gilt $\operatorname{rang}(f)=r$ und $\operatorname{def}(f)=n-r$. Dieses Beispiel ist typisch:
Der folgende Satz zeigt, dass jede lineare Abbildung genau so aussieht.

Kanonische Darstellung einer linearen Abbildung

K203



Satz K2C: kanonische Darstellung einer linearen Abbildung

Sei $f:V\to W$ eine lineare Abbildung von R–Vektorräumen endlicher Dimension $n:=\dim_R(V)$ und $m:=\dim_R(W)$ mit Rang $r:=\operatorname{rang}_R(f)$.

Dann existieren Basen $\mathcal{B}=(v_1,\dots,v_n)$ von V und $\mathcal{C}=(w_1,\dots,w_m)$ von W mit $f(v_i)=w_i$ für $i=1,\dots,r$ und $f(v_i)=0$ für $i=r+1,\dots,n$.

Somit wird f dargestellt durch die Modellmatrix $D^r_{m\times n}=\mathrm{M}^{\mathcal{C}}_{\mathcal{B}}(f)$.

Beweis: Wir wählen eine Basis $w_1,\dots,w_r$ des Bildes $\operatorname{im}(f)\le W$ und ergänzen zu einer Basis $\mathcal{C}=(w_1,\dots,w_m)$ von W. Wir wählen Urbilder $v_1,\dots,v_r\in V$ mit $v_i\mapsto w_i$ und ergänzen durch eine Basis $v_{r+1},\dots,v_n$ des Kerns $\ker(f)$. Dank J2M ist $\mathcal{B}=(v_1,\dots,v_n)$ eine Basis von V. QED

Kanonische Darstellung einer linearen Abbildung

K204
Erläuterung

☺ Die Modellabbildung f_D ist besonders einfach und übersichtlich.
Erfreulicherweise lässt sich *jede* lineare Abbildung so darstellen:

Wir lesen die lineare Abbildung $f:V\to W$ in den richtigen Basen, und schon vereinfacht sich f zu unserer Modellabbildung f_D!

Ausblick: Die Analysis führt den Darstellungssatz K2C fort, lokal für jede glatte Abbildung $f:(\mathbb{R}^n,x_0)\to(\mathbb{R}^m,y_0)$ mit lokal konstantem Rang.

☺ Das ist die einfachst-mögliche Matrixdarstellung der Abbildung f.
Sie entsteht durch die Wahl angepasster Basen für Start und Ziel.

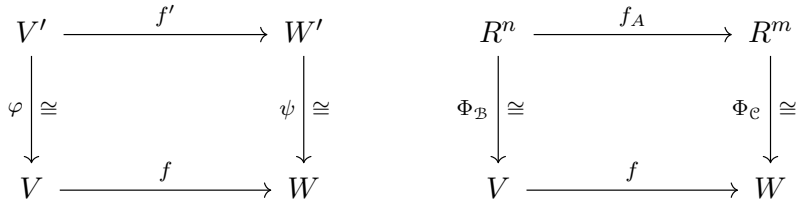
Es ist bemerkenswert, dass hierfür insgesamt nur drei Zahlen nötig sind.
Mit der kanonischen Darstellung lösen wir auch die Klassifikation K2E.

☺ Dabei klären wir zusätzlich zur Existenz auch die Eindeutigkeit:
Die Abbildung f ist äquivalent zu genau einer Modellabbildung.

Diese Klassifikation gibt uns einen guten Überblick aller Möglichkeiten:
Lineare Abbildungen von Vektorräumen sind schließlich sehr simpel!

Äquivalenz linearer Abbildungen

Wir betrachten lineare Abbildungen über einem Ring R:



Definition K2D: Äquivalenz R–linearer Abbildungen

Lineare Abbildungen $f' : V' \to W'$ und $f : V \to W$ heißen **äquivalent**, wenn hierzu Isomorphismen $\varphi : V' \xrightarrow{\sim} V$ und $\psi : W' \to W$ existieren, sodass $f \circ \varphi = \psi \circ f'$ gilt, also $f = \psi \circ f' \circ \varphi^{-1}$ und $f' = \psi^{-1} \circ f \circ \varphi$.

Wir schreiben hierfür $(\varphi, \psi) : f' \cong f$ oder kurz $f' \cong f$

Die Notation $(\varphi, \psi) : f' \cong f$ nennt explizit alle Daten, $f' \cong f$ nur implizit; die Isomorphismen müssen dann aus dem Kontext erschlossen werden.

Äquivalenz linearer Abbildungen

Beispiel: Jede lineare Abbildung $f : V \to W$ endlich-dimensionaler Vektorräume ist äquivalent zu einer Matrixdarstellung:

$$(\Phi_{\mathcal{B}}, \Phi_{\mathcal{C}}) \,:\, f_A \cong f \quad \text{kurz} \quad f_A \cong f \quad \text{mit} \quad A \in R^{m \times n}.$$

Noch bequemer und etwas schludrig schreiben wir $f \cong A$, in Worten: Die Abbildung $f : V \to W$ lässt sich durch die Matrix A darstellen.

Aufgabe: Zeigen Sie, dass $\cong$ eine Äquivalenzrelation zwischen linearen Abbildungen von R–linearen Räumen ist.

Lösung: Wir zeigen Reflexivität, Symmetrie, Transitivität.

Reflexivität: Für jede lineare Abbildung $f : V \to W$ gilt $(\mathrm{id}_V, \mathrm{id}_W) : f \cong f$, denn $f \circ \mathrm{id}_V = \mathrm{id}_W \circ f$.

Symmetrie: Aus $(\varphi, \psi) : f \cong g$, also $g \circ \varphi = \psi \circ f$, folgt $f \circ \varphi^{-1} = \psi^{-1} \circ g$, also $(\varphi^{-1}, \psi^{-1}) : g \cong f$.

Transitivität: Aus $(\varphi, \psi) : f \cong g$ und $(\varphi', \psi') : g \cong h$ folgt $(\varphi' \circ \varphi, \psi' \circ \psi) : f \cong h$, denn $h \circ \varphi' \circ \varphi = \psi' \circ g \circ \varphi = \psi' \circ \psi \circ f$.

Klassifikation linearer Abbildungen bis auf Äquivalenz

🙂 Nach der Klassifikation der endlich-dimensionalen Vektorräume (Satz J2J) folgt nun die Klassifikation ihrer linearen Abbildungen:

Satz K2E: Klassifikation linearer Abbildungen

Gegeben seien zwei lineare Abbildungen $f : V \to W$ und $f' : V' \to W'$ endlich-dimensionaler Vektorräume über einem Divisionsring R.

Genau dann sind f und f' äquivalent, kurz $f \cong f'$, wenn gilt:

$$(\dim V, \dim W, \operatorname{rang} f) = (\dim V', \dim W', \operatorname{rang} f')$$

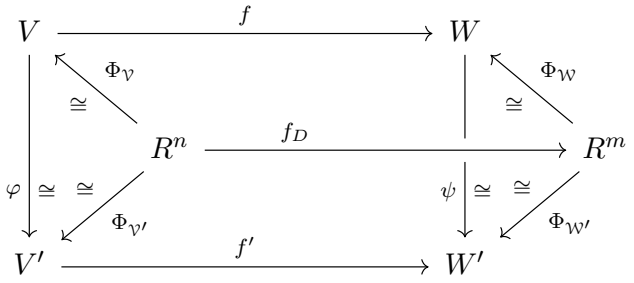
🙂 Die Lineare Algebra mag Ihnen zwar anfangs abstrakt erscheinen, doch die betrachteten Objekte sind schließlich einfach und übersichtlich!

Das Isomorphieproblem für Vektorräume über R wird durch eine einzige Zahl gelöst: die Dimension (als Kardinalität einer Basis), siehe Satz J2J.

Das Isomorphieproblem für lineare Abbildungen $f : V \to W$ wird durch drei einfache Kennzahlen vollständig gelöst: Neben den Dimensionen $\dim V$ und $\dim W$ benötigen Sie nur noch den Rang $\operatorname{rang} f$.

Klassifikation linearer Abbildungen bis auf Äquivalenz

Beweis: „⇒“: Die Äquivalenz $(\varphi, \psi) : f \cong f'$ besagt $f' \circ \varphi = \psi \circ f$ mit $\varphi : V \xrightarrow{\sim} V'$ und $\psi : W \xrightarrow{\sim} W'$. Daraus folgt $\dim V = \dim V'$ und $\dim W = \dim W'$ sowie $\operatorname{im}(f') = \operatorname{im}(f' \circ \varphi) = \operatorname{im}(\psi \circ f) \cong \operatorname{im}(f)$.



„⇐“: Es gelte $(\dim V, \dim W, \operatorname{rang} f) = (\dim V', \dim W', \operatorname{rang} f')$. Dank K2C finden wir Basen mit $D^r_{m \times n} = \mathrm{M}^{\mathcal{W}}_{\mathcal{V}}(f) = \mathrm{M}^{\mathcal{W}'}_{\mathcal{V}'}(f')$. Für $\varphi := \Phi_{\mathcal{V}'} \circ \Phi_{\mathcal{V}}^{-1}$ und $\psi := \Phi_{\mathcal{W}'} \circ \Phi_{\mathcal{W}}^{-1}$ gilt $(\varphi, \psi) : f \cong f'$. QED

Gauß–Algorithmus zur kanonischen Darstellung

Ausprobieren mit Gaël!

Mit Gauß wandeln wir jede Matrix $A \in R^{m\times n}$ zur Modellmatrix $D^r_{m\times n}$:

$$A = \begin{bmatrix} 3 & 6 & -6 & -6 & -1 \\ -2 & -4 & 3 & 1 & 5 \\ -1 & -2 & 3 & 5 & 4 \\ 1 & 2 & 1 & 7 & 1 \end{bmatrix} \xleftrightarrow{\text{Zeilen-operationen}} B = S^{-1}A = \begin{bmatrix} 1 & 2 & 0 & 4 & 0 \\ 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Spalten-operationen

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ * & * & * & 0 & 0 \end{bmatrix} \xleftrightarrow{\text{Zeilen-operationen}} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = D = S^{-1}AT$$

Spalten-operationen

☺ Wir haben $\operatorname{im} D = \langle\, e_1, \ldots, e_r \,\rangle^!_R$ und $\ker D = \langle\, e_{r+1}, \ldots, e_n \,\rangle^!_R$; dank $SD = AT$ folgt $\operatorname{im} A = \langle\, Se_1, \ldots, Se_r \,\rangle^!_R$ und $\ker A = \langle\, Te_{r+1}, \ldots, Te_n \,\rangle^!_R$.

Gauß–Algorithmus zur kanonischen Darstellung

Algo K2F: Gauß–Algorithmus zur kanonischen Darstellung

Eingabe: eine Matrix $A \in R^{m\times n}$ über einem Divisionsring R
Ausgabe: $S, S^{-1} \in \mathrm{GL}_m R$ und $T, T^{-1} \in \mathrm{GL}_n R$ mit $S^{-1}AT = D^r_{m\times n}$

1: Konstruiere S, S^{-1} zur reduzierten Zeilenstufenform $S^{-1}A$
2: Konstruiere T, T^{-1} zur red. Spaltenstufenform $S^{-1}AT = D^r_{m\times n}$
3: return (S, S^{-1}, T, T^{-1})

Beweis: Wir haben in Kapitel B den Gauß–Algorithmus zur reduzierten Zeilenstufenform ausgeführt (Satz B2C). Entsprechendes gilt auch für Spaltenumformungen; diese operieren von rechts. QED

☺ Der Gauß–Algorithmus konstruiert durch elementare Zeilen- bzw. Spaltenoperationen zugleich S, S^{-1} sowie T, T^{-1}, also die gesuchten Transformationsmatrizen zusammen mit ihrem Inversen.

Gauß–Algorithmus zur kanonischen Darstellung

Satz K2F: Gauß–Algorithmus zur kanonischen Darstellung

Sei $A \in R^{m\times n}$ eine Matrix über dem Divisionsring R.

(1) Der Gauß–Algorithmus K2F liefert hierzu invertierbare Matrizen $S, S^{-1} \in \mathrm{GL}_m(R)$ und $T, T^{-1} \in \mathrm{GL}_n(R)$, sodass $AT = SD^r_{m\times n}$ gilt.

(2) Daraus folgt $\operatorname{rang}(A) = r$ und $\operatorname{def}(A) = n - r$ und explizit

$$\operatorname{im}(A) = \langle\, Se_1, \ldots, Se_r \,\rangle^!_R,$$
$$\ker(A) = \langle\, Te_{r+1}, \ldots, Te_n \,\rangle^!_R.$$

☺ Dies ist ein Basiswechsel: Wir lesen die Matrix $A \in R^{m\times n}$ in den richtigen Basen, und schon vereinfacht sich A zur Modellmatrix $D^r_{m\times n}$!

☺ Die Bestimmung von Bild $\operatorname{im}(A)$ und Kern $\ker(A)$ haben wir bereits zuvor in Satz J1P gelöst. Mit Satz K2F sehen Sie hier nun eine elegante Umformulierung; beide Algorithmen tun im Wesentlichen dasselbe.

Gauß–Algorithmus zur kanonischen Darstellung

Beweis: An der Modellmatrix $D = D^r_{m\times n}$ lesen wir ab:

$$\operatorname{im}(D^r_{m\times n}) = \langle\, e_1, \ldots, e_r \,\rangle^!_R \leq R^m,$$
$$\ker(D^r_{m\times n}) = \langle\, e_{r+1}, \ldots, e_n \,\rangle^!_R \leq R^n.$$

Das Bild von A folgern wir aus $AT = SD$ gemäß

$$\operatorname{im}(A) = \operatorname{im}(AT) = \operatorname{im}(SD) = \langle\, Se_1, \ldots, Se_r \,\rangle^!_R.$$

Für den Kern von A finden wir entsprechend:

$$\begin{aligned} Ax = 0 &\iff (AT)T^{-1}x = 0 \iff (SD)T^{-1}x = 0 \\ &\iff T^{-1}x \in \ker(D) = \langle\, e_{r+1}, \ldots, e_n \,\rangle^!_R \\ &\iff x \in T\ker(D) = \langle\, Te_{r+1}, \ldots, Te_n \,\rangle^!_R. \end{aligned}$$

Damit sind Bild und Kern von A explizit bestimmt. QED

Äquivalenz von Matrizen

Für $A, B \in R^{m\times n}$ sowie $S \in \mathrm{GL}_m R$ und $T \in \mathrm{GL}_n R$ gilt:

$$S^{-1}AT = B \quad\Longleftrightarrow\quad AT = SB \quad\Longleftrightarrow\quad A = SBT^{-1}$$

Analog zu linearen Abbildungen (K2D) vereinbaren wir:

Definition K2G: Äquivalenz von Matrizen

Zwei Matrizen $A, B \in R^{m\times n}$ heißen **äquivalent**, wenn invertierbare Matrizen $S \in \mathrm{GL}_m R$ und $T \in \mathrm{GL}_n R$ existieren, sodass $AT = SB$ gilt.
Wir schreiben hierfür $(T, S) : B \cong A$ oder kurz $B \cong A$

Aufgabe: Dies ist eine Äquivalenzrelation auf $R^{m\times n}$ (siehe K206).

Lösung: Wir zeigen Reflexivität, Symmetrie, Transitivität.

Reflexivität: $(E_n, E_m) : A \cong A$, denn $AE_n = E_m A$.

Symmetrie: Aus $(T, S) : B \cong A$ folgt $(T^{-1}, S^{-1}) : A \cong B$.

Transitivität: Aus $(T, S) : A \cong B$ und $(T', S') : B \cong C$ folgt $(T' \circ T, S' \circ S) : A \cong C$, denn $C \circ T' \circ T = S' \circ B \circ T = S' \circ S \circ A$.

Äquivalenz von Matrizen

Analog zur Klassifikation K2E linearer Abbildungen erhalten wir aus dem Gauß–Algorithmus K2F nun die Klassifikation der Matrizen:

Satz K2H: Klassifikation von Matrizen bis auf Äquivalenz

Über jedem Divisionsring R gilt:

(1) Genau dann sind zwei Matrizen $A, B \in R^{m\times n}$ äquivalent, wenn sie gleichen **Rang** haben, also $\operatorname{rang} A = \operatorname{rang} B$ gilt.

(2) In jeder Äquivalenzklasse liegt genau eine Modellmatrix $D^r_{m\times n}$. Dieser kanonische Repräsentant heißt **Gauß–Normalform** (GNF)

Beweis: (1a) „⇒“: Der Rang ist invariant unter Äquivalenz $B = S^{-1}AT$, denn $\operatorname{im}(B) = BR^n = S^{-1}ATR^n = S^{-1}AR^n = S^{-1}\operatorname{im}(A) \cong \operatorname{im}(A)$.

(1b) „⇐“: Dank K2F sind A und B äquivalent zur Modellmatrix $D^r_{m\times n}$. Dank Symmetrie und Transivitität sind sie zueinander äquivalent.

(2) Mit denselben Argumenten folgt (b) Existenz und (a) Eindeutigkeit einer Modellmatrix $D^r_{m\times n}$ in jeder Äquivalenzklasse. QED

Äquivalenz und Invarianz

Das Äquivalenzproblem für Matrizen $A \in R^{m\times n}$ wird durch drei einfache Kennzahlen vollständig gelöst: Neben den Dimensionen (Zeilenzahl m und Spaltenzahl n) benötigen Sie nur noch den Rang $\operatorname{rang} A$.

Der Gauß–Algorithmus K2F erledigt diese Aufgabe gewohnt effizient. Ich betone erneut, dass wir hierzu über einem Divisionsring R arbeiten. Die allgemeine Definition K2G der Äquivalenz gilt über jedem Ring, der Klassifikationssatz K2H hingegen gilt nur über Divisionsringen.

Wir kommen damit erneut auf die grundlegenden Begriffe **Äquivalenz** und **Invarianz** zurück, die uns schon des Öfteren begegnet sind:

Aus Satz E1H kennen wir die wichtigste Invariante der Mathematik: Die Elementezahl ändert sich nicht unter Anwendung von Bijektionen!

In Satz J2J haben wir dies auf R–Vektorräume übertragen: Die R–Dimension ändert sich nicht unter R–linearen Bijektionen!

Allgemeiner übertragen wir dies nun auf den Rang, also die Dimension des Bildraums, von linearen Abbildungen (K2E) und von Matrizen (K2H).

Äquivalenz und Invarianz

Allgemein versteht die Mathematik unter einer **Invariante** folgendes: Jedem der betrachteten Objekte (hier: Matrizen $A \in R^{m\times n}$) wird eine Größe zugeordnet (hier: ihr Rang); diese Größe ändert sich nicht unter den betrachteten Umformungen (hier: Äquivalenz $(T, S) : B \cong A$).

Invarianten sind ein wichtiges Hilfsmittel bei Klassifikationsproblemen: Objekte mit unterschiedlichen Invarianten sind wesentlich verschieden. Manchmal gilt sogar die Umkehrung, und Objekte mit gleichen Werten unter der Invariante lassen sich ineinander umformen. Wir sprechen dann von einer **vollständigen Invarianten**. Genau das liegt hier vor!

Zeilenraum und Spaltenraum

K217

Jede Matrix $A \in R^{m\times n}$ definiert eine Familie von Zeilenvektoren $u_1, \ldots, u_m \in R^{1\times n}$ und von Spaltenvektoren $v_1, \ldots, v_n \in R^{m\times 1}$:

$$A = \begin{bmatrix} \text{—} & u_1 & \text{—} \\ & \vdots & \\ \text{—} & u_m & \text{—} \end{bmatrix} = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix}$$

Diese erzeugen den Zeilenraum bzw. den Spaltenraum:

Zeilenraum: $\mathrm{ZR}(A) := R\cdot u_1 + \cdots + R\cdot u_m = R^{1\times m}\cdot A \leq R^{1\times n}$

Spaltenraum: $\mathrm{SR}(A) := v_1\cdot R + \cdots + v_n\cdot R = A\cdot R^{n\times 1} \leq R^{m\times 1}$

Über einem Divisionsring R verfügen wir zudem über Dimensionen:

Zeilenrang: $\mathrm{zr}(A) := \dim_R \mathrm{ZR}(A)$

Spaltenrang: $\mathrm{sr}(A) := \dim_R \mathrm{SR}(A)$

Wir zeigen nun eine bemerkenswerte Gleichheit:

Zeilenrang = Spaltenrang

Zeilenraum und Spaltenraum

K218
Erläuterung

🙂 Wir folgen den richtigen Konventionen: Der Spaltenraum $\mathrm{SR}(A)$ ist rechtslinear über R, der Zeilenraum $\mathrm{ZR}(A)$ hingegen ist linkslinear!

Jede Matrix $A \in R^{m\times n}$ über einem Ring R induziert zwei Abbildungen:

$$f_A : R^{n\times 1} \to R^{m\times 1} : x \mapsto Ax, \quad \mathrm{im}(f_A) = A\cdot R^{n\times 1} \leq R^{m\times 1}$$
$$g_A : R^{1\times m} \to R^{1\times n} : y \mapsto yA, \quad \mathrm{im}(g_A) = R^{1\times m}\cdot A \leq R^{1\times n}$$

Dabei ist f_A rechtslinear über R, und g_A ist linkslinear über R, gemäß der üblichen Konvention: Matrizen und Skalare operieren auf entgegengesetzten Seiten. Mit dieser Regel sortiert sich alles von selbst!

Sei nun R ein Divisionsring, um den Gauß–Algorithmus anzuwenden: Dank Satz K2J haben beide Abbildungen f_A und g_A den gleichen Rang!

- Der Rang von f_A ist der Spaltenrang von A.
- Der Rang von g_A ist der Zeilenrang von A.

Die beiden Abbildungen f_A und g_A sind zunächst sehr unterschiedlich. Sie entstehen aus derselben Matrix A, aber auf verschiedene Weisen. Die Gleichheit von Spaltenrang und Zeilenrang ist bemerkenswert.

Zeilenraum und Spaltenraum

K219

Lemma K2I: Zeilenoperationen vs Spaltenoperationen

(1) Zeilenoperation durch $S \in \mathrm{GL}_m R$ ändert nicht den Zeilenraum:

$$\mathrm{ZR}(SA) \overset{\text{Def}}{=} R^{1\times m}\cdot S\cdot A = R^{1\times m}\cdot A \overset{\text{Def}}{=} \mathrm{ZR}(A)$$

Die Spaltenräume sind i.A. verschieden, doch immer isomorph:

$$\mathrm{SR}(SA) \overset{\text{Def}}{=} S\cdot A\cdot R^{n\times 1} \cong A\cdot R^{n\times 1} \overset{\text{Def}}{=} \mathrm{SR}(A)$$

(2) Spaltenoperation durch $T \in \mathrm{GL}_n R$ ändert nicht den Spaltenraum:

$$\mathrm{SR}(AT) \overset{\text{Def}}{=} A\cdot T\cdot R^{n\times 1} = A\cdot R^{n\times 1} \overset{\text{Def}}{=} \mathrm{SR}(A)$$

Die Zeilenräume sind i.A. verschieden, doch immer isomorph:

$$\mathrm{ZR}(AT) \overset{\text{Def}}{=} R^{1\times m}\cdot A\cdot T \cong R^{1\times m}\cdot A \overset{\text{Def}}{=} \mathrm{ZR}(A)$$

(3) Zeilenrang und Spaltenrang bleiben dabei immer erhalten! (J2I)

Zeilenraum und Spaltenraum

K220
Erläuterung

Beweis: Da die Matrizen $S \in \mathrm{GL}_m R$ und $T \in \mathrm{GL}_n R$ invertierbar sind, induzieren Sie die folgenden R–linearen Isomorphismen:

$$g_S : R^{1\times m} \xrightarrow{\sim} R^{1\times m} : y \mapsto yS, \qquad g_S^{-1} = g_{S^{-1}}$$
$$f_S : R^{m\times 1} \xrightarrow{\sim} R^{m\times 1} : x \mapsto Sx, \qquad f_S^{-1} = f_{S^{-1}}$$
$$f_T : R^{n\times 1} \xrightarrow{\sim} R^{n\times 1} : x \mapsto Tx, \qquad f_T^{-1} = f_{T^{-1}}$$
$$g_T : R^{1\times n} \xrightarrow{\sim} R^{1\times n} : y \mapsto yT, \qquad g_T^{-1} = g_{T^{-1}}$$

Daraus folgt die Gleichheit $R^{1\times m}\cdot S = R^{1\times m}$ und $T\cdot R^{n\times 1} = R^{n\times 1}$ sowie die Isomorphie der Teilräume $A\cdot R^{n\times 1} \cong S\cdot A\cdot R^{n\times 1}$ in $R^{m\times 1}$ und $R^{1\times m}\cdot A \cong R^{1\times m}\cdot A\cdot T$ in $R^{1\times n}$. QED

🙂 Beachten Sie die akribische Buchführung über rechts und links. Damit werden all unsere Rechnungen einfacher und transparenter! Das gilt allgemein, selbst wenn der Grundring R kommutativ ist.

🙂 Für die Matrizenrechnung müssen wir ohnehin links und rechts unterscheiden, also machen wir es gleich systematisch richtig.

Zeilenrang gleich Spaltenrang

K221

Satz K2J: Zeilenrang und Spaltenrang sind gleich.

Sei R ein Divisionsring. Für jede Matrix $A \in R^{m\times n}$ über R gilt dann:

Zeilenrang = Spaltenrang

Diesen gemeinsamen Wert nennen wir den Rang der Matrix A.

Beweis: Der Gauß–Algorithmus K2F liefert invertierbare Matrizen $S \in \mathrm{GL}_m R$ und $T \in \mathrm{GL}_n R$, sodass $S^{-1}AT = D^r_{m\times n}$. Dank K2I folgt:

$$\mathrm{ZR}(A) \cong \mathrm{ZR}(S^{-1}AT) \quad \text{und} \quad \mathrm{SR}(A) \cong \mathrm{SR}(S^{-1}AT)$$

Zeilen- und Spaltenraum wandeln, doch ihre Dimension bleibt gleich! Dank dem vorangegangenen Lemma K2I lesen wir den Rang ab:

$$\begin{aligned} \mathrm{zr}(A) &\overset{\text{K2I}}{=} \mathrm{zr}(S^{-1}AT) \overset{\text{Gauß}}{=} \mathrm{zr}(D^r_{m\times n}) \overset{\text{klar}}{=} r, \\ \mathrm{sr}(A) &\overset{\text{K2I}}{=} \mathrm{sr}(S^{-1}AT) \overset{\text{Gauß}}{=} \mathrm{sr}(D^r_{m\times n}) \overset{\text{klar}}{=} r. \end{aligned}$$

Für unsere Modellmatrix $D^r_{m\times n}$ ist die Aussage offensichtlich. QED

Zeilenrang gleich Spaltenrang

K222
Erläuterung

Das ist, wenn man's recht denkt, schon ein erstaunliches Ergebnis!

⚠ Zeilenraum und Spaltenraum haben zunächst nichts gemeinsam: Sie liegen in ganz verschiedenen Vektorräumen: $\mathrm{ZR}(A) \leq R^{1\times n}$ und $\mathrm{SR}(A) \leq R^{m\times 1}$. Insbesondere ist $\mathrm{ZR}(A)$ linkslinear über R und $\mathrm{SR}(A)$ rechtslinear über R, allein deshalb können sie nicht isomorph sein. Zeilenraum und Spaltenraum leben in verschiedenen Welten.

🙂 Dennoch haben $\mathrm{ZR}(A)$ und $\mathrm{SR}(A)$ dieselbe Dimension über R!

Der Beweis dank Gauß–Algorithmus K2F ist elegant und recht leicht: Wir müssen nur die Umformungen $S^{-1}AT = D^r_{m\times n}$ genau anschauen. Lemma K2I garantiert, dass sich Zeilen- und Spaltenrang dabei nicht ändern. Für unsere Modellmatrix $D^r_{m\times n}$ ist die Gleichheit offensichtlich.

🙂 Es hilft sehr, links und rechts zu unterscheiden, etwa in Lemma K2I! Ist R kommutativ, also ein Körper, so entfällt die formale Notwendigkeit.

Satz K2J bleibt so oder so erstaunlich und bemerkenswert.

Anwendungsbeispiel

K223
Ausprobieren mit Gaël!

Aufgabe: Sind die Spalten der folgenden Matrix eine Basis des $\mathbb{R}^5$?

$$A = \begin{bmatrix} 1 & 9 & 3 & 4 & 0 \\ 5 & 1 & 7 & 6 & 2 \\ 4 & 3 & 0 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 9 & 3 & 4 & 0 \\ 5 & 1 & 7 & 6 & 2 \\ 4 & 3 & 0 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 9 & 3 & 4 & 0 \\ 5 & 1 & 7 & 6 & 2 \\ 4 & 3 & 0 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 6 & 8 \end{bmatrix}$$

Lösung: Zwischen den Zeilen besteht eine *offensichtliche* Relation! Daher gilt Zeilenrang ≤ 4. Dank Satz K2J folgt Spaltenrang ≤ 4.

⚠ Die letzte Abschätzung ist zunächst *nicht* genauso offensichtlich, dazu müsste man rechnen, etwa mit Gauß J1P zur Zeilenstufenform.

🙂 Dank Satz K2J können wir uns diese erneute Rechnung sparen. Genau diese Rechnung haben wir im Beweis allgemein durchgeführt.

⚠ Die Relationen zwischen den Spalten sind *nicht* offensichtlich! Hier gilt $\ker(A) = \ker(B) = \ker(C) = (119, 52, 15, -158, 98)^\intercal \cdot \mathbb{R}$.

Anwendungsbeispiel

K224
Erläuterung

Als offensichtliche Relationen einer Familie gelten: (a) ein Nullvektor, (b) ein doppelter Vektor, (c) ein Vektor ist Vielfaches eines anderen.

Für die Zeilenvektoren liegt eine solche offensichtliche Relation vor. Relationen zwischen den Spalten $v_1, \ldots, v_5$ sind *nicht* offensichtlich.

Satz K2J garantiert, dass es eine nicht-triviale Relation geben muss, die Rechnung wird also erfolgreich sein. Probieren Sie es mit Gaël!

🙂 Mit dem Gauß–Verfahren J1P finden Sie:

$$119v_1 + 52v_2 + 15v_3 - 158v_4 + 98v_5 = 0$$

Genauer gilt $\ker = (119, 52, 15, -158, 98)^\intercal \cdot \mathbb{R}$, alle Relationen sind also Vielfache der obigen. Ich denke, das ist *nicht* offensichtlich.

🙂 Dies betont den Nutzen des Satzes: Zeilenrang gleich Spaltenrang! Je mehr Sie wissen und verstehen, desto weniger müssen Sie rechnen, Oder: Desto besser können Sie die Ergebnisse Ihrer Rechnungen prognostizieren und überprüfen, Fehler erkennen und beheben.

Zeilenoperationen und Spaltenoperationen

🙂 Wenn es nur darum geht, den Rang einer Matrix zu berechnen, dann dürfen wir Zeilenoperationen und Spaltenoperation beliebig mischen!

⚠ Zur Lösung des linearen Gleichungssystems $Ax = b$ wollen wir das möglichst vermeiden! Hier nutzen wir nur Zeilenoperationen $S \in \mathrm{GL}_m R$; die rechte Seite b transformieren wir dabei sorgsam mit:

$$Ax = b \quad \Longleftrightarrow (S^{-1}A)\,x = S^{-1}b$$

⚠ Wenn wir jedoch neben Zeilenoperationen auch Spaltenoperationen nutzen, so müssen wir auch die Unbekannte x geeignet transformieren:

$$Ax = b \quad \Longleftrightarrow (S^{-1}AT)\,T^{-1}x = S^{-1}b$$

🙂 Der Gauß–Algorithmus K2F transformiert A zur Modellmatrix $D^r_{m\times n}$. Richtig angewendet ist das eine sehr elegante und effiziente Methode.

Zur Vereinfachung genügt es glücklicherweise, nur Zeilenoperationen vorzunehmen: Zur Bestimmung von Bild und Kern siehe Satz J1P.

Zeilenoperationen und Spaltenoperationen

Sie sehen hier erneut ein sehr fruchtbares Zusammenspiel:

- Die Matrizenrechnung bietet uns effiziente Berechnungsverfahren, hier insbesondere den Gauß–Algorithmus in all seinen Varianten.
- Die Lineare Algebra untermauert dies durch eine starke Theorie als Grundlage, hier insbesondere zu Basen und Dimension.

Beide gemeinsam ergänzen und verstärken sich gegenseitig und arbeiten wunderbar zusammen, wie linke und rechte Hand.

Lernen Sie beides zu nutzen!

Matrixdualität und Invertierbarkeit

Aufgabe zur Wiederholung: Sei R ein Divisionsring.
Für jede quadratische Matrix $A \in R^{n\times n}$ sind äquivalent:

1. Surjektivität von f_A: Die Spalten von A erzeugen $R^{n\times 1}$.
2. Injektivität von f_A: Die Spalten von A sind linear unabhängig.
3. Bijektivität von f_A: Die Spalten von A sind eine Basis von $R^{n\times 1}$.
4. Injektivität von g_A: Die Zeilen von A sind linear unabhängig.
5. Surjektivität von g_A: Die Zeilen von A erzeugen $R^{1\times n}$.
6. Bijektivität von g_A: Die Zeilen von A sind eine Basis von $R^{1\times n}$.
7. Die Matrix A ist rechtsinvertierbar.
8. Die Matrix A ist linksinvertierbar.
9. Die Matrix A ist invertierbar.

Erklären Sie für möglichst viele Paare (i, j) mit $i, j \in \{1, \ldots, 9\}$, warum die Aussage i in obiger Liste die Aussage j impliziert. Nennen Sie den entsprechenden Satz, besser die Beweisidee, am besten formulieren Sie den Beweis selbstständig aus.

Matrixdualität und Invertierbarkeit

Satz B2D: Gauß–Algorithmus zur Lösung von $Ax = b$ und Inversion
Satz J1P: Dimensionsformel $\dim\ker f + \dim\operatorname{im} f = \dim V$ für $f : V \to W$
Satz K2J: Gleichheit von Zeilenrang und Spaltenrang für $A \in R^{m\times n}$

⇒	1	2	3	4	5	6	7	8	9
1	=	J1P	J1P		K2J		B2D		
2	J1P	=	J1P					B2D	
3	triv	triv	=						B2D
4				=	J1P’	J1P’	B2D’		
5	K2J			J1P’	=	J1P’		B2D’	
6				triv	triv	=			B2D’
7	B2D			B2D’			=	B2D	B2D
8		B2D			B2D’		B2D	=	B2D
9			B2D			B2D’	triv	triv	=

Ein Apostroph ’ bedeutet, dass wir Satz und Beweis für $Ax = b$ umformulieren zum entsprechenden Ergebnis für $yA = c$.

Die reduzierte Zeilenstufenform ist eindeutig.

Satz K2K: ∃&E der reduzierten Zeilenstufenform

Sei R ein Divisionsring und $A \in R^{m\times n}$ eine Matrix über R.

Existenz: Es existiert eine invertierbare Matrix $S \in \mathrm{GL}_m R$, für die $A' = SA \in R^{m\times n}$ in reduzierter Zeilenstufenform ist.

Eindeutigkeit: Ist zudem $T \in \mathrm{GL}_m R$ invertierbar und auch TA in reduzierter Zeilenstufenform, so gilt die Gleichheit $TA = SA = A'$.

Dies definiert zu A **die reduzierte Zeilenstufenform** $\mathrm{rref}(A) := A'$. Dasselbe gilt für **die reduzierte Spaltenstufenform** $\mathrm{rcef}(A)$ zu A.

⚠ Zu A ist die RZSF A' eindeutig, die Zeilenumformungen von A zu A' hingegen sind es nicht: Im Allgemeinen gilt $S \neq T$, aber $SA = TA = A'$.

🙂 Existenz und Eindeutigkeit sind Grundlage jeder Implementierung: Computer-Algebra-Systeme bieten hierzu den Befehl `rref(A)`.

🙂 Existenz und Eindeutigkeit sind auch willkommen für Klausuren: Der Rechenweg ist nicht eindeutig, das Ergebnis hingegen schon.

Die reduzierte Zeilenstufenform ist eindeutig.

Aufgabe: Beweisen Sie den Satz per Induktion über die Spaltenzahl n.

Lösung: (1) Die Existenz folgt aus dem Gauß–Algorithmus B2C.

(2) Der Fall $n = 0$ einer leeren Matrix ist trivial. Im Folgenden sei $n \geq 1$. Wir zerlegen $A = (v_1, \ldots, v_{n-1}, v_n) \in R^{m\times n}$ in die ersten $n-1$ Spalten $B = (v_1, \ldots, v_{n-1}) \in R^{m\times(n-1)}$ und die letzte Spalte $v_n \in R^{m\times 1}$.

Nach Voraussetzung sind SA und TA in reduzierter Zeilenstufenform, also auch SB und TB. Nach Induktionsvoraussetzung gilt $SB = TB$.

Zwei Fälle sind möglich: (a) Gilt $v_n \in \langle\, v_1, \ldots, v_{n-1} \,\rangle_R = \mathrm{SR}(B)$, also $v_n = Bx$ mit $x \in R^{(n-1)\times 1}$, so folgt $Sv_n = SBx = TBx = Tv_n$.

(b) Andernfalls gilt $v_n \notin \mathrm{SR}(B)$, also $Sv_n \notin \mathrm{SR}(SB)$ und $Tv_n \notin \mathrm{SR}(TB)$. Daraus folgt $Sv_n = Tv_n = e_r$ für diese reduzierten Zeilenstufenformen.

In beiden Fällen schließen wir $SA = TA$. QED

Die reduzierte Zeilenstufenform ist eindeutig.

Alle Lehrbücher zur Linearen Algebra erklären den Gauß–Algorithmus und dazu (mehr oder weniger explizit) die reduzierte Zeilenstufenform.

Erstaunlich viele kehren jedoch die Eindeutigkeit unter den Teppich und sprechen dann doch heimlich von „der“ reduzierten Zeilenstufenform.

Wir wollen es hier besser machen und sowohl die Existenz als auch die Eindeutigkeit klar benennen und beweisen. Das ist ehrliches Handwerk.

Die Eindeutigkeit hat eine ganz konkrete und praktische Bedeutung: Angenommen zwei Studierende untersuchen eine Matrix $A \in R^{m\times n}$, und jeder konstruiert seine RZSF durch seinem eigenen Rechenweg. Finden beide schließlich zu demselben Ergebnis? Satz K2K sagt ja!

Das ist durchaus erstaunlich, denn die Zeilenumformungen lassen noch sehr viele Freiheiten für die Ausführung der Rechnungen.

Die reduzierte Zeilenstufenform ist eindeutig.

Warum ist die Existenz einer reduzierten Zeilenstufenform relativ leicht, doch die Eindeutigkeit vergleichsweise schwierig zu beweisen?

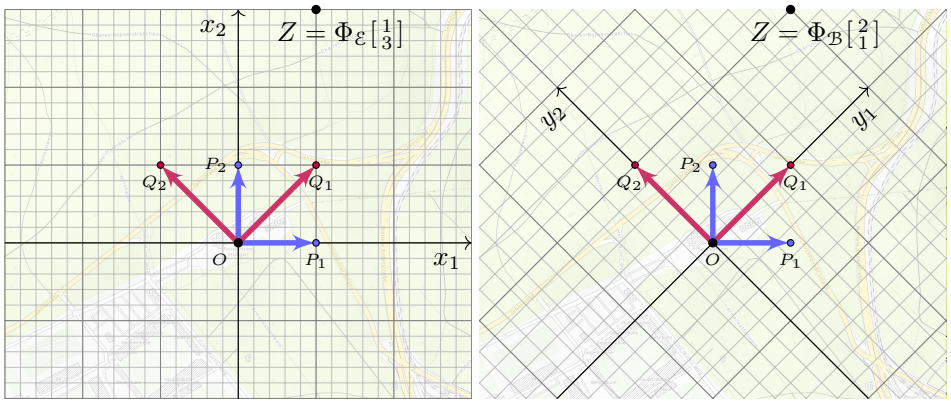
Das führt uns zu zwei einfachen, aber grundlegenden Beobachtungen:

Um zu zeigen, dass eine Frage lösbar ist, genügt es, sie auf *einem* Weg zu lösen: Dies erledigt der universell anwendbare Gauß–Algorithmus. So konnten wir die Existenz einer RZSF bereits in Kapitel B zeigen, durch explizite Konstruktion in Form eines geeigneten Algorithmus.

Um zu zeigen, dass die Lösung eindeutig ist, müssen wir sicherstellen, dass das Ergebnis auf *jedem* Weg dasselbe ist. Das ist etwas kniffliger, hierzu benötigen wir Invarianten und nutzen geschickt den Spaltenraum. Daher beantworten wir diese Frage erst jetzt in Kapitel K.

Basiswechsel und Koordinatentransformation

K233



Aufgabe: Wir betrachten den $\mathbb{R}$–linearen Raum $\mathbb{R}^2$ mit den Basen

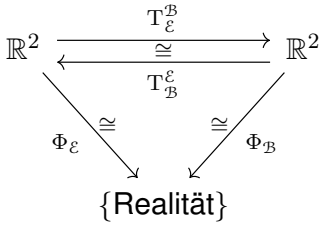
$$\mathcal{E} : e_1 = \begin{bmatrix}1\\0\end{bmatrix},\ e_2 = \begin{bmatrix}0\\1\end{bmatrix} \quad \text{und} \quad \mathcal{B} : b_1 = \begin{bmatrix}1\\1\end{bmatrix},\ b_2 = \begin{bmatrix}-1\\1\end{bmatrix}.$$

Jeder Vektor $v \in \mathbb{R}^2$ schreibt sich eindeutig als $v = e_1x_1 + e_2x_2$ und ebenso $v = b_1y_1 + b_2y_2$ mit $x, y \in \mathbb{R}^2$. Wie rechnen Sie x und y um?

Basiswechsel und Koordinatentransformation

K234
Erläuterung

Ich stelle mir dies wie folgt vor: Beide Koordinatensysteme, $\Phi_{\mathcal{E}}$ und $\Phi_{\mathcal{B}}$, sind Karten für eine physikalische Situation, etwa eine Landkarte.



Die Graphik zeigt eine Karte um den Fernsehturm nebst Gazi-Stadion. Beide Koordinatensysteme haben ihre Vorzüge, je nach Anwendung: $\mathcal{E}$ ist genordet, aber $\mathcal{B}$ passt eventuell besser zu Ihrem Vorhaben.

Jeder Punkt der Realität (im Kartengebiet) lässt sich eindeutig im Koordinatensystem $\Phi_{\mathcal{E}}$ beschreiben, und ebenso in $\Phi_{\mathcal{B}}$. Beispiel:

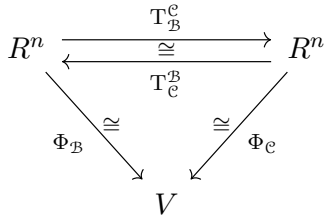
$$Z = \Phi_{\mathcal{E}}[\begin{smallmatrix}1\\3\end{smallmatrix}] = \Phi_{\mathcal{B}}[\begin{smallmatrix}2\\1\end{smallmatrix}]$$

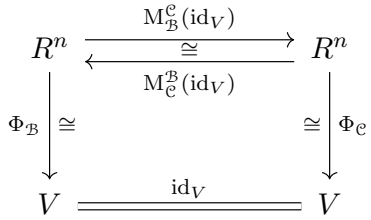
Wir wollen nun die beiden Koordinatensysteme ineinander umrechnen.

Basiswechsel und Koordinatentransformation

K235

🙂 Oft wollen wir eine gegebene Basis durch eine andere ersetzen. Dazu müssen wir nur die alten Koordinaten in die neuen umrechnen:





Die Umrechnung von $\mathcal{B}$ nach $\mathcal{C}$ leistet die **Basiswechselmatrix**

$$\mathrm{T}^{\mathcal{C}}_{\mathcal{B}} := \mathrm{M}^{\mathcal{C}}_{\mathcal{B}}(\mathrm{id}_V).$$

Das bedeutet, wir schreiben die Startbasis $\mathcal{B}$ in der Zielbasis $\mathcal{C}$:

$$\mathrm{id}_V(b_j) = \textstyle\sum_{i=1}^n c_i t_{ij} \ \text{ mit } \ t_{ij} \in R \quad \Longrightarrow \quad \mathrm{T}^{\mathcal{C}}_{\mathcal{B}} = T = (t_{ij})_{ij}$$

Die Koordinaten transformieren sich dann mit der Matrix T:

$$v \overset{\text{Basis}}{=} \textstyle\sum_{j=1}^n b_j x_j \overset{\text{Def}}{=} \sum_{j=1}^n (\sum_{i=1}^n c_i t_{ij}) x_j \overset{\text{Ass}}{=} \sum_{i=1}^n c_i (\sum_{j=1}^n t_{ij} x_j)$$

Die Koordinaten $x \in R^n$ bezüglich $\mathcal{B}$ werden zu $y = Tx$ bezüglich $\mathcal{C}$.

Basiswechsel und Koordinatentransformation

K236
Erläuterung

🙂 Die letzte Gleichung entspricht der Assoziativität von Matrizen. Die Transformation der Koordinaten ist also erfreulich einfach!

🙂 Die Basiswechselmatrix $T = \mathrm{T}^{\mathcal{C}}_{\mathcal{B}}$ ist eigentlich nichts Neues: Es ist die Matrixdarstellung der Identität id_V in den Basen $\mathcal{B}$ und $\mathcal{C}$.

🙂 Ist $V = R^n$ selbst ein Koordinatenraum, so wie im einführenden Beispiel, so können wir die Basis $\mathcal{B}$ als die Spalten einer Matrix B auffassen, und ebenso die Basis $\mathcal{C}$ als die Spalten einer Matrix C.

Die gesuchte Basiswechselmatrix T erfüllt dann die Gleichung

$$B = C \cdot \mathrm{T}^{\mathcal{C}}_{\mathcal{B}} \quad \Longrightarrow \quad \mathrm{T}^{\mathcal{C}}_{\mathcal{B}} = C^{-1}B$$
$$C = B \cdot \mathrm{T}^{\mathcal{B}}_{\mathcal{C}} \quad \Longrightarrow \quad \mathrm{T}^{\mathcal{B}}_{\mathcal{C}} = B^{-1}C$$

In unserem Beispiel ist $\mathcal{C} = \mathcal{E}$ die Standardbasis, daher gilt $C = 1_{n\times n}$, und somit $\mathrm{T}^{\mathcal{C}}_{\mathcal{B}} = B$ sowie $\mathrm{T}^{\mathcal{B}}_{\mathcal{C}} = B^{-1}$. Das vereinfacht die Rechnungen.

Basiswechsel und Koordinatentransformation

K237

Beispiel: Wir betrachten den $\mathbb{R}$–linearen Raum $\mathbb{R}^2$ mit den Basen

$$\mathcal{E}: e_1 = \begin{bmatrix}1\\0\end{bmatrix}, e_2 = \begin{bmatrix}0\\1\end{bmatrix} \quad \text{und} \quad \mathcal{B}: b_1 = \begin{bmatrix}1\\1\end{bmatrix}, b_2 = \begin{bmatrix}-1\\1\end{bmatrix}.$$

Für $\mathrm{T}_{\mathcal{B}}^{\mathcal{E}}$ schreiben wir die Startbasis $\mathcal{B}$ in der Zielbasis $\mathcal{E}$; das ist leicht:

$$\left.\begin{aligned} b_1 &= 1e_1 + 1e_2 \\ b_2 &= -1e_1 + 1e_2 \end{aligned}\right\} \implies \mathrm{T}_{\mathcal{B}}^{\mathcal{E}} = \begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}$$

Für $\mathrm{T}_{\mathcal{E}}^{\mathcal{B}}$ schreiben wir die Startbasis $\mathcal{E}$ in der Zielbasis $\mathcal{B}$ (LGS / Gauß):

$$\left.\begin{aligned} e_1 &= \tfrac{1}{2}b_1 - \tfrac{1}{2}b_2 \\ e_2 &= \tfrac{1}{2}b_1 + \tfrac{1}{2}b_2 \end{aligned}\right\} \implies \mathrm{T}_{\mathcal{E}}^{\mathcal{B}} = \begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\ -\frac{1}{2} & \frac{1}{2}\end{bmatrix}$$

Probe: Gilt $\mathrm{T}_{\mathcal{B}}^{\mathcal{E}} \cdot \mathrm{T}_{\mathcal{E}}^{\mathcal{B}} = 1_{2\times 2}$? und $\mathrm{T}_{\mathcal{E}}^{\mathcal{B}} \cdot \mathrm{T}_{\mathcal{B}}^{\mathcal{E}} = 1_{2\times 2}$? Ja, tatsächlich!

Beispiel:

$$\mathrm{T}_{\mathcal{E}}^{\mathcal{B}} \cdot \Phi_{\mathcal{E}}^{-1}(Z) = \begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\ -\frac{1}{2} & \frac{1}{2}\end{bmatrix} \cdot \begin{bmatrix}1\\3\end{bmatrix} = \begin{bmatrix}2\\1\end{bmatrix} = \Phi_{\mathcal{B}}^{-1}(Z)$$

Basiswechsel und Koordinatentransformation

K238
Erläuterung

Umgekehrt gilt:

$$\mathrm{T}_{\mathcal{B}}^{\mathcal{E}} \cdot \Phi_{\mathcal{B}}^{-1}(Z) = \begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix} \cdot \begin{bmatrix}2\\1\end{bmatrix} = \begin{bmatrix}1\\3\end{bmatrix} = \Phi_{\mathcal{E}}^{-1}(Z)$$

Die Bedingungen $\mathrm{T}_{\mathcal{B}}^{\mathcal{A}} \cdot \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} = 1$ und $\mathrm{T}_{\mathcal{A}}^{\mathcal{B}} \cdot \mathrm{T}_{\mathcal{B}}^{\mathcal{A}} = 1$ dienen hier zur Probe: Dies nutzen Sie zur abschließenden Überprüfung Ihrer Rechnung.

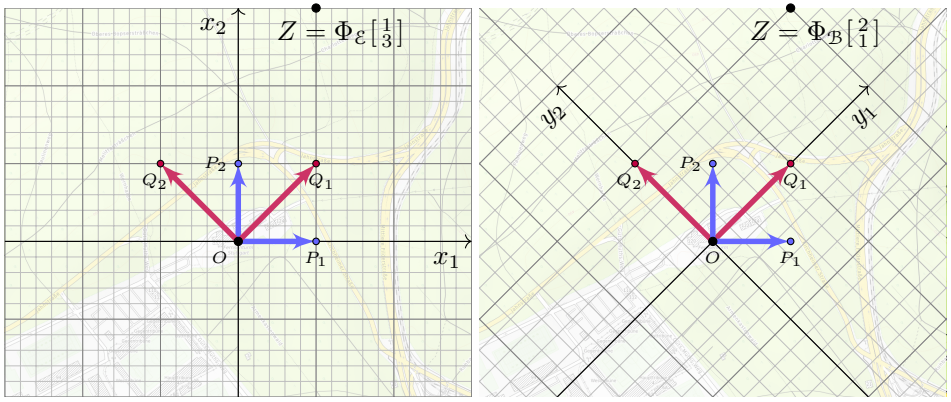
Ebenso können Sie dies auch zur Berechnung nutzen: Wenn Sie die eine Matrix bereits kennen, so erhalten Sie die andere durch Inversion.

Zur Bestimmung einer Basiswechselmatrix bieten sich typischerweise drei Möglichkeiten, die Sie kennen und geschickt nutzen sollten:

1. Sie lösen das lineare Gleichungssystem für die Koeffizienten.
2. Sie invertieren die bereits gefundene, umgekehrte Transformation.
3. In einfachen Fällen lesen Sie die Koeffizienten direkt ab, so wie hier.

Basiswechsel und Koordinatentransformation

K239



Jeder Vektor $v \in \mathbb{R}^2$ schreibt sich eindeutig als $v = e_1x_1 + e_2x_2$ und ebenso $v = b_1y_1 + b_2y_2$ mit $x, y \in \mathbb{R}^2$. Wie rechnen Sie x und y um?

Lösung: Die Umrechnung gelingt durch die Transformationsmatrizen

$$\mathrm{T}_{\mathcal{E}}^{\mathcal{B}} = \begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\ -\frac{1}{2} & \frac{1}{2}\end{bmatrix} : x \mapsto y \quad \text{und} \quad \mathrm{T}_{\mathcal{B}}^{\mathcal{E}} = \begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix} : y \mapsto x.$$

Basiswechsel und Koordinatentransformation

K240
Erläuterung

Damit ist unser (zugegeben einfaches) Transformationsproblem gelöst! Sie sehen zudem die allgemeine Methode: einfach und elegant.

🙂 Die Umrechung der Koordinaten ist eine lineare Abbildung, wie zu erwarten, und kann daher durch eine Matrix dargestellt werden. Genau diese Matrix haben wir nun explizit bestimmt.

🙂 Die Basiswechselmatrix $T = \mathrm{T}_{\mathcal{B}}^{\mathcal{C}}$ ist eigentlich nichts Neues: Es ist die Matrixdarstellung der Identität id_V in den Basen $\mathcal{B}$ und $\mathcal{C}$.

Da Basiswechsel jedoch oft vorkommen, schauen wir genauer hin und halten einige nützliche Rechenregeln für Basiswechsel fest.

Satz K2L: die Transformationsformel

Weiterhin sei R ein Ring sowie V und W (rechts)lineare Räume über R.
Für je zwei Basen $\mathcal{B}, \mathcal{C}$ von V definieren wir die **Basiswechselmatrix**

$$\mathrm{T}^{\mathcal{C}}_{\mathcal{B}} := \mathrm{M}^{\mathcal{C}}_{\mathcal{B}}(\mathrm{id}_V).$$

Für alle Basen $\mathcal{A}, \mathcal{B}, \mathcal{C}$ von V gilt dann:

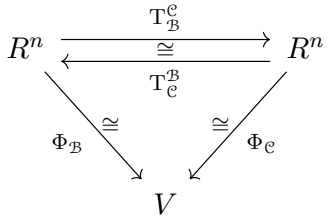
1. Identität: $\mathrm{T}^{\mathcal{B}}_{\mathcal{B}} = 1_{n\times n}$
2. Inversion: $\mathrm{T}^{\mathcal{B}}_{\mathcal{C}} \cdot \mathrm{T}^{\mathcal{C}}_{\mathcal{B}} = 1_{n\times n}$
3. Komposition: $\mathrm{T}^{\mathcal{C}}_{\mathcal{B}} \cdot \mathrm{T}^{\mathcal{B}}_{\mathcal{A}} = \mathrm{T}^{\mathcal{C}}_{\mathcal{A}}$
4. Koordinatentransformation: $\Phi^{-1}_{\mathcal{C}} = \mathrm{T}^{\mathcal{C}}_{\mathcal{B}} \cdot \Phi^{-1}_{\mathcal{B}}$

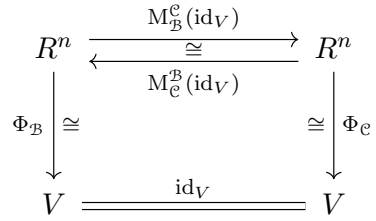
Für jede lineare Abbildung $f : V \to W$ folgt die **Transformationsformel**:

$$\mathrm{M}^{\mathcal{C}'}_{\mathcal{B}'}(f) = \mathrm{T}^{\mathcal{C}'}_{\mathcal{C}} \cdot \mathrm{M}^{\mathcal{C}}_{\mathcal{B}}(f) \cdot \mathrm{T}^{\mathcal{B}}_{\mathcal{B}'}$$

Hierbei sind $\mathcal{B}, \mathcal{B}'$ Basen von V und $\mathcal{C}, \mathcal{C}'$ Basen von W.

Beweis: Aussage (4) ist die Definition von $\mathrm{T}^{\mathcal{C}}_{\mathcal{B}} := \mathrm{M}^{\mathcal{C}}_{\mathcal{B}}(\mathrm{id}_V)$.

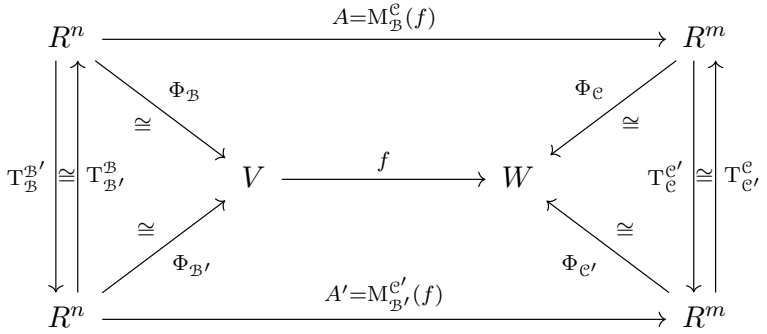




⚠ Zur Vereinfachung der Diagramme identifizieren wir hier jede Matrix $A \in R^{m\times n}$ mit der zugehörigen Abbildungen $f_A : R^n \to R^m$ gemäß K1E.

Die Aussage (1) $\mathrm{M}^{\mathcal{B}}_{\mathcal{B}}(\mathrm{id}_V) = 1_{n\times n}$ ist klar nach Definition.
Die Aussagen (2–3) folgen aus dem Kompositionssatz K1J.

Die Transformationsformel lesen wir aus folgendem Diagramm ab:



Aufgabe: Übersetzen Sie dieses Diagramm in einen Beweis.

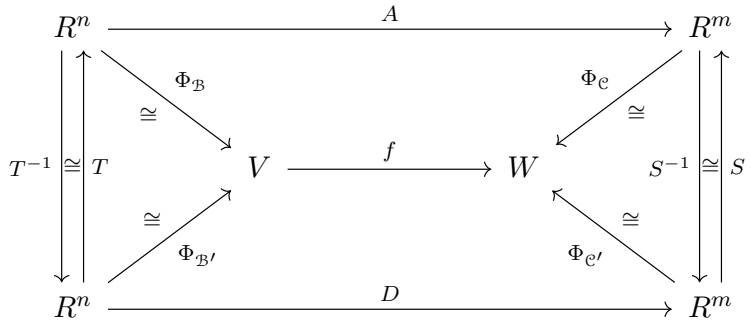
Lösung: Wir formulieren die Konstruktionsschritte explizit aus:
Nach Definition K1F der Matrix $A = \mathrm{M}^{\mathcal{C}}_{\mathcal{B}}(f)$ gilt $f_A = \Phi^{-1}_{\mathcal{C}} \circ f \circ \Phi_{\mathcal{B}}$.
Nach Definition K1F der Matrix $A' = \mathrm{M}^{\mathcal{C}'}_{\mathcal{B}'}(f)$ gilt $f_{A'} = \Phi^{-1}_{\mathcal{C}'} \circ f \circ \Phi_{\mathcal{B}'}$.
Nach Definition K1F der Matrix $T = \mathrm{M}^{\mathcal{B}}_{\mathcal{B}'}(\mathrm{id}_V)$ gilt $f_T = \Phi^{-1}_{\mathcal{B}} \circ \Phi_{\mathcal{B}'}$.
Nach Definition K1F der Matrix $T' = \mathrm{M}^{\mathcal{C}'}_{\mathcal{C}}(\mathrm{id}_V)$ gilt $f_{T'} = \Phi^{-1}_{\mathcal{C}'} \circ \Phi_{\mathcal{C}}$.
Daraus folgt $f_{A'} = f_{T'} \circ f_A \circ f_T$, also $A' = T' \cdot A \cdot T$ wie behauptet.

🙂 Das Diagramm erklärt die Idee und gibt Ihnen einen guten Überlick. Der schrittweise ausformulierte Beweis liefert detaillierte Argumente, in der logisch richtigen Reihenfolge, eventuell ergänzt durch weitere Informationen, im vorliegenden Fall zum Beispiel explizite Formeln.

🙂 Diagramm / Bild und Text / Formel sind bewährte Mittel zur Kommunikation in der Mathematik und angepasst auch außerhalb. Beides ist nützlich und hilfreich. Lernen Sie beides zu nutzen und ineinander zu übersetzen, so wie hier exemplarisch vorgeführt.

Basiswechsel und Transformationsformel

Beispiel: Basiswechsel K2C zur Modellmatrix $D = D^r_{m\times n} = S^{-1}AT$.



Aufgabe: Wie führt der Gauß–Algorithmus zu einem Basiswechsel?

Basiswechsel und Transformationsformel

Lösung: Gegeben sei eine lineare Abbildung $f : V \to W$ endlich-dimensionaler Vektorräume über dem Divisionsring R.

Wir wählen (zunächst beliebige, also willkürliche) Basen $\mathcal{B}$ von V und $\mathcal{C}$ von W. Damit stellen wir f als Matrix $A = \mathrm{M}^{\mathcal{C}}_{\mathcal{B}}(f)$ dar.

Nun wollen wir diese Basen verbessern, also möglichst gut an f anpassen, sodass die darstellende Matrix möglichst einfach wird.

Der Gauß–Algorithmus K2F liefert uns hierzu invertierbare Matrizen $S, S^{-1} \in \mathrm{GL}_m R$ und $T, T^{-1} \in \mathrm{GL}_n R$, sodass $D^r_{m\times n} = S^{-1}AT$.

Dies definiert neue Basen $\mathcal{B}'$ von V und $\mathcal{C}'$ von W, wie im Diagramm gezeigt. Bezüglich dieser angepassten Basen wird f nun dargestellt durch die Modellmatrix $D^r_{m\times n} = \mathrm{M}^{\mathcal{C}'}_{\mathcal{B}'}(f)$. Damit ist das Ziel erreicht.

Basiswechsel und Transformationsformel

Basiswechsel und Transformationsformel

Basiswechsel zur Diagonalisierung

Beispiel: Im Funktionenraum $\mathbb{C}^{\mathbb{R}} = \mathrm{Abb}(\mathbb{R}, \mathbb{C})$ über $\mathbb{C}$ betrachten wir $g(t) = \mathrm{e}^{\mathrm{i}t} = \cos t + \mathrm{i}\sin t$ und $\overline{g}(t) = \mathrm{e}^{-\mathrm{i}t} = \cos t - \mathrm{i}\sin t$. Wir haben

$$V = \langle \cos, \sin \rangle_{\mathbb{C}}^{!} = \left\{ f : \mathbb{R} \to \mathbb{C} : t \mapsto a_1 \cos(t) + a_2 \sin(t) \;\middle|\; a_1, a_2 \in \mathbb{C} \right\}$$
$$= \langle g, \overline{g} \rangle_{\mathbb{C}}^{!} \qquad = \left\{ f : \mathbb{R} \to \mathbb{C} : t \mapsto c_1 \mathrm{e}^{\mathrm{i}t} + c_2 \mathrm{e}^{-\mathrm{i}t} \;\middle|\; c_1, c_2 \in \mathbb{C} \right\}.$$

Aufgabe: (1) Stellen Sie die Ableitung $\partial : V \to V$ in diesen Basen dar.
(2) Berechnen Sie die Basiswechselmatrizen zwischen diesen Basen.
(3) Prüfen Sie Ihre Ergebnisse mit der Transformationsformel.

Lösung: (1) Wir betrachten die Basen $\mathcal{A} = (\cos, \sin)$ und $\mathcal{B} = (g, \bar{g})$.
(1a) Wir finden $\cos' = -\sin$ und $\sin' = \cos$. Die darstellende Matrix ist

$$\mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

(1b) Wir finden $g' = \mathrm{i}g$ und $\overline{g}' = -\mathrm{i}\overline{g}$. Die darstellende Matrix ist also

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix}.$$

Basiswechsel zur Diagonalisierung

Zum guten Abschluss diskutieren wir noch einmal die Ableitung $\partial : V \to V$ auf dem Funktionenraum $V = \langle \cos, \sin \rangle_{\mathbb{C}}^{!} = \langle g, \overline{g} \rangle_{\mathbb{C}}^{!}$.

Die darstellenden Matrizen zu ∂ haben wir bereits im ersten Teil dieses Kapitels bestimmt. Nun vollenden wir dieses schöne Beispiel durch die Betrachtung der Basiswechselmatrizen. Diese Illustration liefert relevantes Anschauungsmaterial, zwar einfach, doch lehrreich.

Basiswechsel zur Diagonalisierung

(2) Wir betrachten die Basen $\mathcal{A} = (\cos, \sin)$ und $\mathcal{B} = (g, \bar{g})$.
(2a) Für $\mathrm{T}_{\mathcal{B}}^{\mathcal{A}}$ schreiben wir die Startbasis $\mathcal{B}$ in der Zielbasis $\mathcal{A}$:

$$\left.\begin{aligned} g(t) &= 1\cos(t) + \mathrm{i}\sin(t) \\ \overline{g}(t) &= 1\cos(t) - \mathrm{i}\sin(t) \end{aligned}\right\} \quad \Longrightarrow \quad \mathrm{T}_{\mathcal{B}}^{\mathcal{A}} = \begin{bmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{bmatrix}$$

(2b) Für $\mathrm{T}_{\mathcal{A}}^{\mathcal{B}}$ schreiben wir die Startbasis $\mathcal{A}$ in der Zielbasis $\mathcal{B}$:

$$\left.\begin{aligned} \cos(t) &= \tfrac{1}{2} g(t) + \tfrac{1}{2} \overline{g}(t) \\ \sin(t) &= \tfrac{1}{2\mathrm{i}} g(t) - \tfrac{1}{2\mathrm{i}} \overline{g}(t) \end{aligned}\right\} \quad \Longrightarrow \quad \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2\mathrm{i}} \\ \frac{1}{2} & -\frac{1}{2\mathrm{i}} \end{bmatrix}$$

Probe: Gilt $\mathrm{T}_{\mathcal{B}}^{\mathcal{A}} \cdot \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} = 1_{2\times 2}$? und $\mathrm{T}_{\mathcal{A}}^{\mathcal{B}} \cdot \mathrm{T}_{\mathcal{B}}^{\mathcal{A}} = 1_{2\times 2}$? Ja, tatsächlich!
(3) Einsetzen in die Transformationsformel $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} \cdot \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) \cdot \mathrm{T}_{\mathcal{B}}^{\mathcal{A}}$:

$$\begin{bmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix} \overset{?}{=} \begin{bmatrix} \frac{1}{2} & \frac{1}{2\mathrm{i}} \\ \frac{1}{2} & -\frac{1}{2\mathrm{i}} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{bmatrix}$$

Ist diese Probe erfolgreich? Rechnen Sie es aus!

Basiswechsel zur Diagonalisierung

Die Bedingungen $\mathrm{T}_{\mathcal{B}}^{\mathcal{A}} \cdot \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} = 1$ und $\mathrm{T}_{\mathcal{A}}^{\mathcal{B}} \cdot \mathrm{T}_{\mathcal{B}}^{\mathcal{A}} = 1$ dienen hier zur Probe: Dies nutzen Sie zur abschließenden Überprüfung Ihrer Rechnung.

Umgekehrt können Sie dies auch zur Berechnung nutzen: Wenn Sie die eine Matrix bereits kennen, so erhalten Sie die andere durch Inversion.

Diagonalisierung eines Endomorphismus

Definition K2M: Diagonalisierung eines Endomorphismus

Sei R ein Ring, wir denken insbesondere an Körper wie $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_p, \ldots$.

(1) Sei $f : V \to V$ linear über R. Eine **diagonalisierende Basis** zu f ist eine Basis $\mathcal{B}$ von V, für die die darstellende Matrix von f diagonal ist:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Existiert eine solche Basis $\mathcal{B}$ von V, so nennen wir f **diagonalisierbar**.

(2) Sei $A \in R^{n\times n}$. Ein **diagonalisierender Basiswechsel** zu A über R ist eine invertierbare Matrix $T \in \mathrm{GL}_n(R)$, so dass $T^{-1}AT$ diagonal ist:

$$T^{-1}AT = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Existiert eine solche Matrix T, so nennen wir A **diagonalisierbar**.

Diagonalisierung eines Endomorphismus

Diagonalisierung ist ein zentrales Anliegen der Linearen Algebra; wir werden dies in den nächsten Kapiteln noch genau untersuchen.

Wir können das *Problem* der Diagonalisierung über jedem beliebigen Ring formulieren, doch in dieser Allgemeinheit scheint eine effektive *Lösung* ziemlich hoffnungslos. Wie üblich fokussieren wir uns auf Divisionsringe, damit wir den Gauß–Algorithmus nutzen können.

Zudem benötigen wir die Determinante aus dem folgenden Kapitel, und diese steht (nur) über allen kommutativen Ringen zur Verfügung. Wir werden daher das Diagonalisierungsproblem ernsthaft nur über kommutativen Divisionsringen angehen, also über Körpern.

🙂 Im Folgenden bearbeiten wir die Diagonalisierung ausschließlich über einem Körper und schreiben Skalare dann traditionell links.

🙂 Der folgende Dreischritt *Definition – Satz – Beispiel* bietet Ihnen bereits handfestes Material und dient hier vor allem als Vorschau.

Diagonalisierung eines Endomorphismus

Definition K2N: Eigenraum einer linearen Abbildung

Sei K ein Körper und hierüber $f : V \to V$ eine K–lineare Abbildung. Zu jedem Skalar $\lambda \in K$ definieren wir den zugehörigen **Eigenraum**

$$\mathrm{E}(\lambda) = \mathrm{Eig}(f, \lambda) := \{\, v \in V \mid f(v) = \lambda v \,\} \stackrel{!}{=} \ker(f - \lambda\,\mathrm{id}_V).$$

Im Falle $\mathrm{E}(\lambda) \neq \{0\}$ nennen wir λ einen **Eigenwert** von f.

Übung: Zeigen Sie die letzte Gleichung und folgern Sie daraus, dass $\mathrm{Eig}(f, \lambda) \leq V$ tatsächlich ein K–linearer Unterraum ist. (Das erfordert Kommutativität von K, egal ob die Skalare links oder rechts stehen.)

Beispiele: Die beiden einfachsten Spezialfälle kennen Sie bereits:

0. Für $\lambda = 0$ ist $\mathrm{Eig}(f, 0) = \ker(f)$ der Kern der Abbildung f.
1. Für $\lambda = 1$ ist $\mathrm{Eig}(f, 1) = \mathrm{fix}(f)$ die Fixpunktmenge von f.

Diagonalisierung eines Endomorphismus

Satz K2O: Diagonalisierung und Eigenraumzerlegung

Genau dann ist $f : V \to V$ diagonalisierbar über dem Körper K, wenn $V = \bigoplus_{\lambda\in K} \mathrm{Eig}(f, \lambda)$ die direkte Summe von Eigenräumen ist.

Relevant sind dabei nur die nicht-trivialen Eigenräume $\mathrm{E}(\lambda) \neq \{0\}$, also nur die Summanden zu Eigenwerten λ der Abbildung f.

Übung: Beweisen Sie die im Satz formulierte Äquivalenz. (Sie finden eine ausführliche Diskussion später in Satz M1I, doch es gibt kein Hindernis, dies nicht jetzt schon zu beweisen. Versuchen Sie es!)

🙂 Anschaulich gesagt: Genau dann ist $f : V \to V$ diagonalisierbar, wenn es genügend Eigenvektoren gibt, um eine Eigenbasis bilden.

🙂 Das folgende Zahlenbeispiel zeigt eine schöne Illustration. Wir halten dazu bereits alle nötigen Werkzeuge in Händen.

Basiswechsel zur Diagonalisierung

K257

Aufgabe: Zum Spaltenvektor $v = \left[\begin{smallmatrix}-1\\1\end{smallmatrix}\right] \in \mathbb{R}^2$ betrachten wir

$$f : \mathbb{R}^2 \to \mathbb{R}^2 : x \mapsto x - v \cdot v^\mathsf{T} \cdot x.$$

(1a) Ist diese Abbildung f linear über $\mathbb{R}$?
(1b) Schreiben Sie f als Matrix A bezüglich der Standardbasis.

Zu $f : \mathbb{R}^2 \to \mathbb{R}^2$ und $\lambda \in \mathbb{R}$ definieren wir den **Eigenraum**

$$\boxed{\mathrm{E}(\lambda) := \left\{ x \in \mathbb{R}^2 \;\middle|\; f(x) = \lambda x \right\}.}$$

(2a) Ist $\mathrm{E}(\lambda)$ in $\mathbb{R}^2$ ein $\mathbb{R}$–linearer Unterraum?
(2b) Bestimmen Sie Basen für $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$.

(3a) Erhalten Sie so eine direkte Summe $\mathrm{E}(+1) \oplus \mathrm{E}(-1) = \mathbb{R}^2$?
(3b) Setzen Sie die Basen aus (2b) zu einer Basis $\mathcal{B}$ von $\mathbb{R}^2$ zusammen.
(3c) Schreiben Sie f als Matrix bezüglich dieser angepassten Basis $\mathcal{B}$.

(4a) Zeichnen Sie $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$ in der Ebene $\mathbb{R}^2$.
(4b) Erklären Sie die Wirkung von f geometrisch.

Basiswechsel zur Diagonalisierung

K258
Erläuterung

Zu jedem Wert $\lambda \in \mathbb{R}$ definieren wir den Eigenraum $\mathrm{E}(\lambda)$ wie gezeigt.
Relevant sind dabei nur die nicht-trivialen Eigenräume $\mathrm{E}(\lambda) \neq \{0\}$.

Für das vorliegende Beispiel sind nur die beiden Werte $\lambda = \pm 1$ relevant, denn für alle $\lambda \in \mathbb{R} \setminus \{\pm 1\}$ gilt $\mathrm{E}(\lambda) = \{0\}$. Probieren Sie Beispiele aus!

Sie lernen in den folgenden Kapiteln, wie Sie die **Eigenwerte** von f bestimmen, also diejenigen Werte λ, für die $\mathrm{E}(\lambda) \neq \{0\}$ gilt.

(Wenn Sie dies später im Rückblick lesen, können Sie es bereits:
Es gelingt mit Determinante und charakteristischem Polynom.)

Unsere Aufgabenstellung umgeht dieses Problem elegant dadurch, dass die beiden Eigenwerte $\lambda = \pm 1$ hier fest vorgegeben werden.

Alle weiteren Rechnungen liegen bereits jetzt in Ihrer Reichweite und bilden eine schöne Illustration all unserer bisherigen Techniken.

Zudem bietet es eine gute Motivation für die folgenden Kapitel zu Determinanten, Eigenwerten und Eigenvektoren.

Basiswechsel zur Diagonalisierung

K259

Lösung: Zum Spaltenvektor $v = \left[\begin{smallmatrix}-1\\1\end{smallmatrix}\right]$ betrachten wir

$$f : \mathbb{R}^2 \to \mathbb{R}^2 : x \mapsto x - v \cdot v^\mathsf{T} \cdot x.$$

(1a) Ja, die Abbildung f ist linear, wie wir direkt nachrechnen:

$$f(x + \lambda y) = \ldots = f(x) + \lambda f(y) \text{ für alle } x, y \in \mathbb{R}^2 \text{ und } \lambda \in \mathbb{R}.$$

(1b) Wir berechnen die Bilder der Basisvektoren:

$$\left.\begin{aligned} f(e_1) = \ldots = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right] = 0 \cdot e_1 + 1 \cdot e_2 \\ f(e_2) = \ldots = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] = 1 \cdot e_1 + 0 \cdot e_2 \end{aligned}\right\} \implies A = \mathrm{M}_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

☺ Die beiden Basisvektoren e_1 und e_2 werden hier vertauscht.

Alternative: Wir formen die Abbildungsvorschrift von f explizit um:

$$\begin{aligned} f(x) &= x - \begin{bmatrix} -1 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 1 \end{bmatrix} \cdot x \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot x - \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \cdot x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot x \end{aligned}$$

Basiswechsel zur Diagonalisierung

K260
Erläuterung

Damit haben wir unsere Abbildung f als Matrix dargestellt und somit in eine sehr übersichtliche Form gebracht: Damit können wir arbeiten!

Für Matrizen haben wir effiziente Standardverfahren, insbesondere den Gauß–Algorithmus zur Lösung von linearen Gleichungssystemen, zur Bestimmung von Bild und Kern etc.

Zum Beispiel können wir nun leicht den Eigenraum $\mathrm{E}(0)$ berechnen:

$$\mathrm{E}(0) = \ker(f) = \ker \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$$

Zur Diagonalisierung suchen wir nicht-triviale Eigenräume.
Die freundliche Aufgabenstellung nimmt uns die Suche ab:
Im vorliegenden Beispiel sind dies $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$.
Diese beiden schauen wir uns nun genauer an!

Basiswechsel zur Diagonalisierung

K261

(2a) Wir betrachten $\mathrm{E}(\lambda) := \{\, x \in \mathbb{R}^2 \mid f(x) = \lambda x \,\}$. Für $x \in \mathbb{R}^2$ gilt:

$$f(x) = \lambda x \iff 0 = f(x) - \lambda x = f(x) - \lambda\,\mathrm{id}(x) = (f - \lambda\,\mathrm{id})(x)$$

Somit ist die Menge $\mathrm{E}(\lambda)$ der Kern der Abbildung $f - \lambda\,\mathrm{id}$:

$$\boxed{\mathrm{E}(\lambda) = \ker(f - \lambda\,\mathrm{id})}$$

Die Abbildung $f - \lambda\,\mathrm{id}$ ist linear (I1I), ihr Kern ist ein Unterraum (I1R).

(2b) Wir bestimmen die Unterräume $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$ wie folgt:

$$\mathrm{E}(+1) = \ker(f - \mathrm{id}) = \ker \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} = \mathbb{R}\, b_1 \quad \text{mit} \quad b_1 := \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\mathrm{E}(-1) = \ker(f + \mathrm{id}) = \ker \begin{bmatrix} +1 & 1 \\ 1 & +1 \end{bmatrix} = \mathbb{R}\, b_2 \quad \text{mit} \quad b_2 := \begin{bmatrix} -1 \\ 1 \end{bmatrix}$$

(3) Wir erhalten so zu f die angepasste Basis $\mathcal{B} = (b_1, b_2)$ von $\mathbb{R}^2$. Nach Konstruktion gilt $f(b_1) = +1 \cdot b_1$ und $f(b_2) = -1 \cdot b_2$, also

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Basiswechsel zur Diagonalisierung

K262
Erläuterung

Wir wechseln von der Standardbasis $\mathcal{E}$ zur angepassten Basis $\mathcal{B}$:

$$\mathcal{E} : e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{und} \quad \mathcal{B} : b_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix},\ b_2 = \begin{bmatrix} -1 \\ 1 \end{bmatrix}$$

Dadurch diagonalisieren wir die Darstellungsmatrix von f:

$$A = \mathrm{M}_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \rightsquigarrow \quad D = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}$$

Auf Seite K237 haben wir bereits die Basiswechselmatrizen bestimmt:

$$\mathrm{T}_{\mathcal{B}}^{\mathcal{E}} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \quad \text{und} \quad \mathrm{T}_{\mathcal{E}}^{\mathcal{B}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

Wenn Sie dies üben möchten, können Sie diese numerischen Daten in die Transformationsformel K2L einsetzen und auf Konsistenz prüfen.

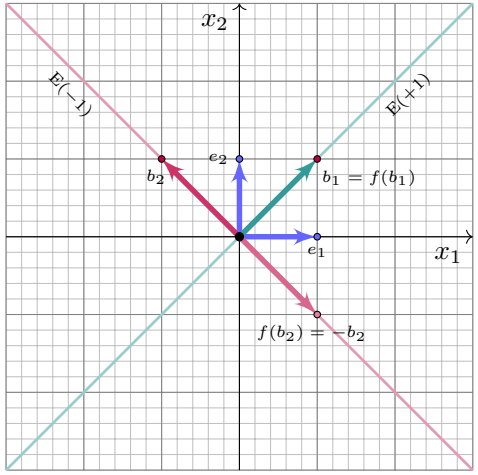
Basiswechsel zur Diagonalisierung

K263

(4) In der angepassten Basis $\mathcal{B} = (b_1, b_2)$ können wir die Abbildung f besonders einfach darstellen… und daher auch leichter zeichnen!

$$\mathrm{M}_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$ ist die Spiegelung an der Hauptdiagonalen.

Basiswechsel zur Diagonalisierung

K264
Erläuterung

Eine solcherart angepasste Basis $\mathcal{B}$ zu f ist etwas ganz Besonderes: Bezüglich $\mathcal{B}$ wird f durch eine Diagonalmatrix dargestellt, wie erhofft.

Wir nennen dies eine **diagonalisierende Basis** zu f, wie oben in Definition K2M vereinbart, oder auch kurz eine **Eigenbasis** zu f.

Die Eigenräume unserer Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$ sind etwas Natürliches. Glücklicherweise erhalten wir hier $\mathbb{R}^2 = \mathrm{E}(+1) \oplus \mathrm{E}(-1)$, wie erhofft.

Die Wahl der jeweiligen Basen $b_1 \in \mathrm{E}(+1)$ und $b_2 \in \mathrm{E}(-1)$ ist hingegen etwas willkürlich; wir können auch Vielfache dieser Vektoren wählen.

🙂 Die so gewonnene Eigenbasis $\mathcal{B}$ zeigt uns, was f eigentlich tut: Hier offenbart die Abbildung f ihr wahres Wesen, ihren Charakter, hier erkennen wir f sofort als Spiegelung.

Injektive lineare Abbildungen

K301
Erläuterung

Aufgabe: Wie viele injektive Abbildungen gibt es?

(1) Wie viele Injektionen $f : \{1,2,3\} \hookrightarrow \{1,2,3,4,5\}$ gibt es?
Was gilt für Injektionen $f : X = \{1,\dots,k\} \hookrightarrow Y = \{1,\dots,n\}$?

(2) Wie viele $\mathbb{F}_2$–lineare Injektionen $f : \mathbb{F}_2^3 \hookrightarrow \mathbb{F}_2^5$ gibt es?
Was gilt allgemein für $\mathbb{F}_q$–lineare Injektionen $f : \mathbb{F}_q^k \hookrightarrow \mathbb{F}_q^n$?

Lösung: (1a) Wir können die möglichen Abbildungen direkt abzählen: Für $f(1)$ haben wir noch alle 5 Wahlen, für $f(2)$ bleiben noch 4 Wahlen, für $f(3)$ nur noch 3 Wahlen. Insgesamt gibt es $5 \cdot 4 \cdot 3 = 60$ Injektionen. Alternative: Es gibt genau $3!\binom{5}{3} = 6 \cdot 10 = 60$ Injektionen (siehe E249).

(1b) Für endliche Mengen X, Y mit $\sharp X = k$ und $\sharp Y = n$ gilt (Satz E2L):

$$\sharp \operatorname{Inj}(X,Y) = n \cdot (n-1) \cdots (n-k+1) = \binom{n}{k} \cdot k!$$

Hierbei zählt der Binomialkoeffizient $\binom{n}{k} = \sharp\binom{Y}{k}$ die k–elementigen Teilmengen $A \subseteq Y$ der n–elementigen Menge Y (Satz E2I).
Im Spezialfall $k = n$ erhalten wir $\sharp \operatorname{Bij}(X,Y) = n!$.

Injektive lineare Abbildungen

K302
Erläuterung

(2a) Wir nutzen geschickt das Prinzip der linearen Fortsetzung (K1B). Für $f(e_1) \in \mathbb{F}_q^5 \setminus \{0\}$ haben wir $2^5 - 2^0 = 31$ Wahlen, für $f(e_2)$ bleiben $2^5 - 2^1 = 30$ Wahlen, für $f(e_3)$ bleiben schließlich $2^5 - 2^2 = 28$ Wahlen. Insgesamt gibt es $31 \cdot 30 \cdot 28 = 26040$ Injektionen $f : \mathbb{F}_2^3 \hookrightarrow \mathbb{F}_2^5$ über $\mathbb{F}_2$.

(2b) Seien V, W Vektorräume über $\mathbb{F}_q$ mit $\dim(V) = k$ und $\dim(W) = n$. Die Anzahl der $\mathbb{F}_q$–linearen Injektionen $f : V \to W$ ist wie in (2a):

$$\sharp \operatorname{Inj}_{\mathbb{F}_q}(V,W) = \prod_{i=0}^{k-1} (q^n - q^i)$$

Im Spezialfall $k = n$ erhalten wir

$$\sharp \operatorname{Iso}_{\mathbb{F}_q}(V,W) = \sharp \operatorname{GL}_n \mathbb{F}_q = \prod_{i=0}^{n-1} (q^n - q^i)$$

Das sind die Anzahlen, die wir aus Satz J2H kennen.

Surjektive lineare Abbildungen

K303
Erläuterung

Aufgabe: Wie viele surjektive Abbildungen gibt es?

(3) Wie viele Surjektionen $f : \{1,2,3,4,5\} \twoheadrightarrow \{1,2,3\}$ gibt es?
Was gilt für Surjektionen $f : X = \{1,\dots,k\} \twoheadrightarrow Y = \{1,\dots,n\}$?

(4) Wie viele $\mathbb{F}_2$–lineare Surjektionen $f : \mathbb{F}_2^5 \twoheadrightarrow \mathbb{F}_2^3$ gibt es?
Was gilt allgemein für $\mathbb{F}_q$–lineare Surjektionen $f : \mathbb{F}_q^k \twoheadrightarrow \mathbb{F}_q^n$?

Lösung: (3b) Wir zerlegen die Menge X in Fasern (wie in Satz E2L):

$$\operatorname{Sur}(X,Y) \cong \left\{ (Q, \bar{f}) \;\middle|\; Q \in \left\{ {X \atop n} \right\},\ \bar{f} : Q \xrightarrow{\sim} Y \right\}$$

Jede Surjektion $f : X \twoheadrightarrow Y$ ist eindeutig bestimmt durch ihre Zerlegung $Q \in \left\{ {X \atop n} \right\}$ in Fasern und die Bijektion $\bar{f} : Q \xrightarrow{\sim} Y$. Wir haben also:

$$\sharp \operatorname{Sur}(X,Y) = \sum_{Q \in \left\{ {X \atop r} \right\}} \sharp \operatorname{Bij}(Q,Y) = \left\{ {k \atop n} \right\} \cdot n!$$

Hierbei zählt die Stirling–Zahl $\left\{ {k \atop n} \right\} = \sharp\left\{ {X \atop n} \right\}$ die n–elementigen Partitionen $Q \in \left\{ {X \atop n} \right\}$ der k–elementigen Menge X (wie in Satz E2K).

(3a) Für $(k,n) = (5,3)$ finden wir $\left\{ {5 \atop 3} \right\} = 25$ und $3! = 6$, also insgesamt $\sharp \operatorname{Sur}(\{1,2,3,4,5\},\{1,2,3\}) = 25 \cdot 6 = 150$ Surjektionen (siehe E249).

Surjektive lineare Abbildungen

K304
Erläuterung

(4b) Seien V, W Vektorräume über $\mathbb{F}_q$ mit $\dim(V) = k$ und $\dim(W) = n$.

$$\operatorname{Sur}_{\mathbb{F}_q}(V,W) \cong \left\{ (U, \bar{f}) \;\middle|\; U \leq V,\ \bar{f} : V/U \xrightarrow{\sim} W \right\}$$

Jede $\mathbb{F}_q$–lineare Surjektion $f : V \twoheadrightarrow W$ ist eindeutig bestimmt durch ihren Kern $U = \ker(f) \leq V$ mit der Dimension $\dim(U) = k - n$ (J2N) und den induzierten $\mathbb{F}_q$–linearen Isomorphismus $\bar{f} : V/U \xrightarrow{\sim} W$ (I2B). Daraus gewinnen wir dank Satz J2H:

$$\sharp \operatorname{Sur}_{\mathbb{F}_q}(V,W) = \binom{k}{k-n}_q \cdot \sharp \operatorname{GL}_n \mathbb{F}_q$$

(4a) In unserem Beispiel mit $q = 2$ und $(k,n) = (5,3)$ finden wir

$$\binom{5}{2}_2 = \frac{(2^5 - 2^0)(2^5 - 2^1)}{(2^2 - 2^0)(2^2 - 2^1)} = \frac{31 \cdot 30}{3 \cdot 2} = 155,$$

$$\sharp \operatorname{GL}_3 \mathbb{F}_2 = (2^3 - 2^0)(2^3 - 2^1)(2^3 - 2^2) = 7 \cdot 6 \cdot 4 = 168,$$

also insgesamt $\sharp \operatorname{Sur}_{\mathbb{F}_2}(\mathbb{F}_2^5, \mathbb{F}_2^3) = 155 \cdot 168 = 26040$ Surjektionen über $\mathbb{F}_2$.

Lineare Abbildungen mit vorgegebenem Rang

K305 Erläuterung

Aufgabe: Wie viele Abbildungen mit vorgegebenem Rang gibt es?

(5) Wie viele Abbildungen $f : \{1,2,3,4\} \to \{1,2,3\}$ treffen 2 Punkte? Was gilt für $f : X = \{1,\dots,k\} \to Y = \{1,\dots,n\}$ mit $\sharp\,\mathrm{im}(f) = r$?

(6) Wie viele $\mathbb{F}_2$–lineare Abbildung $f : \mathbb{F}_2^4 \to \mathbb{F}_2^3$ vom Rang 2 gibt es? Was gilt für $\mathbb{F}_q$–lineare Abbildungen $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$ vom Rang r?

Lösung: (5b) Wir nutzen geschickt die kanonische Faktorisierung E3I:

$$\begin{aligned}\mathrm{Abb}(X,Y)_r &:= \{\, f : X \to Y \mid \sharp\,\mathrm{im}(f) = r \,\}\\ &\cong \{\, (Q, \bar f, B) \mid Q \in \tbinom{X}{r},\ B \in \tbinom{Y}{r},\ \bar f : Q \xrightarrow{\sim} B \,\}\end{aligned}$$

Jede Abbildung $f : X \to Y$ mit $\sharp\,\mathrm{im}(f) = r$ ist eindeutig bestimmt durch ihre Zerlegung $Q \in \left\{ {X \atop r} \right\}$ in Fasern und ihre Bildmenge $B \in \binom{Y}{r}$ sowie die induzierte Bijektion $\bar f : Q \xrightarrow{\sim} B$ zwischen beiden. Wir haben also:

$$\sharp\,\mathrm{Abb}(X,Y)_r = \textstyle\sum_{Q \in \left\{ {X \atop r} \right\}} \sum_{B \in \binom{Y}{r}} \sharp\,\mathrm{Bij}(Q,B) = \left\{ {k \atop r} \right\} \cdot \binom{n}{r} \cdot r!$$

(5a) Für $(k,n,r) = (4,3,2)$ finden wir $\left\{ {4 \atop 2} \right\} = 7$ und $\binom{3}{2} = 3$ und $2! = 2$, also insgesamt $\sharp\,\mathrm{Abb}(\{1,2,3,4\},\{1,2,3\})_2 = 7 \cdot 3 \cdot 2 = 42$.

Lineare Abbildungen mit vorgegebenem Rang

K306 Erläuterung

(6b) Seien V, W Vektorräume über $\mathbb{F}_q$ mit $\dim(V) = k$ und $\dim(W) = n$.

$$\begin{aligned}\mathrm{Hom}_{\mathbb{F}_q}(V,W)_r &:= \{\, f : V \to W \mid \sharp\,\mathrm{rang}(f) = r \,\}\\ &\cong \{\, (U, \bar f, B) \mid U \le V,\ B \le V,\ \bar f : V/U \xrightarrow{\sim} B,\ \dim B = r \,\}\end{aligned}$$

Jede $\mathbb{F}_q$–lineare Abbildung $f : V \to W$ vom Rang $r \in \mathbb{N}$ ist eindeutig bestimmt durch ihren Bildraum $B = \mathrm{im}(f) \le W$ mit $\dim(B) = r$ (J2K), ihren Kern $U = \ker(f) \le V$ mit $\dim(U) = k - r$ (J2N) und schließlich den Isomorphismus $\bar f : V/U \xrightarrow{\sim} B$ (I2B). Daraus gewinnen wir (J2H):

$$\sharp\,\mathrm{Hom}_{\mathbb{F}_q}(V,W)_r = \tbinom{k}{k-r}_q \cdot \tbinom{n}{r}_q \cdot \sharp\,\mathrm{GL}_r\,\mathbb{F}_q$$

(6a) In unserem Beispiel mit $q = 2$ und $(k,n,r) = (4,3,2)$ finden wir

$$\begin{aligned}\sharp\,\mathrm{GL}_2\,\mathbb{F}_2 &= (2^2 - 2^0)(2^2 - 2^1) = 3 \cdot 2 = 6,\\ \tbinom{4}{2}_2 &= \tfrac{(2^4-2^0)(2^4-2^1)}{(2^2-2^0)(2^2-2^1)} = \tfrac{15 \cdot 14}{3 \cdot 2} = 35,\\ \tbinom{3}{2}_2 &= \tfrac{(2^3-2^0)(2^3-2^1)}{(2^2-2^0)(2^2-2^1)} = \tfrac{7 \cdot 6}{3 \cdot 2} = 7,\end{aligned}$$

also insgesamt $\sharp\,\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^4, \mathbb{F}_2^3)_2 = 35 \cdot 7 \cdot 6 = 1470$.

Lineare Abbildungen mit vorgegebenem Rang

K307 Erläuterung

Zusammenfassend erhalten wir den folgenden schönen Satz:

Satz K3A: Anzahl der Abbildungen mit vorgegebenem Rang

Seien V, W Vektorräume über $\mathbb{F}_q$ mit $\dim(V) = k$ und $\dim(W) = n$ und

$$\mathrm{Hom}_{\mathbb{F}_q}(V,W)_r := \{\, f : V \to W \mid \sharp\,\mathrm{rang}(f) = r \,\}.$$

Für jeden Rang $r \in \mathbb{N}$ haben wir:

$$\sharp\,\mathrm{Hom}_{\mathbb{F}_q}(V,W)_r = \binom{k}{r}_q \cdot \binom{n}{r}_q \cdot \sharp\,\mathrm{GL}_r\,\mathbb{F}_q$$

Im Spezialfall $r = k$ erhalten wir $\sharp\,\mathrm{Inj}_{\mathbb{F}_q}(V,W) = \binom{n}{r}_q \cdot \sharp\,\mathrm{GL}_r\,\mathbb{F}_q$.

Im Spezialfall $r = n$ erhalten wir $\sharp\,\mathrm{Sur}_{\mathbb{F}_q}(V,W) = \binom{k}{r}_q \cdot \sharp\,\mathrm{GL}_r\,\mathbb{F}_q$.

Im Spezialfall $r = k = n$ erhalten wir $\sharp\,\mathrm{Iso}_{\mathbb{F}_q}(V,W) = \sharp\,\mathrm{GL}_r\,\mathbb{F}_q$.

Beweis: Wir strukturieren die Menge $\mathrm{Hom}_{\mathbb{F}_q}(X,Y)_r$ wie in der vorigen Aufgabe ausgeführt und gewinnen daraus die ersehnte Abzählung. Zudem nutzen wir die Spiegelsymmetrie $\binom{k}{k-r}_q = \binom{k}{r}_q$. QED

Abbildungen mit vorgegebenem Rang

K308 Erläuterung

Zum Vergleich wiederholen wir die Zählung für beliebige Abbildungen:

♦ Satz E2M: Anzahl der Abbildungen mit vorgegebenem Rang

Seien X, Y endliche Mengen mit $\sharp X = k$ und $\sharp Y = n$ Elementen sowie

$$\mathrm{Abb}(X,Y)_r := \{\, f : X \to Y \mid \sharp\,\mathrm{im}(f) = r \,\}.$$

Für jeden Rang $r \in \mathbb{N}$ haben wir:

$$\sharp\,\mathrm{Abb}(X,Y)_r = \left\{ {k \atop r} \right\} \cdot \binom{n}{r} \cdot r!$$

Im Spezialfall $r = k$ erhalten wir $\sharp\,\mathrm{Inj}(X,Y) = \binom{n}{r} \cdot r!$.

Im Spezialfall $r = n$ erhalten wir $\sharp\,\mathrm{Sur}(X,Y) = \left\{ {k \atop r} \right\} \cdot r!$.

Im Spezialfall $r = k = n$ erhalten wir $\sharp\,\mathrm{Bij}(X,Y) = r!$.

Beachten Sie die k-n-Symmetrie in Satz K3A; sie geht in E2M verloren. Im Modell $V = \mathbb{F}_q^k$ und $W = \mathbb{F}_q^n$ haben wir $\mathrm{Hom}_{\mathbb{F}_q}(V,W) \cong \mathbb{F}_q^{n \times k}$ (K1E). Die Transposition gibt uns eine Bijektion $\mathbb{F}_q^{n \times k} \cong \mathbb{F}_q^{k \times n}$, und dabei bleibt der Rang r erhalten, denn es gilt Spaltenrang gleich Zeilenrang (K2J).

Kapitel L

Signatur und Determinante

Algebra is the offer made by the devil to the mathematician.
The devil says: I will give you this powerful machine, it will answer
any question you like. All you need to do is give me your soul:
give up geometry and you will have this marvelous machine.

Sir Michael Atiyah (1929–2019)

Inhalt dieses Kapitels L

Motivation und Überblick

Wir diskutieren in diesem Kapitel zwei grundlegende Konstruktionen:
(1) Die Signatur $\operatorname{sign}(f) \in \{\pm 1, 0\}$ einer Selbstabbildung $f : X \to X$, zunächst für die Modellmenge $X = \{1 < 2 < \cdots < n\}$, dann allgemein für jede endliche Menge X. Die Signatur ist multiplikativ, genauer ein Homomorphismus von Monoiden bzw. Gruppen:

$$\begin{array}{ccc} (\mathrm{E}_X, \circ, \mathrm{id}_X) & \xrightarrow[\operatorname{sign}=\operatorname{sign}_X]{} & (\{\pm 1, 0\}, \cdot, 1) \\ \cup & & \cup \\ (\mathrm{S}_X, \circ, \mathrm{id}_X) & \xrightarrow[f \mapsto \operatorname{sign}(f)]{} & (\{\pm 1\}, \cdot, 1) \end{array}$$

(2) Im Anschluss an die Signatur konstruieren wir ihre große Schwester, die Determinante $\det(f) \in K$ einer linearen Selbstabbildung $f : V \to V$ über einem kommutativen Ring K. Dies gelingt zunächst leichter für den Modellraum $V = K^n$, dann für jeden K–linearen Raum V mit endlicher Basis. Auch die Determinante ist multiplikativ, wir erhalten so:

$$\begin{array}{ccc} (\mathrm{End}_K(V), \circ, \mathrm{id}_V) & \xrightarrow[\det=\det_V]{} & (K, \cdot, 1) \\ \cup & & \cup \\ (\mathrm{Aut}_K(V), \circ, \mathrm{id}_V) & \xrightarrow[f \mapsto \det(f)]{} & (K^\times, \cdot, 1) \end{array}$$

Motivation und Überblick

Die Analogie zwischen diesen beiden Konstruktionen ist frappierend. Wir beginnen zunächst mit der Signatur; sie ist leichter zu verstehen, einfacher herzustellen und anschließend für die Determinante hilfreich.

Ich erkläre das Vorgehen für die Signatur betont ausführlich, in Zeitlupe. Anschließend führen wir es für die Determinante dann genauso aus. Daher ist es gut, mit der leichter verständlichen Signatur zu üben.

Für die Determinante beginne ich mit der geometrischen Motivation als orientiertes Volumen. Das ist besonders anschaulich und leicht fasslich (und so nutzt die Analysis später die Determinante für die Integration).

Daraus extrahieren wir die algebraische Definition und beweisen dann die Existenz und die Eindeutigkeit sowie die wichtigsten Eigenschaften. Es entsteht eine wunderschöne, harmonische und elegante Theorie!

Erste Beispiele, Rechnungen und Anwendungen runden das Bild ab. Die Vorlesung legt die Fundamente. Zum tieferen Verständnis und zur routinierten Rechenfertigkeit empfehle ich nachdrücklich die Übungen!

Ergänzung der Methoden

Die Signatur ist eine allgegenwärtige kombinatorische Invariante.
Ich begnüge mich hier knapp mit einer spektakulären Anwendung,
der Lösung des berühmt-berüchtigten 15-Puzzles (Satz L1S).

Ebenso spielt die Determinante nahezu überall eine prominente Rolle,
wo lineare Gleichungssysteme gelöst (L2P), Matrizen invertiert (L2S)
oder lineare Abbildungen von Vektorräumen untersucht werden (L3D).

Determinanten sind ein wunderbares theoretisches Werkzeug, doch in
hoher Dimension zunächst schwer zu berechnen. Ihre Kraft entfalten sie
daher erst im Zusammenspiel mit und als Ergänzung zu praktischen
Methoden, insbesondere dem Gauß–Algorithmus und seinen Varianten.

Meist sind es gerade die individuellen Stärken verschiedener Ansätze,
die sich bestens ergänzen und das Zusammenwirken zum Erfolg führen.
Sie werden dies hier in der Linearen Algebra des Öfteren erleben,
und darüber hinaus sehr häufig in der Mathematik.

Didaktisches Vorgehen

Determinanten sind ein elegantes und weitreichendes Werkzeug.
Zur Erkundung dieses Gebiets wähle ich das folgende Vorgehen,
das hier mustergültig zelebriert wird:

1. Motivation: Was wollen wir erreichen?
2. Konstruktion: Existenz einer Lösung
3. Charakterisierung: Eindeutigkeit der Lösung
4. Eigenschaften: Beziehungen und Formeln
5. Berechnung: effiziente Algorithmen
6. Erste Beispiele und Anwendungen

Diese verschiedenen Aspekte und Argumente stützen und ergänzen
sich gegenseitig. Es wäre töricht, nur auf Algorithmen zu schielen, ohne
die Fundamente zu legen, oder umgekehrt eine Theorie aufzubauen, die
kaum einer Berechnung zugänglich ist. Auch das kann man tun,
in der Not frisst der Teufel bekanntlich Fliegen, doch ideal ist es nicht.

Für Determinanten hingegen spielt alles glücklich zusammen!

Algorithmen der Linearen Algebra

Ich gehe in dieser Vorlesung zur Linearen Algebra ganz bewusst
und angemessen ausführlich auch auf algorithmische Aspekte ein.
Mathematik findet nicht nur, aber eben auch auf dem Computer statt.
Ich präzisiere dazu Datenstrukturen und Algorithmen soweit möglich.

Unser treues Arbeitspferd ist der extrem nützliche Gauß–Algorithmus:
Wir nutzen ihn erfolgreich sowohl zu Rechnungen als auch für Beweise!
Seine guten Dienste leistet das Gauß–Verfahren auch in diesem Kapitel,
Sie dürfen sich freuen, dass Ihre Investition weiter reiche Früchte trägt.

Die algorithmische Sichtweise ist für Programmierung und Anwendung
unverzichtbar, daran besteht kein Zweifel. Ich bin zudem überzeugt,
dass sie auch für das mathematische Verständnis vorteilhaft ist.
Das mag überraschen, hat aber ganz naheliegende Gründe:

Die Formulierung als Computerprogramm zwingt uns zur Präzision.
Das ist in den meisten Situationen ein strenger, doch guter Test.
Manche sagen: „Du hast es erst dann verstanden, wenn du es einem
Computer beibringen kannst.“ Das ist etwas extrem, aber doch nützlich.

Algorithmen der Linearen Algebra

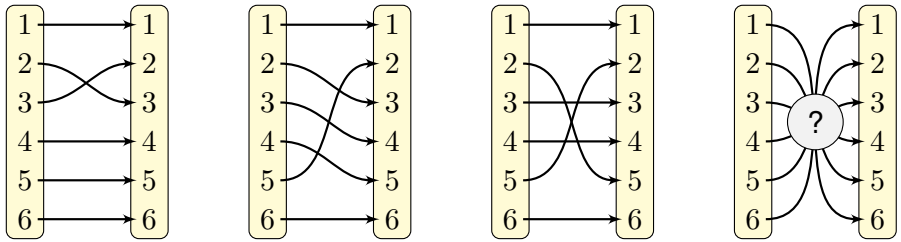
Die Mathematik ist wunderschön und nützlich, und dies gilt meiner
Überzeugung nach sowohl für theoretische Grundlagen als auch für
praktische Umsetzungen, ebenso für Theoreme wie für Algorithmen.
Beide arbeiten zusammen wie linke und rechte Hand.

Genau besehen ist die Unterscheidung nur eine Frage des fachlichen
Schwerpunkts und der persönlichen Präferenz: Auch Algorithmen wollen
bewiesen werden, auch Sätze wollen angewendet werden.
Bitte begreifen Sie daher beides als integralen Teil der Mathematik.

Diese Grundphilosophie führe ich auch in diesem Kapitel fort
und suche eine ehrliche Balance zwischen Theorie und Praxis.
Beim ersten Kontakt mag Ihnen alles theoretisch vorkommen,
doch wir legen zugleich die praktischen Werkzeuge bereit.

Zu Ihrer erfolgreichen Arbeit benötigen Sie immer beides: präzise
Begriffe und effiziente Methoden. Sie werden dies spüren und in Ihren
eigenen Rechnungen gut nutzen können, angefangen in den Übungen
zur Linearen Algebra und anschließend weit darüber hinaus.

Anschauliches Beispiel: ein Kartrennen



Aufgabe: Nach dem Rennen sind für jeden Kart die Startposition $i \in X = \{1, \ldots, n\}$ und zudem die Zielposition $\sigma(i) \in X$ bekannt.

(1) Wie viele Überholmanöver gab es mindestens?
(2) Wie viele Überholmanöver gab es tatsächlich?

Lösung: Wir betrachten die Menge der **Inversionen** aka **Fehlstände**:

$$\mathrm{Inv}(\sigma) := \big\{\, \{i,j\} \subseteq X \;\big|\; i < j \;\wedge\; \sigma(i) > \sigma(j) \,\big\}$$

Mit $\mathrm{inv}(\sigma) := \sharp\,\mathrm{Inv}(\sigma)$ bezeichnen wir die Anzahl der Inversionen.

(1) Es gab mindestens $\mathrm{inv}(\sigma)$ Überholmanöver! Warum? Siehe (2)!

Anschauliches Beispiel: ein Kartrennen

Wir treffen hier stillschweigend ein paar vereinfachende Annahmen:

(a) Die Zuordnung $\sigma : X \to X$ von Start zu Ziel ist eine Permutation.

- Alle Karts haben eine feste Startreihenfolge (Pole-Position) und die Reihenfolge beim Zieleinlauf ist eindeutig (keine Gleichzeitigkeit).
- Es gilt Erhaltung: Während des Rennens gehen keine Karts verloren, und es kommen natürlich auch keine neuen hinzu.

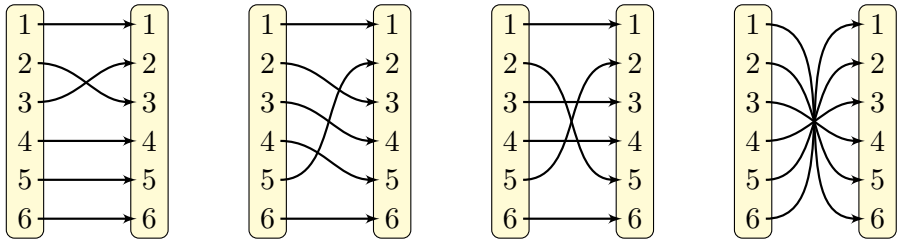
(b) Wir gehen davon aus, dass jeweils nur paarweise überholt wird, so dass wir nur paarweise Überholmanöver zählen müssen und können.

Das ist durchaus realistisch und anschaulich plausibel: Die Fahrbahn ist breit genug für zwei Karts nebeneinander, aber nicht für drei.

Notation: Wir schreiben kurz und bequem $\{i \neq j\}$ bzw. $\{i < j\}$ für die Menge $\{i, j\}$ mit $i \neq j$ bzw. sortiert mit der Ordnung $i < j$.

Wir nennen ein Paar $\{i \neq j\} \subseteq X$ **gerade**, falls $i < j$ und $\sigma(i) < \sigma(j)$, und **ungerade**, falls $i < j$ und $\sigma(i) > \sigma(j)$. Letzteres nennt man eine **Inversion** oder einen **Fehlstand**, manchmal auch eine **Fehlstellung**.

Anschauliches Beispiel: ein Kartrennen



$\mathrm{inv} = 1$ $\quad$ $\mathrm{inv} = 3$ $\quad$ $\mathrm{inv} = 5$ $\quad$ $\mathrm{inv} = \frac{n(n-1)}{2}$

(2) Die tatsächliche Anzahl ist eventuell größer, um eine gerade Zahl!

$$\sharp\,\text{Überholmanöver} \;=\; \sharp\,\mathrm{Inv}(\sigma) + 2n, \quad n \in \mathbb{N}$$

Beweis durch doppeltes Abzählen: Betrachte jedes Paar $\{i < j\}$.

- Für $\sigma(i) < \sigma(j)$ gab es $0 + 2n_{ij}$ Überholmanöver, wobei $n_{ij} \in \mathbb{N}$.
- Für $\sigma(i) > \sigma(j)$ gab es $1 + 2n_{ij}$ Überholmanöver, wobei $n_{ij} \in \mathbb{N}$.

Wir erhalten alle Überholmanöver, indem wir über alle Paare summieren. Die Gesamtzahl ist demnach $\sharp\,\mathrm{Inv}(\sigma) + 2n$ mit $n = \sum_{i<j} n_{ij} \in \mathbb{N}$. QED

Anschauliches Beispiel: ein Kartrennen

Aufgabe: Ist der folgende Rennbericht glaubwürdig?

„Ein kurioses Rennen! Die Reihenfolge der sechs Wagen hat sich vom Start zum Ziel komplett umgekehrt. Dennoch war der Verlauf des Rennens eher langweilig, mit insgesamt nur 20 Überholmanövern."

Lösung: Das ist unmöglich! Hier gilt nämlich $\mathrm{inv}(\sigma) = \binom{6}{2} = \frac{6 \cdot 5}{2} = 15$. Möglich wären $15, 17, 19, 21, 23, \ldots$ Überholmanöver, aber niemals 20.

☺ Diese einfache Rechnung hat recht oft durchschlagende Wirkung. Genau um diese Parität geht es uns hier und in den folgenden Sätzen!

Definition L1A: Parität und Inversionen einer Permutation

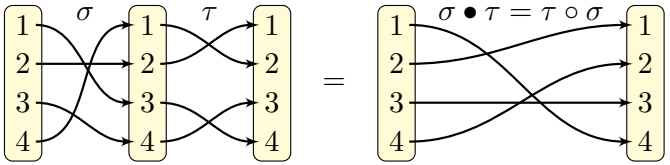
Zu jeder Permutation $\sigma \in \mathrm{S}_n$ definieren wir ihre **Parität**

$$\varepsilon : \mathrm{S}_n \to \mathbb{Z}_2 = \{0,1\} : \sigma \mapsto \mathrm{inv}(\sigma) \bmod 2, \quad \text{wobei wie vereinbart}$$
$$\mathrm{inv}(\sigma) := \sharp\,\mathrm{Inv}(\sigma), \quad \mathrm{Inv}(\sigma) := \big\{\, \{i,j\} \subseteq X \;\big|\; i < j \;\wedge\; \sigma(i) > \sigma(j) \,\big\}.$$

Eine Permutation $\sigma \in \mathrm{S}_n$ heißt **un/gerade**, falls $\mathrm{inv}(\sigma)$ un/gerade ist.

Erinnerung: die symmetrische Gruppe

L105



(1) Wir betrachten eine Menge X und ihre **Selbstabbildungen**:

$$\mathrm{E}_X = \mathrm{End}(X) := \mathrm{Abb}(X,X) = \{\, f : X \to X \,\}$$

Graphisch ist die Rechtskomposition natürlicher, wie oben zu sehen; in Formeln schreiben wir $i \mapsto \sigma(i)$, da ist die Linkskomposition bequemer. Die Komposition definiert das Monoid $(\mathrm{E}_X, \bullet, \mathrm{id}_X)$ bzw. $(\mathrm{E}_X, \circ, \mathrm{id}_X)$, mit der Konvention $\sigma \bullet \tau = \tau \circ \sigma$ und $(\tau \circ \sigma)(i) = \tau(\sigma(i))$ für alle $i \in X$.

(2) Darin liegt die Gruppe der **Selbstbijektionen** aka **Permutationen**:

$$\mathrm{S}_X = \mathrm{Sym}(X) = \mathrm{Aut}(X) := \mathrm{End}(X)^\times = \mathrm{Bij}(X,X) = \{\, \sigma : X \xrightarrow{\sim} X \,\}.$$

Dies definiert die **symmetrische Gruppe** $(\mathrm{S}_X, \bullet, \mathrm{id}_X)$ bzw. $(\mathrm{S}_X, \circ, \mathrm{id}_X)$.

(3) Für $X = \{1, 2, \ldots, n\}$ schreiben wir kurz $\mathrm{E}_n := \mathrm{E}_X$ und $\mathrm{S}_n := \mathrm{S}_X$.

Fehlstände der inversen Permutation

L106
Erläuterung

Beispiel L1B: Fehlstände der inversen Permutation

Für jede Permutation $\sigma \in \mathrm{S}_n$ gilt $\mathrm{Inv}(\sigma^{-1}) = \sigma(\mathrm{Inv}(\sigma))$.
Die Anzahl der Fehlstände ist daher gleich: $\mathrm{inv}(\sigma^{-1}) = \mathrm{inv}(\sigma)$.

In Worten: Die Fehlstände $\mathrm{Inv}(\sigma) \subseteq \binom{X}{2}$ notieren wir im Start von σ.
Die Fehlstände von σ^{-1} sind das Bild der Fehlstände von σ. Ausführlich:

Ist $\sigma : X \xrightarrow{\sim} X$ bijektiv, so auch die Abbildung auf Paaren:

$$\sigma_2 : \tbinom{X}{2} \xrightarrow{\sim} \tbinom{X}{2} : \{\, i \neq j \,\} \mapsto \{\, k \neq \ell \,\} = \{\, \sigma(i) \neq \sigma(j) \,\}$$

Dazu stiftet die inverse Permutation σ^{-1} die Umkehrabbildung:

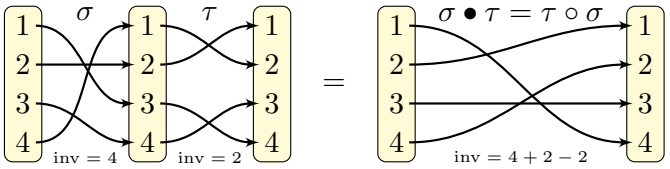
$$\sigma_2^{-1} : \tbinom{X}{2} \xrightarrow{\sim} \tbinom{X}{2} : \{\, k \neq \ell \,\} \mapsto \{\, i \neq j \,\} = \{\, \sigma^{-1}(i) \neq \sigma^{-1}(j) \,\}$$

Für jede Teilmenge $A \subseteq \binom{X}{2}$ schreiben wir dann kurz (siehe D233)

$$\begin{aligned} \sigma(A) \quad &= (\sigma_2)_*(A) \quad = \big\{\, \{\sigma(i), \sigma(j)\} \;\big|\; \{i,j\} \in A \,\big\}, \\ \sigma^{-1}(A) &= (\sigma_2^{-1})_*(A) = \big\{\, \{\sigma^{-1}(k), \sigma^{-1}(\ell)\} \;\big|\; \{k,\ell\} \in A \,\big\}. \end{aligned}$$

Die Parität ist ein Gruppenhomomorphismus.

L107



Satz L1C: Die Parität ist ein Gruppenhomomorphismus.

(1) Bei Komposition von zwei Permutationen $\sigma, \tau \in \mathrm{S}_n$ gilt:

$$\mathrm{Inv}(\sigma \bullet \tau) = \mathrm{Inv}(\tau \circ \sigma) = \mathrm{Inv}(\sigma) \mathbin{\triangle} \sigma^{-1}(\mathrm{Inv}(\tau))$$

Hier steht $\triangle$ für die symmetrische Differenz $A \mathbin{\triangle} B = (A \cup B) \smallsetminus (A \cap B)$.
(2) Die Anzahl der Fehlstände ist additiv minus paarweise Auslöschung:

$$\mathrm{inv}(\tau \circ \sigma) = \mathrm{inv}(\sigma) + \mathrm{inv}(\tau) - 2 \cdot \sharp\big[\mathrm{Inv}(\sigma) \cap \sigma^{-1}(\mathrm{Inv}(\tau))\big]$$

Jede Auslöschung entspricht zwei Inversionen, die sich aufheben.
(3) Die Parität ist somit ein Gruppenhomomorphismus:

$$\varepsilon : (\mathrm{S}_n, \circ, \mathrm{id}_X) \to (\mathbb{Z}_2, +, 0) : \sigma \mapsto \mathrm{inv}(\sigma) \bmod 2$$

Die Parität ist ein Gruppenhomomorphismus.

L108
Erläuterung

Aufgabe: Erklären Sie diese Gleichungen in Worten und in Skizzen.
Beweisen Sie diese Aussagen anschließend formal und ausführlich.

Lösung: (1) Das Paar $\{i \neq j\}$ wird invertiert von $\sigma \bullet \tau = \tau \circ \sigma$,
wenn es entweder von σ oder anschließend von τ invertiert wird.
Wird es zweimal invertiert, so endet es in gerader Reihenfolge.

(2) Die Anzahl der Fehlstände ist additiv minus der nötigen Korrektur:
Jede Auslöschung entspricht zwei Inversionen, die sich aufheben.

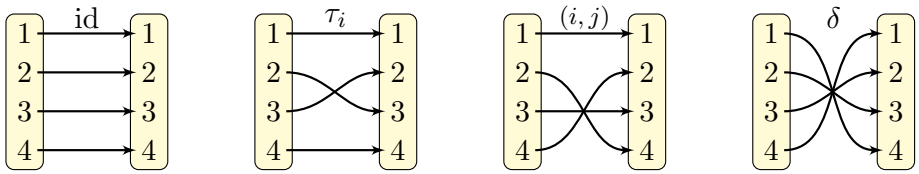
(3) Daher ist die Anzahl $\mathrm{inv}(\tau \circ \sigma)$ additiv modulo 2.

Beweis: (1) Es gilt $\{i \neq j\} \mapsto \{\sigma(i) \neq \sigma(j)\} \mapsto \{\tau(\sigma(i)) \neq \tau(\sigma(j))\}$.
Genau dann endet dies in einem Fehlstand für $\sigma \bullet \tau = \tau \circ \sigma$, wenn
entweder $\{i,j\}$ durch σ invertiert *oder* $\{\sigma(i), \sigma(j)\}$ durch τ invertiert.

(2) Für die symmetrische Differenz gilt $A \mathbin{\triangle} B = (A \cup B) \smallsetminus (A \cap B)$.
Im endlichen Fall folgt $\sharp(A \mathbin{\triangle} B) = \sharp A + \sharp B - 2 \cdot \sharp(A \cap B)$, siehe E2B.

(3) Additivität modulo 2 folgt sofort aus Aussage (2). QED

Die extremen Permutationen



Lemma L1D: die extremen Permutationen

(0) Für jede Permutation $\sigma \in \mathrm{S}_n$ gilt $\mathrm{Inv}(\sigma) \subseteq \binom{X}{2}$, und somit

$$0 \;\leq\; \mathrm{inv}(\sigma) \;\leq\; \tbinom{n}{2} = \tfrac{n(n-1)}{2}.$$

(1) Die beiden Extreme sind eindeutig:
(a) Genau dann gilt $\mathrm{inv}(\sigma) = 0$, wenn $\sigma = \mathrm{id} : i \mapsto i$.
(b) Genau dann gilt $\mathrm{inv}(\sigma) = \binom{n}{2}$, wenn $\sigma = \delta : i \mapsto n+1-i$.

(2) Genau dann gilt $\mathrm{inv}(\sigma) = 1$, wenn $\sigma = \tau_i := (i, i+1)$ für ein i gilt.
Dies nennen wir eine **elementare** oder **fundamentale Transposition**.

(3) Für jede beliebige Transposition $\sigma = (i,j)$ gilt $\mathrm{inv}(\sigma) = 2\,|i-j| - 1$,
denn für $i < j$ haben wir $\mathrm{Inv}(\sigma) = \{\, \{i,j\} \,\} \cup \{\, \{i,k\}, \{k,j\} \mid i < k < j \,\}$.

Die extremen Permutationen

Beweis: (0) Fehlstände sind Paare $\{i \neq j\} \subseteq X$. Dank E2I gilt:

$$\sharp \binom{X}{2} = \binom{n}{2} = \frac{n(n-1)}{2}$$

Wir charakterisieren die beiden Extreme:

(a) „⇐“: Es gilt $\mathrm{Inv}(\mathrm{id}) = \emptyset$, also $\mathrm{inv}(\mathrm{id}) = 0$.
„⇒“: Im Falle $\mathrm{inv}(\sigma) = 0$ gibt es keine Fehlstände,
also gilt $\sigma(1) = 1$, dann $\sigma(2) = 2$, usw. bis $\sigma(n) = n$.

(b) „⇐“: Es gilt $\mathrm{Inv}(\delta) = \binom{X}{2}$, also $\mathrm{inv}(\delta) = \binom{n}{2}$.
„⇒“: Im Falle $\mathrm{inv}(\sigma) = \binom{n}{2}$ ist jedes Paar ein Fehlstand,
also gilt $\sigma(1) = n$, dann $\sigma(2) = n-1$, usw. bis $\sigma(n) = 1$.

(2) „⇐“: Es gilt $\mathrm{Inv}(\tau_i) = \{\{i, i+1\}\}$, also $\mathrm{inv}(\tau_i) = 1$.
„⇒“: Wir haben $\mathrm{inv}(\sigma) = 1$, also $\mathrm{Inv}(\sigma) = \{\{i < j\}\}$.
Demnach gilt $\mathrm{Inv}(\sigma \circ (i,j)) = \emptyset$, also $\sigma = (i,j)$ dank (1a).
Zudem wissen wir $\mathrm{inv}(\sigma) \overset{(3)}{=} 2(j-i) - 1 \overset{!}{=} 1$, also $j = i+1$.

(3) Die Berechnung von $\mathrm{Inv}(\tau)$ und $\mathrm{inv}(\tau)$ ist klar. QED

Erzeugung durch Fundamentaltranspositionen

Die Fundamentaltranspositionen erzeugen die symmetrische Gruppe:

$$\mathrm{S}_n = \big\langle\, \tau_1 = (1,2),\ \tau_2 = (2,3),\ \ldots,\ \tau_{n-1} = (n-1,1) \,\big\rangle$$

Satz L1E: Erzeugung durch Fundamentaltranspositionen

(0) Sei $\sigma \in \mathrm{S}_n$ eine Permutation. Es gilt $\mathrm{inv}(\tau_i) = 1$, dank L1C also

$$\mathrm{inv}(\sigma \circ \tau_i) = \mathrm{inv}(\sigma) \pm 1 \quad \text{und} \quad \mathrm{inv}(\tau_i \circ \sigma) = \mathrm{inv}(\sigma) \pm 1.$$

(1) Im Falle $\mathrm{inv}(\sigma) > 0$ existieren $i, j \in \{1, \ldots, n-1\}$ mit

$$\mathrm{inv}(\sigma \circ \tau_i) = \mathrm{inv}(\sigma) - 1 \quad \text{und} \quad \mathrm{inv}(\tau_j \circ \sigma) = \mathrm{inv}(\sigma) - 1.$$

(2) Jede Permutation $\sigma \in \mathrm{S}_n$ ist ein Produkt der Form $\sigma = \tau_{i_1} \tau_{i_2} \cdots \tau_{i_\ell}$.
Die minimale Länge $\ell \in \mathbb{N}$ ist $\mathrm{inv}(\sigma)$. Allgemein gilt $\ell \in \mathrm{inv}(\sigma) + 2\mathbb{N}$.

Beweis: (1a) Gilt $\sigma(1) < \sigma(2) < \cdots < \sigma(n)$, so folgt $\sigma = \mathrm{id}$, dank L1D.
Im Falle $\mathrm{inv}(\sigma) > 0$ gilt $\sigma \neq \mathrm{id}$. Also existiert $i \in \{1, \ldots, n-1\}$ mit
$\sigma(i) > \sigma(i+1)$. Damit erreichen wir $\mathrm{inv}(\sigma \circ \tau_i) = \mathrm{inv}(\sigma) - 1$.

Erzeugung durch Fundamentaltranspositionen

(1b) Gilt $\sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n)$, so folgt $\sigma = \mathrm{id}$, dank L1D.
Im Falle $\mathrm{inv}(\sigma) > 0$ gilt $\sigma \neq \mathrm{id}$. Also existiert $j \in \{1, \ldots, n-1\}$ mit
$\sigma^{-1}(j) > \sigma^{-1}(j+1)$. Damit erreichen wir $\mathrm{inv}(\tau_j \circ \sigma) = \mathrm{inv}(\sigma) - 1$.

(2) Dies folgt per Induktion über $\mathrm{inv}(\sigma)$ dank (1). Die Ungleichung
$\ell \geq \mathrm{inv}(\sigma)$ und die Parität $\ell = \mathrm{inv}(\sigma) + 2n$ folgen aus (0). QED

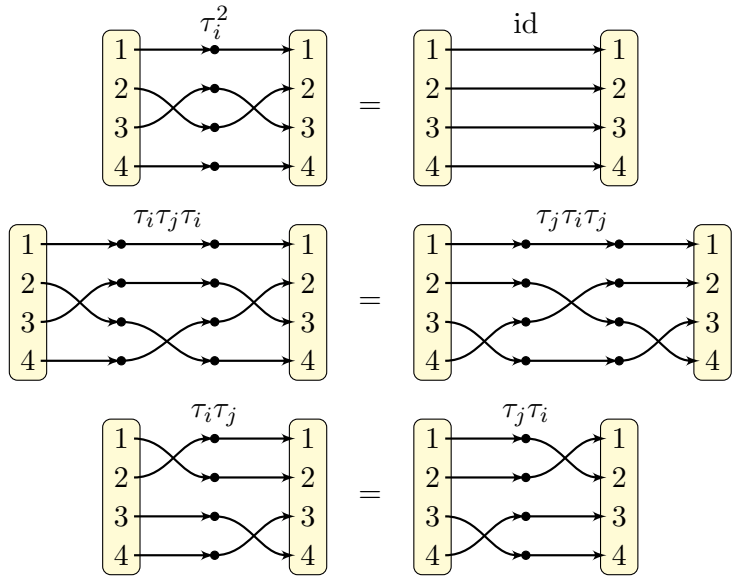
🙂 Das ist der mathematische Satz hinter unserem Kartrennen:
Jede Zielreihenfolge σ kann durch Überholmanöver erreicht werden.
Dazu sind mindestens $\mathrm{inv}(\sigma)$ Überholmanöver $\tau_1, \ldots, \tau_{n-1}$ notwendig.
Die tatsächliche Anzahl ist eventuell größer, um eine gerade Zahl.

🙂 Zur Beschreibung und Analyse dieser Situation haben wir nun eine gute Notation: bequem und genau. Der Satz präzisiert die Aussagen.

🙂 Die Fundamentaltranspositionen $\tau_1, \tau_2, \ldots, \tau_{n-1} \in \mathrm{S}_n$ erzeugen die gesamte symmetrische Gruppe S_n. Zudem können wir für jede Permutation σ die benötigte Länge genau angeben.

Übung: (3) Bestimmen Sie Inv und inv zu $\delta \circ \sigma$ und $\sigma \circ \delta$.
(4) Existieren i, j mit $\mathrm{inv}(\sigma \circ \tau_i) = \mathrm{inv}(\tau_j \circ \sigma) = \mathrm{inv}(\sigma) + 1$?

Die fundamentalen Relationen



Für die Fundamentaltranspositionen $\tau_1, \ldots, \tau_{n-1}$ gelten die Relationen $\tau_i^2 = \mathrm{id}$ sowie $\tau_i\tau_j\tau_i = \tau_j\tau_i\tau_j$ für $|i-j| = 1$ und $\tau_i\tau_j = \tau_j\tau_i$ für $|i-j| \geq 2$.

Die fundamentalen Relationen

Übung: Schreiben Sie diese Graphiken in Zykelschreibweise aus und rechnen Sie so nach, dass diese Relationen allgemein gelten.

🙂 Die Relation $\tau_i^2 = \mathrm{id}$ besagt lediglich, dass τ_i die Ordnung 2 hat. Dies gilt für jede beliebige Transposition, also insbesondere auch hier.

🙂 Die zweite Relation $\tau_i\tau_j\tau_i = \tau_j\tau_i\tau_j$ für $|i-j| = 1$ ist Artins berühmte Zopfrelation; sie tritt hier natürlich für benachbarte Transpositionen auf.

🙂 Die letzte Relation kennen Sie bereits im allgemeineren Kontext: Je zwei disjunkte Permutationen kommutieren (E1B).

Übung: Diese Relationen respektieren die Parität: Modulo 2 ist die Anzahl der Kreuzungen / Transpositionen auf beiden Seiten gleich! Das zeigt graphisch-anschaulich den Ursprung dieser Invariante.

Übung: Sei $h : (\mathrm{S}_n, \circ, \mathrm{id}_X) \to (A, \cdot, 1)$ ein Homomorphismus in eine abelsche Gruppe und $a = h(\tau_1) \in A$ das Bild von τ_1. Dann gilt $a^2 = 1$ und $h(\sigma) = a^{\varepsilon(\sigma)}$ für alle $\sigma \in \mathrm{S}_n$. *Hinweis:* Nutzen Sie die fundamentalen Relationen und zeigen Sie $h(\tau_i) = a$. Schließen Sie mit Satz L1E.

Präsentation durch Erzeuger und Relationen

Satz L1F: Präsentation durch Erzeuger und Relationen

Die symmetrische Gruppe S_n lässt sich wie folgt präsentieren durch Erzeuger und Relationen:

$$\mathrm{S}_n = \left\langle \tau_1, \ldots, \tau_{n-1} \;\middle|\; \begin{array}{ll} \tau_i^2 = 1 & \text{für alle } i \\ \tau_i\tau_j\tau_i = \tau_j\tau_i\tau_j & \text{für } |i-j| = 1 \\ \tau_i\tau_j = \tau_j\tau_i & \text{für } |i-j| \geq 2 \end{array} \right\rangle$$

Das beinhaltet zwei Aussagen: (1) Jede Permutation $\sigma \in \mathrm{S}_n$ ist ein Produkt der Fundamentaltranspositionen $\tau_1, \ldots, \tau_{n-1}$ (Satz L1E).

(2) Eine solche Darstellung ist nicht eindeutig: Genau dann stellen zwei solche Produkte dieselbe Permutation σ dar, wenn sie sich durch die angegebenen Relationen ineinander überführen lassen.

Dieser Satz lässt sich graphisch sehr direkt und anschaulich verstehen und so auch beweisen! (Genauso formuliert und beweist man Artins Präsentation der Zopfgruppe in der Geometrischen Topologie.)

Präsentation durch Erzeuger und Relationen

Anschaulich gesagt: Ein Wort in den elementaren Transpositionen $\tau_1, \ldots, \tau_{n-1}$, das sie hier graphisch ablesen, beschreibt den Verlauf des Rennens. Der Rennverlauf legt das Ergebnis σ eindeutig fest.

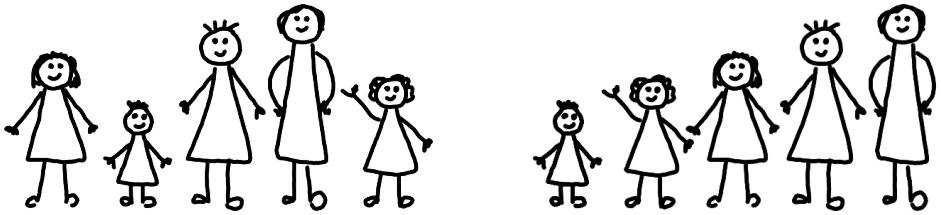
Umgekehrt legt das Ergbnis σ den Rennverlauf *nicht* eindeutig fest, und den Unterschied sehen Sie hier: Er entsteht genau durch die hier gezeigten Relationen; diese führen vom einen zum anderen Verlauf.

Sie sehen also: In unserem anschaulichen Beispiel des Kartrennens steckt elementare, doch wunderschöne Mathematik: die Theorie der symmetrischen Gruppe und der elementaren Transpositionen.

🙂 Das ist schön und nützlich, damit können Sie wunderbar rechnen.

In Zukunft werden Sie ein Rennen nie mehr mit denselben Augen sehen, sondern den mathematischen Kern durchschauen können.

Unordnung und Umordnung



Probleme mit Unordnung und Umordnung begegnen Ihnen sicher öfters!

Nehmen Sie zum Beispiel an, dass Sie eine bestehende Reihenfolge sortieren wollen und dabei nur Nachbarn vertauschen wollen / können. Wie stellen Sie das an? mit möglichst wenigen Vertauschungen? Vermutlich lösen Sie das Problem intuitiv genau richtig!

In diesem Fall misst die Anzahl der Fehlstände die Komplexität des Problems. Der Satz L1E sagt Ihnen genau, wie es geht, und dass es nicht besser gehen kann. Damit ist dieses Problem vollständig gelöst.

Unordnung und Umordnung

Wozu brauchen wir die Theorie, wenn alles so anschaulich gelingt?

Erstens: Wir brauchen eine gute Notation, um Daten und Operationen präzise zu beschreiben, hier also Permutationen und Vertauschungen. Nur so können wir die Strukturen klären und dazu Aussagen beweisen.

Zweitens: Meist möchten Sie Ihr Vorgehen einem Computer übertragen, einen allgemein gültigen Algorithmus entwickeln und programmieren. Hier hilft Mathematik durch gute Notation und beweisbare Aussagen.

Drittens: Wer garantiert Ihnen, dass die Sortierung durch einen Trick nicht doch mit weniger Nachbarschaftsvertauschungen möglich ist? Für kleine Daten scheint alles klar, doch für große Datenmengen wird das Problem schnell unübersichtlich. Satz L1E schafft Sicherheit.

Bemerkung: Ein guter Sortieralgorithmus, der auf Vertauschung von Nachbarn beruht, benötigt schlimmstenfalls $n(n-1)/2$ Vertauschungen. Noch besser gelingt es, wenn wir beliebige Vertauschungen zulassen. Hier sind $\approx n \ln n$ paarweise Vergleiche das Optimum.

Erzeugendensysteme für die symmetrische Gruppe

Satz L1G: Erzeugendensysteme für S_n.

Die Transpositionen in S_n erzeugen die symmetrische Gruppe S_n.
Ebenso gilt $\mathrm{S}_n = \langle\, E_n^s \,\rangle$ für jede der folgenden Familien:

$$E_n^1 = \{\, (i,j) \mid i < j \,\}$$
$$E_n^2 = \{\, (1,2), (1,3), \ldots, (1,n) \,\}$$
$$E_n^3 = \{\, (1,2), (2,3), \ldots, (n-1,n) \,\}$$
$$E_n^4 = \{\, (1,2), (1,2,\ldots,n) \,\}$$

Insbesondere lässt sich die Gruppe S_n durch zwei Elemente erzeugen.

Aufgabe: Beweisen Sie diese Aussagen!

Hinweis: Wir betrachten die symmetrischen Gruppen als Teilmengen $\{\mathrm{id}\} = \mathrm{S}_0 = \mathrm{S}_1 \subset \mathrm{S}_2 \subset \ldots \subset \mathrm{S}_n \subset \ldots$ und nutzen Induktion über $n \in \mathbb{N}$. Formal gelingt dies durch $\mathrm{S}_n = \{\, \sigma : \mathbb{N} \xrightarrow{\sim} \mathbb{N} \mid \mathrm{supp}(\sigma) \subseteq \{1,\ldots,n\} \,\}$.

Erzeugendensysteme für die symmetrische Gruppe

Beweis: (1) Sei $G_n = \langle\, E_n^s \,\rangle \leq \mathrm{S}_n$ die erzeugte Untergruppe.
Die entscheidenden zwei Eigenschaften der Familie E_n^s sind:

1. Zu jedem Element $i \in \{1,\ldots,n\}$ existiert $\rho \in G_n$ mit $\rho(i) = n$.
2. Es gilt $G_{n-1} \leq G_n$, so dass wir induktiv vorgehen können.

Das ist jeweils sorgsam zu prüfen und gelingt meist leicht.
Für $s = 1, 2, 3$ gilt sogar $E_{n-1}^s \subseteq E_n^s$, somit $\langle\, E_{n-1}^s \,\rangle \subseteq \langle\, E_n^s \,\rangle$.
Lediglich für $s = 4$ ist die Eigenschaft (2) nicht offensichtlich.

(2) Wir zeigen nun $\mathrm{S}_n \leq G_n$ per Induktion über n.
Die Aussage ist trivial für $n \leq 1$. Sei also $n \geq 2$.
Die Aussage $\mathrm{S}_{n-1} \leq G_{n-1}$ sei bereits bewiesen.
Sei $\sigma \in \mathrm{S}_n$. Zu $i := \sigma(n)$ wählen wir $\rho \in G_n \leq \mathrm{S}_n$ mit $\rho(i) = n$.
Somit gilt $(\rho \circ \sigma)(n) = n$, also $\rho \circ \sigma \in \mathrm{S}_{n-1} \leq G_{n-1} \leq G_n$.
Daraus folgt $\sigma \in \rho^{-1} \circ G_n = G_n$. Wir schließen $\mathrm{S}_n \leq G_n$. QED

Die Signatur einer Selbstabbildung

Satz L1H: die Signatur einer Selbstabbildung

Zu $n \in \mathbb{N}$ betrachten wir die endliche Menge $X = \{1, \ldots, n\} \subset \mathbb{N} \subset \mathbb{Q}$.

(0) Zu jeder Selbstabbildung $f : X \to X$ definieren wir die **Signatur**

$$\operatorname{sign}(f) := \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \in \{\pm 1, 0\}.$$

Dies heißt auch **Signum** oder **Vorzeichen** von f.

(1) Die Signatur ist multiplikativ, das heißt $\operatorname{sign}(g \circ f) = \operatorname{sign}(g) \cdot \operatorname{sign}(f)$ für alle $f, g : X \to X$. Wir haben also einen Monoidhomomophismus

$$\operatorname{sign} = \operatorname{sign}_X \; : \; (\mathrm{E}_X, \circ, \mathrm{id}_X) \to (\{\pm 1, 0\}, \cdot, 1) \; : \; f \mapsto \operatorname{sign}(f)$$

(2) Genau dann ist $f \in \mathrm{E}_X$ invertierbar, wenn $\operatorname{sign}(f) \in \{\pm 1, 0\}$ dies ist. Durch Einschränkung erhalten wir so den Gruppenhomomorphismus

$$\operatorname{sign} = \operatorname{sign}_X \; : \; (\mathrm{S}_X, \circ, \mathrm{id}_X) \to (\{\pm 1\}, \cdot, 1) \; : \; \sigma \mapsto \operatorname{sign}(\sigma).$$

Die Signatur einer Selbstabbildung

Die bequeme Kurzschreibweise $\{i \neq j\}$ bedarf der Erläuterung.

$$\operatorname{sign}(f) := \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j}$$

Das Produkt erstreckt sich über alle (ungeordneten) Paare $\{i, j\} \in \binom{X}{2}$, also zweielementige Mengen $\{i, j\} \subseteq X$, und das bedeutet $i \neq j$.
Jeder Faktor ist wohldefiniert, da invariant unter Vertauschung:

$$\{i, j\} \;\mapsto\; \frac{f(i) - f(j)}{i - j} = \frac{f(j) - f(i)}{j - i}$$

Wir können jede Paarmenge $\{i, j\}$ sortieren und erhalten

$$\operatorname{sign}(f) = \prod_{\{i < j\}} \frac{f(i) - f(j)}{i - j}.$$

Das ist dasselbe Produkt wie oben: Die Indexmenge ist dieselbe und die Faktoren sind dieselben. Nur die Schreibweise hat sich geändert.
Beide Schreibweisen haben jeweils ihre Vorteile.

Die Signatur einer Selbstabbildung

Beweis: (0) Zur Wohldefiniertheit müssen wir zeigen:

$$\operatorname{sign}(f) := \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \overset{!}{\in} \{\pm 1, 0\}$$

Für $f : X \to X$ sind bijektiv, surjektiv, injektiv äquivalent (Zählsatz E1H).

(0a) Ist f nicht injektiv, so gibt es $i \neq j$ mit $f(i) = f(j)$, also:

$$\operatorname{sign}(f) = 0$$

(0b) Ist $f : X \xrightarrow{\sim} X$ bijektiv, so auch die Abbildung auf Paaren (E2I):

$$f_2 \; : \; \binom{X}{2} \xrightarrow{\sim} \binom{X}{2} \; : \; \{\, i \neq j \,\} \mapsto \{\, k \neq \ell \,\} = \{\, f(i) \neq f(j) \,\}$$

Die Umkehrfunktion zu f_2 ist $(f_2)^{-1} = (f^{-1})_2$. Daraus folgt:

$$\big|\operatorname{sign}(f)\big| = \prod_{\{i \neq j\}} \frac{|f(i) - f(j)|}{|i - j|} = \frac{\prod_{\{k \neq \ell\}} |k - \ell|}{\prod_{\{i \neq j\}} |i - j|} = 1$$

Die Signatur einer Selbstabbildung

(1) Wir zeigen nun für alle $f, g : X \to X$ die Multiplikativität

$$\operatorname{sign}(g \circ f) = \operatorname{sign}(g) \cdot \operatorname{sign}(f).$$

(1a) Ist f nicht injektiv, so ist auch $g \circ f$ nicht injektiv, also gilt

$$\operatorname{sign}(g \circ f) = 0 \quad \text{und} \quad \operatorname{sign}(g) \cdot \operatorname{sign}(f) = 0.$$

(1b) Ist $f : X \xrightarrow{\sim} X$ hingegen bijektiv, so finden wir

$$\begin{aligned}
\operatorname{sign}(g \circ f) &= \prod_{\{i \neq j\}} \frac{g(f(i)) - g(f(j))}{i - j} \\
&= \prod_{\{i \neq j\}} \frac{g(f(i)) - g(f(j))}{f(i) - f(j)} \cdot \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \\
&= \prod_{\{k \neq \ell\}} \frac{g(k) - g(\ell)}{k - \ell} \cdot \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \\
&= \operatorname{sign}(g) \cdot \operatorname{sign}(f)
\end{aligned}$$

Charakterisierung der Signatur

Das gigantische Produkt aus L1H dient zur *Konstruktion* der Signatur, zur *Berechnung* nutzen Sie es lieber nicht, das wäre zu aufwändig. Dazu entwickeln wir gleich effizientere Methoden, siehe Satz L1K. Zuvor diskutieren wir eine konzise Beschreibung der Signatur:

Satz L1I: Charakterisierung der Signatur

Sei $n \in \mathbb{N}_{\geq 2}$ und $X = \{1, \dots, n\}$ und hierauf $\tau_1 = (1,2)$.

(1) Die Signatur $\operatorname{sign} : (\mathrm{E}_X, \circ, \mathrm{id}_X) \to (\mathbb{C}, \cdot, 1)$ ist multiplikativ und erfüllt $\operatorname{sign}(\tau_1) = -1$. Diese Eigenschaft charakterisiert die Signatur eindeutig!

(2) Die Signatur ist der einzige surjektive Gruppenhomomorphismus

$$\operatorname{sign} : (\mathrm{S}_X, \circ, \mathrm{id}_X) \twoheadrightarrow (\{\pm 1\}, \cdot, 1).$$

(3) Sei $h : (\mathrm{S}_X, \circ, \mathrm{id}_X) \to (A, \cdot, 1)$ ein Gruppenhomomorphismus in eine abelsche Gruppe und $a = h(\tau_1)$. Dann gilt $h(\sigma) = a^{\varepsilon(\sigma)}$ für alle $\sigma \in \mathrm{S}_X$.

Aufgabe: Beweisen Sie diese Aussagen. *Tipp:* Beginnen Sie mit (3).

Charakterisierung der Signatur

Lösung: (3) Zu je zwei Punkten $i \neq j$ in X existiert eine Permutation $\tau \in \mathrm{S}_X$ mit $\tau(i) = 1$ und $\tau(j) = 2$. Somit gilt $(i,j) = \tau^{-1} \circ (1,2) \circ \tau$, also $h(i,j) = h(\tau)^{-1} \cdot h(1,2) \cdot h(\tau) = h(1,2)$, da $(A, \cdot, 1)$ abelsch ist.

Wegen $(1,2)^2 = \mathrm{id}$ in S_X gilt $a^2 = 1$ in A, demnach hat a die Ordnung 2. Jede Permutation $\sigma \in \mathrm{S}_X$ ist ein Produkt von ℓ Transpositionen (L1E). Demnach gilt $h(\sigma) = a^\ell = a^{\varepsilon(\sigma)}$ für die Parität $\varepsilon(\sigma) = \ell \bmod 2$.

(1) Die Existenz der Signatur $\operatorname{sign} : (\mathrm{E}_X, \circ, \mathrm{id}_X) \to (\mathbb{C}, \cdot, 1)$ haben wir in Satz L1H geklärt. Sie ist multiplikativ und erfüllt $\operatorname{sign}(\tau_1) = -1$.

Die Eindeutigkeit folgt aus (3): Sei $h : (\mathrm{E}_X, \circ, \mathrm{id}_X) \to (\mathbb{C}, \cdot, 1)$ multiplikativ mit $h(\tau_1) = -1$. Dann gilt $h(\sigma) = (-1)^{\varepsilon(\sigma)} = \operatorname{sign}(\sigma)$ für alle $\sigma \in \mathrm{S}_X$.

Zu $\sigma \in \mathrm{E}_X \smallsetminus \mathrm{S}_X$ existieren $i \neq j$ in X mit $\sigma(i) = \sigma(j)$, also $\sigma = \sigma \circ (i,j)$. Somit gilt $h(\sigma) = h(\sigma) \cdot h(i,j) = -h(\sigma)$, also $h(\sigma) = 0 = \operatorname{sign}(\sigma)$.

(2) Sei $h : (\mathrm{S}_X, \circ, \mathrm{id}_X) \twoheadrightarrow (\{\pm 1\}, \cdot, 1)$ ein Gruppenhomomorphismus. Wir unterscheiden die beiden Fälle $h(\tau_1) \in \{\pm 1\}$ und nutzen (3):
(2a) Im Falle $h(\tau_1) = 1$ ist h trivial, denn $h(\sigma) = 1^{\varepsilon(\sigma)} = 1$ für alle $\sigma \in \mathrm{S}_X$.
(2b) Im Falle $h(\tau_1) = -1$ gilt $h = \sigma$, denn $h(\sigma) = (-1)^{\varepsilon(\sigma)} = \operatorname{sign}(\sigma)$.

Charakterisierung der Signatur

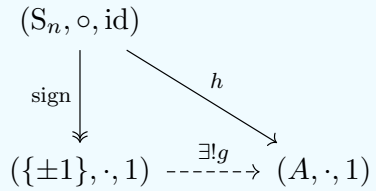
Zu $n \in \mathbb{N}_{\geq 2}$ existieren genau zwei Gruppenhomomorphismen

$$\mathbf{1}, \operatorname{sign} \; : \; (\mathrm{S}_n, \circ, \mathrm{id}) \to (\{\pm 1\}, \cdot, 1),$$

nämlich neben der konstanten Einsabbildung nur die Signatur.

Korollar L1J: Signatur als Abelschmachung

Die Signatur $\operatorname{sign} : (\mathrm{S}_n, \circ, \mathrm{id}) \to (\{\pm 1\}, \cdot, 1)$ ist ein Homomorphismus in die abelsche Gruppe $(\{\pm 1\}, \cdot, 1)$ und in folgendem Sinne universell:



Zu jedem Homomorphismus $h : (\mathrm{S}_n, \circ, \mathrm{id}) \to (A, \cdot, 1)$ in eine abelsche Gruppe existiert genau ein Homomorphismus $g : (\{\pm 1\}, \cdot, 1) \to (A, \cdot, 1)$ mit $h = g \circ \operatorname{sign}$. Das heißt, g macht das obige Diagramm kommutativ.

Charakterisierung der Signatur

Beweis: (1) Eindeutigkeit: Sei g ein Homomorphismus mit $h = g \circ \operatorname{sign}$. Es folgt $g(+1) = 1$ und $g(-1) = g(\operatorname{sign}(\tau)) = h(\tau)$ für jede Transposition $\tau \in \mathrm{S}_n$. Transpositionen existieren dank der Voraussetzung $n \geq 2$. Das legt g eindeutig fest, also gibt es höchstens eine Lösung g.

(2) Wir zeigen die Existenz von g durch die folgende Konstruktion. Wir setzen $a := h(\tau)$ und damit $g(+1) = 1$ sowie $g(-1) = a$. Wegen $\tau^2 = \mathrm{id}$ in S_n gilt $a^2 = 1$ in A, also ist g ein Gruppenhomomorphismus. Dank L1I gilt dann $h(\sigma) = a^{\varepsilon(\sigma)} = g(\operatorname{sign}(\sigma))$ für alle $\sigma \in \mathrm{S}_n$. QED

Effiziente Berechnung der Signatur

Satz L1K: effiziente Berechnung der Signatur

(1) Für jede Permutation $\sigma \in \mathrm{S}_X$ gilt $\operatorname{sign}(\sigma) = (-1)^{\operatorname{inv}(\sigma)} = (-1)^{\varepsilon(\sigma)}$.

(2) Für jede Transposition $\tau = (a, b) \in \mathrm{S}_X$ gilt somit $\operatorname{sign}(\tau) = -1$.

(3) Für jeden ℓ–Zykel $\sigma = (a_1, a_2, \ldots, a_\ell) \in \mathrm{S}_X$ gilt $\operatorname{sign}(\sigma) = (-1)^{\ell-1}$.

Beispiel: Aus der Zykelzerlegung E1C lässt sich die Signatur ablesen.

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 7 & 4 & 6 & 2 & 3 & 8 \end{bmatrix} = \underset{+}{(1)}\ \underset{-}{(2,5,4,7)}\ \underset{+}{(6)}\ \underset{+}{(3,9,8)}$$

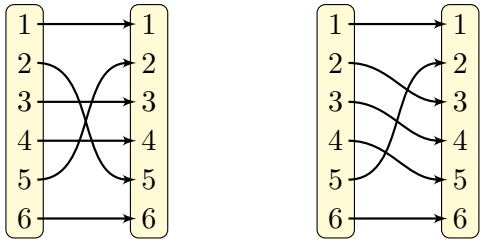
☺ Das ist die bequemste und effizienteste Berechnung der Signatur. (Jedes Produkt von Zykeln genügt hier, es muss nicht disjunkt sein.)

☺ Die Untersuchung aller Paare $\{i \neq j\}$ hat quadratischen Aufwand, denn $\binom{n}{2} = \frac{n(n-1)}{2}$. Die Konstruktion der Zykel hat linearen Aufwand.

☺ Zykelregel L1K und Multiplikativität L1H kommen auch ganz ohne Hilfsstruktur aus und gelten allgemein auf jeder Menge Y (Satz L1O).

Effiziente Berechnung der Signatur

Beispiele:



Beweis: (1) Wir wissen bereits $\operatorname{sign}(\sigma) \in \{\pm 1\}$, daher gilt:

$$\operatorname{sign}(\sigma) = \prod_{\{i \neq j\}} \underbrace{\frac{\sigma(i) - \sigma(j)}{i - j}}_{< 0 \text{ gdw } \{i,j\} \in \operatorname{Inv}(\sigma)} = (-1)^{\operatorname{inv}(\sigma)}$$

(2) Für $\tau = (a, b)$ gilt $\operatorname{inv}(\tau) = 2\,|a - b| - 1$, siehe L1D. Dank (1) folgt

$$\operatorname{sign}(\tau) = (-1)^{\operatorname{inv}(\tau)} = -1.$$

(3) Wir haben $\sigma = (a_1, a_2, \ldots, a_\ell) = (a_1, a_2) \circ (a_2, a_3) \circ \cdots \circ (a_{\ell-1}, a_\ell)$. Dank (2) und Multiplikativität L1H folgt $\operatorname{sign}(\sigma) = (-1)^{\ell-1}$. QED

Effiziente Berechnung der Signatur

Aufgabe: Formulieren Sie einen effizienten Algorithmus (wie E1C) zur Berechnung der Signatur $\operatorname{sign}(\sigma)$ von $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Gelingt es mit linearem Aufwand in n? Aufwand $\binom{n}{2}$ ist nicht optimal!

Algo L1L: Berechnung der Signatur

Eingabe: eine Abbildung $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$
Ausgabe: die Signatur $\operatorname{sign}(\sigma) = s \in \{\pm 1, 0\}$

```
1:  s ← +1; visited ← (0,...,0) ∈ {0,1}^n   // markiere besuchte Punkte
2:  for i from 1 to n do                    // durchlaufe alle Punkte
3:    if visited[i] = 0 then                // falls neuer Zykel...
4:      j ← i; s ← −s                       // eröffne den Zykel
5:      repeat                              // durchlaufe den Zykel...
6:        j ← σ(j); s ← −s                  // nächster Punkt des Zykels
7:        if visited[j] = 1 then return 0   // σ ist nicht injektiv
8:        visited[j] ← 1                    // markiere als besucht
9:      until j = i                         // schließe den Zykel
10: return s                                // Signatur mitgezählt
```


Effiziente Berechnung der Signatur

Bemerkung L1M: die Signatur und ihre Hilfsstrukturen

Zur **Konstruktion** der Signatur nutzen wir zusätzliche Struktur:

- Eine totale Ordnung $(X, \leq) = \{\, 1 < 2 < \cdots < n \,\}$: Damit definieren wir die Menge $\operatorname{Inv}(\sigma)$ der Fehlstände und zeigen kombinatorisch, dass die Parität (L1A) ein Gruppenhomomorphismus ist (L1C).
- Eine Einbettung $X \hookrightarrow K$ in einen Körper K, etwa $X \subset \mathbb{Q}$: Damit stellen wir die Signatur als ein Produkt dar (L1H) und weisen algebraisch ihre Multiplikativität in K nach.

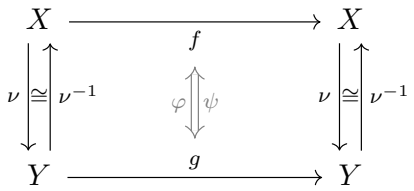
Im geordneten Körper $(\mathbb{Q}, \leq)$ treffen beide Methoden zusammen.

Zur effizienten **Berechnung** der Signatur jedoch sind diese Strukturen schließlich gar nicht mehr notwendig, wie der obige Algorithmus zeigt. Die Ordnung auf $X = \{1, 2, \ldots, n\}$ nutzen wir nur noch zur Organisation der Schleife und zu unserer Buchhaltung. Der folgende Satz erklärt dies.

Die Signatur einer Selbstabbildung

Gegeben sei eine beliebige endliche Menge Y mit $n = \sharp Y < \infty$.
Wie definieren wir die Signatur $\operatorname{sign}_Y : (\mathrm{E}_Y, \circ, \mathrm{id}_Y) \to (\{\pm 1, 0\}, \cdot, 1)$?

Wir wählen willkürlich irgendeine Abzählung $\nu : X = \{1, \ldots, n\} \xrightarrow{\sim} Y$.



Lemma L1N: $X \cong Y$ impliziert $\mathrm{S}_X \cong \mathrm{S}_Y$

Jede Bijektion $\nu : X \xrightarrow{\sim} Y$ stiftet einen Isomorphismus

$$\begin{aligned}(\varphi, \psi) \;:\; (\mathrm{E}_X, \circ, \mathrm{id}_X) &\cong (\mathrm{E}_Y, \circ, \mathrm{id}_Y)\\ : \;(\mathrm{S}_X, \circ, \mathrm{id}_X) &\cong (\mathrm{S}_Y, \circ, \mathrm{id}_Y)\end{aligned}$$

mit $\varphi : f \mapsto g = \nu \circ f \circ \nu^{-1}$ und $\psi : g \mapsto f = \nu^{-1} \circ g \circ \nu$.

Die Signatur einer Selbstabbildung

Beweis: Die Aussage ist klar. Falls nicht, so ist es eine gute Übung: Alle Daten liegen explizit vor, es genügt sorgsames Nachrechnen!

Aufgabe: Führen Sie den behaupteten Isomorphismus aus.

Lösung: Es gilt $\psi(\varphi(f)) = \nu^{-1} \circ (\nu \circ f \circ \nu^{-1}) \circ \nu = f$ und ebenso $\varphi(\psi(g)) = g$. Wir haben also ein Bijektionspaar $(\varphi, \psi) : \mathrm{E}_X \cong \mathrm{E}_Y$.

Die Abbildung φ respektiert die Komposition: Es gilt $\varphi(\mathrm{id}_X) = \mathrm{id}_Y$ und

$$\varphi(f' \circ f) = \nu \circ f' \circ f \circ \nu^{-1} = \nu f' \nu^{-1} \circ \nu f \nu^{-1} = \varphi(f') \circ \varphi(f).$$

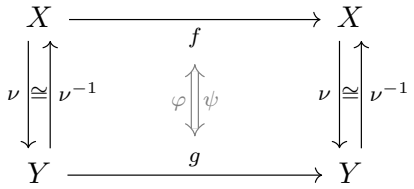
Gleiches gilt für ψ. Also haben wir ein Isomorphismenpaar (φ, ψ). QED

☺ Auf der „nackten“ Menge Y haben wir zunächst keinerlei Struktur; diese führen wir durch unsere „Koordinaten“ $\nu : X \xrightarrow{\sim} Y$ erst ein.

☺ Ich erkläre dieses Vorgehen hier betont ausführlich, in Zeitlupe. Wir werden dies später für die Determinante genauso ausführen. Daher ist es gut, mit der leichter fasslichen Signatur zu üben.

Die Signatur einer Selbstabbildung

Als Hilfskonstrukt wählen wir eine Abzählung $\nu : X = \{1, \ldots, n\} \xrightarrow{\sim} Y$.



Satz L1O: die Signatur einer Selbstabbildung

(0) Mit der Abzählung $\nu : X = \{1, \ldots, n\} \xrightarrow{\sim} Y$ definieren wir

$$\operatorname{sign}_Y \;:\; \mathrm{E}_Y \to \{\pm 1, 0\} \;:\; g \mapsto \operatorname{sign}_Y(g) := \operatorname{sign}_X(\nu^{-1} \circ g \circ \nu).$$

Diese Abbildung sign_Y ist wohldefiniert, das heißt unabhängig von ν.

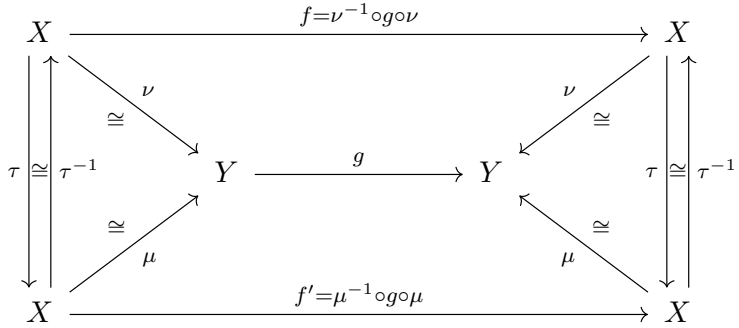
(1) Wir erhalten so den ersehnten Monoidhomomorphismus

$$\operatorname{sign}_Y = \operatorname{sign}_X \circ \psi \;:\; (\mathrm{E}_Y, \circ, \mathrm{id}_Y) \to (\{\pm 1, 0\}, \cdot, 1).$$

Weiterhin gilt die Zykelregel L1K zur effizienten Berechnung.

Invarianz der Signatur

Beweis: (0) Wir vergleichen zwei Bijektionen $\mu, \nu : X \xrightarrow{\sim} Y$:



Wir haben $f' = \tau \circ f \circ \tau^{-1}$ mit $\tau = \mu^{-1} \circ \nu : X \xrightarrow{\sim} X$, also:

$$\operatorname{sign}_X(f') = \operatorname{sign}_X(\tau) \cdot \operatorname{sign}_X(f) \cdot \operatorname{sign}_X(\tau)^{-1} = \operatorname{sign}_X(f)$$

Somit ist die Signatur $\operatorname{sign}_Y(g) := \operatorname{sign}_X(f) = \operatorname{sign}_X(f')$ wohldefiniert, da unabhängig von den willkürlich gewählten Abzählungen ν, μ. QED

Die alternierende Gruppe

Sei X eine endliche Menge, etwa $X = \{1, \ldots, n\}$ als Standardmodell.
Für Selbstabbildungen $f : X \to X$ haben wir die **Signatur** (L1H / L1O), und sie ist ein Homomorphismus von Monoiden bzw. Gruppen:

$$\begin{aligned} \operatorname{sign} = \operatorname{sign}_X &: (\mathrm{E}_X, \circ, \mathrm{id}_X) \to (\{\pm 1, 0\}, \cdot, 1) : f \mapsto \operatorname{sign}(f) \\ &: (\mathrm{S}_X, \circ, \mathrm{id}_X) \to (\{\pm 1\}, \cdot, 1) \quad : \sigma \mapsto \operatorname{sign}(\sigma) \end{aligned}$$

Dabei gilt $\operatorname{sign}(\sigma) = (-1)^{\operatorname{inv}(\sigma)} = (-1)^{\varepsilon(\sigma)}$ dank der **Parität** (L1C / L1K)

$$\varepsilon : (\mathrm{S}_n, \circ, \mathrm{id}_X) \to (\mathbb{Z}_2, +, 0) : \sigma \mapsto \operatorname{inv}(\sigma) \bmod 2.$$

Jede Permutation $\sigma \in \mathrm{S}_X$ ist ein Produkt von Transpositionen (L1E):

0 Im Falle $\operatorname{sign}(\sigma) = +1$ hat jedes solche Produkt gerade Länge.

1 Im Falle $\operatorname{sign}(\sigma) = -1$ hat jedes solche Produkt ungerade Länge.

Definition L1P: die alternierende Gruppe

Die geraden Permutationen bilden die **alternierende Gruppe**

$$\mathrm{A}_X = \operatorname{Alt}(X) := \ker(\operatorname{sign}_X) = \{\, \sigma \in \mathrm{S}_X \mid \operatorname{sign}(\sigma) = +1 \,\} \leq \mathrm{S}_X \,.$$

Die alternierende Gruppe

🙂 Die traditionelle Benennung ist ein grandioser Etikettenschwindel: Die symmetrische Gruppe ist nicht symmetrisch, und die alternierende Gruppe alterniert nicht, aber so wurden die Namen nun mal vergeben.

Beispiel: Für $X = \{1\}$ haben wir:

$$\begin{aligned} \mathrm{S}_1 &= \operatorname{Sym}(X) = \{\, \mathrm{id}_X \,\} \\ \mathrm{A}_1 &= \operatorname{Alt}(X) \;\; = \{\, \mathrm{id}_X \,\} \end{aligned}$$

Beispiel: Für $X = \{1, 2\}$ haben wir:

$$\begin{aligned} \mathrm{S}_2 &= \operatorname{Sym}(X) = \{\, \mathrm{id}_X,\ (1,2) \,\} \\ \mathrm{A}_2 &= \operatorname{Alt}(X) \;\; = \{\, \mathrm{id}_X \,\} \end{aligned}$$

Beispiel: Für $X = \{1, 2, 3\}$ haben wir:

$$\begin{aligned} \mathrm{S}_3 &= \operatorname{Sym}(X) = \{\, \mathrm{id}_X,\ (1,2,3),\ (1,3,2),\ (1,2),\ (1,3),\ (2,3) \,\} \\ \mathrm{A}_3 &= \operatorname{Alt}(X) \;\; = \{\, \mathrm{id}_X,\ (1,2,3),\ (1,3,2) \,\} \end{aligned}$$

Übung: Schreiben Sie ebenso S_4 und A_4 explizit aus!

Die alternierende Gruppe

Satz L1Q: Ordnung der alternierenden Gruppe

Sei X eine endliche Menge mit Elementezahl $n = \sharp X \geq 2$.

(0) Die Signatur definiert eine kurze exakte Sequenz von Gruppen:

$$1 \longrightarrow \mathrm{A}_X \xhookrightarrow{\text{inc}} \mathrm{S}_X \xrightarrow{\operatorname{sign}_X} \{\pm 1\} \longrightarrow 1$$

(1) Für jede ungerade Permutation $\tau \in \mathrm{S}_X$, mit $\operatorname{sign}(\tau) = -1$, gilt

$$\mathrm{S}_X = \mathrm{A}_X \sqcup (\tau \circ \mathrm{A}_X) = \mathrm{A}_X \sqcup (\mathrm{A}_X \circ \tau).$$

(2) Für die Gruppenordnung (Elementezahl) gilt demnach:

$$\sharp \mathrm{S}_X = n! \quad \text{und} \quad \sharp \mathrm{A}_X = n!/2$$

Beweis: (0) Die Signatur $\operatorname{sign}_X : \mathrm{S}_X \to \{\pm 1\}$ ist surjektiv mit Kern A_X. (1) Dies haben wir in Satz G1R nachgerechnet. (2) Wir nutzen hier die Bijektion $\mathrm{A}_X \cong \tau \circ \mathrm{A}_X$ mit $\sigma \mapsto \rho = \tau \circ \sigma$ und $\sigma = \tau^{-1} \circ \rho \mapsfrom \rho$. QED

Die alternierende Gruppe

Exakte Sequenzen kennen Sie bereits für lineare Abbildungen (I2H). Allgemein für Gruppen definieren wir Exaktheit durch *Bild gleich Kern*: An jeder Stelle ist das Bild von links gleich dem Kern nach rechts.

Im vorliegenden Beispiel bündelt die Exaktheit drei Aussagen:

1 Die Signatur $\operatorname{sign}_X : \mathrm{S}_X \to \{\pm 1\}$ ist surjektiv.

2 Der Kern ist die alternierende Gruppe $\ker(\operatorname{sign}_X) = \mathrm{A}_X$.

3 Die Inklusion $\mathrm{A}_X \hookrightarrow \mathrm{S}_X$ in die symmetrische Gruppe ist injektiv.

Daraus folgt die Zerlegung (1) in die Fasern der Abbildung sign_X.

Dies kann man hier auch direkt sehen: Für jede Permutation $\sigma \in \mathrm{S}_X$ gilt entweder $\sigma \in \mathrm{A}_X$, nämlich im Falle $\operatorname{sign}(\sigma) = +1$, oder $\tau^{-1} \circ \sigma \in \mathrm{A}_X$, im verbleibenden Falle $\operatorname{sign}(\sigma) = -1$, also $\sigma \in \tau \circ \mathrm{A}_X$.

Bei disjunkter Vereinigung addieren sich die Elementezahlen (E2A). Zudem haben wir eine Bijektion $\mathrm{A}_X \cong \tau \circ \mathrm{A}_X$ wie oben gezeigt. Also gilt $2 \cdot \sharp \mathrm{A}_X = \sharp \mathrm{S}_X = n!$, siehe E2H.

Anwendungsbeispiel: das 15-Puzzle

A :

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	+

B :

10	1	3	−
6	2	11	4
7	14	8	12
9	15	13	5

C :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	+

Aufgabe: (1) Wie / Kommen Sie von B zurück zur Anfangsposition A?
(2) Können Sie von Position C jemals zur Anfangsposition gelangen?

A :

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

$\sigma(1)$	$\sigma(2)$	$\sigma(3)$	$\sigma(4)$
$\sigma(5)$	$\sigma(6)$	$\sigma(7)$	$\sigma(8)$
$\sigma(9)$	$\sigma(10)$	$\sigma(11)$	$\sigma(12)$
$\sigma(13)$	$\sigma(14)$	$\sigma(15)$	$\sigma(16)$

+	−	+	−
−	+	−	+
+	−	+	−
−	+	−	+

Invariante: Das Produkt $s(\sigma) \cdot \operatorname{sign}(\sigma)$ ist konstant und anfangs gleich 1.

Anwendungsbeispiel: das 15-Puzzle

Erfunden hat dieses Schiebe-Puzzle Noyes Chapman aus New York. Im Jahr 1880 hat es weltweit einen phänomenalen Hype ausgelöst, vor allem in den USA, Kanada und Europa. Weiter befeuert wurde die Hysterie, als Sam Lloyd für die Lösung des 14-15-Puzzles (C) einen Preis von 1000 Dollar auslobte, das entspricht heute etwa 25 000 Dollar.

Es wurde sogar davon berichtet, dass Arbeitnehmer nicht zu ihrer Arbeit erschienen, und Ladenbesitzer ihre Läden nicht öffneten, weil alle wie besessen einer Lösung dieser logischen Knobelei nachjagten.

🙂 Ausbezahlt wurde der Preis jedoch nie, und Sam Lloyd wusste das vermutlich schon im Vorhinein. Genau darum geht es in der Aufgabe!

Anwendungsbeispiel: das 15-Puzzle

Fun fact: Recht genau hundert Jahre später errang Rubik's Cube eine ähnliche Popularität. Rubik selbst erklärte, seine Erfindung wurde vom 15-Puzzle inspiriert. Beide sind bis heute sehr beliebt.

🙂 In beiden Rätseln steckt eine ganze Menge Mathematik, genauer die Theorie von Permutationsgruppen, in unterhaltsamer Einkleidung.

🙂 Wenn Sie Spaß an solchen Knobeleien und Geduldspielen haben, so lösen Sie das Beispiel B. Formulieren Sie ein allgemeines Verfahren, mit dem Sie jede (mögliche?) Problemstellung des 15-Puzzles lösen.

Anwendungsbeispiel: das 15-Puzzle

Lösung des 15-Puzzles

Lösung: (1) Ja, das Problem B ist lösbar: Es gibt eine Zugfolge von B nach A. Hierzu benötigen Sie vor allem Geduld. Mathematik hilft (L1S).

(2) Nein, das ist unmöglich. Hier hilft keine Geduld, nur Mathematik!

Ausführlich: Jede Spielposition ist eine Permutation $\sigma \in \mathrm{S}_{16}$, wobei die Nummer 16 das leere Feld darstellt. Jeder Spielzug $\sigma \mapsto \sigma' = (i,j) \circ \sigma$ ist die Nachschaltung einer Transposition (i,j): Sie dürfen die Nummern $i = \sigma(a)$ und $j = \sigma(b)$ vertauschen, wenn die Felder a und b benachbart sind und zudem $i = 16$ oder $j = 16$ gilt. Das freie Feld 16 wandert dabei um genau eine Position. Wir beginnen in der Anfangsposition A mit der Permutation id und Signatur $+$. Nach jedem Zug sehen Sie die Signatur $\mathrm{sign}(\sigma)$ direkt am angegebenen Schachbrettmuster $s(\sigma)$. Genial!

Lösung des 15-Puzzles

Beispiel: In Position B zeigt das freie Feld $s = -$, die Permutation β sollte also ungerade sein. Probieren Sie es aus! Die Rechnung ist eine sehr gute praktische Übung, am besten effizient dank Zykelregel L1K.

Die tatsächliche Ausführung der Lösung ist damit noch nicht vollbracht, aber immerhin wissen wir, dass eine Lösung existiert (dank Satz L1S), und sich die Suche lohnt. Vor dem Start der fieberhaften Suche ist dies die entscheidende Information, der Rest ist dann Geduldsarbeit.

Beispiel: In Position C zeigt das freie Feld $s = +$, die Permutation γ müsste also gerade sein. Das ist sie aber offensichtlich nicht!

Auch dies ist eine hilfreiche Information: Wir brauchen die Suche gar nicht starten, denn es gibt nachweislich keine Lösung.

Lösung des 15-Puzzles

Zusammengefasst und noch eleganter formuliert:

Sei $s(\sigma)$ das Vorzeichen $+/-$ des freien Feldes im obigen Muster. Weiterhin sei $\mathrm{sign}(\sigma)$ die Signatur der Permutation σ, wie zuvor erklärt.

Lemma L1R: die Invariante des 15-Puzzles

Das Produkt $I(\sigma) = s(\sigma) \cdot \mathrm{sign}(\sigma)$ bleibt bei jedem Zug unverändert, da jedesmal beide Faktoren ihr Vorzeichen wechseln.

🙂 Ist diese Paritätsbedingung verletzt, so ist das Puzzle unlösbar: Die Positionen α, γ mit $I(\alpha) \neq I(\gamma)$ lassen sich nicht ineinander überführen.

🙂 Es ist viel besser, ein Stündchen in das Erlernen der Signatur zu stecken als Monate einer Lösung nachzujagen, die gar nicht existiert!

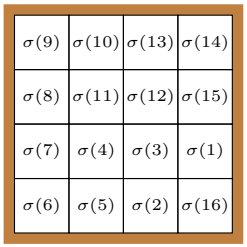
Interessanterweise gilt die Umkehrung: Ist die Paritätsbedingung erfüllt, so ist das Puzzle lösbar. Das ist etwas mühsamer zu konstruieren. Algebraisch bedeutet es, die alternierende Gruppe zu erzeugen!

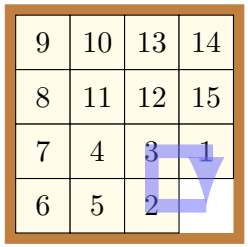
Lösung des 15-Puzzles

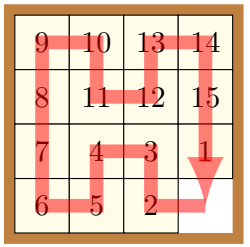
Satz L1S: Lösung des 15-Puzzles

Beim 15-Puzzle ist genau die Hälfte der Spielpositionen σ von der Startposition α aus erreichbar, nämlich solche, mit $I(\sigma) = I(\alpha)$.

Beweis: (1) „Höchstens die Hälfte“ folgt aus der Invariante I.
(2) „Mindestens die Hälfte“ zeigen wir durch folgende Konstruktion. Zur Vereinfachung nummerieren wir die Felder neu wie gezeigt.







Wir können die Zykel $(1,2,3)$ und $(1,2,\ldots,15)$ realisieren, wie gezeigt. Diese erzeugen die gesamte alternierende Gruppe A_{15} (Satz L1T). QED

Erzeugendensysteme für die alternierende Gruppe

Analog zur symmetrischen Gruppe S_n (L1G) und motiviert durch das 15-Puzzle untersuchen wir nun Erzeugendensysteme für A_n.

Satz L1T: Erzeugendensysteme für A_n.

Die 3–Zykel in A_n erzeugen die alternierende Gruppe A_n.
Ebenso gilt $\mathrm{A}_n = \langle\, E_n^s \,\rangle$ für jede der folgenden Familien:

$$E_n^1 = \{\, (i,j,k) \mid i<j<k \,\}$$
$$E_n^2 = \{\, (1,2,3), (1,2,4), \ldots, (1,2,n) \,\}$$
$$E_n^3 = \{\, (1,2,3), (1,3,4), \ldots, (1,n-1,n) \,\}$$
$$E_n^4 = \{\, (1,2,3), (2,3,4), \ldots, (n-2,n-1,n) \,\}$$
$$E_n^5 = \{\, (1,2)(2,3), (1,2)(3,4), \ldots, (1,2)(n-1,n) \,\}$$
$$E_n^6 = \begin{cases} \{\, (1,2,3), (1,2,\ldots,n) \,\} & \text{falls } n \text{ ungerade,} \\ \{\, (1,2,3), (2,3,\ldots,n) \,\} & \text{falls } n \text{ gerade.} \end{cases}$$

Insbesondere lässt sich die Gruppe A_n durch zwei Elemente erzeugen.

Erzeugendensysteme für die alternierende Gruppe

Beweis: (1) Sei $G_n = \langle\, E_n^s \,\rangle \leq \mathrm{S}_n$ die erzeugte Untergruppe.
Die entscheidenden drei Eigenschaften der Familie E_n^s sind:

1. Alle Permutationen sind gerade, $E_n^s \subseteq \mathrm{A}_n$, somit gilt $G_n \leq \mathrm{A}_n$.
2. Zu jedem Element $i \in \{1,\ldots,n\}$ existiert $\rho \in G_n$ mit $\rho(i) = n$.
3. Es gilt $G_{n-1} \leq G_n$, so dass wir induktiv vorgehen können.

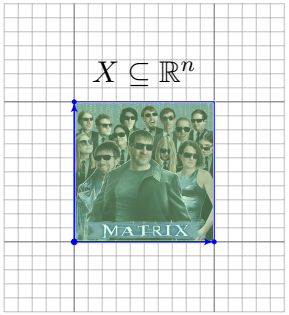
Das ist jeweils sorgsam zu prüfen und gelingt meist leicht.
Für $s = 1,\ldots,5$ gilt sogar $E_{n-1}^s \subseteq E_n^s$, somit $\langle\, E_{n-1}^s \,\rangle \subseteq \langle\, E_n^s \,\rangle$.
Lediglich für $s = 6$ ist die Eigenschaft (3) nicht offensichtlich.

(2) Wir zeigen nun $\mathrm{A}_n \leq G_n$ per Induktion über n.
Die Aussage ist trivial für $n \leq 2$. Sei also $n \geq 3$.
Die Aussage $\mathrm{A}_{n-1} \leq G_{n-1}$ sei bereits bewiesen.
Sei $\sigma \in \mathrm{A}_n$. Zu $i := \sigma(n)$ wählen wir $\rho \in G_n \leq \mathrm{A}_n$ mit $\rho(i) = n$.
Somit gilt $(\rho \circ \sigma)(n) = n$, also $\rho \circ \sigma \in \mathrm{A}_{n-1} \leq G_{n-1} \leq G_n$.
Daraus folgt $\sigma \in \rho^{-1} \circ G_n = G_n$. Wir schließen $\mathrm{A}_n \leq G_n$. QED

Erzeugendensysteme für die alternierende Gruppe

Erzeugendensysteme für die alternierende Gruppe

Geometrische Motivation: Volumen und Determinante

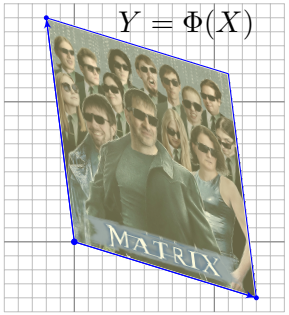


lineare Abbildung

$$\Phi : \mathbb{R}^n \to \mathbb{R}^n$$
$$x \mapsto y = Ax$$

Zahlenbeispiel:

$$A = \begin{bmatrix} 1.3 & -0.2 \\ -0.4 & 1.6 \end{bmatrix}$$



Wie verhält sich das Volumen unter der linearen Abbildung Φ?

$$\boxed{\mathrm{vol}_n(Y) = \mathrm{vol}_n(X) \cdot |\det(A)|}$$

Jede lineare Abbildung $\Phi : \mathbb{R}^n \to \mathbb{R}^n$ können wir als Matrix $A \in \mathbb{R}^{n \times n}$ darstellen (K1E). Die Determinante $\det(A)$ misst die Volumenänderung.

Geometrische Motivation: Volumen und Determinante

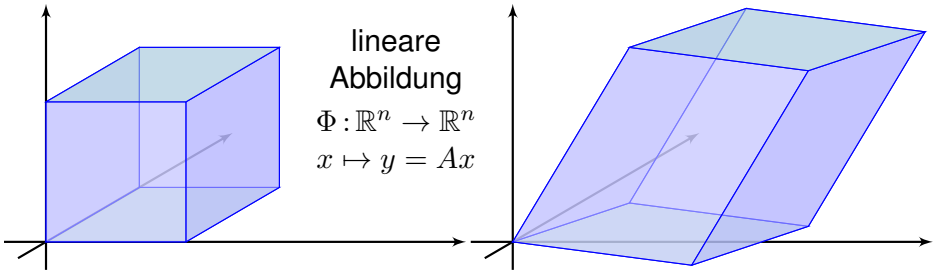
Wie verhält sich das Volumen von $X \subseteq \mathbb{R}^n$ unter Transformationen? Der einfachste und grundlegende Fall sind lineare Abbildungen. Hier liefert die Determinante die Antwort, kurz und elegant.

Determinanten sind ein wunderschönes Thema mit vielen Facetten. Es hat zahlreiche Anwendungen, theoretischer und praktischer Natur, innerhalb der (Linearen) Algebra, und außerhalb sogar noch mehr.

Mit Determinanten können Sie nicht nur Volumina berechnen, sondern auch lineare Gleichungssysteme lösen und Matrizen invertieren und noch vieles mehr. Die Determinante ist ein Universalwerkzeug.

Dazu später... zunächst nutzen wir die geometrische Anschauung.

Geometrische Motivation: Volumen und Determinante



lineare Abbildung

$$\Phi : \mathbb{R}^n \to \mathbb{R}^n$$
$$x \mapsto y = Ax$$

Je n Vektoren $\mathcal{A} = (a_1, \ldots, a_n)$ im $\mathbb{R}^n$ spannen ein **Parallelotop** auf:

$$P = \{\, a_1 x_1 + \cdots + a_n x_n \mid x_1, \ldots, x_n \in [0,1] \,\} = A \cdot [0,1]^n$$

Dies ist das Bild des **Einheitswürfels** $[0,1]^n$ unter der Abbildung Φ.
Wir untersuchen nun das **orientierte Volumen**

$$v : \mathbb{R}^{n \times n} \to \mathbb{R} : A \mapsto v(A) \quad \text{sodass} \quad \mathrm{vol}_n(P) = |v(A)|.$$

Ziele: präzise Definition? gute Eigenschaften? effiziente Berechnung?

Geometrische Motivation: Volumen und Determinante

Ich nenne P hier allgemein ein **Parallelotop**. In Dimension $n = 2$ ist dies ein **Parallelogramm**, in Dimension $n = 3$ nennt man dies auch ein **Parallelepiped** oder einen **Spat**. Die Rechnungen sehen in jeder Dimension gleich aus, daher lege ich die Dimension n hier nicht fest.

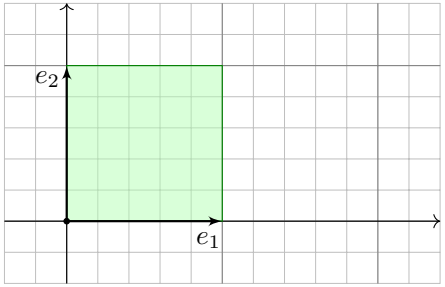
Die **Volumenverzerrung** spielt in der Analysis eine wichtige Rolle bei der Transformationsformel der mehrdimensionalen Integration. Die Matrix ist dort die **Jacobi-Matrix** der Koordinatentransformation und die Determinante ist die sogenannte **Funktionaldeterminante**. Den algebraischen Teil dieser Theorie bereiten wir hier vor.

Notation: Wir fassen die Familie $\mathcal{A} = (a_1, \ldots, a_n)$ der Spaltenvektoren $a_1, \ldots, a_n \in \mathbb{R}^n$ als die Spalten der Matrix $A \in \mathbb{R}^{n \times n}$ zusammen.

Im Folgenden unterscheide ich daher nicht penibel zwischen der Familie $\mathcal{A} = (a_1, \ldots, a_n) \in (\mathbb{R}^n)^n$ und der Matrix $A = (a_1, \ldots, a_n) \in \mathbb{R}^{n \times n}$.

Das vereinfacht uns etwas die Schreib- und Sprechweise.
Die Indizes ergeben sich jeweils aus dem Kontext.

Determinante als orientiertes Volumen

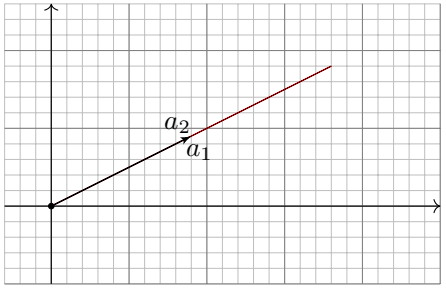


1. Normierung: Für die Standardbasis $(e_1, \ldots, e_n)$ gilt

$$v(e_1, \ldots, e_n) = 1.$$

Wir sagen hierzu, die Abbildung v ist **normiert**.

Determinante als orientiertes Volumen

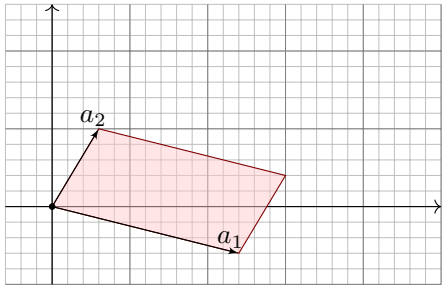


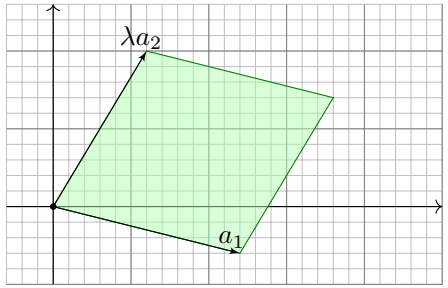
2. Degenerierung: Gilt $a_i = a_j$ für ein Paar $i \neq j$, so folgt

$$v(a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n) = 0.$$

Wir sagen hierzu, die Abbildung v ist **alternierend**.

Determinante als orientiertes Volumen





3. Skalierung: Für alle $\lambda \in \mathbb{R}$ gilt

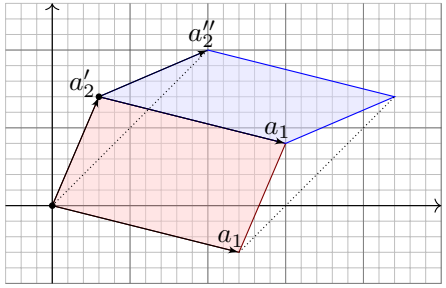
$$v(a_1, \ldots, \lambda a_i, \ldots, a_n) = \lambda v(a_1, \ldots, a_i, \ldots, a_n).$$

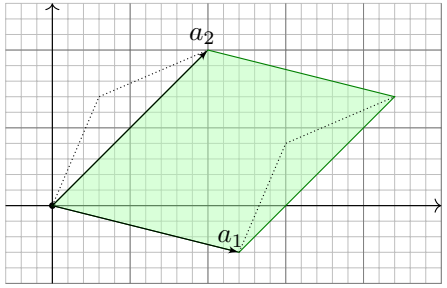
Für $\lambda < 0$ kehrt sich das Vorzeichen um: orientiertes Volumen!

☺ Der Absolutbetrag $|v(A)|$ misst das geometrische Volumen des Parallelotops, also die Volumenverzerrung der Abbildung $\Phi_{\mathcal{A}} : \mathbb{R}^n \to \mathbb{R}^n$.

☺ Das Vorzeichen $\operatorname{sign} v(A)$ misst, ob die Familie $\mathcal{A} = (a_1, \ldots, a_n)$ rechtshändig oder linkshändig ist (bzgl. der Standardbasis des $\mathbb{R}^n$).

Determinante als orientiertes Volumen





4. Additivität: Für $a_i = a_i' + a_i''$ in $\mathbb{R}^n$ gilt

$$v(a_1, \ldots, a_i' + a_i'', \ldots, a_n) = v(a_1, \ldots, a_i', \ldots, a_n) + v(a_1, \ldots, a_i'', \ldots, a_n)$$

Zusammenfassend: Die Abbildung v ist $\mathbb{R}$–linear in jeder Spalte a_i.

Eindeutigkeit? Können wir das Volumen damit eindeutig bestimmen? und effizient berechnen? Oder fehlen noch weitere Forderungen?

Existenz? Sind unsere Wünsche erfüllbar, also widerspruchsfrei? Oder haben wir hier bereits zu viele Forderungen erhoben?

Multilinear, alternierend, normiert

Definition L2A: multilinear, alternierend, normiert

Sei K ein kommutativer Ring und $v : K^{n\times\ell} \to K$ eine Abbildung,

$$v \;:\; (a_1, \dots, a_i, \dots, a_\ell) \mapsto v(a_1, \dots, a_i, \dots, a_\ell).$$

(1) Wir nennen v **multilinear** über K, falls v linear in jeder Spalte ist:

$$\begin{aligned} v(a_1, \dots, a_i'+a_i'', \dots, a_\ell) &= v(a_1, \dots, a_i', \dots, a_\ell) + v(a_1, \dots, a_i'', \dots, a_\ell), \\ v(a_1, \dots, \lambda \cdot a_i, \dots, a_\ell) \;\; &= \lambda \cdot v(a_1, \dots, a_i, \dots, a_\ell) \end{aligned}$$

für alle $a_1, \dots, a_i, a_i', a_i'', \dots, a_\ell \in K^n$ und $\lambda \in K$.

(2) Wir nennen v **alternierend**, falls aus der Gleichheit $a_i = a_j$ zweier Spalten $i \neq j$ stets $v(a_1, \dots, a_i, \dots, a_j, \dots, a_\ell) = 0$ folgt.

Wir nennen v **antisymmetrisch**, falls Vertauschung das Vorzeichen wechselt gemäß $v(\dots, a_i, \dots, a_j, \dots) = -v(\dots, a_j, \dots, a_i, \dots)$.

Wir nennen v **symmetrisch**, falls Vertauschung nichts ändert.

(3) Im Falle $n = \ell$ nennen wir v **normiert**, falls $v(e_1, \dots, e_n) = 1$ gilt.

Multilinear, alternierend, normiert

Hier und im Folgenden sei K ein kommutativer Ring.

- Wir betrachten die linearen Räume K^n und $K^{n\times\ell}$ über K.
- Skalare $\lambda \in K$ multiplizieren wir wahlweise von links oder rechts.

Jede Matrix $A \in K^{n\times\ell}$ können wir auffassen als Familie $\mathcal{A} = (a_1, \dots, a_\ell)$ von Spaltenvektoren $a_1, \dots, a_\ell \in K^n$. Wir nutzen also $K^{n\times\ell} \cong (K^n)^\ell$.

Die Abbildung $v : K^{n\times\ell} \to K$ nimmt als Eingabe ℓ Spaltenvektoren $a_1, \dots, a_\ell \in K^n$ und liefert als Ausgabe einen Skalar $v(a_1, \dots, a_\ell) \in K$.

Für A nutzen wir die traditionelle Indizierung: erst Zeile, dann Spalte. Der Eintrag $a_{ki} = a_{k,i}$ bezeichnet den $k$ten Eintrag der $i$ten Spalte a_i. Die Familie der Zeilen wäre in dieser Hinsicht hier etwas bequemer.

Die Familie $(a_1, \dots, a_\ell)$ suggeriert umgekehrt: erst Spalte, dann Zeile. In dieser Sichtweise als Spaltenvektoren haben wir also $(a_i)_k = a_{ki}$. Das ist leider nicht besonders elegant, aber nicht weiter tragisch.

☺ Die Determinante, auf die wir zuarbeiten, erweist sich als invariant unter Transposition $A \mapsto A^\mathsf{T}$, also geben beide Sichtweisen dasselbe.

Einmal Null, immer Null

Uns interessiert hier vor allem der Fall $n = \ell$. Wir wollen zeigen: Es existiert genau eine multilineare, alternierende und normierte Abbildung $v : K^{n\times n} \to K$, und diese nennen wir **die Determinante**. Das ist die Aussage des Hauptsatzes L2G zu Determinanten.

Zur Vorbereitung stellen wir einfache Rechenregeln zusammen. Wir beginnen mit der folgenden, sehr einfachen Beobachtung:

Bemerkung L2B: einmal Null, immer Null

Allein mit der Additivität folgt aus $a_i = 0$ bereits $v(A) = 0$, denn

$$\begin{aligned} v(\dots, a_{i-1}, 0, a_{i+1}, \dots) &= v(\dots, a_{i-1}, 0+0, a_{i+1}, \dots) \\ &= v(\dots, a_{i-1}, 0, a_{i+1}, \dots) + v(\dots, a_{i-1}, 0, a_{i+1}, \dots). \end{aligned}$$

Dasselbe folgt ebenso aus der K–Homogenität für $\lambda = 0$:

$$v(\dots, a_{i-1}, 0 \cdot 0, a_{i+1}, \dots) = 0 \cdot v(\dots, a_{i-1}, 0, a_{i+1}, \dots)$$

Der Skalar $0 = 0_K$ und der Vektor $0 = 0_{K^n}$ haben hier dasselbe Symbol. Das ist schon arg knausrig, aber daran haben Sie sich schon gewöhnt.

Transvektion ändert nichts.

Lemma L2C: Transvektion ändert nichts.

Ist $v : K^{n\times\ell} \to K$ multilinear und alternierend so gilt

$$v(\dots, a_i, \dots, a_j + \lambda a_i, \dots) = v(\dots, a_i, \dots, a_j, \dots)$$

Beweis: Wir nutzen die Linearität in Spalte j:

$$\begin{aligned} &v(\dots, a_i, \dots, a_j + \lambda a_i, \dots) \\ &= v(\dots, a_i, \dots, a_j, \dots) + \lambda\, v(\dots, a_i, \dots, a_i, \dots) \end{aligned}$$

Da v alternierend ist, verschwindet der letzte Summand. QED

Das ist eine einfache Rechnung, doch die Konsequenzen sind enorm: Das Lemma zeigt, dass wir den Gauß–Algorithmus anwenden können: Bei Transvektionen ändert sich der Wert von v nicht, wie hier zu sehen Bei Skalierung einer Spalte nutzen wir die Linearität (K–Homogenität). Es bleiben noch Vertauschungen, die untersuchen wir als nächstes…

Aus alternierend folgt antisymmetrisch.

Lemma L2D: Aus alternierend folgt antisymmetrisch.

(1) Sei v multilinear. Ist v alternierend, so auch antisymmetrisch.

$$(\star) \qquad v(\dots, a_i, \dots, a_j, \dots) = -v(\dots, a_j, \dots, a_i, \dots)$$

(2) Über jedem Körper K der Charakteristik $\neq 2$ gilt die Umkehrung.

Beweis: (1) Wir nutzen die Additivität in den Spalten $i \neq j$:

$$\begin{aligned} 0 &\overset{\text{alt}}{=} v(\dots, a_i + a_j, \dots, a_i + a_j, \dots) \\ &\overset{\text{add}}{=} + v(\dots, a_i, \dots, a_i, \dots) + v(\dots, a_i, \dots, a_j, \dots) \\ &\quad + v(\dots, a_j, \dots, a_i, \dots) + v(\dots, a_j, \dots, a_j, \dots) \end{aligned}$$

(2) Aus $(\star)$ und $a_i = a_j$ mit $i \neq j$ folgt $2v(\dots, a_i, \dots, a_j, \dots) = 0$.
Nach Division durch 2 erhalten wir $v(\dots, a_i, \dots, a_j, \dots) = 0$. QED

Gegenbeispiel: Die Multiplikation $\cdot : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2 : (a, b) \mapsto a \cdot b$ ist anti/symmetrisch, aber nicht alternierend, da $1 \cdot 1 = 1 \neq 0$.

Permutationsmatrizen und Signatur

Jede Abbildung $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ definiert eine Matrix

$$P_\sigma := (e_{\sigma(1)}, \dots, e_{\sigma(n)}) \in K^{n \times n}.$$

Im Falle $\sigma \in \mathrm{S}_n$ nennen wir P_σ die **Permutationsmatrix** zu σ.

Beispiel: Für $\sigma = (1,2,3) = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right]$ und $\tau = (2,3) = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right]$ in S_3 gilt

$$P_\sigma = (e_2, e_3, e_1) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \text{ und } P_\tau = (e_1, e_3, e_2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Lemma L2E: Permutationsmatrix und Signatur

Ist $v : K^{n \times n} \to K$ multilinear und alternierend, so gilt

$$\boxed{v(P_\sigma) = \operatorname{sign}(\sigma) \cdot v(E).}$$

Ist v zudem normiert durch $v(E) = 1$, so folgt $v(P_\sigma) = \operatorname{sign}(\sigma)$.

Beweis: Ist σ nicht injektiv, so gilt $v(P_\sigma) = 0$ (L2A) und $\operatorname{sign}(\sigma) = 0$ (L1H). Jede Permutation $\sigma \in \mathrm{S}_n$ ist Produkt $\sigma = \tau_1 \tau_2 \cdots \tau_\ell$ von Transpositionen (L1E), also $\operatorname{sign}(\sigma) = (-1)^\ell$ (L1K) und $v(P_\sigma) = (-1)^\ell \cdot v(E)$ (L2D). QED

Permutationsmatrizen und Signatur

Die Matrix P_σ entspricht der linearen Abbildung

$$K^n \to K^n \; : \; e_i \mapsto e_{\sigma(i)}.$$

Dabei gilt $P_\sigma \cdot P_\tau = P_{\sigma \circ \tau}$ und $P_{\sigma^{-1}} = P_\sigma^{-1} = P_\sigma^\intercal$. Wir haben also:

$$\begin{aligned} P \; : \; (\mathrm{E}_n, \circ, \mathrm{id}) &\hookrightarrow (K^{n \times n}, \cdot, 1_{n \times n}) \quad : \sigma \mapsto P_\sigma \\ (\mathrm{S}_n, \circ, \mathrm{id}) &\hookrightarrow (\mathrm{GL}_n K, \cdot, 1_{n \times n}) \end{aligned}$$

Ist $v : K^{n \times n} \to K$ multilinear, alternierend und normiert, so haben wir:

$$\begin{array}{ccc} (\mathrm{E}_n, \circ, \mathrm{id}) & \xrightarrow{\sigma \mapsto P_\sigma} & (K^{n \times n}, \cdot, 1_{n \times n}) \\ \Big\downarrow{\scriptstyle \mathrm{sign}} & & \Big\downarrow{\scriptstyle v \mid \det} \\ (\{\pm 1, 0\}, \cdot, 1) & \xrightarrow{s \mapsto s \cdot 1_K} & (K, \cdot, 1) \end{array}$$

Wir interpretieren hier und im Folgenden die Signatur $\operatorname{sign}(\sigma) \in \{\pm 1, 0\}$ als Element des Rings K, genauer könnten wir schreiben $\operatorname{sign}(\sigma) \cdot 1_K$.

Die Kommutativität des Grundrings K ist notwendig.

Der Unterschied zwischen alternierend und antisymmetrisch ist recht subtil und spielt vor allem in Charakteristik 2 eine ernsthafte Rolle. Wir wollen alle Fälle einheitlich behandeln und wählen daher bewusst den stärkeren Begriff: alternierend. Damit passt alles zusammen.

Die Kommutativität von K fordern wir nicht nur aus Bequemlichkeit:

Bemerkung L2F: Die Kommutativität von K ist notwendig.

Eine multilineare normierte Abbildung $v : K^{n \times n} \to K$ kann es für $n \geq 2$ nur über einem *kommutativen* Ring K geben. Für $a, b \in K$ gilt nämlich

$$v \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = a \cdot v \begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix} = a \cdot b \cdot v \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = a \cdot b,$$

$$v \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = b \cdot v \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = b \cdot a \cdot v \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = b \cdot a.$$

🙂 Der folgende Satz besagt, dass die Kommutativität von K bereits ausreicht, um die Existenz und die Eindeutigkeit einer multilinearen, alternierenden, normierten Abbildung $K^{n \times n} \to K$ sicherzustellen.

Der Hauptsatz zu Determinanten

L217

Satz L2G: Existenz, Eindeutigkeit, Eigenschaften

Sei K ein kommutativer Ring. In jeder Dimension $n \in \mathbb{N}$ existiert genau eine multilineare, alternierende, normierte Abbildung $v : K^{n\times n} \to K$.

Diese Abbildung nennen wir die **Determinante** und schreiben hierfür

$$\det = \det_K^n \,:\, K^{n\times n} \to K.$$

1. Es gilt $\det A = \sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n}$. (Leibniz)
2. Die Determinante ist transpositionsinvariant: $\det(A^\mathsf{T}) = \det(A)$.
3. Die Determinante ist multiplikativ: $\det(A \cdot B) = \det(A) \cdot \det(B)$.
4. Genau dann ist $A \in K^{n\times n}$ invertierbar, wenn $\det(A) \in K$ dies ist.
5. Es gilt $AA' = A'A = \det(A)E$, also $A^{-1} = \det(A)^{-1}A'$. (Cramer)

Zu $A = (a_1, \ldots, a_n)$ definieren wir die **adjunkte Matrix** $A' = \operatorname{adj}(A)$ durch die Cofaktoren $a'_{ij} := \det(a_1, \ldots, a_{i-1}, e_j, a_{i+1}, \ldots, a_n)$.

🙂 Explizite polynomielle Formeln. 🙂 Sofort praktisch für kleine n.

Definition und Eigenschaften der Determinante

L218
Erläuterung

Ich fasse hier die wichtigsten Aussagen zu Determinanten übersichtlich zusammen und nenne dies daher den **Hauptsatz zu Determinanten**. Er dient als Zusammenfassung und Vorschau; alles Wesentliche steckt bereits kurz & knapp drin, wir packen es anschließend sorgfältig aus.

Ich möchte dies an den Anfang stellen, um Ihnen einen ersten Überblick zu geben. So können Sie schon sehen, oder besser erahnen, wozu die Determinante so alles gut ist. Die Details, Beweise und Beispiele folgen. Es gibt noch mehr Schönes zu berichten, hier das Wichtigste in Kürze.

Ich betone hier, dass die Determinante durch ein Polynom gegeben ist, zwar ein großes Polynom, doch recht simpel und übersichtlich gebaut. Insbesondere zur Inversion $A \mapsto A^{-1}$ bietet $A^{-1} = \det(A)^{-1} \operatorname{adj}(A)$ eine geschlossene Formel, als rationale Funktion: stetig, differenzierbar.

Für kleine n ist dies sofort praktisch einsetzbar, für große n jedoch ist die naive Anwendung der Leibniz–Formel rasch zu aufwändig ($n!$). Dazu entwickeln wir ergänzend noch weit effizientere Verfahren, allen voran geht hier natürlich der Gauß–Algorithmus (n^3).

Beispiel $n = 2$: Inversion von 2×2–Matrizen

L219

Notation: Man schreibt oft kurz $|A| := \det(A)$. Vorsicht! Hier droht die Gefahr einer Verwechslung mit Beträgen, Längen und Normen.

Für $n = 0$ haben wir $K^{0\times 0} = \{()\}$ und $\det_K^0 : K^{0\times 0} \to K : () \mapsto 1$.

Für $n = 1$ ist $\det_K^1 : K^{1\times 1} \xrightarrow{\sim} K : (a) \mapsto a$ ein Isomorphismus.

Der erste interessante Fall entsteht in Dimension $n = 2$:

Beispiel L2H: Determinante und Inversion von 2×2–Matrizen

Für 2×2–Matrizen ist die Determinante gegeben durch

$$\det = \det_K^2 \,:\, K^{2\times 2} \to K \,:\, \begin{bmatrix} a & c \\ b & d \end{bmatrix} \mapsto \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc.$$

Genau dann ist A in $K^{2\times 2}$ invertierbar, wenn $\det A$ in K invertierbar ist. Für die Inversion haben wir eine einfache, rationale Adjunktenformel:

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$$

Beispiel $n = 2$: Inversion von 2×2–Matrizen

L220
Erläuterung

Übung: (1) Lesen Sie den Hauptsatz L2G nochmal genaustens durch und folgern Sie daraus für $n = 2$ die obigen Formeln in Beispiel L2H.

(2) Die explizit gegebene Inversionsformel können Sie direkt prüfen: Multiplizieren Sie die Matrizen A und A^{-1}, dies muss $1_{2\times 2}$ ergeben!

Lösung: (1a) Die Leibniz–Formel summiert über $\mathrm{S}_2 = \{\mathrm{id}, (1, 2)\}$.
(1b) Für die Adjunkte finden wir z.B. $a'_{12} = \det(e_2, a_2) = \left|\begin{smallmatrix} 0 & c \\ 1 & d \end{smallmatrix}\right| = -c$.
Probieren Sie es selbst: So finden Sie alle Terme der Inversionsformel!

(2) Sie kennen diese schöne Formel bereits aus Kapitel B, Satz B1E. Dies gelingt auch ganz direkt, fast ohne Theorie: Stehen die expliziten Formeln einmal vor Ihnen, so genügt Nachrechnen (oder Anwenden).

Im jetzigen Kontext erweist sich der Fall $n = 2$ als der erste Schimmer einer allgemeinen Theorie der Determinanten. Alles fügt sich.

🙂 Determinante und Inversion von 2×2–Matrizen wird Ihnen häufig nützen, daher sollten Sie beides im Schlaf beherrschen.

Beispiel $n = 3$: Sarrus–Regel aka Jägerzaun

🙂 Im Fall $n = 2$ können Sie noch alles direkt per Hand nachrechnen.
Ab $n \geq 3$ sorgt die allgemeine Theorie für Ordnung und Übersicht.

Beispiel L2ı: Determinante und Inversion von 3×3–Matrizen

Jede 3×3–Matrix $A \in K^{3\times 3}$ ist die Determinante gegeben durch

$$\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{cases} +\, a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -\, a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} \end{cases}$$

Diese **Regel von Sarrus** lässt sich als **Jägerzaunregel** merken.

Genau dann ist A in $K^{3\times 3}$ invertierbar, wenn $\det A$ in K invertierbar ist.
Für die Inversion haben wir eine explizite, rationale Adjunktenformel:

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} a_{22}a_{33} - a_{23}a_{32} & a_{13}a_{32} - a_{12}a_{33} & a_{12}a_{23} - a_{13}a_{22} \\ a_{23}a_{31} - a_{21}a_{33} & a_{11}a_{33} - a_{13}a_{31} & a_{13}a_{21} - a_{11}a_{23} \\ a_{21}a_{32} - a_{22}a_{31} & a_{12}a_{31} - a_{11}a_{32} & a_{11}a_{22} - a_{12}a_{21} \end{bmatrix}$$

Ab $n \geq 4$ ist die Leibniz–Formel aufwändiger, mit $n!$ Summanden.

Beispiel $n = 3$: Sarrus–Regel aka Jägerzaun

Übung: Lesen Sie den Hauptsatz L2G nochmal genaustens durch und folgern Sie daraus für $n = 3$ die obigen Formeln in Beispiel L2ı. (Sie können gerne später mit mehr Erfahrung darauf zurückkommen, in jedem Falle sollten Sie viel rechnen, um Zutrauen zu gewinnen.)

Die explizit gegebene Inversionsformel können Sie direkt nachprüfen. Das ist allerdings wenig erquicklich. Schon hier scheint ist es mir viel effizienter und auch lehrreicher, den allgemeinen Fall zu verstehen. Allgemeine Theorie und konkrete Zahlenbeispiele ergänzen sich!

🙂 Die Jägerzaunregel ist in Rechnungen oft hilfreich, daher sollten Sie die ganz einfachen Formeln auswendig und fehlerfrei beherrschen.

Schon die Inversionsformel in Dimension $n = 3$ scheint mir zu vertrackt, um sie stur auswendig zu lernen. Mit System geht es viel besser!

Investieren Sie Ihre kostbare Zeit lieber in das genaue Verständnis des Hauptsatzes L2G: Aus diesem können Sie je nach Bedarf alle weiteren Formeln ableiten, wie hier gezeigt. Das ist ein allgemeines Prinzip.

Anwendungsbeispiel zur Invertierbarkeit

Aufgabe: Für welche Werte $\lambda \in \mathbb{R}$ ist die folgende Matrix invertierbar?

$$A(\lambda) = \begin{bmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{bmatrix} \in \mathbb{R}^{3\times 3}$$

Lösung: Wir berechnen die Determinante und finden:

$$\det A(\lambda) = \begin{vmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{vmatrix} = 60 - 12\lambda$$

Für alle $\lambda \in \mathbb{R} \smallsetminus \{5\}$ ist die Matrix $A(\lambda)$ in $\mathbb{R}^{3\times 3}$ invertierbar.

$$A(5) = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \notin \mathrm{GL}_3\,\mathbb{R}$$

Für $\lambda = 5$ erhalten wir die Telefonmatrix; diese hat nur Rang 2.

🙂 Dieses Phänomen gilt für jeden der neun Einträge der Telefonmatrix: Wenn wir beliebig wenig daran wackeln, so wird die Matrix invertierbar!

Anwendungsbeispiel zur Invertierbarkeit

Die drei Spalten der Telefonmatrix ($\lambda = 5$) sind linear abhängig, sie spannen im $\mathbb{R}^3$ nur einen Unterraum der Dimension 2 auf.

Für $\lambda \neq 5$ hingegen sind die drei Spalten linear unabhängig und bilden somit eine Basis des $\mathbb{R}^3$. Die Determinante hilft!

Übrigens geht dieses System um $\lambda = 5$ von einer rechtshändigen in eine linkshändige Basis über, dazwischen kann es keine Basis sein.

Übung: (1) Platzieren Sie die Variable λ an verschiedene Stellen der Telefonmatrix und untersuchen Sie die Determinante wie oben.

(2) Untersuchen Sie dieses Beispiel genauso über $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$.

☹ Im Gauß–Algorithmus müssen Sie Fallunterscheidungen treffen: null oder nicht? Das ist für eine einzelne Rechnung kein Problem, erschwert aber den Überblick für eine Familie $\lambda \mapsto A(\lambda)$ wie hier.

🙂 Die Determinante ist ein sympathisches Polynom und erfordert keine Fallunterscheidungen: Alles gelingt einheitlich, alle Fälle gleich.
Die einzige Entscheidung $\det A \stackrel{?}{=} 0$ entsteht erst ganz zum Schluss!

Konstruktion der Determinante

Weiterhin sei K ein kommutativer Ring und $n \in \mathbb{N}$ eine natürliche Zahl.

Definition L2J: Konstruktion der Determinante

Wir konstruieren $\det = \det_K^n : K^{n\times n} \to K$ durch die **Leibniz–Formel**

$$\begin{aligned}\det(A) &= \textstyle\sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot \prod_{j=1}^n a_{\sigma(j),j} \\ &= \textstyle\sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n}\end{aligned}$$

und nennen diese Abbildung die **Determinante** in Dimension n über K.

- ☺ Explizite polynomielle Formel. ☺ Direkt anwendbar für kleine n.
- ☺ Daraus folgern wir alle weiteren Eigenschaften und Rechenregeln.

Die Leibniz–Formel ist ein guter Startpunkt, aber noch nicht das Ende:

- ☹ Naive Anwendung der Leibniz–Formel ist für große n aufwändig ($n!$).
- ☺ Eine effiziente Berechnung gelingt mit dem Gauß–Algorithmus (n^3).

Invarianz unter Transposition

Satz L2K: Invarianz unter Transposition

Die Determinante ist invariant unter Transposition: $\det(A^\mathsf{T}) = \det(A)$.

Beweis: Für jede Permutation $\sigma \in \mathrm{S}_n$ gilt dank Sortierung der Faktoren

$$a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n} = a_{1,\sigma^{-1}(1)} \cdot a_{2,\sigma^{-1}(2)} \cdots a_{n,\sigma^{-1}(n)}.$$

Zudem gilt $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma^{-1})$. Durchläuft σ alle Elemente von S_n, so durchläuft auch das Inverse σ^{-1} alle Elemente von S_n. Wir erhalten:

$$\begin{aligned}\det(A^\mathsf{T}) &\overset{\text{Def}}{=} \textstyle\sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a^\mathsf{T}_{\sigma(1),1} \cdot a^\mathsf{T}_{\sigma(2),2} \cdots a^\mathsf{T}_{\sigma(n),n} \\ &\overset{\text{Def}}{=} \textstyle\sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} \\ &\overset{\text{Inv}}{=} \textstyle\sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma^{-1}) \cdot a_{1,\sigma^{-1}(1)} \cdot a_{2,\sigma^{-1}(2)} \cdots a_{n,\sigma^{-1}(n)} \\ &\overset{\text{Sort}}{=} \textstyle\sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n} \overset{\text{Def}}{=} \det(A)\end{aligned}$$

Somit ist die Determinante transpositionsinvariant. QED

Die Determinante tut, was eine Determinante tun muss.

Satz L2L: Die Determinante erfüllt die Axiome.

Die Determinante $\det = \det_K^n$ ist normiert, multilinear und alternierend.

Beweis: (1) Für die Einheitsmatrix $E = 1_{n\times n}$ und $\sigma \in \mathrm{S}_n$ gilt

$$\operatorname{sign}(\sigma) \cdot e_{\sigma(1),1} \cdot e_{\sigma(2),2} \cdots e_{\sigma(n),n} = \begin{cases} 1 & \text{für } \sigma = \mathrm{id}, \\ 0 & \text{für } \sigma \neq \mathrm{id}. \end{cases}$$

(2) Die Determinante $A \mapsto \det(A)$ ist linear in jeder Spalte:

$$\begin{aligned}&\det(a_1, \ldots, a'_i + \lambda a''_i, \ldots, a_n) \\ &= \textstyle\sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdots (a'_{\sigma(i),i} + \lambda a''_{\sigma(i),i}) \cdots a_{\sigma(n),n} \\ &= \ldots = \det(a_1, \ldots, a'_i, \ldots, a_n) + \lambda \det(a_1, \ldots, a''_i, \ldots, a_n)\end{aligned}$$

(3) Sei $A \in K^{n\times n}$ mit $a_i = a_j$ für ein Paar $i \neq j$. Zu $\tau = (i, j)$ haben wir $\mathrm{S}_n = \mathrm{A}_n \sqcup \tau \circ \mathrm{A}_n$. Für jede Permutation $\sigma \in \mathrm{A}_n$ und $\sigma' = \tau \circ \sigma$ gilt:

$$a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} = a_{1,\sigma'(1)} \cdot a_{2,\sigma'(2)} \cdots a_{n,\sigma'(n)}$$

In der Leibniz–Formel löschen sich so alle Terme paarweise aus. QED

Die Determinante tut, was eine Determinante tun muss.

Axiome sind grundlegende Annahmen, Forderungen, Wünsche, ...
Damit haben wir die wesentlichen Eigenschaften knapp und präzise zusammengefasst, die wir von der Determinante erwarten / erhoffen.

☺ Das Wünschen ist immer erlaubt, doch nicht alles ist erfüllbar.
Der vorige Satz L2L garantiert, dass unsere Wünsche tatsächlich erfüllt werden können; der folgende Satz L2M sichert zudem die Eindeutigkeit.

☺ Ich habe die drei Axiome (multilinear, alternierend, normiert) hier zunächst für die Spalten formuliert. Das ist etwas willkürlich: Für Spalten scheint mir die Notation $(a_1, \ldots, a_n)$ etwas bequemer.

☺ Alles gilt genauso für Zeilen, dank Invarianz unter Transposition.
Die Determinante ist also multilinear, alternierend, normiert in den Spalten (nach Definition) und ebenso in den Zeilen (dank Satz).

Andere Autoren gehen umgekehrt vor, das Ergebnis ist dasselbe...
Zum Glück! Es gibt eben nur eine Determinante, für alle dieselbe.
Dies bringt uns schließlich zum folgenden Eindeutigkeitssatz.

Der Eindeutigkeitssatz

Satz L2M: Eindeutigkeitssatz für die Determinante

Ist $v : K^{n\times n} \to K$ multilinear und alternierend, so gilt

$$\boxed{v(A) = v(E) \cdot \det(A)}$$

für alle Matrizen $A \in K^{n\times n}$. Ist v zudem normiert, so folgt $v = \det$.

Beweis: Jeder Spaltenvektor $a_j \in K^n$ ist eine Linearkombination $a_j = \sum_{i=1}^n e_i a_{ij}$ der Standardbasis $e_1, \dots, e_n \in K^n$. Daraus folgt:

$$\begin{aligned} v(a_1, \dots, a_n) &= v\big(\textstyle\sum_{i_1=1}^n e_{i_1} a_{i_1,1},\ \dots,\ \sum_{i_n=1}^n e_{i_n} a_{i_n,n}\big) \\ &\overset{(1)}{=} \textstyle\sum_{i_1=1}^n \cdots \sum_{i_n=1}^n a_{i_1,1} \cdots a_{i_n,n}\, v(e_{i_1}, \dots, e_{i_n}) \\ &= \textstyle\sum_{\sigma\in \mathrm{E}_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n}\, v(P_\sigma) \quad \text{mit } \sigma : k \mapsto i_k \\ &\overset{(2)}{=} \textstyle\sum_{\sigma\in \mathrm{S}_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n}\, \operatorname{sign}(\sigma)\, v(E) \end{aligned}$$

Wir nutzen hier: v ist (1) multilinear und (2) alternierend (L2E). QED

Der Multiplikationssatz

Satz L2N: Die Determinante ist multiplikativ.

Für alle quadratischen Matrizen $A, B \in K^{n\times n}$ gilt:

$$\boxed{\det(A \cdot B) = \det(A) \cdot \det(B)}$$

Wir erhalten so den Monoidhomomorphismus

$$\det\ :\ (K^{n\times n}, \cdot, 1_{n\times n}) \to (K, \cdot, 1).$$

Beweis: Wir halten $A \in K^{n\times n}$ fest und betrachten die Abbildung

$$v\ :\ K^{n\times n} \to K\ :\ B \mapsto \det(A \cdot B) = \det(Ab_1, \dots, Ab_n).$$

Diese ist multilinear und alternierend in den Spalten $b_1, \dots, b_n$ von B.
Dank des Eindeutigkeitssatzes L2M gilt $v(B) = v(E) \cdot \det(B)$, also

$$\det(A \cdot B) \overset{\text{Def}}{=} v(B) \overset{\text{L2M}}{=} v(E) \cdot \det(B) \overset{\text{Def}}{=} \det(A) \cdot \det(B).$$

Somit ist die Determinante multiplikativ für alle $A, B \in K^{n\times n}$. QED

Vom Eindeutigkeitssatz zum Multiplikationssatz

☺ Dieses Vorgehen ist einfach genial, raffiniert und effizient! Aus dem Eindeutigkeitssatz L2M folgt mit einem Schlag die Multiplikativität L2N.

An dieser Stelle bin ich jedesmal aufs Neue erstaunt und begeistert. Wieder einmal gilt: Kaum macht man es richtig, schon funktioniert's!

In manchen Büchern zur Linearen Algebra wird die Multiplikativität auf anderen Wegen bewiesen, zum Beispiel mit dem Gauß–Algorithmus. Das ist möglich, doch unser obiges Argument ist unschlagbar elegant.

Ich versuche daher bewusst, obskur-stumpfsinnige Rechnungen durch klar-scharfsinnige Argumente zu ersetzen, soweit dies hier möglich ist. Ab und an müssen wir tapfer durchrechnen, da führt kein Weg vorbei.

☺ Unsere sorgsamen Rechnungen haben sich wieder einmal gelohnt. Zugegeben, auch wir mussten uns einigen Index-Schlachten stellen, doch wir haben obsiegt und tragen nun reiche Beute davon. Darauf können wir im Folgenden weiter aufbauen.

Die Determinante ist nicht additiv!

Bemerkung L2O: Warnung, die Determinante ist nicht additiv!

(0) In Dimension $n \geq 2$ ist die Determinante

$$\det = \det_K^n\ :\ (K^{n\times n}, \cdot, 1_{n\times n}) \to (K, \cdot, 1)$$

ein Monoidhomomorphismus, aber **kein Ringhomomorphismus**!
(1) Die Determinante ist multiplikativ, aber **nicht additiv**:
Ein besonders einfaches Gegenbeispiel ist

$$\det \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0 \quad \text{und} \quad \det \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = 0 \quad \text{aber} \quad \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1.$$

(2) Die Determinante $\det_K^n$ ist insgesamt **K–homogen vom Grad n**:
Für jede Matrix $A \in K^{n\times n}$ und jeden Skalar $\lambda \in K$ gilt

$$\det(\lambda A) = \lambda^n \det(A).$$

Insbesondere gilt $\det(-A) = (-1)^n \det(A)$.

Die Cramersche Regel und das Determinantenverfahren

Satz L2P: Cramersche Regel / Determinantenverfahren

Gegeben seien die Matrix $A \in K^{n\times n}$ und zwei Vektoren $x, b \in K^n$.
(1) Gilt $Ax = b$, also $b = \sum_{i=1}^n a_i x_i$, so folgt für alle $j \in \{1, \dots, n\}$:

$$\det(\dots, a_{j-1}, b, a_{j+1}, \dots) = \det(A) \cdot x_j$$

(2) Ist $\det(A)$ in K invertierbar, so lösen wir $Ax = b$ eindeutig durch

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \frac{1}{\det A} \begin{bmatrix} \det(b, a_2, \dots, a_n) \\ \det(a_1, b, \dots, a_n) \\ \vdots \\ \det(a_1, a_2, \dots, b) \end{bmatrix}.$$

Beweis: (1) Die Determinante ist multilinear und alternierend (L2L):

$$\det(\dots, a_{j-1}, b, a_{j+1}, \dots) = \sum_{i=1}^n \det(\dots, a_{j-1}, a_i, a_{j+1}, \dots) \cdot x_i$$

Alle Terme mit $i \neq j$ verschwinden, es bleibt nur $\det(A) \cdot x_j$. QED

Die Cramersche Regel und das Determinantenverfahren

🙂 Die Determinante filter den gewünschten Koeffizienten x_j heraus! Die **Cramersche Regel** bietet eine geschlossene Formel zur Lösung linearer Gleichungssysteme – unter der Voraussetzung $\det A \in K^\times$. Diese Lösungsmethode heißt daher auch **Determinantenverfahren**.

🙂 In kleiner Dimension n kann dieses Verfahren direkt eingesetzt werden und liefert die eindeutige Lösung x mit vertretbarem Aufwand.

☹ Zur Berechnung müssen $n + 1$ Determinanten bestimmt werden; in Spezialfällen ist das leicht, aber allgemein für große n zu aufwändig. Daher sind andere Lösungsmethoden meist vorzuziehen, etwa das Gauß–Verfahren oder algorithmische Verfeinerungen der Numerik.

🙂 Dennoch ist die Cramersche Regel aus theoretischer Sicht hilfreich: Sie garantiert (im klassischen Fall $K = \mathbb{R}, \mathbb{C}$), dass die gesuchte Lösung x stetig von den Eingabedaten A und b abhängt (sogar differenzierbar). Wenn wir A und b nur wenig ändern, so bewegt auch x sich nur wenig.

🙂 Genauer haben wir für x eine explizite rationale Funktion in den Koeffizienten von A und b, also einen Quotienten von Polynomen.

Anwendungsbeispiel zum Determinantenverfahren

Ausprobieren mit Gaël!

Aufgabe: Wir betrachten zu jedem Parameter $\lambda \in \mathbb{R}$ die reelle Matrix

$$A(\lambda) = \begin{bmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{bmatrix} \in \mathbb{R}^{3\times 3}.$$

Bestimmen Sie alle Lösungen $x \in \mathbb{R}^3$ der Gleichung $A(\lambda)\, x = e_1$.

Lösung: Wir wissen bereits $\det A(\lambda) = 60 - 12\lambda$, siehe L223.
Für $\lambda \neq 5$ können wir das Determinantenverfahren L2P nutzen.

$$\begin{vmatrix} \mathbf{1} & 2 & 3 \\ \mathbf{0} & \lambda & 6 \\ \mathbf{0} & 8 & 9 \end{vmatrix} \overset{\text{L2I}}{=} 9\lambda - 48, \quad \begin{vmatrix} 1 & \mathbf{1} & 3 \\ 4 & \mathbf{0} & 6 \\ 7 & \mathbf{0} & 9 \end{vmatrix} \overset{\text{L2I}}{=} 6, \quad \begin{vmatrix} 1 & 2 & \mathbf{1} \\ 4 & \lambda & \mathbf{0} \\ 7 & 8 & \mathbf{0} \end{vmatrix} \overset{\text{L2I}}{=} 32 - 7\lambda.$$

Zu jedem Parameter $\lambda \in \mathbb{R} \smallsetminus \{5\}$ finden wir so die einzige Lösung:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \overset{\text{L2P}}{=} \frac{1}{\det A} \begin{bmatrix} \det(b, a_2, a_3) \\ \det(a_1, b, a_3) \\ \det(a_1, a_2, b) \end{bmatrix} \overset{\text{L2I}}{=} \frac{1}{60 - 12\lambda} \begin{bmatrix} 9\lambda - 48 \\ 6 \\ 32 - 7\lambda \end{bmatrix}$$

Für $\lambda = 5$ nutzen wir Gauß B2C… Die Lösungsmenge ist hier leer.

Anwendungsbeispiel zum Determinantenverfahren

Ausprobieren mit Gaël!

Sie können nun konkrete Werte einsetzen, etwa $\lambda = \dots, 3, 4, 6, 7, \dots$, oder allgemein die geforderte Gleichung $A(\lambda)\, x = e_1$ nachprüfen.

🙂 Die Lösung ist eine **rationale Funktion** der Eingabedaten.
Sie sehen an diesem Zahlenbeispiel klar die Vor- und Nachteile, die ich oben bereits zum Determinantenverfahren erläutert habe.

⚠ Im Sonderfall $\lambda = 5$ gilt $\det A(5) = 0$, die Matrix ist also **singulär**: Das Determinantenverfahren bricht hier zusammen! Wir müssen daher separat rechnen: Das Gauß–Verfahren B2C nützt immer, so auch hier.

$$\left[\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 4 & 5 & 6 & 0 \\ 7 & 8 & 9 & 0 \end{array}\right] \xrightarrow[\text{B2C}]{\text{Gauß}} \left[\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 4/3 \\ 0 & 0 & 0 & 1 \end{array}\right]$$

🙂 Da $\det A(5) \in \mathbb{R}$ nicht invertierbar ist, ist auch $A(5) \in \mathbb{R}^{3\times 3}$ nicht invertierbar (L2G), demnach gilt $\ker A(5) \neq \{0\}$ (B2D). Die Gleichung $Ax = b$ hat also entweder gar keine Lösung oder aber unendlich viele. Das Gauß–Verfahren zeigt hier: e_1 liegt nicht im Bild von $A(5)$.

Determinante und Kern einer Matrix

Satz L2Q: Determinante und Kern einer Matrix

Sei K ein Integritätsring, etwa $\mathbb{Z}$ oder ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Für jede quadratische Matrix $A \in K^{n\times n}$ gilt dann:

$$\begin{array}{rcl} \det(A) = 0 & \iff & \ker(A) \neq \{0\} \\ \det(A) \neq 0 & \iff & \ker(A) = \{0\} \end{array}$$

In Worten: Genau dann gilt $\det A = 0$, wenn die Spalten der Matrix A linear abhängig sind. Dasselbe gilt für die Zeilen der Matrix A (L2K).

Beweis: (1) Für $x \in K^n$ mit $Ax = 0$ gilt dank Cramerscher Regel L2P $\det(A) \cdot x_j = \det(\dots, a_{j-1}, 0, a_{j+1}, \dots) = 0$. Aus $x \neq 0$ folgt $\det(A) = 0$.

(2) Sei $\ker A = \{0\}$. (a) Ist K ein Körper, dann ist A invertierbar (B2D): Es existiert $B \in K^{n\times n}$ mit $AB = BA = 1_{n\times n}$, somit $\det(A)\det(B) = 1$.

(b) Wir nutzen den Bruchkörper $Q \geq K$ (E3L), im Beispiel $\mathbb{Z}$ also $\mathbb{Q} \geq \mathbb{Z}$. Dank (a) gilt $\det^n_Q(A) \neq 0$, dank Leibniz $\det^n_K(A) = \det^n_Q(A)$. QED

Determinante und Kern einer Matrix

🙂 Der letzte Schritt des Beweises von Körper zu Integritätsringen ist etwas trickreich. Im konkreten Beispiel $\mathbb{Z} \leq \mathbb{Q}$ ist das Argument leicht:

Wir setzen $\ker_{\mathbb{Z}}(A) = \{0\}$ voraus und wollen $\det_{\mathbb{Z}}(A) \neq 0$ zeigen.

Aus $\ker_{\mathbb{Z}}(A) = \{0\}$ folgern wir zunächst $\ker_{\mathbb{Q}}(A) = \{0\}$. Beweis per Kontraposition: Für $0 \neq x \in \mathbb{Q}^n$ mit $Ax = 0$ multiplizieren wir mit einem gemeinsamen Nenner $m \in \mathbb{N}_{\geq 1}$ der Koordinaten $x_1, \dots, x_n \in \mathbb{Q}$ und erhalten $0 \neq mx \in \mathbb{Z}^n$ mit $A(mx) = m(Ax) = 0$, also $mx \in \ker_{\mathbb{Z}}(A)$.

Dank $\ker_{\mathbb{Q}}(A) = \{0\}$ können wir (a) anwenden und schließen, dass A über $\mathbb{Q}$ invertierbar ist (dank Gauß B2D): Es existiert $B \in \mathbb{Q}^{n\times n}$ mit $AB = BA = 1_{n\times n}$, somit $\det^n_{\mathbb{Q}}(A)\det^n_{\mathbb{Q}}(B) = 1$, also $\det^n_Q(A) \neq 0$. Dank Leibniz–Formel L2G folgt schließlich $\det^n_{\mathbb{Z}}(A) = \det^n_{\mathbb{Q}}(A) \neq 0$.

⚠ Wir benötigen für Satz L2Q wirklich einen Integritätsring.

Gegenbeispiel: Die Matrix $A = \left[\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right] \in \mathbb{Z}_6^{2\times 2}$ hat nicht-verschwindende Determinante $\det A = 2$, doch nicht-trivialen Kern $\ker A = \{\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 3 \\ 0 \end{smallmatrix}\right]\}$.

Der Beweis zeigt allgemein: Ist $\ker A \neq \{0\}$, so ist $\det A$ ein Nullteiler. In einem Integritätsring, insbesondere Körper, bedeutet das $\det A = 0$.

Determinantenkriterium für lineare Unabhängigkeit

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \in \mathbb{Z}^{3\times 3}.$$

Beispiel: Die drei Spalten der Telefonmatrix $A \in \mathbb{Z}^{3\times 3}$ sind linear abhängig über $\mathbb{Z}$, denn $\det A = 0$. Die ersten beiden Spalten sind jedoch linear unabhängig, denn $\left|\begin{smallmatrix} 4 & 5 \\ 7 & 8 \end{smallmatrix}\right| = -3$, $\left|\begin{smallmatrix} 1 & 2 \\ 4 & 5 \end{smallmatrix}\right| = -3$, $\left|\begin{smallmatrix} 1 & 2 \\ 7 & 8 \end{smallmatrix}\right| = -6$.

Satz L2R: Determinantenkriterium für lineare Unabhängigkeit

Sei K ein Integritätsring, etwa $\mathbb{Z}$ oder ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Genau dann sind die Spalten von $A \in K^{n\times r}$ linear unabhängig, wenn es eine Untermatrix M der Größe $r \times r$ gibt mit $\det M \neq 0$.

Beweis: Analog zu Satz L2Q. Versuchen Sie es als Übung!

🙂 Im klassischen Fall $K = \mathbb{R}, \mathbb{C}$ ist die Determinante zudem stetig: Wenn wir $a_1, \dots, a_r \in K^n$ nur wenig ändern, so bleiben sie unabhängig!

Determinantenkriterium für lineare Unabhängigkeit

Zunächst sollten wir den Begriff „Untermatrix“ präzise ausformulieren: Sei $A : I \times J \to K$ eine Matrix mit $I = \{1, \dots, n\}$ und $J = \{1, \dots, r\}$. Eine **Untermatrix** $M = A|_{I'\times J'}$ der Größe $r \times r$ ist die Einschränkung auf r Zeilen $I' = \{i_1 < \dots < i_r\}$ und r Spalten $J' = \{j_1 < \dots < j_r\}$.

Lösung: „⇐“: Sei $M = A|_{I'\times J}$ eine $r \times r$–Untermatrix mit $\det M \neq 0$. Wir projizieren die Vektoren $a_1, \dots, a_r \in K^I$ vermöge $p : K^I \to K^{I'}$ durch Einschränkung $a \mapsto a|_{I'}$ der Koordinaten von I auf I'. Sie sind linear unabhängig im Bild $K^{I'}$ (L2Q), also auch in K^I (J1I).

„⇒“: (a) Wie im vorigen Beweis von L2Q sei K zunächst ein Körper. Der Gauß–Algorithmus B2C überführt A in Spaltenstufenform A' vom Rang r (K2J). Die Untermatrix M der r Pivotzeilen erfüllt $\det M \neq 0$. (Alternativ kann man A^T in Zeilenstufenform überführen dank L2K.)

(b) Wir nutzen den Bruchkörper $Q \geq K$ (E3L), im Beispiel $\mathbb{Z}$ also $\mathbb{Q} \geq \mathbb{Z}$. Dank (a) gilt $\det^r_Q(M) \neq 0$, dank Leibniz $\det^r_K(M) = \det^r_Q(M)$. QED

Wir wenden die Cramersche Regel auf $AX = 1_{n\times n}$ an und erhalten:

Satz L2S: Adjunkte und Inversionsformel

Zu jeder Matrix $A = (a_1, \ldots, a_n) \in K^{n\times n}$ definieren wir ihre **adjunkte Matrix** $A' = \operatorname{adj}(A) \in K^{n\times n}$ oder **komplementäre Matrix** durch

$$a'_{ij} := \det(a_1, \ldots, a_{i-1}, e_j, a_{i+1}, \ldots, a_n).$$

(1) Die Matrix A und ihre Adjunkte A' erfüllen

$$\boxed{A' \cdot A = A \cdot A' = \det(A) \cdot 1_{n\times n}.}$$

(2) Ist $\det(A)$ in K invertierbar, so auch A in $K^{n\times n}$ dank

$$\boxed{A^{-1} = \det(A)^{-1} \operatorname{adj}(A).}$$

☺ Zur Inversion $A \mapsto A^{-1}$ bietet somit $A^{-1} = \det(A)^{-1} \operatorname{adj}(A)$ eine geschlossene Formel, als rationale Funktion: stetig, differenzierbar.

Beweis: (1a) Wir berechnen $D = A' \cdot A$ koeffizientenweise:

$$\begin{aligned} d_{ik} &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^n a'_{ij} a_{jk} \\ &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^n \det(a_1, \ldots, a_{i-1}, e_j, a_{i+1}, \ldots, a_n) a_{jk} \\ &\overset{\text{Lin}}{=} \det(a_1, \ldots, a_{i-1}, \textstyle\sum_{j=1}^n e_j a_{jk}, a_{i+1}, \ldots, a_n) \\ &\overset{\text{Def}}{=} \det(a_1, \ldots, a_{i-1}, a_k, a_{i+1}, \ldots, a_n) \overset{\text{Alt}}{=} \begin{cases} \det(A) & \text{falls } k = i, \\ 0 & \text{falls } k \neq i. \end{cases} \end{aligned}$$

Demnach gilt $A' \cdot A = \det(A) 1_{n\times n}$, wie behauptet.

(1b) Ebenso finden wir $A \cdot A' = \det(A) \cdot 1_{n\times n}$. (Übung!)

Am geschicktesten gelingt dies so: Für die Transponierte $B = A^\intercal$ finden wir $\operatorname{adj}(B) = \operatorname{adj}(A)^\intercal$, siehe L275 und L276. Daraus folgt:

$$A \cdot A' = B^\intercal \cdot B'^\intercal = (B' \cdot B)^\intercal = (\det(B) \cdot 1_{n\times n})^\intercal = \det(A) \cdot 1_{n\times n}$$

(2) Im Falle $\det(A) \in K^\times$ erhalten wir $A^{-1} = \det(A)^{-1} \cdot A'$. QED

Korollar L2T: Determinante und Inversion

Sei K ein kommutativer Ring.

(1) Genau dann ist $A \in K^{n\times n}$ invertierbar, wenn $\det(A) \in K$ dies ist.

$$\mathrm{GL}_n(K) = \{\, A \in K^{n\times n} \mid \det(A) \in K^\times \,\}$$

Für jede invertierbare Matrix $A \in \mathrm{GL}_n(K)$ gilt $\det(A^{-1}) = \det(A)^{-1}$.

(2) Die Matrixinversion ist eine explizit gegebene, rationale Funktion:

$$\iota : \mathrm{GL}_n(K) \to \mathrm{GL}_n(K) : A \mapsto A^{-1} = \det(A)^{-1}\,\mathrm{adj}(A)$$

Alle Operationen der Gruppe $(\mathrm{GL}_n K, \cdot, 1_{n\times n}, \iota)$ sind rational über K, also jeweils ein Bruch von Polynomen in den Matrixkoeffizienten.

Beweis: (1) „⇒/⊆“: Sei $A \in K^{n\times n}$ invertierbar, das heißt, es existiert $B \in K^{n\times n}$ mit $A \cdot B = B \cdot A = 1_{n\times n}$. Dank Multiplikativität L2N folgt $\det(A)\cdot\det(B) = \det(A\cdot B) = \det(1_{n\times n}) = 1$, also $\det(A) \in K^\times$.

„⇐/⊇“ und (2): Die Inversionsformel verdanken wir Satz L2S. QED

Beispiel: In Dimension $n = 2$ haben wir (L2H):

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$$

Beispiel: In Dimension $n = 3$ haben wir (L2I):

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \Rightarrow \det A = \begin{cases} +\,a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -\,a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} \end{cases}$$

$$A^{-1} = \frac{1}{\det A}\begin{bmatrix} a_{22}a_{33}-a_{23}a_{32} & a_{13}a_{32}-a_{12}a_{33} & a_{12}a_{23}-a_{13}a_{22} \\ a_{23}a_{31}-a_{21}a_{33} & a_{11}a_{33}-a_{13}a_{31} & a_{13}a_{21}-a_{11}a_{23} \\ a_{21}a_{32}-a_{22}a_{31} & a_{12}a_{31}-a_{11}a_{32} & a_{11}a_{22}-a_{12}a_{21} \end{bmatrix}$$

☺ Im klassischen Fall $K = \mathbb{R}, \mathbb{C}$ können wir die Stetigkeit nutzen: Wenn wir $A \in \mathrm{GL}_n(K)$ nur wenig ändern, so bleibt $A + \varepsilon S$ invertierbar!

☺ Die Inversion $A \mapsto A^{-1}$ ist rational, und somit nicht nur stetig ($\mathscr{C}^0$), sondern differenzierbar ($\mathscr{C}^1$), sogar glatt ($\mathscr{C}^\infty$), gar analytisch ($\mathscr{C}^\omega$), ...

Bemerkung L2U

Sei K ein Körper. In $K^{n\times n}$ ist $\mathrm{GL}_n(K) = \{\, A \in K^{n\times n} \mid \det(A) \neq 0 \,\}$ die Nicht-Nullstellen-Menge eines Polynoms in den Koeffizienten.

Über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ folgt daraus (dank Analysis / Topologie): Die Teilmenge $\mathrm{GL}_n \mathbb{K} \subset \mathbb{K}^{n\times n}$ ist offen und dicht, und ihr Komplement hat Maß 0:

1. Fast alle Matrizen sind invertierbar (volles Lebesgue–Maß),
2. nicht-invertierbare werden invertierbar durch kleine Störung,
3. invertierbare Matrizen bleiben invertierbar bei kleiner Störung.

Anschaulich bedeutet (1): Wenn Sie zufällig (stetig verteilt) eine Matrix $A \in \mathbb{R}^{n\times n}$ wählen, dann ist diese invertierbar mit Wkt 100%. Das ist klar in Dimension $n = 1$; in Dimension $n \geq 2$ folgt es aus der Determinante.

Ich nenne dies hier als schönen Ausblick. Die nötigen Begriffe und Techniken hierzu lernen Sie in der Analysis und in der Topologie.

Wir ahnen dies bereits im endlichen Fall über $\mathbb{F}_q$ für $q \to \infty$ (Satz J2H), denn der Anteil der invertierbaren Matrizen konvergiert gegen 100%:

$$\frac{\sharp\,\mathrm{GL}_n\,\mathbb{F}_q}{\sharp\,\mathbb{F}_q^{n\times n}} = \frac{q^n-1}{q^n}\cdot\frac{q^n-q}{q^n}\cdots\frac{q^n-q^{n-1}}{q^n}$$
$$= (1-q^{-1})(1-q^{-2})\ldots(1-q^{-n}) \;\to\; 1$$

Über einem großen endlichen Körper $\mathbb{F}_q$ ist eine zufällige Matrix also „nahezu sicher“ invertierbar. Über dem unendlichen Körper $\mathbb{K} = \mathbb{R}, \mathbb{C}$ ist dies tatsächlich der Fall, im Sinne des Lebesgue–Maßes.

☺ Die nicht-invertierbaren Matrizen in $\mathbb{K}^{n\times n}$ sind topologisch und maßtheoretisch gesehen also vernachlässigbar. Ihre algebraische Untersuchung ist selbstverständlich trotzdem wichtig, um alle Fälle zu behandeln. Nicht alle Matrizen sind zufällig, ganz im Gegenteil!

Determinante von Dreiecksmatrizen

Aufgabe: Berechnen Sie die Determinante jeder oberen Dreiecksmatrix

$$A = \begin{bmatrix} \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{bmatrix}$$

(1) mit Spaltenoperationen L2C sowie (2) mit der Leibniz–Formel L2J.

Lösung: (1) Die Determinante ist multilinear, alternierend und normiert (L2L), somit insbesondere invariant unter Transvektionen (L2C). Also:

$$\begin{vmatrix} \lambda_1 & * & * \\ 0 & * & * \\ 0 & 0 & \lambda_n \end{vmatrix} \overset{\text{L2L}}{=}_{\text{L2C}} \lambda_1 \begin{vmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & 0 & \lambda_n \end{vmatrix} \overset{\text{L2L}}{=}_{\text{L2C}} \cdots \overset{\text{L2L}}{=}_{\text{L2C}} \lambda_1 \cdots \lambda_n \begin{vmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{vmatrix} \overset{\text{L2L}}{=} \lambda_1 \cdots \lambda_n$$

(2) Nur die Identität $\sigma = \mathrm{id}$ liefert einen Beitrag in der Summe

$$\det(A) = \sum\nolimits_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n}.$$

Auch hier finden wir also $\det(A) = \lambda_1 \cdots \lambda_n$.

Determinante von Dreiecksmatrizen

In der Rechnung (1) nutzen wir die drei definierenden Eigenschaften. Sie sehen hier noch einmal sehr schön, wie diese zusammenwirken:

(a) Aus der $i$ten Spalte können wir den Faktor λ_i herausziehen.

(b) Durch Transvektionen können wir dann die $i$te Zeile aufräumen.

Die Schritte (a) und (b) wiederholen wir für alle $i = 1, 2, \ldots, n$.

(c) Die Determinante der Einheitsmatrix ist $\det(1_{n\times n}) = 1$.

🙂 Wir setzen die Skalare $\lambda_1, \ldots, \lambda_n \in K$ nicht als invertierbar voraus. Bitte beachten Sie die sorgsam gewählte Reihenfolge der Operationen in den Schritten (a) und (b), die ganz ohne Divisionen auskommen.

Für solche Rechnungen nutzen wir allgemein die Bemerkung L2W zur Determinante unter Spalten- und Zeilenoperationen.

🙂 Die einfache, elegante Rechnung in (2) gelingt sofort. Hier bietet die Leibniz–Formel gewisse Vorteile.

Determinante von Dreiecksmatrizen

Satz L2V: Determinante einer Dreiecksmatrix

(1) Sei $A \in K^{n\times n}$ eine (obere/untere) Dreiecksmatrix:

$$A = \begin{bmatrix} \lambda_1 & * & * & * \\ 0 & \lambda_2 & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & \lambda_n \end{bmatrix} \quad \text{oder} \quad \begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ * & \lambda_2 & 0 & 0 \\ * & * & \ddots & 0 \\ * & * & * & \lambda_n \end{bmatrix}$$

In diesem Fall gilt $\det(A) = \lambda_1 \lambda_2 \cdots \lambda_n$ dank Leibniz–Formel L2J.

(2) Entsprechendes gilt für jede (obere/untere) Block-Dreiecksmatrix:

$$A = \begin{bmatrix} A_{11} & * & * & * \\ 0 & A_{22} & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & A_{\ell\ell} \end{bmatrix} \quad \text{oder} \quad \begin{bmatrix} A_{11} & 0 & 0 & 0 \\ * & A_{22} & 0 & 0 \\ * & * & \ddots & 0 \\ * & * & * & A_{\ell\ell} \end{bmatrix}$$

In diesem Fall gilt $\det(A) = \det(A_{11}) \cdot \det(A_{22}) \cdots \det(A_{\ell\ell})$ dank L2J.

Beispiel: eine Block-Dreiecksmatrix

Aufgabe: Bestimmen Sie die Determinante der folgenden 9×9–Matrix:

$$A = \begin{bmatrix} 1 & 2 & * & * & * & * & * & * & * \\ 3 & 4 & * & * & * & * & * & * & * \\ 0 & 0 & 2 & * & * & * & * & * & * \\ 0 & 0 & 0 & 3 & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 4 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 5 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & \lambda & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 7 & 8 & 9 \end{bmatrix}$$

Lösung: Dies ist eine Block-Dreiecksmatrix (L2V). Daher erhalten wir:

$$\det(A) = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \cdot \begin{vmatrix} 2 & * & * & * \\ 0 & 3 & * & * \\ 0 & 0 & 4 & * \\ 0 & 0 & 0 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{vmatrix} = (-2) \cdot 120 \cdot (60 - 12\lambda)$$

$$= -2880 \cdot (5 - \lambda)$$

Determinante von Dreiecksmatrizen

Beweis des Satzes: (1) Wir betrachten eine obere Dreiecksmatrix A und berechnen die Determinante mit der Leibniz–Formel L2J:

$$\det(A) = \sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdot a_{\sigma(2),2} \cdots a_{\sigma(n),n}$$

Gilt $\sigma(i) > i$ für einen Index i, so ist dieser Summand gleich Null.
Die einzige Permutation $\sigma \in \mathrm{S}_n$ mit $\sigma(i) \leq i$ für alle i ist $\sigma = \mathrm{id}$.
Daraus folgt $\det(A) = \lambda_1\lambda_2 \cdots \lambda_n$, wie im Satz angegeben.

☺ Alternativ zur Leibniz–Formel können wir Spaltenoperationen oder Zeilenoperationen nutzen, wie in der vorigen Aufgabe L249 ausgeführt. Beide Sichtweisen sind lehrreich und führen zum ersehnten Ergebnis.

Determinante von Dreiecksmatrizen

(2) Die allgemeine Formel für Block-Dreiecksmatrizen beweisen wir ganz genauso, lediglich die Buchführung der Summe ist aufwändiger.

☺ Die Idee ist ganz anschaulich: Eine Permutationen $\sigma \in \mathrm{S}_n$ trägt nur dann etwas bei, wenn Sie auf den diagonalen Matrizen gefangen ist.

(a) Wir betrachten eine obere Block-Dreiecksmatrix, auf der Diagonalen stehen die Matrizen $A_{11}, \ldots, A_{\ell\ell}$ mit $A_{jj} \in K^{n_j \times n_j}$ der Größe $n_j \in \mathbb{N}_{\geq 1}$.
Wir zerlegen die Indexmenge $I = \{1, \ldots, n\}$ mit $n = n_1 + \cdots + n_\ell$ in $I = I_1 \sqcup \cdots \sqcup I_\ell$ mit $I_1 = \{1, \ldots, n_1\}$ und $I_j = \max I_{j-1} + \{1, \ldots, n_j\}$.
Gilt $\sigma(i) > I_j$ für einen Index $i \in I_j$, so ist dieser Summand gleich Null.
Es bleiben nur die Permutationen $\sigma \in \mathrm{S}_n$ mit $\sigma(I_j) = I_j$ für $j = 1, \ldots, \ell$.

(b) Wir nutzen die Untergruppe $U = \mathrm{Sym}(I_1) \times \cdots \times \mathrm{Sym}(I_\ell) \leq \mathrm{Sym}(I)$.
Für $\sigma \in U$ haben wir die Zerlegung $\sigma = \sigma_1 \sqcup \cdots \sqcup \sigma_\ell$ mit $\sigma_j \in \mathrm{Sym}(I_j)$.
Die Signatur ist multiplikativ gemäß $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma_1) \cdots \operatorname{sign}(\sigma_\ell)$;
dies sehen wir an den Fehlständen oder der Zykelzerlegung.

Determinante von Dreiecksmatrizen

(c) Mit diesen Vorbereitungen berechnen wir die Determinante:

$$\begin{aligned}
\det(A) &\overset{\text{Def}}{=} \textstyle\sum_{\sigma\in \mathrm{Sym}(I)} \operatorname{sign}(\sigma) \prod_{i\in I} a_{\sigma(i),i} \\
&\overset{\text{(a)}}{=} \textstyle\sum_{\sigma\in U} \operatorname{sign}(\sigma) \prod_{i\in I} a_{\sigma(i),i} \\
&\overset{\text{(b)}}{=} \textstyle\sum_{\sigma\in U} \prod_{j=1}^{\ell} \operatorname{sign}(\sigma_j) \prod_{i\in I_j} a_{\sigma_j(i),i} \\
&\overset{\text{(b)}}{=} \textstyle\prod_{j=1}^{\ell} \sum_{\sigma_j\in \mathrm{Sym}(I_j)} \operatorname{sign}(\sigma_j) \prod_{i\in I_j} a_{\sigma_j(i),i} \\
&\overset{\text{Def}}{=} \textstyle\prod_{j=1}^{\ell} \det(A_{jj})
\end{aligned}$$

Wir erhalten also $\det(A) = \det(A_{11}) \cdot \det(A_{22}) \cdots \det(A_{\ell\ell})$. QED

Die Idee ist anschaulich klar: Eine Permutationen $\sigma \in \mathrm{S}_n$ trägt nur dann etwas bei, wenn Sie auf den diagonalen Matrizen gefangen ist, $\sigma \in U$.

Damit können wir die Summe der Leibniz–Formel nun umformen.
Hier sehen Sie, wie es geht. Wie immer gilt: Gute Notation hilft!

Determinante von Dreiecksmatrizen

Bemerkung: Alternativ zur Leibniz–Formel können wir auch für jede Block-Dreiecksmatrix A Zeilenoperationen bzw. Spaltenoperationen nutzen, um A auf Dreiecksform $A' = SA$ bzw. $A'' = AT$ zu bringen.

Dies geschieht separat in jedem Block A_{jj}, also erhalten wir auch hier

$$\det(A) = \det(A_{11}) \cdot \det(A_{22}) \cdots \det(A_{\ell\ell}).$$

Übung: Führen Sie auch diese zweite Beweisidee sorgfältig aus. Vergleichen Sie beide Beweise: Welcher gefällt Ihnen besser?

☺ Bei diesen Rechnungen nutzen wir die Bemerkung L2w zur Determinante unter Spalten- und Zeilenoperationen.

Die Determinante und das Gauß–Verfahren

Bemerkung L2W: Spalten- und Zeilenoperationen

Elementare Spaltenoperationen ändern die Determinante wie folgt:

1. Transvektion $T_{ij}(\lambda)$ ändert nichts (L2C), $\det(T_{ij}(\lambda)) = 1$.
2. Skalierung $S_i(\mu)$ multipliziert mit μ (L2L), $\det(S_i(\mu)) = \mu$.
3. Vertauschung P_{ij} multipliziert mit -1 (L2E), $\det(P_\sigma) = \operatorname{sign}(\sigma)$.

Dasselbe gilt für Zeilenoperationen, dank Transpositionsinvarianz L2K.

Über jedem Körper K erhalten wir daraus den folgenden Algorithmus:

Algo L2X: Berechnung der Determinante

Eingabe: eine Matrix $A \in K^{n\times n}$ über einem Körper K
Ausgabe: die Determinante $\det(A) \in K$

1: Bringe A in Dreiecksform $B = SA$, etwa mit Gauß B2C
2: return $\det(A) = \det(S)^{-1} \det(B)$ dank L2N und L2W

☺ Die Berechnung gelingt mit höchstens n^3 Operationen in K.

Die Determinante und das Gauß–Verfahren

Wir nutzen gerne und erfolgreich die Umformung von Matrizen mittels elementarer Zeilen- und Spaltenoperationen. Bemerkung L2W fasst zusammen, wie sich die Determinante bei diesen Umformungen verhält.

☺ Insbesondere können wir über einem Körper das Gauß–Verfahren anwenden, um die Determinante zu berechnen. Beides sind starke Methoden, und sie fügen sich hier nun wunderbar zusammen.

☺ Das Gauß–Verfahren B2C ist sehr effizient: Es benötigt $\leq n^2$ Zeilenoperationen und $\leq n^3$ arithmetische Operationen in K.

Das ist eine gigantische Verbesserung gegenüber den fatalen $n \cdot n!$ Operationen, die eine naive Anwendung der Leibniz–Formel erfordert.

Um diesen Unterschied möglichst eindrücklich zu illustrieren, stelle ich die ersten Werte von n^3 und $n \cdot n!$ in der folgenden Tabelle gegenüber.

Übung: Wie lange benötigt ein Rechner mit einer Billion Operationen pro Sekunde? (TerraFlops = 10^{12} floating point operations per second)

Die Determinante und das Gauß–Verfahren

Vergleich von Gauß–Verfahren und Leibniz–Formel:

Größe n	Aufwand n^3	Aufwand $n \cdot n!$
1	1	1
2	8	4
3	27	18
4	64	96
5	125	600
6	216	4320
7	343	35 280
8	512	322 560
9	729	3 265 920
10	1000	36 288 000
20	8000	$\approx 5 \cdot 10^{19}$
30	27000	$\approx 8 \cdot 10^{33}$
40	64000	$\approx 3 \cdot 10^{49}$

Die Determinante und das Gauß–Verfahren

Sie sehen an dieser Tabelle: Für $n = 2, 3$ liegen beide Verfahren gleich auf, je nach Zählung noch mit leichtem Vorteil für die Leibniz–Formel.

Ab $n = 4$ macht sich die Bürde der Fakultät in $n \cdot n!$ bemerkbar, und für $n \geq 5$ explodiert dieser Term geradezu, während n^3 moderat wächst.

Das erklärt eindrücklich, warum die Berechnung der Determinante mit der Leibniz–Formel für $n = 2, 3$ recht beliebt ist, aber danach nicht mehr!

⚠ Wählen Sie Ihren Rechenweg immer mit Bedacht und Umsicht! Egal ob Sie selbst per Hand rechnen oder den Computer rechnen lassen, die Anzahl der Rechenschritte ist eine wichtige Ressource.

Das Ergebnis ist zwar *theoretisch* auf beiden Wegen dasselbe, doch diese Garantie nützt Ihnen *praktisch* herzlich wenig, wenn Sie Jahre, Jahrtausende oder Jahrmillionen auf das Ergebnis warten müssen.

☺ Es ist schön und nützlich, dass wir dank Leibniz für die Determinante über eine polynomielle Darstellung verfügen. Diese Formel hat viele gute Eigenschaften, effiziente Berechenbarkeit gehört nicht dazu. Diesen Teil übernimmt Gauß. Gemeinsam sind sie stark!

Beispiel: Zeilen- und Spaltenoperationen

Aufgabe: Berechnen Sie die Determinante der folgenden Matrix:

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 \\ 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{bmatrix}$$

(0) Ist die Leibniz–Formel hier geeignet? (1) Wie effizient ist Gauß?
(2) Geht es mit Umsicht und Geschick noch besser? Anleitung:

(3) Subtrahiere die $i$te Zeile von der $(i-1)$ten Zeile für $i = 2, \dots, 10$.
Anschließend addiere die erste Spalte zu jeder weiteren Spalte.

Beispiel: Zeilen- und Spaltenoperationen

Manche Menschen behaupten, die Determinante großer Matrizen könne man nicht mit vertretbarem Aufwand berechnen. Das ist nicht wahr!

Hier sehen Sie eine 10×10–Matrix, die Sie per Hand ausrechnen. Wenn Sie geschickt vorgehen, dann ist die Rechnung sogar leicht.

🙂 Gauß geht immer, diese Methode löst das allgemeine Problem. Dieses universelle Verfahren ist weiterhin unser treues Arbeitspferd.

Das stumpfsinnige Rechnen macht dem Computer rein gar nichts aus — mir schon! Und ich bin mir sicher, Ihnen geht es ganz ähnlich.

🙂 Wenn Sie von Hand rechnen, dann möchten Sie genauer hinsehen und Vereinfachungen nutzen, um den Aufwand weiter zu reduzieren.

Daher ist die sture Anwendung des Gauß–Algorithmus zwar möglich, sie führt immer zum Ziel, aber sie ist nicht immer der beste Weg.

Typische Strategie: Wie kommen wir schnell zu einer Dreiecksmatrix? Im vorliegenden Beispiel gibt die Aufgabenstellung eine Anleitung.

Beispiel: Zeilen- und Spaltenoperationen

Lösung: (3) Wir gehen geschickt vor und/oder folgen der Anleitung.
Wir subtrahieren die $i$te Zeile von der $(i-1)$ten Zeile für $i = 2, \dots, 10$:

$$\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 \\ 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix} = \begin{vmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix}$$

Die Determinante bleibt dabei gleich: Transvektion ändert nichts (L2w).
Dass dies ein Schritt in die richtige Richtung ist, sehen wir gleich…

Beispiel: Zeilen- und Spaltenoperationen

Ausprobieren mit Gaël!

Wir addieren die erste Spalte zu jeder weiteren Spalte:

$$\begin{vmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & -2 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & -2 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & -2 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & -2 & 0 & 0 \\ * & * & * & * & * & * & * & * & -2 & 0 \\ * & * & * & * & * & * & * & * & * & 9 \end{vmatrix}$$

So gewinnen wir eine Dreiecksmatrix (L2v). Nun lesen wir mühelos ab:

$$\det(A) = -9 \cdot (-2)^8 = -2304$$

Sie können die Matrix A auch stur nach Gauß–Algorithmus behandeln.
Probieren Sie es aus, am besten mit unserem Online-Tool Gaël!

Die Vandermonde–Determinante

Aufgabe: Berechnen Sie die Determinante der Vandermonde–Matrix

$$V = V(x_0, \dots, x_n) := (x_i^j)_{i=0,1,\dots,n}^{j=0,1,\dots,n} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix}.$$

Diese berühmte Matrix tritt häufig auf, insbesondere bei der Polynominterpolation, siehe B309. Ihre Invertierbarkeit haben wir in Satz B3A bereits geklärt, nun berechnen wir explizit ihre Determinante $\det V$.

Lösung: Wir berechnen die kleinen Fälle und suchen nach Mustern. Diese wollen wir anschließend für alle $n \in \mathbb{N}$ per Induktion beweisen.

Der Fall $n = 0$ ist trivial, der Fall $n = 1$ sehr einfach:

$$\begin{vmatrix} 1 \end{vmatrix} = 1, \qquad \begin{vmatrix} 1 & x_0 \\ 1 & x_1 \end{vmatrix} = x_1 - x_0$$

Hieran erkennen wir leider noch keine allgemeine Regel.

Die Vandermonde–Determinante

Für $n = 2$ suchen wir insbesondere nach einer Rekursion:

$$\begin{vmatrix} 1 & x_0 & x_0^2 \\ 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \end{vmatrix} \overset{(1)}{=} \begin{vmatrix} 1 & x_0 & x_0^2 \\ 0 & x_1 - x_0 & x_1^2 - x_0^2 \\ 0 & x_2 - x_0 & x_2^2 - x_0^2 \end{vmatrix}$$

(1) Spalte 0 aufräumen: Wir subtrahieren Zeile 0 von jeder Zeile $i > 0$.
(2) Wir ziehen den Faktor $(x_i - x_0)$ aus jeder Zeile $i > 0$ (dank G2D):

$$\begin{vmatrix} 1 & x_0 & x_0^2 \\ 0 & 1 & x_1 + x_0 \\ 0 & 1 & x_2 + x_0 \end{vmatrix} \overset{(3)}{=} \begin{vmatrix} 1 & x_0 & 0 \\ 0 & 1 & x_1 \\ 0 & 1 & x_2 \end{vmatrix}$$

(3) Aufräumen: Wir subtrahieren $x_0$mal Spalte 1 von Spalte 2.
Wir erhalten so eine Block-Dreiecksmatrix aus 1 und $V(x_1, x_2)$.
Nun können wir den vorigen Fall $n = 1$ anwenden! Wir erhalten:

$$\begin{vmatrix} 1 & x_0 & x_0^2 \\ 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \end{vmatrix} = (x_1 - x_0)(x_2 - x_0)(x_2 - x_1) = \prod_{i<j} (x_j - x_i)$$

Die Vandermonde–Determinante

Satz L2Y: die Vandermonde–Matrix und ihre Determinante

Sei K ein kommutativer Ring und $x_0, x_1, \dots, x_n \in K$. Dann gilt:

$$V = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix} \quad \Longrightarrow \quad \det V = \prod_{i<j} (x_j - x_i)$$

Beweis: Dies folgt per Induktion über n nach dem obigen Vorbild. QED

Aufgabe: Führen Sie den nächsten Fall $n = 3$ aus, dann allgemein.
Das ist eine gute Übung zur Rechenfertigkeit mit Determinanten.
Wie so oft verstehen Sie es erst, wenn Sie es selbst tun!

Erkläre es mir, und ich werde es vergessen.
Zeige es mir, und ich werde mich erinnern.
Lass es mich tun, und ich werde es verstehen.

(Konfuzius, 551–497 v.Chr.)

Die Vandermonde–Determinante

Lösung: Für $n = 3$ verfahren wir nach obigem Muster:

$$\begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \end{vmatrix} \overset{(1)}{=} \begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 0 & x_1 - x_0 & x_1^2 - x_0^2 & x_1^3 - x_0^3 \\ 0 & x_2 - x_0 & x_2^2 - x_0^2 & x_2^3 - x_0^3 \\ 0 & x_3 - x_0 & x_3^2 - x_0^2 & x_3^3 - x_0^3 \end{vmatrix}$$

(1) Spalte 0 aufräumen: Wir subtrahieren Zeile 0 von jeder Zeile $i > 0$.
(2) Wir ziehen den Faktor $(x_i - x_0)$ aus jeder Zeile $i > 0$ (dank G2D):

$$\begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 0 & 1 & x_1 + x_0 & x_1^2 + x_1 x_0 + x_0^2 \\ 0 & 1 & x_2 + x_0 & x_2^2 + x_2 x_0 + x_0^2 \\ 0 & 1 & x_3 + x_0 & x_3^2 + x_3 x_0 + x_0^2 \end{vmatrix} \overset{(3)}{=} \begin{vmatrix} 1 & x_0 & 0 & 0 \\ 0 & 1 & x_1 & x_1^2 \\ 0 & 1 & x_2 & x_2^2 \\ 0 & 1 & x_3 & x_3^2 \end{vmatrix}$$

(3) Aufräumen: Wir subtrahieren $x_0$mal Spalte 1 von Spalte 2, dann x_0^2mal Spalte 1 von Spalte 3, und x_0 mal Spalte 2 von Spalte 3. Voilà!

☺ Der allgemeine Induktionsbeweis verläuft ganz genau so.

Die Vandermonde–Determinante

Die Vandermonde–Determinante

Die Vandermonde–Determinante

Die Vandermonde–Determinante

Die Streichungsmatrix A_{ij}

Aus $A \in K^{n\times n}$ bilden wir die **Streichungsmatrix** $A_{ij} \in K^{(n-1)\times(n-1)}$:

$$A_{ij} = \begin{bmatrix} a_{1,1} & \dots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i,1} & \dots & a_{i,j-1} & a_{i,j} & a_{i,j+1} & \dots & a_{i,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & a_{n,j} & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix}$$

Wir löschen aus A die $i$te Zeile und die $j$te Spalte und erhalten A_{ij}. Die so entstehende Matrix hat eine Zeile und eine Spalte weniger.

Diese Streichungsmatrix A_{ij} können wir recht häufig zur rekursiven Berechnung nutzen, wie die folgenden typischen Beispiele zeigen.

Die Ersetzungsmatrix A^+_{ij}

Beispiel: Aus der Matrix $A \in K^{n\times n}$ bilden wir die **Ersetzungsmatrix**

$$A^+_{ij} = \begin{bmatrix} a_{1,1} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix}.$$

Wir tauschen (i,j) nach $(1,1)$ und erhalten eine Block-Diagonalmatrix:

$$\det A^+_{ij} = (-1)^{i+j} \det A_{ij}$$

Von unserer Matrix A^+_{ij} zur Block-Diagonalmatrix $\operatorname{diag}(1, A_{ij})$ tauschen wir $i-1$ mal benachbarte Zeilen und $j-1$ mal benachbarte Spalten, daher das Vorzeichen $(-1)^{i+j-2} = (-1)^{i+j}$. In Blockform können wir schließlich Satz L2v anwenden und erhalten $\det \operatorname{diag}(1, A_{ij}) = \det A_{ij}$.

Die Spalten-Ersetzungsmatrix $A^|_{ij}$

Beispiel: In der Matrix $A \in K^{n\times n}$ ersetzen wir die $j$te Spalte durch e_i:

$$A^|_{ij} = \begin{bmatrix} a_{1,1} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i,1} & \dots & a_{i,j-1} & 1 & a_{i,j+1} & \dots & a_{i,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix}$$

Wir tauschen (i,j) nach $(1,1)$ zu einer oberen Block-Dreiecksmatrix:

$$\det A^|_{ij} = (-1)^{i+j} \det A_{ij}$$

Das Vorzeichen entsteht genau wie zuvor für die Matrix A^+_{ij} erklärt.
Alternativ: $\det A^|_{ij} = \det A^+_{ij}$ durch Leerräumen der $i$ten Zeile (L2w).

Die Zeilen-Ersetzungsmatrix A^-_{ij}

Beispiel: In der Matrix $A \in K^{n\times n}$ ersetzen wir die $i$te Zeile durch e_j^T:

$$A^-_{ij} = \begin{bmatrix} a_{1,1} & \dots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & a_{n,j} & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix}$$

Wir tauschen (i,j) nach $(1,1)$ zu einer unteren Block-Dreiecksmatrix:

$$\det A^-_{ij} = (-1)^{i+j} \det A_{ij}$$

Das Vorzeichen entsteht genau wie zuvor für die Matrix A^+_{ij} erklärt.
Alternativ: $\det A^-_{ij} = \det A^+_{ij}$ durch Leerräumen der $j$ten Spalte (L2w).

Die rekursive Laplace–Entwicklung

Satz L2z: Entwicklungssatz von Laplace

Die Determinante von $A \in K^{n\times n}$ lässt sich rekursiv berechnen durch Entwicklung nach der $j$ten Spalte oder nach der $i$ten Zeile:

$$\det A \;=\; \sum_{i=1}^{n}(-1)^{i+j}a_{ij}\det A_{ij} \;=\; \sum_{j=1}^{n}(-1)^{i+j}a_{ij}\det A_{ij}$$

Hierbei entsteht A_{ij} durch Streichen der $i$ten Zeile und der $j$ten Spalte.

Beweis: (1) Die $j$te Spalte ist $a_j = \sum_{i=1}^n e_i a_{ij}$, also gilt:

$$\begin{aligned}\det A &= \det(a_1,\ldots,a_{j-1},\textstyle\sum_{i=1}^n e_i a_{ij},a_{j+1},\ldots,a_n)\\ &= \textstyle\sum_{i=1}^n a_{ij}\det(a_1,\ldots,a_{j-1},e_i,a_{j+1},\ldots,a_n)\\ &= \textstyle\sum_{i=1}^n a_{ij}\det A^{|}_{ij} = \sum_{i=1}^n(-1)^{i+j}a_{ij}\det A_{ij}\end{aligned}$$

(2) Entsprechend entwickeln wir nach der $i$ten Zeile (L2K). QED

Notation: Das Produkt $\tilde a_{ij} := (-1)^{i+j}\det A_{ij}$ heißt der **Cofaktor** zu a_{ij}. Die Cofaktormatrix $\tilde A = (\tilde a_{ij})_{ij}$ ist transponiert zur Adjunkten $\operatorname{adj}(A)$.

Die rekursive Laplace–Entwicklung

Das hier auftretende Vorzeichen $(-1)^{i+j}$ bildet ein Schachbrettmuster:

$$\begin{bmatrix} + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \end{bmatrix}$$

Die Laplace–Entwicklung ist eine Umformulierung der Leibniz–Formel, die Summe über alle Permutationen in S_n wird nur anders durchlaufen. Beide haben zunächst denselben Aufwand und sind gleich in/effizient.

🙂 Die Laplace–Entwicklung lohnt sich, wenn A viele Nullen enthält: Diese Terme fallen sofort weg, und die Rechnung vereinfacht sich.

Die rekursive Laplace–Entwicklung

Aufgabe: Entwickeln Sie geschickt die Determinante von

$$A = \begin{bmatrix}7&3&0\\2&1&5\\4&2&0\end{bmatrix} \quad\text{und}\quad B = \begin{bmatrix}3&1&2&2\\4&0&0&2\\7&2&1&0\\0&5&8&3\end{bmatrix}.$$

Lösung: (1) Wir entwickeln $\det(A)$ nach der dritten Spalte:

$$\begin{vmatrix}7&3&0\\2&1&5\\4&2&0\end{vmatrix} = +0\cdot\begin{vmatrix}2&1\\4&2\end{vmatrix} - 5\cdot\begin{vmatrix}7&3\\4&2\end{vmatrix} + 0\cdot\begin{vmatrix}7&3\\2&1\end{vmatrix} = (-5)\cdot 2 = -10$$

(2) Wir entwickeln $\det(B)$ nach der zweiten Zeile:

$$\begin{vmatrix}3&1&2&2\\4&0&0&2\\7&2&1&0\\0&5&8&3\end{vmatrix} = -4\begin{vmatrix}1&2&2\\2&1&0\\5&8&3\end{vmatrix} + 0\begin{vmatrix}3&2&2\\7&1&0\\0&8&3\end{vmatrix} + 0\begin{vmatrix}3&1&2\\7&2&0\\0&5&3\end{vmatrix} + 2\begin{vmatrix}3&1&2\\7&2&1\\0&5&8\end{vmatrix}$$

$$= -4\cdot\big[2\cdot 11 + 3\cdot(-3)\big] + 2\cdot\big[3\cdot 11 - 7\cdot(-2)\big] = 42$$

Die rekursive Laplace–Entwicklung

Ausprobieren mit Gaël!

Das Beispiel A ist sehr klein und einfach, Sie durchschauen es sofort. Als Service und zur Betonung habe ich auch die Nullterme angegeben; sie fallen weg, und normalerweise würde man sie direkt übergehen. Sie dienen hier allein zur graphischen Erklärung des Verfahrens.

Beim Beispiel B hingegen müssen wir schon etwas länger rechnen. Insbesondere spüren Sie, dass es sich um eine Rekursion handelt: Die 3×3–Streichungsmatrizen müssen ebenfalls berechnet werden. Die Einsparung entsteht allein durch die Nullterme!

🙂 Es lohnt sich für B bereits, den Gauß–Algorithmus zu nutzen!

Übung: Berechnen Sie $\det(A)$ und $\det(B)$ zum direkten Vergleich durch Zeilen- und Spaltenumformungen wie im Gauß–Algorithmus. Wie viele Operationen in K benötigen Sie jeweils?

Übung: Ohne Einsparungen durch Nulleinträge hat die rekursive Laplace–Entwicklung denselben Aufwand wie die Leibniz–Formel: Beide benötigen $n\cdot n!$ Operationen im Grundkörper K.

Ist jede invertierbare Matrix quadratisch?

L301

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}\cdot\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\0&0&0\end{pmatrix}\overset{!}{=}\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

$$A\cdot B\overset{?}{=}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

Gibt es invertierbare Matrizen $A \in R^{n\times m}$, die nicht quadratisch sind?

- Ja, klar, über dem Nullring $R = \{0\}$ mit $0 = 1$ ist das trivial.
- Es gibt weitere Beispiele (J1O), etwa über $R = \mathrm{End}_K(K[X])$.

Damit gilt $R^m \cong R^n$; der Begriff „Dimension“ hat dann keinen Sinn.

Viele „vernünftige“ Ringe erfüllen die Invarianz der Dimension (J1L):

- Über jedem Divisionsring haben wir den Gauß–Algorithmus (B2D).
- Über jedem kommutativen Ring haben wir die Determinante (L2G).

Ist jede invertierbare Matrix quadratisch?

L302
Erläuterung

☺ Erst die Invarianz der Dimension, wie in J1L definiert, erlaubt es uns, jedem freien R–linearen Raum V eine Dimension $\dim_R(V)$ zuzuordnen.

⚠ Über manchen Ringen hat der Begriff „Dimension“ keinen Sinn!

Zur Erinnerung (J1O): Sei K ein Körper. Im Ring $R = \mathrm{End}_K(K[X])$ haben wir die Elemente $a : P(X) \mapsto P(X^2)$ und $b : P(X) \mapsto XP(X^2)$ sowie $(c, d) : P \mapsto (P_0, P_1)$ mit $P = P_0(X^2) + XP_1(X^2)$, also explizit

$$a(P) = (p_0, 0, p_1, 0, p_2, 0, \dots), \qquad c(P) = (p_0, p_2, p_4, p_6, p_8, \dots),$$
$$b(P) = (0, p_0, 0, p_1, 0, p_2, \dots), \qquad d(P) = (p_1, p_3, p_5, p_7, p_9, \dots).$$

Überraschenderweise gelten damit die Gleichungen

$$\begin{pmatrix}c\\d\end{pmatrix}\begin{pmatrix}a & b\end{pmatrix} = \begin{pmatrix}ca & cb\\da & db\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}c\\d\end{pmatrix} = ac + bd = 1.$$

Die Matrizen $\left(\begin{smallmatrix}c\\d\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}a & b\end{smallmatrix}\right)$ stiften somit einen Isomorphismus $R^1 \cong R^2$. Wider die Intuition haben wir also die verblüffende Gleichung

$$\begin{pmatrix}c&0\\d&0\end{pmatrix}\begin{pmatrix}a&b\\0&0\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

Invertierbare Matrizen über einem kommutativen Ring

L303

Satz L3A: invertierbare Matrizen

Gegeben sei ein kommutativer Ring K mit $0 \neq 1$. Seien $m, n \in \mathbb{N}$.

(1) Für alle $A \in K^{n\times m}$ und $B \in K^{m\times n}$ mit $A \cdot B = 1_{n\times n}$ gilt $m \geq n$.

(2) Ist die Matrix $A \in K^{n\times m}$ invertierbar, so folgt $n = m$.

Beweis: (1) Angenommen, es gäbe ein Gegenbeispiel mit $m < n$.
Wir ergänzen A, B zu $A', B' \in K^{n\times n}$ durch Nullspalten bzw. Nullzeilen:

$$\left(\begin{array}{c|c}A & 0\end{array}\right)\cdot\begin{pmatrix}B\\\hline 0\end{pmatrix} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

Weiter gilt $A' \cdot B' = 1_{n\times n}$. Auf quadratische (!) Matrizen können wir die Determinante anwenden. Die Determinante ist multiplikativ (L2N), also:

$$\det(A') \cdot \det(B') = \det(A' \cdot B') = \det(1_{n\times n}) = 1$$

Andererseits gilt $\det(A') = \det(B') = 0$ (L2B), ein Widerspruch! QED

Invertierbare Matrizen über einem kommutativen Ring

L304
Erläuterung

☺ Es gibt weitere Beweise für diese fundamentale Eigenschaft (1).
Über jedem Divisionsring gilt (1) dank Gauß–Algorithmus (B2D).

Satz L3B: Transferprinzip

Sei $\varphi : S \to R$ ein Homomorphismus von Ringen (hier immer mit Eins).
Gilt die Aussage (1) über dem Ring R, so auch über dem Ring S.

Beweis: Wir setzen φ komponentenweise fort zu $\varphi : S^{p\times q} \to R^{p\times q}$.
Dies respektiert die Addition und die Multiplikation von Matrizen.

Gegeben seien Matrizen $A \in S^{n\times m}$ und $B \in S^{m\times n}$ mit $A \cdot B = 1_{n\times n}$.
Daraus folgt $\varphi(A) \cdot \varphi(B) = \varphi(A \cdot B) = \varphi(1_{n\times n}) = \varphi(1_{n\times n})$ über R.
Nach Voraussetzung über R gilt demnach $m \geq n$. QED

Beispiel: Für den Ring $\mathbb{Z}$ können wir die Einbettung $\mathrm{inc} : \mathbb{Z} \hookrightarrow \mathbb{Q}$ nutzen und ebenso den Quotienten $q : \mathbb{Z} \twoheadrightarrow \mathbb{F}_p$ für eine Primzahl $p \in \mathbb{N}_{\geq 2}$:

☺ So können wir für den Ring $\mathbb{Z}$ neben der Determinante L3A auch den Gauß–Algorithmus B2D nutzen, indirekt über $\mathbb{Z} \hookrightarrow \mathbb{Q}$ oder $\mathbb{Z} \twoheadrightarrow \mathbb{F}_p$.

Invarianz der Dimension

Satz L3C: Invarianz der Dimension

Sei K ein kommutativer Ring mit $0 \neq 1$. Für alle $m, n \in \mathbb{N}$ gilt:

1. Ist $f : K^m \twoheadrightarrow K^n$ eine K–lineare Surjektion, so gilt $m \geq n$.
2. Ist $f : K^m \hookrightarrow K^n$ eine K–lineare Injektion, so gilt $m \leq n$.
3. Ist $f : K^m \xrightarrow{\sim} K^n$ eine K–lineare Bijektion, so gilt $m = n$.

Somit erfüllt der Ring K die Invarianz der Dimension (J1L).

Beweis: (1) Zu jedem $i = 1, \ldots, n$ wählen wir $v_i \in K^m$ mit $f(v_i) = e_i$. Sei $g : K^n \to K^m$ die lineare Abbildung mit $g(e_i) = v_i$ (PLF, Satz K1B). Damit gilt $f \circ g = \mathrm{id}_{K^n}$ (K1A). Die darstellenden Matrizen $A \in K^{n \times m}$ zu f und $B \in K^{m \times n}$ zu g erfüllen $A \cdot B = 1_{n \times n}$. Daraus folgt $m \geq n$ (L3A).

(3) Dank (1) gilt $m \geq n$. Mit $f^{-1} : K^n \xrightarrow{\sim} K^m$ (I1G) folgt $n \geq m$. QED

Aussage (2) ist algebraisch raffinierter und wird hier nicht bewiesen. Zwecks Symmetrie will ich jedoch alle drei Aussagen beisammen halten.

Invarianz der Dimension

Die Aussage des Satzes ist die vertraute Invarianz der Dimension, die Sie bereits aus Kapitel J kennen, nun über kommutativen Ringen. Der Satz gilt auch über Divisionsringen dank Gauß–Algorithmus (J1K). Beide Versionen beinhalten kommutative Divisionsringe, also Körper

Zum Beweis benötigen wir stichhaltige Argumente, und dies gelingt mit starken Werkzeugen: über kommutativen Ringen die Determinante, über Divisionsringen der Gauß–Algorithmus.

Bemerkung: Zur Dimension $\dim_R(V)$ benötigen wir zwei Zutaten:

1. Der R–lineare Raum V muss frei sein, also mindestens eine Basis haben; das gilt leider nicht immer, siehe J1B. Es gilt für alle Vektorräume, siehe J2B und J2C.
2. Der Ring R muss die Invarianz der Dimension erfüllen: Je zwei Basen von V haben dann dieselbe Länge. Dazu haben wir die Sätze J1K und L3C.

Ein erstes Anwendungsbeispiel

Aufgabe: (1) Sind die Gruppen $(\mathbb{Z}^m, +)$ und $(\mathbb{Z}^n, +)$ isomorph?
(2) Wie viele Homomorphismen $(\mathbb{Z}^n, +) \to (\mathbb{Z}/a, +)$ gibt es für $a \in \mathbb{N}_{\geq 2}$?
(3) Lösen Sie mit der Rechnung (2) erneut das Isomorphieproblem (1).

Lösung: (1) Jede abelsche Gruppe ist ein $\mathbb{Z}$–linearer Raum (I1K), und jeder Gruppenhomomorphismus ist automatisch linear über $\mathbb{Z}$. Dank Invarianz der Dimension L3C gilt: Aus $\mathbb{Z}^m \cong \mathbb{Z}^n$ folgt $m = n$.

(2) Glücklicherweise ist $\mathbb{Z}^n$ frei über $\mathbb{Z}$, mit Basis $e_1, \ldots, e_n$ (J1C). Dank Prinzip der linearen Fortsetzung (K1B) haben wir die Bijektion

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}/a) \xrightarrow{\sim} \mathrm{Abb}(\{e_1, \ldots, e_n\}, \mathbb{Z}/a) \,:\, f \mapsto f|_B.$$

Demnach gilt $\sharp\,\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}/a) = a^n$. Anschaulich: Wir müssen für jeden der Basisvektoren $e_1, \ldots, e_n$ ein Bildelement $f(e_k) \in \mathbb{Z}/a$ vorgeben.

(3) Aus der Isomorphie $(\mathbb{Z}^m, +) \cong (\mathbb{Z}^n, +)$ folgt die Gleichheit von $\sharp\,\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^m, \mathbb{Z}/a) = a^m$ und $\sharp\,\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}/a) = a^n$, also $m = n$ (A1B).

Ein erstes Anwendungsbeispiel

☺ Dieser einfache Trick (2) beantwortet die Frage (1) direkt durch Abzählen, ohne Determinante oder Gauß–Algorithmus.

Für je zwei natürliche Zahlen $m \neq n$ gilt demnach $\mathbb{Z}^m \ncong \mathbb{Z}^n$.
Für diese grundlegende Tatsache gibt es viele schöne Beweise...

Den ersten Beweis (1) habe ich zur Illustration des Invarianzsatzes L3C angeführt. Er schießt zwar mit Kanonen auf Spatzen... doch er trifft.

Auch der zweite Beweis (2) ist lehrreich, denn er betont das Prinzip der linearen Fortsetzung und ist ansonsten vollkommen elementar.

Bemerkung: Der wohl einfachste Beweis gelingt mit der Spur (B1I):

$$\mathrm{tr} = \mathrm{tr}_n \,:\, \mathbb{Z}^{n \times n} \to \mathbb{Z} \,:\, A \mapsto \textstyle\sum_{k=1}^{n} a_{kk} = a_{11} + a_{22} + \cdots + a_{nn}$$

Aus $(f, g) : \mathbb{Z}^n \cong \mathbb{Z}^m$ erhalten wir Matrizen $A \in \mathbb{Z}^{m \times n}$ und $B \in \mathbb{Z}^{n \times m}$ mit $AB = 1_{m \times m}$ und $BA = 1_{n \times n}$. Daraus folgt $\mathrm{tr}(AB) = m$ und $\mathrm{tr}(BA) = n$. Dank Satz B1J gilt $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ über $\mathbb{Z}$, also $m = n$.

Die Determinante eines Endomorphismus

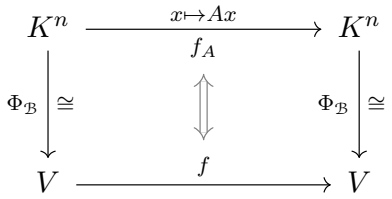
Über jedem kommutativen Ring K haben wir die Determinante (L2G)

$$\det = \det_K^n \,:\, (K^{n\times n}, \cdot, 1_{n\times n}) \to (K, \cdot, 1) \,:\, A \mapsto \det(A).$$

Allgemeiner sei V ein linearer Raum mit einer endlichen Basis über K.
Wie definieren wir die Determinante für lineare Abbildungen $f : V \to V$?

$$\det_V \,:\, (\mathrm{End}_K(V), \circ, \mathrm{id}_V) \to (K, \cdot, 1) \,:\, f \mapsto \det_V(f)$$

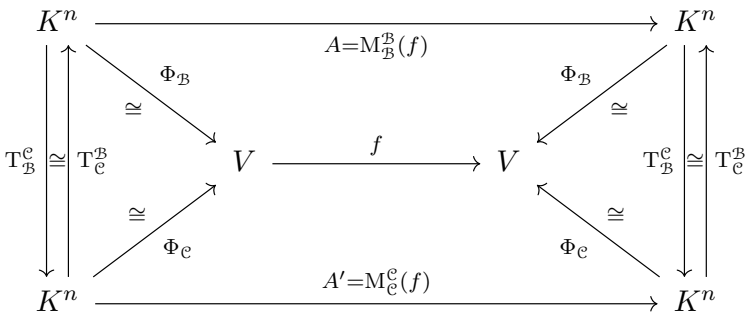
Wir wählen willkürlich irgendeine Basis $\mathcal{B}$ von V (J2B):



Aufgabe: Können wir $\det_V(f) := \det_K^n(A)$ so wohl definieren?
Ist das Ergebnis unabhängig von der willkürlich gewählten Basis $\mathcal{B}$?

Die Determinante eines Endomorphismus

Lösung: Wir vergleichen zwei Basen $\mathcal{B}$ und $\mathcal{C}$ des Raums V über K:
Dank Invarianz der Dimension L3C haben beide dieselbe Länge n.



In $K^{n\times n}$ haben wir $A' = T \cdot A \cdot T^{-1}$ mit $T = \mathrm{T}_\mathcal{B}^\mathcal{C}$ und $T^{-1} = \mathrm{T}_\mathcal{C}^\mathcal{B}$.
Dank Multiplikativität L2N der Determinante gilt:

$$\det(A') = \det(T) \cdot \det(A) \cdot \det(T)^{-1} = \det(A)$$

Somit ist die Determinante $\det_V(f) := \det(A) = \det(A')$ wohldefiniert,
da unabhängig von den willkürlich gewählten Basen $\mathcal{B}$ und $\mathcal{C}$.

Die Determinante eines Endomorphismus

Satz L3D: die Determinante eines Endomorphismus

(0) Sei K ein kommutativer Ring und V ein linearer Raum mit einer endlichen Basis über K. Mit der Wahl einer Basis $\mathcal{B}$ definieren wir

$$\det_V \,:\, \mathrm{End}_K(V) \to K \,:\, f \mapsto \det_V(f) := \det(\mathrm{M}_\mathcal{B}^\mathcal{B}(f)).$$

Diese Abbildung $\det_V$ ist wohldefiniert, das heißt basisunabhängig:
Jede andere Wahl einer Basis führt zu demselben Ergebnis.

(1) Wir erhalten so den ersehnten Monoidhomomorphismus

$$\det_V \,:\, (\mathrm{End}_K(V), \circ, \mathrm{id}_V) \to (K, \cdot, 1) \,:\, f \mapsto \det_V(f).$$

Genau dann ist $f \in \mathrm{End}_K(V)$ invertierbar, wenn $\det(f) \in K$ dies ist.

(2) Ist K ein Integritätsring, etwa ein Körper, so gilt:

$$\det(f) = 0 \iff \ker(f) \neq \{0\}$$
$$\det(f) \neq 0 \iff \ker(f) = \{0\}$$

Die Determinante eines Endomorphismus

Beweis: Die Wohldefiniertheit (0) haben wir in der vorigen Aufgabe nachgerechnet. Die weiteren Aussagen kennen wir bereits für die Determinante von Matrizen (L2T, L2Q) und übertragen diese nun auf Endomorphismen vermöge des Ringisomorphismus K1K:

$$(\mathrm{L}_\mathcal{B}^\mathcal{B}, \mathrm{M}_\mathcal{B}^\mathcal{B}) \,:\, (K^{n\times n}, +, \cdot) \;\cong\; (\mathrm{End}_K(V), +, \circ)$$

🙂 Wir setzen hier voraus, dass V frei und von endlicher Dimension ist.
Über einem Körper K müssen wir die Existenz einer Basis nicht fordern, sie folgt aus dem Basisauswahlsatz J2B. In diesem Fall vereinfacht sich die Voraussetzung zu: K ist ein Körper und $\dim_K(V) < \infty$.

🙂 Die Matrixdarstellung $A = \mathrm{M}_\mathcal{B}^\mathcal{B}(f)$ ist ein Hilfskonstrukt zur Definition der Determinante auf V. Sie dient ebenso zur effizienten Berechnung, denn für die Matrix $A \in K^{n\times n}$ halten wir alle Werkzeuge bereit!
Das Ergebnis jedoch ist von der Basiswahl unabhängig.

Anwendungsbeispiel zur Determinante

Beispiel: Wir betrachten die Ableitung ∂ auf dem $\mathbb{C}$–Vektorraum

$$V = \langle \cos(2t), \sin(2t), \cos(3t), \sin(3t) \rangle_{\mathbb{C}}^{!}$$
$$= \langle \mathrm{e}^{2\mathrm{i}t}, \mathrm{e}^{-2\mathrm{i}t}, \mathrm{e}^{3\mathrm{i}t}, \mathrm{e}^{-3\mathrm{i}t} \rangle_{\mathbb{C}}^{!} \;\leq\; \mathbb{C}^{\mathbb{R}}.$$

Gemeint ist $f_1 : \mathbb{R} \to \mathbb{C} : t \mapsto \cos(2t)$ usw. und $g_1 : \mathbb{R} \to \mathbb{C} : t \mapsto \mathrm{e}^{2\mathrm{i}t}$ usw.

Aufgabe: Berechnen Sie die Determinante $\det_V(\partial : V \to V)$.

Lösung: Wir wählen eine Basis von V, etwa $\mathcal{A}$ oder $\mathcal{B}$ wie oben, und stellen den Endomorphismus ∂ bezüglich dieser Basis als Matrix dar:

$$\mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) = \begin{bmatrix} 0 & 2 & 0 & 0 \\ -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & -3 & 0 \end{bmatrix} \quad \text{bzw.} \quad \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} 2\mathrm{i} & 0 & 0 & 0 \\ 0 & -2\mathrm{i} & 0 & 0 \\ 0 & 0 & 3\mathrm{i} & 0 \\ 0 & 0 & 0 & -3\mathrm{i} \end{bmatrix}$$

Damit finden wir $\det_V(\partial) = \det \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) = \det \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = 36$.

🙂 Jede Basiswahl führt zu demselben Ergebnis.

Anwendungsbeispiel zu Eigenräumen

Wir führen Beispiel K257 fort: Zu $v = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right] \in \mathbb{R}^2$ betrachten wir

$$f : \mathbb{R}^2 \to \mathbb{R}^2 : x \mapsto x - v \cdot v^{\mathsf{T}} \cdot x.$$

Aufgabe: (1) Finden Sie alle $\lambda \in \mathbb{R}$ mit nicht-trivialem **Eigenraum**

$$\mathrm{E}(\lambda) := \{\, x \in \mathbb{R}^2 \mid f(x) = \lambda x \,\} = \ker(f - \lambda\,\mathrm{id}).$$

(2) Bestimmen Sie die Eigenräume. (3) Finden Sie eine Eigenbasis.

Lösung: (1) Zur Bestimmung von λ nutzen wir die **Determinante**:

$$\ker(f - \lambda\,\mathrm{id}) \neq \{0\} \quad \overset{\text{L3D}}{\Longleftrightarrow} \quad \det(f - \lambda\,\mathrm{id}) = 0$$

Zur Berechnung wählen wir eine Basis, etwa $\mathcal{E} = (e_1, e_2)$, und finden

$$A = \mathrm{M}_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \det(A - \lambda \cdot 1_{2\times 2}) = \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - 1.$$

Dies ist das **charakteristische Polynom** von A bzw. von f.
Seine Nullstellen sind in diesem Beispiel $\lambda = +1$ und $\lambda = -1$.
Dies sind die **Eigenwerte** der Matrix A bzw. der Abbildung f.

Anwendungsbeispiel zu Eigenräumen

Zur Erinnerung wiederhole ich die weitere Rechnung von Seite K257:
(2) Wir bestimmen die Eigenräume $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$ wie folgt:

$$\mathrm{E}(+1) = \ker(f - \mathrm{id}) = \ker \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} = \mathbb{R}\, b_1 \quad \text{mit} \quad b_1 := \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\mathrm{E}(-1) = \ker(f + \mathrm{id}) = \ker \begin{bmatrix} +1 & 1 \\ 1 & +1 \end{bmatrix} = \mathbb{R}\, b_2 \quad \text{mit} \quad b_2 := \begin{bmatrix} -1 \\ 1 \end{bmatrix}$$

Für alle weiteren $\lambda \in \mathbb{R} \smallsetminus \{\pm 1\}$ gilt $\mathrm{E}(\lambda) = \{0\}$ dank Satz L3D.

(3) Wir erhalten $\mathbb{R}^2 = \mathrm{E}(+1) \oplus \mathrm{E}(-1)$ und die Basis $\mathcal{B} = (b_1, b_2)$ von $\mathbb{R}^2$.
Nach Konstruktion gilt $f(b_1) = +1 \cdot b_1$ und $f(b_2) = -1 \cdot b_2$, und somit

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Auf Seite K237 haben wir bereits die Basiswechselmatrizen bestimmt:

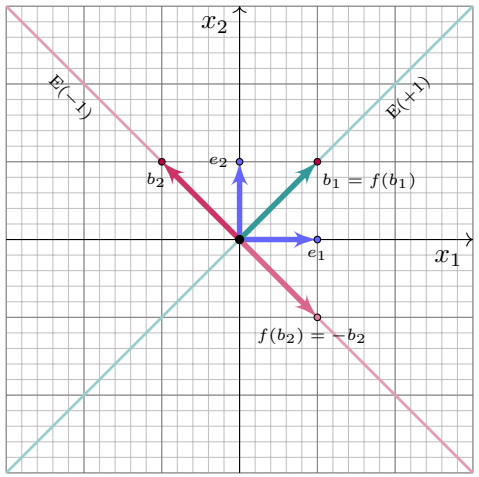
$$\mathrm{T}_{\mathcal{B}}^{\mathcal{E}} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \quad \text{und} \quad \mathrm{T}_{\mathcal{E}}^{\mathcal{B}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

Anwendungsbeispiel zu Eigenräumen

🙂 In der angepassten Basis $\mathcal{B} = (b_1, b_2)$ können wir die Abbildung f besonders einfach darstellen… Den Eigenräumen sei Dank!

$$\mathrm{M}_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$ ist die Spiegelung an der Hauptdiagonalen.

Die spezielle lineare Gruppe

Über jedem kommutativen Ring K haben wir die Determinante (L2G)

$$\det = \det_K^n : (K^{n\times n}, \cdot, 1_{n\times n}) \to (K, \cdot, 1) : A \mapsto \det(A).$$

Die invertierbaren Matrizen bilden die **allgemeine lineare Gruppe**

$$\mathrm{GL}_n(K) \overset{\text{L2T}}{=} \left\{ A \in K^{n\times n} \,\middle|\, \det_K^n(A) \in K^\times \right\}$$

Ist V ein linearer Raum mit endlicher Basis über K, so haben wir:

$$\mathrm{GL}(V) \overset{\text{L3D}}{=} \left\{ f : V \to V \,\middle|\, \det_V(f) \in K^\times \right\}$$

Definition L3E: die spezielle lineare Gruppe

Die Matrizen mit Determinante 1 bilden die **spezielle lineare Gruppe**

$$\mathrm{SL}_n(K) := \ker(\det_K^n) = \left\{ A \in K^{n\times n} \,\middle|\, \det_K^n(A) = 1 \right\}.$$

Ebenso definieren wir die Gruppe der **speziellen Automorphismen**

$$\mathrm{SL}(V) := \ker(\det_V) = \left\{ f : V \to V \,\middle|\, \det_V(f) = 1 \right\}.$$

Die spezielle lineare Gruppe

Die allgemeine lineare Gruppe $\mathrm{GL}(V)$ besteht aus den K–linearen Automorphismen $f : V \xrightarrow{\sim} V$, daher sind die folgenden Bezeichnungen ebenso üblich:

$$\mathrm{GL}(V) = \mathrm{Aut}_K(V)$$
$$\mathrm{SL}(V) = \mathrm{SAut}_K(V)$$

Beide Schreibweisen bedeuten dasselbe, jede hat ihre eigenen Vorteile. In der Nähe zu Matrizen schreibe ich hier lieber $\mathrm{GL}(V)$; in der Nähe zu Gruppen und ähnlichen Strukturen schreibe ich entsprechend $\mathrm{Aut}_K(V)$.

Die Determinante hat diese ganz besondere Eigenschaft (L2T): Genau dann ist $A \in K^{n\times n}$ invertierbar, wenn $\det A \in K$ invertierbar ist Daher können wir $\mathrm{GL}_n(K)$ durch die Determinante charakterisieren. Über einem Körper K vereinfacht sich dies weiter zu $\det(A) \neq 0$.

Für die spezielle lineare Gruppe verlangen wir nun $\det(A) = 1$. Somit ist $\mathrm{SL}_n(K)$ durch eine polynomielle Gleichung definiert.

Die spezielle lineare Gruppe

Beispiel: In Dimension $n = 1$ gilt $\mathrm{GL}_1(K) = K^\times$ und $\mathrm{SL}_1(K) = \{1\}$.

Beispiel: In Dimension $n = 2$ haben wir:

$$\mathrm{GL}_2(K) \overset{\text{L2T}}{=} \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \,\middle|\, ad - bc \in K^\times \right\}$$
$$\mathrm{SL}_2(K) \overset{\text{L3E}}{=} \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \,\middle|\, ad - bc = 1 \right\}$$

Bemerkung: Auf $\mathrm{GL}_n(K)$ ist die Inversion $A^{-1} = \det(A)^{-1}\,\mathrm{adj}(A)$ eine rationale Funktion (L2T), speziell auf $\mathrm{SL}_n(K)$ sogar ein Polynom!

$$A \in \mathrm{SL}_n(K) \implies A^{-1} = \mathrm{adj}(A), \qquad \begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix},$$

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}^{-1} = \begin{bmatrix} a_{22}a_{33} - a_{23}a_{32} & a_{13}a_{32} - a_{12}a_{33} & a_{12}a_{23} - a_{13}a_{22} \\ a_{23}a_{31} - a_{21}a_{33} & a_{11}a_{33} - a_{13}a_{31} & a_{13}a_{21} - a_{11}a_{23} \\ a_{21}a_{32} - a_{22}a_{31} & a_{12}a_{31} - a_{11}a_{32} & a_{11}a_{22} - a_{12}a_{21} \end{bmatrix}$$

Die spezielle lineare Gruppe

Die Determiante $\det : K^{n\times n} \to K$ ist ein explizites Polynom, dank der Leibniz–Formel L2G. Gleiches gilt für die Adjunktion $\mathrm{adj} : K^{n\times n} \to K^{n\times n}$. Daraus erhalten wir die Inversion $A \mapsto A^{-1} = \det(A)^{-1}\,\mathrm{adj}(A)$ als eine geschlossene Formel: eine explizit gegebene rationale Funktion (L2S).

Ich habe bereits die Besonderheit rationaler Funktionen betont: Über $K = \mathbb{R}, \mathbb{C}$ sind diese insbesondere stetig ($\mathscr{C}^0$), zudem differenzierbar ($\mathscr{C}^1$), glatt ($\mathscr{C}^\infty$), sogar analytisch ($\mathscr{C}^\omega$), … Auch Sicht der Analysis haben sie alle guten Eigenschaften, die wir uns nur wünschen können.

Für Polynome gelten all diese schönen Eigenschaften weiterhin, zudem sind Polynome noch einfacher: Wir müssen nicht einmal dividieren.

Allgemeine und spezielle lineare Gruppe

Satz L3F: allgemeine und spezielle lineare Gruppe

(0) Die Determinante definiert eine kurze exakte Sequenz von Gruppen:

$$1 \longrightarrow \mathrm{SL}_n(K) \xhookrightarrow{\text{inc}} \mathrm{GL}_n(K) \underset{\iota}{\overset{\det_K^n}{\twoheadrightarrow}} K^\times \longrightarrow 1$$

(1) Zu $\det_K^n$ existiert ein rechtsinverser Gruppenhomomorphismus

$$\iota : K^\times = \mathrm{GL}_1(K) \hookrightarrow \mathrm{GL}_n(K) : s \mapsto \mathrm{diag}(s, 1, \ldots, 1).$$

(2) Daraus folgt die Bijektion (jedoch i.A. kein Gruppenisomorphismus)

$$\varphi : \mathrm{SL}_n(K) \times K^\times \xrightarrow{\sim} \mathrm{GL}_n(K) : (A, s) \mapsto A \cdot \iota(s).$$

Ihre Umkehrabbildung ist $\psi(B) = (\, B \cdot \iota(\det(B)^{-1}),\ \det(B)\,)$.

(3) Ist $K = \mathbb{F}_q$ ein endlicher Körper der Ordnung q, so gilt

$$\sharp\,\mathrm{GL}_n\,\mathbb{F}_q = \prod_{k=0}^{n-1}(q^n - q^k) \qquad \text{und} \qquad \sharp\,\mathrm{SL}_n\,\mathbb{F}_q = \frac{\sharp\,\mathrm{GL}_n\,\mathbb{F}_q}{q-1}.$$

Allgemeine und spezielle lineare Gruppe

☺ Dieser Satz L3F zur allgemeinen und speziellen linearen Gruppe entspricht Satz L1Q zur symmetrischen und alternierenden Gruppe.

Aufgabe: Weisen Sie die Aussagen dieses Satzes sorgfältig nach! Alle Daten liegen explizit vor, es genügt geduldiges Nachrechnen.

Lösung: (0) Die Determinante ist ein Monoidhomomorphismus (L2N) $\det_K^n : (K^{n\times n}, \cdot, 1_{n\times n}) \to (K, \cdot, 1)$. Durch Einschränkung erhalten wir den Gruppenhomomorphismus $\det_K^n : (\mathrm{GL}_n(K), \cdot, 1_{n\times n}) \to (K^\times, \cdot, 1)$.

(1) Die Abbildung $\iota : (K, \cdot, 1) \hookrightarrow (K^{n\times n}, \cdot, 1_{n\times n}) : s \mapsto \mathrm{diag}(s, 1, \ldots, 1)$ ist ein Monoidhomomorphismus. Durch Einschränkung erhalten wir den Gruppenhomomorphismus $\iota : (K^\times, \cdot, 1) \to (\mathrm{GL}_n(K), \cdot, 1_{n\times n})$.

Dabei gilt $\det_K^n \circ \iota = \mathrm{id}$, denn $\det_K^n(\iota(s)) = s$ für alle $s \in K$ dank L2V. Insbesondere ist $\det_K^n$ surjektiv und ι injektiv. (Letzteres war klar.) Der Kern von $\det_K^n$ ist $\mathrm{SL}_n(K)$, also ist die Sequenz (0) exakt.

Allgemeine und spezielle lineare Gruppe

(2) Die Abbildungen φ und ψ sind explizit gegeben.

(2a) Nach Konstruktion gilt $\psi \circ \varphi = \mathrm{id}$, denn wir haben

$$(A, s) \mapsto B = A \cdot \iota(s) \mapsto (\, B \cdot \iota(\det(B)^{-1}),\ \det(B)\,) = (A, s).$$

Hierzu nutzen wird die Multiplikativität L2N der Determinante:

$$\det(B) = \det(A \cdot \iota(s)) = \det(A) \cdot \det(\iota(s)) = 1 \cdot s = s$$

(2b) Ebenso gilt $\varphi \circ \psi = \mathrm{id}$, denn wir haben

$$B \mapsto (\, B \cdot \iota(\det(B)^{-1}),\ \det(B)\,) \mapsto B \cdot \iota(\det(B)^{-1}) \cdot \iota(\det(B)) = B$$

Somit ist $(\varphi, \psi) : \mathrm{SL}_n(K) \times K^\times \cong \mathrm{GL}_n(K)$ ein Bijektionspaar.

⚠ Warnung: Das Bijektionspaar (φ, ψ) ist i.A. kein Isomorphismus! Die koordinatenweise Multiplikation auf dem kartesischen Produkt $\mathrm{SL}_n(K) \times K^\times$ entspricht nicht der Matrixmultiplikation in $\mathrm{GL}_n(K)$. Diese grundlegende Beobachtung führen wir in (2c) kurz aus.

Allgemeine und spezielle lineare Gruppe

(2c) Ist die Gruppe $K^\times$ nicht trivial, so existiert $s \in K^\times \smallsetminus \{1\}$.
Wir betrachten dann das folgende Gegenbeispiel zur Multiplikativität:

$$S = \iota(s) = \begin{bmatrix} s & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad SA = \begin{bmatrix} 0 & -s \\ 1 & 0 \end{bmatrix}, \quad AS = \begin{bmatrix} 0 & -1 \\ s & 0 \end{bmatrix}.$$

Also sind $\varphi((1, s) \cdot (A, 1)) = AS$ und $\varphi(1, s) \cdot \varphi(A, 1) = SA$ verschieden!

☺ Die richtige Gruppenstruktur auf $\mathrm{SL}_n(K) \times \iota(K^\times)$ ist hier also nicht das direkte Produkt, sondern ein sogenanntes semidirektes Produkt:

$$\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes \iota(K^\times)$$

Mehr hierzu lernen Sie in der Algebra / Gruppentheorie.

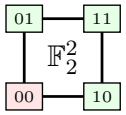
(3) Aus der Bijektion (2) folgt für die Gruppenordnungen:

$$\sharp\,\mathrm{GL}_n(K) = \sharp\,\mathrm{SL}_n(K) \cdot \sharp K^\times$$

Speziell für jeden endlichen Körper $K = \mathbb{F}_q$ wissen wir $\sharp K^\times = q - 1$ und kennen zudem die Gruppenordnung $\sharp\,\mathrm{GL}_n(K)$ aus Satz J2H.

Beispiele zu linearen Gruppen

Aufgabe: (1) Wie viele Elemente haben die Gruppen $\mathrm{GL}_2\,\mathbb{F}_2$ und S_3?
(2) Sind diese beiden Gruppen isomorph?



Lösung: (1) Wir finden $\sharp\,\mathrm{GL}_2\,\mathbb{F}_2 = 3 \cdot 2$ (J2H) und $\sharp\,\mathrm{S}_3 = 3!$ (E2H).

(2) Wir nutzen die Abbildung $f : \mathrm{GL}_n(K) \to \mathrm{Sym}(K^n \smallsetminus \{0\}) : A \mapsto f_A$. Sie ist ein Gruppenhomomorphismus (K1K) und zudem injektiv (K1E).

Speziell für $n = 2$ und $K = \mathbb{F}_2$ ist f bijektiv dank Elementezahl (E1H). Somit ist $f : \mathrm{GL}_2\,\mathbb{F}_2 \xrightarrow{\sim} \mathrm{Sym}(\mathbb{F}_2^2 \smallsetminus \{0\})$ ein Gruppenisomorphismus.

Wir wählen eine Abzählung $(\nu, \mu) : \{1, 2, 3\} \cong \mathbb{F}_2^2 \smallsetminus \{0\}$. Diese stiftet einen Gruppenisomorphismus $(\varphi, \psi) : \mathrm{S}_3 \cong \mathrm{Sym}(\mathbb{F}_2^2 \smallsetminus \{0\})$ (L1N).

☺ Zusammengefasst erhalten wir das schöne Ergebnis:

Satz L3G: $\mathrm{GL}_2\,\mathbb{F}_2 \cong \mathrm{S}_3$

Die Gruppen $\mathrm{GL}_2\,\mathbb{F}_2 = \mathrm{SL}_2\,\mathbb{F}_2$ und $\mathrm{Sym}(\mathbb{F}_2^2 \smallsetminus \{0\}) \cong \mathrm{S}_3$ sind isomorph.

Beispiele zu linearen Gruppen

Jede Matrix $A \in K^{n\times n}$ definiert ihre zugehörige lineare Abbildung $f_A : K^n \to K^n : x \mapsto Ax$. Ist A zudem invertierbar, so ist f_A bijektiv, also eine Permutation der Menge K^n. Die Null wird dabei immer fest gehalten, wir können sie daher sofort aus der Menge K^n entfernen.

Genau diese Zuordnung $f : \mathrm{GL}_n(K) \to \mathrm{Sym}(K^n \smallsetminus \{0\}) : A \mapsto A$ nutzen wir hier. Dieser der Konstruktion ist natürlich, ohne willkürliche Wahlen. Der letzte Teil $\mathrm{Sym}(\mathbb{F}_2^2 \smallsetminus \{0\}) \cong \mathrm{S}_3$ gelingt auch leicht, doch hier müssen wir willkürliche Wahlen treffen, nämlich die Menge $\mathbb{F}_2^2 \smallsetminus \{0\}$ abzählen.

☺ Der Satz ist in gewisser Weise ein „numerischer Zufall“ aus dem die genannte Isomorphie folgt: Die ganz kleinen Elementezahlen lassen einfach keinen Platz und erzwingen so die Isomorphie.

Bemerkung: Für den Körper $K = \mathbb{F}_2$ gilt $\mathrm{GL}_n\,\mathbb{F}_2 = \mathrm{SL}_n\,\mathbb{F}_2$.
Auch für den Polynomring $K = \mathbb{F}_2[X]$ über $\mathbb{F}_2$ gilt $K^\times = \{1\}$.
Somit haben wir auch hier die Gleichheit $\mathrm{GL}_n(K) = \mathrm{SL}_n(K)$.

Beispiele zu linearen Gruppen

Aufgabe: Wie viele Elemente hat der Matrixring $\mathbb{F}_3^{2\times 2}$ sowie darin die allgemeine lineare Gruppe $\mathrm{GL}_2\,\mathbb{F}_3$ und die spezielle $\mathrm{SL}_2\,\mathbb{F}_3$?

Lösung: Dank unserer Vorbereitung L3F ist die Rechnung leicht:

$$\begin{array}{lllll} \sharp\mathbb{F}_3^{2\times 2} &= 3^4 & & = 81 \\ \sharp\,\mathrm{GL}_2\,\mathbb{F}_3 &= (3^2-1)(3^2-3) &= 8\cdot 6 &= 48 \\ \sharp\,\mathrm{SL}_2\,\mathbb{F}_3 &= \sharp\,\mathrm{GL}_2\,\mathbb{F}_3/\sharp\,\mathbb{F}_3^\times &= 48/2 &= 24 \end{array}$$

☺ Zur Interpretation als Wahrscheinlichkeiten siehe J218.

Bemerkung: Die Gruppen $\mathrm{SL}_2\,\mathbb{F}_3$ und S_4 haben dieselbe Ordnung, sind aber nicht isomorph: Das Zentrum von $\mathrm{GL}_2\,\mathbb{F}_3$ ist $Z(\mathrm{SL}_2\,\mathbb{F}_3) = \{\pm E\}$. Die symmetrische Gruppe hat triviales Zentrum, $Z(\mathrm{S}_4) = \{\mathrm{id}\}$.

Für die Struktur der Gruppe ist ihre Elementezahl der erste Schritt, aber im Allgemeinen noch lange nicht ausreichend für Isomorphie. Die Quotientengruppe $\mathrm{PSL}_2\,\mathbb{F}_3 := \mathrm{SL}_2\,\mathbb{F}_3/Z(\mathrm{SL}_2\,\mathbb{F}_3)$ ist isomorph zu A_4.

Beispiele zu linearen Gruppen

Aufgabe: Wie viele Elemente hat der Matrixring $\mathbb{F}_5^{2\times 2}$ sowie darin die allgemeine lineare Gruppe $\mathrm{GL}_2\,\mathbb{F}_5$ und die spezielle $\mathrm{SL}_2\,\mathbb{F}_5$?

Lösung: Dank unserer Vorbereitung L3F ist die Rechnung leicht:

$$\begin{array}{lllll} \sharp\mathbb{F}_5^{2\times 2} &= 5^4 & & = 625 \\ \sharp\,\mathrm{GL}_2\,\mathbb{F}_5 &= (5^2-1)(5^2-5) &= 24\cdot 20 &= 480 \\ \sharp\,\mathrm{SL}_2\,\mathbb{F}_5 &= \sharp\,\mathrm{GL}_2\,\mathbb{F}_5/\sharp\,\mathbb{F}_5^\times &= 480/4 &= 120 \end{array}$$

☺ Zur Interpretation als Wahrscheinlichkeiten siehe J218.

Bemerkung: Das Zentrum $Z(\mathrm{SL}_2\,\mathbb{F}_5)$ besteht aus den beiden Matrizen $\pm E$. Die Quotientengruppe $\mathrm{PSL}_2\,\mathbb{F}_5 := \mathrm{SL}_2\,\mathbb{F}_5/Z(\mathrm{SL}_2\,\mathbb{F}_5)$ hat demnach 60 Elemente. Die alternierende Gruppe A_5 hat ebenfalls 60 Elemente.

Hier kommt es zu einem weiteren erstaunlichen Zusammentreffen: Diese beiden Gruppen sind isomorph, es gilt also $\mathrm{PSL}_2\,\mathbb{F}_5 \cong \mathrm{A}_5$. Mehr hierzu lernen Sie in der Algebra / Gruppentheorie.

Euklidischer Algorithmus und $\mathrm{SL}_2(\mathbb{Z})$

Beispiel: Über dem Ring $\mathbb{Z}$ der ganzen Zahlen haben wir

$$\mathrm{GL}_2\,\mathbb{Z} \overset{\text{L2T}}{=} \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathbb{Z}^{2\times 2} \;\middle|\; ad-bc = \pm 1 \right\},$$

$$\mathrm{SL}_2\,\mathbb{Z} \overset{\text{L3E}}{=} \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathbb{Z}^{2\times 2} \;\middle|\; ad-bc = +1 \right\}.$$

Hierin betrachten wir zwei Transvektionen und eine Skalierung:

$$X = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Satz L3H: Erzeuger für $\mathrm{SL}_2\,\mathbb{Z}$ und $\mathrm{GL}_2\,\mathbb{Z}$

Es gilt $\mathrm{SL}_2\,\mathbb{Z} = \langle\, X, Y \,\rangle$ und $\mathrm{GL}_2\,\mathbb{Z} = \langle\, X, Y, Z \,\rangle$.

Beweis: Die Gleichung $ad - bc = \pm 1$ bedeutet $\mathrm{ggT}(a,b) = 1$ (A2I).
Mit den Zeilenoperationen $X^{\pm 1}$ und $Y^{\pm 1}$ führen wir den euklidischen Algorithmus auf der ersten Spalte aus, bis wir E oder Z erreichen. QED

Euklidischer Algorithmus und $\mathrm{SL}_2(\mathbb{Z})$

Aufgabe: (0) Liegt die Matrix $M = \left[\begin{smallmatrix} 29 & -8 \\ 11 & -3 \end{smallmatrix}\right]$ in der Gruppe $\mathrm{SL}_2\,\mathbb{Z}$?
(1) Schreiben Sie M als ein Produkt über $X = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ und $Y = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.
(2) Erfinden und lösen Sie selbst weitere Zahlenbeispiele dieser Art.
(3) Formulieren Sie Ihr Vorgehen als Algorithmus mit Induktionsbeweis.

Lösung: (0) Ja, denn $\det M = 29 \cdot (-3) - 11 \cdot (-8) = -87 + 88 = 1$.
(1) Wir nutzen $X^{\pm}$ und $Y^{\pm}$ als Zeilenoperationen (Operation von links) und wenden den euklidischen Algorithmus auf die erste Spalte an.

$$M = \begin{bmatrix} 29 & -8 \\ 11 & -3 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 18 & -5 \\ 11 & -3 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 7 & -2 \\ 11 & -3 \end{bmatrix} \xrightarrow{X^-} \begin{bmatrix} 7 & -2 \\ 4 & -1 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 3 & -1 \\ 4 & -1 \end{bmatrix}$$

$$\xrightarrow{X^-} \begin{bmatrix} 3 & -1 \\ 1 & 0 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix} \xrightarrow{Y^-} \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \xrightarrow{X^-} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \xrightarrow{Y^+} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E$$

Zusammenfassend erhalten wir $E = YX^{-1}Y^{-2}X^{-1}Y^{-1}X^{-1}Y^{-2}M$,
und daraus die ersehnte Produktdarstellung $M = Y^2XYXY^2XY^{-1}$.

Euklidischer Algorithmus und $\mathrm{SL}_2(\mathbb{Z})$

Wir konzentrieren uns hier (etwas willkürlich) auf die erste Spalte (a,b) und führen darauf den euklidischen Algorithmus A2H aus. Im Beispiel führe ich dies in Zeitlupe vor. Wenn wir gleich das k–Fache addieren möchten, so nutzen wir bequem die Potenzen X^k bzw. Y^k für $k \in \mathbb{Z}$.

Die zweite Spalte (c,d) erfüllt $ad - bc = 1$, dies sind also (bis auf die Vorzeichen) die zu (a,b) gehörigen Bézout–Koeffizienten, die wir mit denselben Operationen mitführen. Bitte schauen Sie sich hierzu nochmal Satz A2I und den Algorithmus von Euklid–Bézout an.

🙂 Wir können mit Fug und Recht sagen: Die Arithmetik der Gruppe $\mathrm{SL}_2\,\mathbb{Z}$ entspricht dem guten alten euklidischen Algorithmus über $\mathbb{Z}$ – in der besonders bequemen und effizienten Matrixschreibweise.

Euklidischer Algorithmus und $\mathrm{SL}_2(\mathbb{Z})$

Aufgabe: (0) Ist die Matrix $M = \left[\begin{smallmatrix} 31 & -5 \\ 316 & -51 \end{smallmatrix}\right]$ über $\mathbb{Z}$ invertierbar?
(1) Stellen Sie M dar als ein Produkt in den Erzeugern X, Y, Z.

Lösung: (0) Ja, es gilt $M \in \mathrm{GL}_2\,\mathbb{Z}$, denn

$$\det M = 31 \cdot (-51) - 316 \cdot (-5) = -1581 + 1580 = -1.$$

(1) Wir nutzen $X^{\pm}$ und $Y^{\pm}$ als Zeilenoperationen (Operation von links) und wenden den euklidischen Algorithmus auf die erste Spalte an.

$$M = \begin{bmatrix} 31 & -5 \\ 316 & -51 \end{bmatrix} \xrightarrow{X^{-10}} \begin{bmatrix} 31 & -5 \\ 6 & -1 \end{bmatrix} \xrightarrow{Y^{-5}} \begin{bmatrix} 1 & 0 \\ 6 & -1 \end{bmatrix} \xrightarrow{X^{-6}} \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} = Z$$

Zusammenfassend erhalten wir $Z = X^{-6}Y^{-5}X^{-10}M$,
und daraus die ersehnte Produktdarstellung $M = X^{10}Y^5X^6Z$.

Erzeuger für die Gruppen $\mathrm{GL}_n(K)$ und $\mathrm{SL}_n(K)$

Satz L3I: Transvektionen erzeugen $\mathrm{SL}_n(K)$.

Sei K ein Körper und $n \in \mathbb{N}_{\geq 2}$. (1) Die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$ wird erzeugt von den Transvektionen und Skalierungen:

$$\mathrm{GL}_n(K) = \left\langle\, T_{ij}(\lambda),\ S_i(\mu) \;\middle|\; i \neq j,\ \lambda \in K,\ \mu \in K^\times \,\right\rangle$$

(2) Genauer genügt eine einzige Skalierung, etwa $S_1(\mu)$ mit $\mu \in K^\times$.

(3) Die spezielle lineare Gruppe wird erzeugt von Transvektionen:

$$\mathrm{SL}_n(K) = \left\langle\, T_{ij}(\lambda) \;\middle|\; i \neq j,\ \lambda \in K \,\right\rangle$$

Beweis: (1) Analog zum Gauß–Algorithmus B2C können wir allein mit Zeilentransvektionen jede invertierbare Matrix $A \in \mathrm{GL}_n(K)$ überführen in $D = \mathrm{diag}(\mu_1, \mu_2, \ldots, \mu_n)$, und mit Skalierungen weiter zu $E = 1_{n\times n}$.

(2) Von D gelangen wir zu $D' = \mathrm{diag}(\mu, 1, \ldots, 1)$ mit $\mu = \mu_1\mu_2\cdots\mu_n$ allein durch Zeilen- und Spaltentransvektionen (Übung, siehe unten).

(3) Falls wir mit $\det(A) = 1$ starten, so gilt $\mu = \det(A) = 1$. (L2W). QED

Erzeuger für die Gruppen $\mathrm{GL}_n(K)$ und $\mathrm{SL}_n(K)$

Aufgabe: Überführen Sie allein mit Transvektionen

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \quad \text{in} \quad \begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix} \quad \text{wobei } a \in K^\times.$$

Lösung: Wir bezeichnen die Zeilen mit R_1, R_2, die Spalten mit C_1, C_2.

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \xrightarrow{C_2 \leftarrow C_2 + C_1 \cdot 1} \begin{bmatrix} a & a \\ 0 & b \end{bmatrix} \xrightarrow{R_2 \leftarrow R_2 + (1-b)a^{-1} \cdot R_1} \begin{bmatrix} a & a \\ 1-b & 1 \end{bmatrix} \xrightarrow{R_1 \leftarrow R_1 + (-a) \cdot R_2} \begin{bmatrix} ab & 0 \\ 1-b & 1 \end{bmatrix} \xrightarrow{C_1 \leftarrow C_1 + C_2 \cdot (b-1)} \begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix}$$

Ebenso überführen wir $\mathrm{diag}(\mu_1, \mu_2, \ldots, \mu_n)$ in $\mathrm{diag}(\mu, 1, \ldots, 1)$.

Erzeuger für die Gruppen $\mathrm{GL}_n(K)$ und $\mathrm{SL}_n(K)$

Diese Rechnung gelingt über jedem Ring K, kommutativ oder nicht. Ich habe deshalb hier umsichtig die übliche Konvention angewendet: Der Grundring operiert auf Zeilen von links und auf Spalten von rechts.

Wir dividieren hier einmal durch a, daher setzen wir $a \in K^\times$ voraus. Damit gelingen die Operationen über jedem Ring, wie hier gezeigt.

Zusammenfassend erhalten wir so die gewünschte Umformung als Operation von Transvektionen (Zeilen von links, Spalten von rechts):

$$\begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ (1-b)a^{-1} & 1 \end{bmatrix} \cdot \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ b-1 & 1 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix}$$

Somit ist $\mathrm{diag}(c, c^{-1}) \in \mathrm{SL}_2(K)$ ein Produkt von vier Transvektionen:

$$\begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -c^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c(1-c) & 1 \end{bmatrix}$$

Insbesondere sehen wir so, dass die spezielle lineare Gruppe $\mathrm{SL}_n(K)$ über jedem Körper K bereits von den Transvektionen erzeugt wird.

Erzeuger für die Gruppen $\mathrm{GL}_n(K)$ und $\mathrm{SL}_n(K)$

☺ Die Arithmetik und die Struktur der Gruppen $\mathrm{SL}_n(K) \leq \mathrm{GL}_n(K)$ entsprechen dem guten alten Gauß–Algorithmus – in der besonders bequemen und effizienten Matrixschreibweise wie in Satz L3I erklärt.

Aussagen (1) und (2) sowie ihr Beweis gelten wörtlich genauso über jedem Divisionsring. Zu Aussage (3) benötigen wir die Determinante, denn diese liegt schon der Definition der Gruppe $\mathrm{SL}_n(K) = \ker(\det_K^n)$ zu Grunde. Die Determinante haben wir nur für kommutative Ringe!

Für einen Divisionsring R können wir nun umgekehrt vorgehen, und die spezielle lineare Gruppe über R *definieren* durch

$$\mathrm{SL}_n(R) := \left\langle\, T_{ij}(\lambda) \;\middle|\; i \neq j,\ \lambda \in R \,\right\rangle.$$

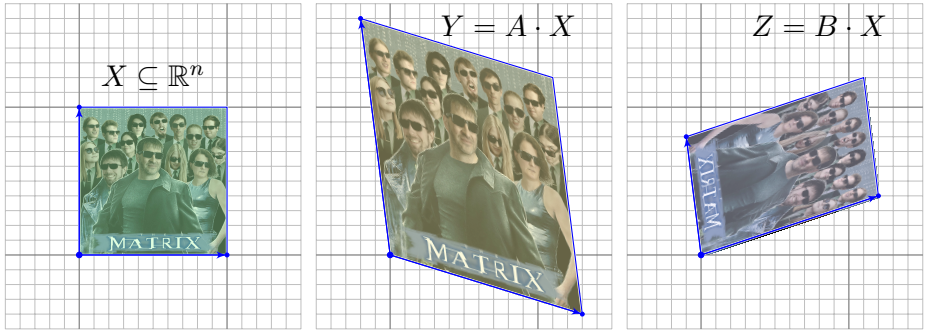
Diese Definition kommt demnach ganz ohne die Determinante aus. Im kommutativen Falle, also über jedem Körper, stimmt diese Setzung mit unserer vorigen Definition L3E überein. Wir können Satz L3I also auch so lesen: Beide Konstruktionen führen zu derselben Gruppe!

Geometrische Motivation: Volumen und Orientierung

Aufgabe: Wie wirken die Matrizen

$$A = \begin{bmatrix} 1.3 & -0.2 \\ -0.4 & 1.6 \end{bmatrix} \quad \text{und} \quad B = \begin{bmatrix} -0.1 & 1.2 \\ 0.8 & 0.4 \end{bmatrix}$$

als Abbildungen $f_A, f_B : \mathbb{R}^2 \to \mathbb{R}^2$ auf Flächeninhalt und Orientierung?



Lösung: Wir finden $\det(f_A) = \det(A) = +2$ und $\det(f_B) = \det(B) = -1$.
Der Flächeninhalt wird von f_A verdoppelt, aber von f_B beibehalten.
Die Orientierung wird von f_A beibehalten, aber von f_B umgekehrt.

Geometrische Motivation: Volumen und Orientierung

Zum guten Abschluss dieses facettenreichen Kapitels kommen wir auf unsere ursprüngliche, geometrische Motivation zurück:

Die Determinante über $\mathbb{R}$ misst Volumen und Orientierung.

Dies wollen wir nun illustrieren und erste Anwendungen erklären.

Geometrische Motivation: Volumen und Orientierung

Die Verzerrung des geometrischen Volumens wird gemessen durch

$$v : (\mathbb{R}^{n\times n}, \cdot, 1_{n\times n}) \xrightarrow{\det} (\mathbb{R}, \cdot, 1) \xrightarrow{\text{abs}} (\mathbb{R}_{\geq 0}, \cdot, 1) : A \mapsto |\det(A)|,$$
$$(\mathrm{GL}_n \mathbb{R}, \cdot, 1_{n\times n}) \xrightarrow{\det} (\mathbb{R}^\times, \cdot, 1) \xrightarrow{\text{abs}} (\mathbb{R}_{>0}, \cdot, 1).$$

Der Kern des Gruppenhomomorphismus v ist

$$\mathrm{SL}_n^{\pm}(\mathbb{R}) := \ker(v) = \{\, A \in \mathbb{R}^{n\times n} \mid \det(A) = \pm 1 \,\}.$$

Das Orientierungsverhalten wird gemessen durch

$$\text{sign} : (\mathbb{R}^{n\times n}, \cdot, 1_{n\times n}) \xrightarrow{\det} (\mathbb{R}, \cdot, 1) \xrightarrow{\text{sign}} (\{\pm 1, 0\}, \cdot, 1),$$
$$(\mathrm{GL}_n \mathbb{R}, \cdot, 1_{n\times n}) \xrightarrow{\det} (\mathbb{R}^\times, \cdot, 1) \xrightarrow{\text{sign}} (\{\pm 1\}, \cdot, 1).$$

Dies zerlegt die Gruppe $\mathrm{GL}_n(\mathbb{R})$ in zwei Klassen:

$$\mathrm{GL}_n^+(\mathbb{R}) := \ker(\text{sign}) = \{\, A \in \mathbb{R}^{n\times n} \mid \det(A) > 0 \,\},$$
$$\mathrm{GL}_n^-(\mathbb{R}) := \{\, A \in \mathbb{R}^{n\times n} \mid \det(A) < 0 \,\}.$$

Geometrische Motivation: Volumen und Orientierung

Beispiele: Wir haben oben $A \in \mathrm{GL}_n^+(\mathbb{R})$ und $B \in \mathrm{GL}_n^-(\mathbb{R})$ gesehen.
Zu $\mathrm{GL}_n^+(\mathbb{R})$ gehören alle Drehungen (vorerst nur anschaulich).
Zu $\mathrm{GL}_n^-(\mathbb{R})$ gehören alle Spiegelungen (vorerst nur anschaulich).

Was ist eine Orientierung des Raumes $\mathbb{R}^n$? Wie stellen wir fest, ob ein Automorphismus $f : \mathbb{R}^n \xrightarrow{\sim} \mathbb{R}^n$ die Orientierung erhält oder umkehrt? Bemerkenswerterweise ist die zweite Frage leichter als die erste!

Ist V ein $\mathbb{R}$–linearer Raum endlicher Dimension, so setzen wir:

$$\mathrm{GL}^+(V) := \{\, f : V \to V \mid \det_V(f) > 0 \,\}$$
$$\mathrm{GL}^-(V) := \{\, f : V \to V \mid \det_V(f) < 0 \,\}$$

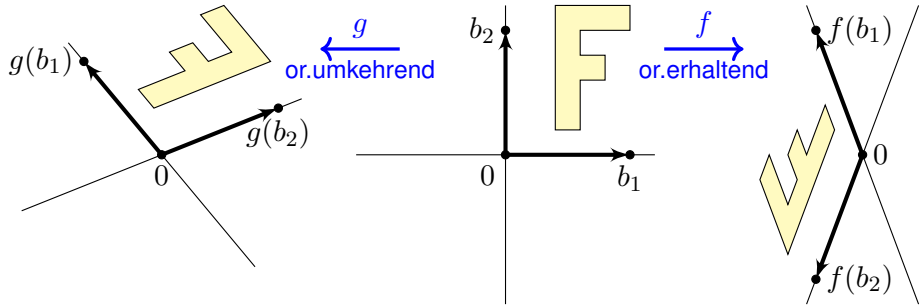
Jeder Automorphismus $f \in \mathrm{GL}^+(V)$ heißt **orientierungserhaltend**.
Jeder Automorphismus $f \in \mathrm{GL}^-(V)$ heißt **orientierungsumkehrend**.

Hierbei sind $\mathrm{GL}_n^+(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$ und $\mathrm{GL}^+(V) \leq \mathrm{GL}(V)$ Untergruppen, nicht jedoch $\mathrm{GL}_n^-(\mathbb{R})$ und $\mathrm{GL}^-(V)$: Letztere sind nicht abgeschlossen unter Multiplikation, und sie enthalten auch nicht das Einselement.

Wie orientieren wir einen $\mathbb{R}$–Vektorraum?

L345

Wir haben nun erklärt, wann eine $\mathbb{R}$–lineare Abbildung $f : V \to V$ „die Orientierung erhält“ oder aber „die Orientierung umkehrt“.
Dabei haben wir noch nicht definiert, was eine Orientierung ist.
Das ist kein Versehen, sondern die logisch richtige Reihenfolge!



Beispiel: Die reelle Gerade $\mathbb{R}$ wird orientiert durch ihre Ordnung $\leq$.
Wie orientieren wir die Ebene $\mathbb{R}^2$? oder den Raum $\mathbb{R}^3$? oder $\mathbb{R}^n$?
Allgemein einen $\mathbb{R}$–Vektorraum V endlicher Dimension?

Wie orientieren wir einen $\mathbb{R}$–Vektorraum?

L346
Erläuterung

Was eine **Orientierung** des Raums $\mathbb{R}^n$ oder V allgemein sein soll, ist zunächst keineswegs offensichtlich. Es erfordert Scharfsinn!

Geometrische Sichtweise im $\mathbb{R}^n$: Zwei Basen $\mathcal{B} = (b_1, \ldots, b_n)$ und $\mathcal{B}' = (b'_1, \ldots, b'_n)$ des $\mathbb{R}^n$ sind **orientierungsäquivalent**, wenn es einen Weg $\gamma : [0,1] \to \mathrm{GL}_n \mathbb{R}$ von $\mathcal{B}$ nach $\mathcal{B}'$ gibt: Die Spalten von $\gamma(t)$ sind zu jedem Zeitpunkt $t \in [0,1]$ eine Basis des $\mathbb{R}^n$ und deformieren $\mathcal{B}$ in $\mathcal{B}'$.

Algebraische Sichtweise: In Satz L3L zeigen wir folgende Äquivalenz: Dies ist genau dann möglich, wenn die Basiswechselmatrix $A \in \mathbb{R}^{n\times n}$ von $\mathcal{B}$ nach $\mathcal{B}'$ eine **positive Determinante** hat, also $\det A > 0$ erfüllt. Diese algebraische Eigenschaft erheben wir nun zur Definition L3J.

Pragmatische Sichtweise: Wir benötigen ein Entscheidungsverfahren. Eine **Orientierung** sagt jeder Basis, ob sie positiv oder negativ ist, wobei orientierungsäquivalente Basen denselben Wert bekommen und orientierungsumgekehrte Basen entgegengesetzte Werte.

Orientierungen eines $\mathbb{R}$–Vektorraums

L347

Definition L3J: Orientierungen eines $\mathbb{R}$–Vektorraums

Zwei Basen $\mathcal{B} = (b_1, \ldots, b_n)$ und $\mathcal{B}' = (b'_1, \ldots, b'_n)$ eines $\mathbb{R}$–Vektorraums V nennen wir **orientierungsäquivalent**, wenn die Basiswechselmatrix $A \in \mathbb{R}^{n\times n}$, definiert durch $b_j = \sum_{i=1}^n b'_i a_{ij}$, positive Determinante hat.
Das ist eine Äquivalenzrelation: reflexiv, symmetrisch, transitiv. (Übung!)

Die Äquivalenzklasse $[\mathcal{B}]$ der Basis $\mathcal{B}$ nennen wir eine **Orientierung** auf V, und das Paar $(V, [\mathcal{B}])$ einen **orientierten** $\mathbb{R}$–Vektorraum.

Es gibt genau zwei Orientierungen auf V: neben $[\mathcal{B}] = [b_1, b_2, \ldots, b_n]$ die umgekehrte Orientierung $-[\mathcal{B}] = [-b_1, b_2, \ldots, b_n] = [b_2, b_1, \ldots, b_n]$.

Jeder $\mathbb{R}$–Isomorphismus $h : V \xrightarrow{\sim} V'$ transportiert die Orientierung $[\mathcal{B}] = [b_1, \ldots, b_n]$ auf V zu $h_*([\mathcal{B}]) = [h(b_1), \ldots, h(b_n)]$ auf V'.

Ein $\mathbb{R}$–linearer Isomorphismus $h : (V, [\mathcal{B}]) \xrightarrow{\sim} (V', [\mathcal{B}'])$ orientierter Vektorräume heißt **orientierungserhaltend**, falls $h_*([\mathcal{B}]) = [\mathcal{B}']$ gilt, und andernfalls **orientierungsumkehrend**, falls $h_*([\mathcal{B}]) = -[\mathcal{B}']$ gilt.

Orientierungen eines $\mathbb{R}$–Vektorraums

L348
Erläuterung

Beachten Sie das raffinierte Vorgehen, es ist logisch korrekt!
Reflexivität, Symmetrie und Transitivität folgen aus der Definition K2L des Basiswechsels und der Multiplikativität L2N der Determinante.

Diese Definition teilt die Basen von V in genau zwei Klassen:
Es gibt genau zwei Orientierungen, „die eine“ und „die andere“.
Beide sind unterschieden, wie oben erklärt, aber gleichberechtigt.

Dimension $n = 0$ ist hierbei (technisch bedingt) eine Ausnahme.

Wenn Sie einen $\mathbb{R}$–Vektorraum V orientieren wollen, dann müssen Sie explizit angeben, welche der beiden Orientierungen Sie auswählen.
Dimension $n = 1$ ist klar. Der erste interessante Fall ist $n = 2$.
Ich nehme daher meist stillschweigend $n \geq 2$ an.

Ein $\mathbb{R}$–linearer Automorphismus $f : V \xrightarrow{\sim} V$ ist orientierungserhaltend, falls $f([\mathcal{B}]) = [\mathcal{B}]$ gilt, und orientierungsumkehrend, falls $f([\mathcal{B}]) = -[\mathcal{B}]$.

🙂 Dies ist unabhängig von der Basiswahl und gleichbedeutend damit, dass die darstellende Matrix $A \in \mathbb{R}^{n\times n}$ positive / negative Determinante hat. Wir erhalten also die eingangs formulierte Vorzeichenregel.

Orientierungen des Koordinatenraums $\mathbb{R}^n$

Besonders einfach und vertraut ist der Koordinatenraum $\mathbb{R}^n$:

Beispiel: Der Koordinatenraum $\mathbb{R}^n$ kommt mit seiner **Standardbasis**

$$\mathcal{E} = (e_1, \dots, e_n).$$

Diese definiert auf $\mathbb{R}^n$ die **Standardorientierung**

$$[\mathcal{E}] = [e_1, \dots, e_n].$$

Jede Basis $\mathcal{B} = (b_1, \dots, b_n)$ des $\mathbb{R}^n$ ist gleich oder entgegengesetzt zu $\mathcal{E}$ orientiert, also „rechtshändig“ $[\mathcal{B}] = [\mathcal{E}]$ oder „linkshändig“ $[\mathcal{B}] = -[\mathcal{E}]$.

Für $n = 1$ ist $[e_1]$ die übliche, positive Orientierung von $(\mathbb{R}, \leq)$, entgegengesetzt ist die negative Orientierung $-[e_1] = [-e_1]$.
Die Standardorientierung $[e_1, e_2]$ auf $\mathbb{R}^2$ und $[e_1, e_2, e_3]$ auf $\mathbb{R}^3$ stellen wir anschaulich durch eine Rechte-Hand-Regel dar.

Anschaulich: Die Basis $\mathcal{B}$ lässt sich stetig in $\mathcal{E}$ überführen oder nicht.
Genauer: $\mathrm{GL}_n \mathbb{R}$ hat zwei Wegkomponenten, $\mathrm{GL}_n^+ \mathbb{R}$ und $\mathrm{GL}_n^- \mathbb{R}$.

Orientierungen des Koordinatenraums $\mathbb{R}^n$

Ich betone nachdrücklich, dass „rechtshändig“ und „linkshändig“ keine absoluten Begriffe sind, sondern immer nur relativ zu einer gewählten Referenzbasis; hier ist dies die Standardbasis $\mathcal{E}$ des Raums $\mathbb{R}^n$, oder allgemein eine ausgezeichnete Basis $\mathcal{B}$ von V über $\mathbb{R}$.

Jeder Mensch, der schon einmal über seine Hände nachgedacht hat, wird feststellen: Beide sind eigentlich gleich, und doch auf subtile Weise verschieden. Sie sehen nun den mathematischen Grund: Der Übergang von „links“ nach „rechts“ führt über eine negative Basiswechselmatrix.

Zunächst sind beide Hände gleich gut geeignet. Wir wählen (willkürlich) eine davon als Referenz, die andere ist dann dazu entgegengesetzt. Die Natur hat uns einen Repräsentanten jeder Klasse mitgegeben! Daher sind unsere Hände sehr hilfreich für unsere Anschauung.

Als allgemeine, mathematische Erklärung taugt unsere vage Anschauung jedoch nicht; dafür haben wir die Definition L3J.

Orientierungen eines $\mathbb{R}$–Vektorraums

Beispiel: Wie orientieren Sie folgenden Untervektorraum $U \leq \mathbb{R}^4$?

$$U = \{\, x \in \mathbb{R}^4 \mid x_1 + x_2 + x_3 + x_4 = 0 \,\}$$

Wie immer gibt es zwei Orientierungen, keine ist schöner als die andere.
Es gilt $\dim_{\mathbb{R}}(U) = 3$, also $U \cong \mathbb{R}^3$, doch die Wahl eines Isomorphismus ist nicht eindeutig oder kanonisch. Wir müssen willkürlich eine Basis $\mathcal{B} = (b_1, b_2, b_3)$ *wählen*, um eine Orientierung $[\mathcal{B}]$ auf U zu *vereinbaren*.

Beispiel: Wie orientieren Sie folgenden Untervektorraum $V \leq \mathbb{R}^{\mathbb{R}}$?

$$V = \langle\, 1, \cos, \sin \,\rangle_{\mathbb{R}}^{!}$$

Die beiden möglichen Orientierungen sind

$$[1, \cos, \sin] = [\cos, \sin, 1] = \dots \quad \text{und} \quad [1, \sin, \cos] = [\cos, 1, \sin] = \dots.$$

Beide Orientierungen sind verschieden, doch a priori gleichberechtigt.
Kurzum: Die Orientierung $[\mathcal{B}]$ auf V ist eine zusätzliche Struktur!

Orientierungen eines $\mathbb{R}$–Vektorraums

Für den Koordinatenraum $\mathbb{R}^n$ scheint alles leicht und übersichtlich. Doch es gibt viele weitere $\mathbb{R}$–Vektorräume, nicht nur den $\mathbb{R}^n$.

Ich wähle bewusst knifflige Beispiele $U \leq \mathbb{R}^4$ und $V \leq \mathbb{R}^{\mathbb{R}}$, um vom $\mathbb{R}^n$ wegzukommen, denn da drängt sich die Standardbasis allzu sehr auf. Für U und V haben wir keine „kanonische“ Basis oder Orientierung.

Wenn Sie einen $\mathbb{R}$–Vektorraum V orientieren wollen, dann müssen Sie explizit angeben, welche der beiden Orientierungen Sie auswählen. Die Orientierung $[\mathcal{B}]$ auf V ist nicht etwa „naturgegeben“, sondern eine zusätzliche Struktur, ein weiteres Datum, eine ergänzende Information.

Orientierungsverhalten eines Automorphismus

Aufgabe: Ist die Ableitung $\partial : V \to V$ auf $V = \langle \cos, \sin \rangle_{\mathbb{R}}^{!}$ orientierungserhaltend oder orientierungsumkehrend?

Lösung: Wir berechnen die Determinante $\det(\partial) \in \mathbb{R}$.
Hierzu wählen wir eine Basis von V, etwa $\mathcal{B} = (\cos, \sin)$.

$$A = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \Longrightarrow \quad \det_V(\partial) = \det_{\mathbb{R}}^2(A) = +1$$

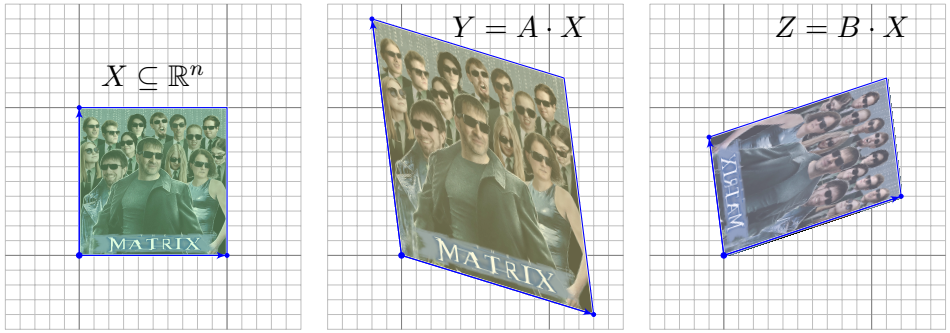
Das bedeutet, $\partial : V \to V$ ist ein Automorphismus, zudem orientierungserhaltend und volumentreu, kurz $\partial \in \mathrm{SL}(V)$.

☺ Diese Eigenschaften sind unabhängig von der Wahl der Basis! (L3D)

Orientierungsverhalten eines Automorphismus

Determinante: Volumen und Orientierung

Die Determinante ist geometrisch motiviert als orientiertes Volumen. Dies hat uns direkt zur algebraischen Definition geführt: multilinear, alternierend, normiert. Daraus haben wir eine Fülle phantastischer Eigenschaften abgeleitet. Schließlich kehren wir zur Geometrie zurück.



Sie verfügen nun über die nötigen mathematischen Werkzeuge, sowohl die theoretischen Grundlagen als auch praktische Verfahren.

Auf unserem Weg der präzisen Ausarbeitung hat sich wunderschöne Mathematik entfaltet, die Sie fortan gewinnbringend anwenden können.

Determinante: Volumen und Orientierung

Die Gruppen $\mathrm{GL}_n^+(\mathbb{R})$ und $\mathrm{GL}_n(\mathbb{R})$

Satz L3K: die Gruppe $\mathrm{GL}_n^+(\mathbb{R})$

(0) Die Determinante definiert eine kurze exakte Sequenz von Gruppen:

$$1 \longrightarrow \mathrm{SL}_n(\mathbb{R}) \xrightarrow{\text{inc}} \mathrm{GL}_n^+(\mathbb{R}) \underset{\iota}{\overset{\det}{\rightleftarrows}} \mathbb{R}_{>0} \longrightarrow 1$$

Zudem haben wir $\iota : \mathbb{R}_{>0} \hookrightarrow \mathrm{GL}_n^+(\mathbb{R}) : \mu \mapsto \mathrm{diag}(\mu, 1, \ldots, 1)$ wie in L3F.

(1) Die positive lineare Gruppe $\mathrm{GL}_n^+(\mathbb{R})$ wird erzeugt von den Transvektionen und den positiven Skalierungen:

$$\mathrm{GL}_n^+(\mathbb{R}) = \left\langle\, T_{ij}(\lambda),\ S_i(\mu) \;\middle|\; i \neq j,\ \lambda \in \mathbb{R},\ \mu \in \mathbb{R}_{>0} \,\right\rangle$$

(2) Genauer genügt eine einzige Skalierung, etwa $S_1(\mu)$ mit $\mu \in \mathbb{R}_{>0}$.

Beweis: (1) Analog zum Gauß–Algorithmus B2C können wir allein mit Zeilentransvektionen jede invertierbare Matrix $A \in \mathrm{GL}_n(\mathbb{R})$ überführen in $\mathrm{diag}(\mu_1, \mu_2, \ldots, \mu_n)$ und dann (2) weiter zu $\mathrm{diag}(\mu, 1, \ldots, 1)$ (L3I). Falls wir mit $\det(A) > 0$ starten, so gilt $\mu = \det(A) > 0$ (L2W). QED

Die Gruppen $\mathrm{GL}_n^+(\mathbb{R})$ und $\mathrm{GL}_n(\mathbb{R})$

Ein **Weg** in $\mathrm{GL}_n(\mathbb{R})$ ist eine stetige Abbildung $\gamma : [0,1] \to \mathrm{GL}_n(\mathbb{R})$ des reellen Intervalls $[0,1]$ in den Zielraum $\mathrm{GL}_n(\mathbb{R})$. Dabei heißt $A = \gamma(0)$ der Startpunkt und $B = \gamma(1)$ der Zielpunkt von γ. Wir sagen auch, der Weg γ verläuft von A nach B, oder γ verbindet A mit B.

Satz L3L: Die Gruppe $\mathrm{GL}_n^+(\mathbb{R})$ ist wegzusammenhängend.

(1) Die positive lineare Gruppe $\mathrm{GL}_n^+(\mathbb{R})$ ist wegzusammenhängend:
Je zwei Matrizen $A, B \in \mathrm{GL}_n^+(\mathbb{R})$ lassen sich verbinden durch einen Weg $\gamma : [0,1] \to \mathrm{GL}_n^+(\mathbb{R})$ von $\gamma(0) = A$ nach $\gamma(1) = B$.

(2) Die Gruppe $\mathrm{GL}_n(\mathbb{R}) = \mathrm{GL}_n^+(\mathbb{R}) \sqcup \mathrm{GL}_n^-(\mathbb{R})$ hat zwei Komponenten:
Genau dann lassen sich $A, B \in \mathrm{GL}_n(\mathbb{R})$ verbinden durch einen Weg $\gamma : [a,b] \to \mathrm{GL}_n(\mathbb{R})$, wenn beide dasselbe Vorzeichen haben.

Beispiel: Für $n = 1$ und $\mathbb{R}^\times = \mathbb{R}_{>0} \sqcup \mathbb{R}_{<0}$ ist dies sofort plausibel. Die Anschauung trügt hier nicht! Der Zwischenwertsatz garantiert: Jede stetige Funktion $f : [a,b] \to \mathbb{R}$ nimmt jeden Wert s zwischen $f(a)$ und $f(b)$ an, das heißt, es existiert $t \in [a,b]$ mit $f(t) = s$.

Die Gruppen $\mathrm{GL}_n^+(\mathbb{R})$ und $\mathrm{GL}_n(\mathbb{R})$

Beweis: (1a) Zu jedem Erzeuger $T_{ij}(\lambda)$ und $S_i(\mu)$ in $\mathrm{GL}_n^+(\mathbb{R})$ haben wir

$$\tau : [0,1] \to \mathrm{GL}_n^+(\mathbb{R}) : t \mapsto T_{ij}(t\lambda),$$
$$\sigma : [0,1] \to \mathrm{GL}_n^+(\mathbb{R}) : t \mapsto S_i(1 + t(\mu - 1)).$$

Der Weg τ verbindet die Einheitsmatrix $\tau(0) = E$ mit $\tau(1) = T_{ij}(\lambda)$.
Der Weg σ verbindet die Einheitsmatrix $\sigma(0) = E$ mit $\sigma(1) = S_i(\mu)$.

(1b) Dank Satz L3K können wir jede Matrix $A \in \mathrm{GL}_n^+(\mathbb{R})$ darstellen als ein Produkt $A = A_1 A_2 \cdots A_\ell$ der Erzeuger $A_k \in \{\, T_{ij}(\lambda), S_i(\mu) \,\}$.
Zu jedem Index $k = 1, 2, \ldots, \ell$ haben wir wie in (1a) erklärt einen Weg $\alpha_k : [0,1] \to \mathrm{GL}_n^+(\mathbb{R})$ von $\alpha_k(0) = E$ nach $\alpha_k(1) = A_k$. Wir erhalten:

$$\alpha : [0,1] \to \mathrm{GL}_n^+(\mathbb{R}) : \alpha(t) = \alpha_1(t)\alpha_2(t)\cdots\alpha_\ell(t)$$

Diese Abbildung ist stetig, somit ein Weg von $\alpha(0) = E$ nach $\alpha(1) = A$.

🙂 Erfreulicher Nebeneffekt unserer Sorgfalt: Der so konstruierte Weg α ist eine Polynomfunktion vom Grad $\leq \ell$ in jedem Matrixeintrag.

Die Gruppen $\mathrm{GL}_n^+(\mathbb{R})$ und $\mathrm{GL}_n(\mathbb{R})$

(1c) Zu $A, B \in \mathrm{GL}_n^+(\mathbb{R})$ existieren dank (1b) Wege $\alpha, \beta : [0,1] \to \mathrm{GL}_n^+(\mathbb{R})$ von der Einheitsmatrix $\alpha(0) = \beta(0) = E$ nach $\alpha(1) = A$ bzw. $\beta(1) = B$.
Daraus erhalten wir den Weg $\gamma : [0,1] \to \mathrm{GL}_n^+(\mathbb{R}) : \gamma(t) = \alpha(1-t)\beta(t)$ von $\gamma(0) = A$ nach $\gamma(1) = B$. Damit ist Aussage (1) bewiesen.

🙂 Auch der Weg γ ist eine Polynomfunktion in jedem Matrixeintrag.

(2a) Für $A, B \in \mathrm{GL}_n^+(\mathbb{R})$ haben wir in (1) einen Weg konstruiert.

(2b) Für $A, B \in \mathrm{GL}_n^-(\mathbb{R})$ verbinden wir $S_1(-1)A$ und $S_1(-1)B$ durch γ in $\mathrm{GL}_n^+(\mathbb{R})$, somit verläuft der Weg $S_1(-1)\gamma$ in $\mathrm{GL}_n^-(\mathbb{R})$ von A nach B.

(2c) Für Matrizen $A, B \in \mathrm{GL}_n(\mathbb{R})$ mit entgegengesetzten Vorzeichen $\mathrm{sign}\, A \neq \mathrm{sign}\, B$ existiert kein Weg $\gamma : [0,1] \to \mathrm{GL}_n(\mathbb{R})$ von A nach B.
Angenommen, $\gamma : [0,1] \to \mathrm{GL}_n(\mathbb{R}) \subset \mathbb{R}^{n \times n}$ verläuft von A nach B. Da γ und $\det : \mathbb{R}^{n \times n} \to \mathbb{R}$ stetig sind, gilt dies auch für die Komposition $f = \det \circ \gamma : [0,1] \to \mathbb{R}$ mit $f(t) = \det(\gamma(t))$. Dank Zwischenwertsatz existiert $t_0 \in [0,1]$ mit $f(t_0) = 0$. Somit ist die Matrix $\gamma(t_0) \in \mathbb{R}^{n \times n}$ nicht invertierbar, ein Widerspruch. QED

Die Gruppe $\mathrm{GL}_n(\mathbb{C})$ ist wegzusammenhängend

Die Gruppe $\mathrm{GL}_1(\mathbb{R}) = \mathbb{R} \smallsetminus \{0\} = \mathbb{R}_{>0} \sqcup \mathbb{R}_{<0}$ hat zwei Komponenten.
Hierin lassen sich die Punkte ± 1 nicht durch einen Weg verbinden.

Hingegen ist die Gruppe $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C} \smallsetminus \{0\}$ wegzusammenhängend:
In der gelochten Ebene $\mathbb{C} \smallsetminus \{0\}$ können wir je zwei Punkte verbinden.

Lemma L3M: Die Gruppe $\mathbb{C}^\times$ ist wegzusammenhängend.

Seien $z_0, z_1 \in \mathbb{C}^\times$. In Polarkoordinaten haben wir $z_k = \mathrm{e}^{w_k}$ mit $w_k \in \mathbb{C}$.
Der Weg $\gamma : [0,1] \to \mathbb{C}^\times : t \mapsto \mathrm{e}^{(1-t)w_0 + tw_1}$ läuft von z_0 nach z_1.

Diese Eigenschaft hat Konsequenzen in jeder höheren Dimension:

Satz L3N: Die Gruppe $\mathrm{GL}_n(\mathbb{C})$ ist wegzusammenhängend.

Die allgemeine lineare Gruppe $\mathrm{GL}_n(\mathbb{C})$ ist wegzusammenhängend:
Je zwei invertierbare Matrizen $A, B \in \mathrm{GL}_n(\mathbb{C})$ lassen sich verbinden durch einen Weg $\gamma : [0,1] \to \mathrm{GL}_n(\mathbb{C})$ von $\gamma(0) = A$ nach $\gamma(1) = B$.

Aufgabe: Beweisen Sie diesen Satz nach dem Vorbild von $\mathrm{GL}_n^+(\mathbb{R})$.

Die Gruppe $\mathrm{GL}_n(\mathbb{C})$ ist wegzusammenhängend

Lösung: Wir nutzen Satz L3I im Spezialfall des Körpers $K = \mathbb{C}$:

$$\mathrm{GL}_n(\mathbb{C}) = \left\langle\, T_{ij}(\lambda),\ S_i(\mu) \;\middle|\; i \neq j,\ \lambda \in \mathbb{C},\ \mu \in \mathbb{C}^\times \,\right\rangle$$

(a) Zu jedem Erzeuger $T_{ij}(\lambda)$ und $S_i(\mu)$ haben wir $\mu = \mathrm{e}^w$ und somit

$$\tau : [0,1] \to \mathrm{GL}_n(\mathbb{C}) : t \mapsto T_{ij}(t\lambda),$$
$$\sigma : [0,1] \to \mathrm{GL}_n(\mathbb{C}) : t \mapsto S_i(\mathrm{e}^{tw}).$$

Der Weg τ verbindet die Einheitsmatrix $\tau(0) = E$ mit $\tau(1) = T_{ij}(\lambda)$.
Der Weg σ verbindet die Einheitsmatrix $\sigma(0) = E$ mit $\sigma(1) = S_i(\mu)$.

Ab hier verläuft der Beweis wörtlich wie (1b) und (1c) zu Satz L3L.

Bemerkung: Die Zweiteilung $\mathbb{R}^\times = \mathbb{R}_{>0} \sqcup \mathbb{R}_{<0}$ ist eine Besonderheit des Körpers $\mathbb{R}$. Sie beruht auf der vollständigen Ordnung von $\mathbb{R}$ und der so definierten Orientierung auf $\mathbb{R}$: Diese erklärt hier „links“ und „rechts“.

Daraus gewinnen wir die Zweiteilung $\mathrm{GL}_n(\mathbb{R}) = \mathrm{GL}_n^+(\mathbb{R}) \sqcup \mathrm{GL}_n^-(\mathbb{R})$ und schließlich die beiden Orientierungen des Raumes $\mathbb{R}^n$.

Die Gruppe $\mathrm{GL}_n(\mathbb{C})$ ist wegzusammenhängend

Satz L3O: Jede komplexe Nichtnullstellenmenge ist wegzshgd.

Sei $P \in \mathbb{C}[Z_1, \ldots, Z_n]$ ein Polynom, $P \neq 0$, und $f : \mathbb{C}^n \to \mathbb{C} : z \mapsto P(z)$ die zugehörige Polynomfunktion. Dann ist die Nichtnullstellenmenge $X := f^{-1}(\mathbb{C}^\times) = \{\, z \in \mathbb{C}^n \mid P(z) \neq 0 \,\}$ wegzusammenhängend.

Beweis: (1) Für $n = 1$ ist dies leicht: Zu jedem Polynom $P \in \mathbb{C}[Z] \smallsetminus \{0\}$ ist die Nullstellenmenge $f^{-1}(\{0\}) = \{\, z \in \mathbb{C} \mid P(z) = 0 \,\}$ endlich (G3K).
Das Komplement $X = \{\, z \in \mathbb{C} \mid P(z) \neq 0 \,\}$ ist wegzusammenhängend, denn je zwei Punkte in X lassen sich durch einen Weg in X verbinden.

(2) Zu $a \neq b$ in X sei $g : \mathbb{C} \to \mathbb{C}^n : z \mapsto a + z(b-a)$ die komplexe Gerade durch $g(0) = a$ und $g(1) = b$. Die Polynomfunktion $h = f \circ g : \mathbb{C} \to \mathbb{C}$ hat endlich viele Nullstellen. Darauf können wir nun (1) anwenden:
Es existiert ein Weg $\gamma : [0,1] \to \mathbb{C}$ von 0 nach 1 in $h^{-1}(\mathbb{C}^\times) \subset \mathbb{C}$.
Somit läuft der Weg $g \circ \gamma : [0,1] \to \mathbb{C}^n$ von a nach b in $f^{-1}(\mathbb{C}^\times) \subset \mathbb{C}^n$, denn zu jedem Zeitpunkt $t \in [0,1]$ gilt $f(g(\gamma(t))) = h(\gamma(t)) \neq 0$. QED

Die Gruppe $\mathrm{GL}_n(\mathbb{C})$ ist wegzusammenhängend

Warnung: Für reelle Polynome gilt Satz L3O nicht! Zum Beispiel ist die Menge $\mathbb{R} \smallsetminus \{0\} = \{\, x \in \mathbb{R} \mid x \neq 0 \,\}$ nicht wegzusammenhängend.
Auch $\mathbb{R}^2 \smallsetminus \mathbb{R} = \{\, (x,y) \in \mathbb{R}^2 \mid y \neq 0 \,\}$ ist nicht wegzusammenhängend, doch $\mathbb{R}^2 \smallsetminus \{0\} = \{\, (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \neq 0 \,\}$ ist wegzusammenhängend.
Hingegen ist das Komplement $\mathbb{R}^2 \smallsetminus \mathbb{S}^1 = \{\, (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 - 1 \neq 0 \,\}$ der Kreislinie $\mathbb{S}^1 \subset \mathbb{R}^2$ nicht wegzusammenhängend.

Aufgabe: Beweisen Sie mit dem vorigen Satz L3O erneut, dass die Gruppe $\mathrm{GL}_n(\mathbb{C})$ wegzusammenhängend ist.

Lösung: Dank der Determinante L2G haben wir die Mengengleichheit

$$\mathrm{GL}_n(\mathbb{C}) = \left\{\, A \in \mathbb{C}^{n \times n} \;\middle|\; \det A \neq 0 \,\right\}.$$

Die Determinante ist gegeben durch die explizite, polynomielle Formel

$$\det : \mathbb{C}^{n \times n} \to \mathbb{C} : A \mapsto \textstyle\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n}.$$

Dank Satz L3O ist daher die Menge $\mathrm{GL}_n(\mathbb{C})$ wegzusammenhängend.

Zusammenfassung zur Determinante

Zusammenfassung zur Determinante $\det = \det_K^n : K^{n\times n} \to K$
über einem kommutativen Ring K, etwa Integritätsring oder Körper.

Geometrische Motivation über $\mathbb{R}$: orientiertes Volumen.

Algebraische Definition L2A: multilinear, alternierend, normiert.

Hauptsatz L2G: Existenz (L2L) und Eindeutigkeit (L2M).

Eigenschaften: antisymmetrisch (L2D), $\det(P_\sigma) = \operatorname{sign}(\sigma)$ (L2E), invariant unter Transvektion (L2C) und unter Transposition (L2K), multiplikativ (L2N), Inversionsformel $A^{-1} = \det(A)^{-1} \operatorname{adj}(A)$ (L2S). Genau dann ist A invertierbar, wenn $\det A$ invertierbar ist (L2T). Cramersche Regel (L2P), $\det A = 0$ gdw $\ker(A) \neq \{0\}$ (L2Q).

Berechnung: Leibniz–Formel (L2J) und Laplace–Entwicklung (L2Z) beide mit Aufwand $n \cdot n!$, Gauß–Algorithmus (L2X) mit Aufwand n^3, dazu Determinante unter Spalten- und Zeilenoperationen (L2W), Regel für 2×2–Matrizen (L2H) und für 3×3–Matrizen (L2I), Dreiecksmatrizen und Block-Dreiecksmatrizen (L2V).

Zusammenfassung zur Determinante

Erste Anwendungen: Über jedem kommutativen Ring K mit $0 \neq 1$ ist jede invertierbare Matrix quadratisch (L3A) und daher gilt auch hier die ersehnte Invarianz der Dimension (L3C).

Auf jedem K–linearen Raum V mit endlicher Basis $\mathcal{B}$ haben wir die Determinante $\det_V : \operatorname{End}_K(V) \to K : f \mapsto \det_V(f) = \mathrm{M}_\mathcal{B}^\mathcal{B}(f)$ mit allen guten Eigenschaften der Matrixdeterminante (L3D).

Der Kern der Determinante $\det : \mathrm{GL}_n(K) \twoheadrightarrow K^\times$ ist die spezielle lineare Gruppe $\mathrm{SL}_n(K) = \ker(\det)$. Diese wird erzeugt von Transvektionen… über jedem Körper K (L3I) und auch über dem Ring $\mathbb{Z}$ (L3H).

Die allgemeine lineare Gruppe $\mathrm{GL}_n(\mathbb{R}) = \mathrm{GL}_n^+(\mathbb{R}) \sqcup \mathrm{GL}_n^-(\mathbb{R})$ über $\mathbb{R}$ zerfällt in zwei Komponenten, positiv und negativ (L3L).

Diese Zweiteilung definiert zwei Orientierungen auf dem Raum $\mathbb{R}^n$ und somit auf jedem endlich-dimensionalen $\mathbb{R}$–Vektorraum V (L3J).

Über dem Körper $\mathbb{C}$ ist die allgemeine lineare Gruppe $\mathrm{GL}_n(\mathbb{C})$ hingegen wegzusammenhängend (L3N); hier tritt diese Zweiteilung nicht auf.

Inversion quadratischer Matrizen

Wir betrachten quadratische Matrizen $A, B \in R^{n\times n}$ über einem Ring R und fragen: Folgt aus $AB = 1_{n\times n}$ bereits $BA = 1_{n\times n}$, also $B = A^{-1}$?

Aufgabe: (0) Finden Sie Gegenbeispiele! Beantworten Sie die Frage (1) für jeden Divisionsring R und (2) für jeden kommutativen Ring R.

Lösung: (0) Wir nutzen unser unvergessliches Gegenbeispiel J1O: Hierzu sei K ein Körper. Im Endomorphismenring $R = \operatorname{End}_K(K[X])$ haben wir die Elemente $a : P(X) \mapsto P(X^2)$ und $b : P(X) \mapsto XP(X^2)$ sowie $(c, d) : P \mapsto (P_0, P_1)$ mit $P = P_0(X^2) + XP_1(X^2)$, also explizit

$$a(P) = (p_0, 0, p_1, 0, p_2, 0, \dots), \qquad c(P) = (p_0, p_2, p_4, p_6, p_8, \dots),$$
$$b(P) = (0, p_0, 0, p_1, 0, p_2, \dots), \qquad d(P) = (p_1, p_3, p_5, p_7, p_9, \dots).$$

Bemerkenswerterweise gelten damit die Gleichungen

$$\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ca & cb \\ da & db \end{pmatrix} \qquad = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} ac + bd & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Inversion quadratischer Matrizen

☺ Es ist heilsam, mit Gegenbeispielen zu beginnen: Diese bewahren Sie vor dem naiven Irrglauben, die Aussage sei „klar“ oder „trivial“.

Sie sehen daran eindrücklich, dass hier wirklich etwas zu zeigen ist. So motiviert lösen wir nun die beiden wichtigsten, positiven Fälle:

(1) Über jedem Divisionsring R hilft uns der Gauß–Algorithmus!

Für jede quadratische Matrix $A \in R^{n\times n}$ gilt nämlich dank Satz B2D: A ist rechtsinvertierbar $\Leftrightarrow$ A ist linksinvertierbar $\Leftrightarrow$ A ist invertierbar. Jede Rechtsinverse zu A ist eine Linksinverse zu A und umgekehrt.

(2) Über jedem kommutativen Ring R hilft uns die Determinante!

Aus $AB = 1_{n\times n}$ folgt $1 = \det(AB) = \det(A)\det(B)$, also ist $\det(A)$ in R invertierbar. Dank Satz L2S ist die Matrix A dann in $K^{n\times n}$ invertierbar durch $A^{-1} = \det(A)^{-1} \operatorname{adj}(A)$. Aus $AB = 1_{n\times n}$ folgt also $B = A^{-1}$.

☺ Am Ende geht alles gut aus. Es bedarf jedoch eines Beweises! Genau das ist der Nutzen des mahnenden Gegenbeispiels J1O.

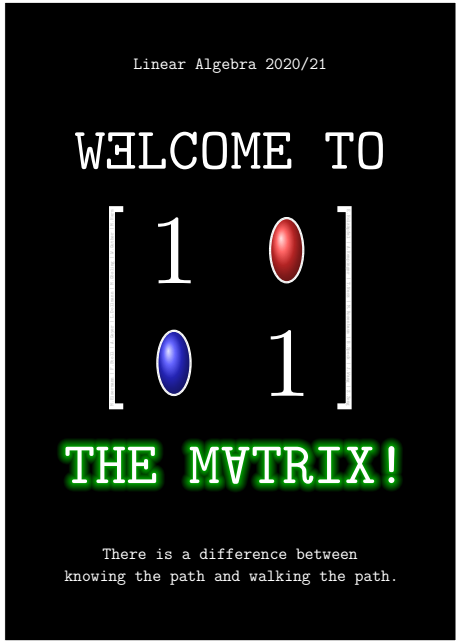
Kapitel M

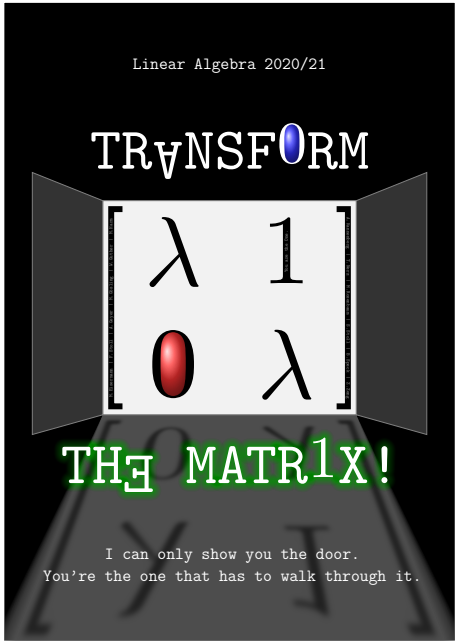
Eigenvektoren und Diagonalisierung

Live as if you were to die tomorrow.
Learn as if you were to live forever.
Mahatma Gandhi (1869–1948)

Inhalt dieses Kapitels M

Willkommen zur Fortsetzung der Linearen Algebra!

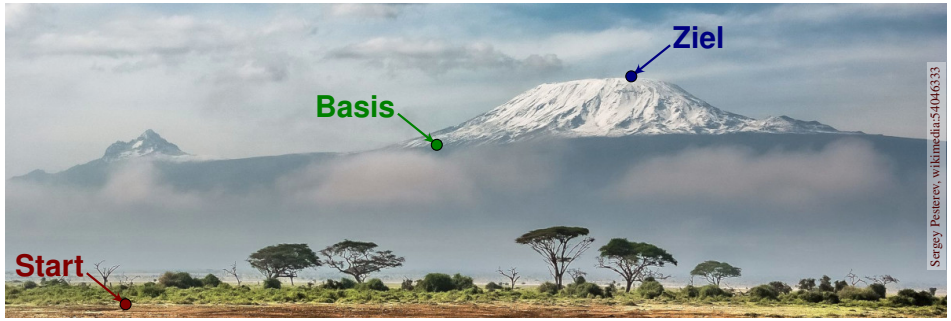




Das Ziel und der Weg

Mathematik ist schön und nützlich, zwar anstrengend doch lohnend!

Five percent of the people think; ten percent of the people think they think; and the other eighty-five percent would rather die than think.“
Thomas A. Edison (1847–1931)



„Because in the end, you won't remember the time you spent working in the office or mowing your lawn. Climb that goddamn mountain!“
Jack Kerouac (1922–1969)

Rückblick auf das Wintersemester: die Grundlagen

M005
Überblick

Mathematische Grundlagen	Algebraische Grundlagen	Lineare Strukturen
Mathematische Logik und Beweistechniken	Monoide und Gruppen	Lineare Räume und lineare Abbildungen
Mengen und Abbildungen	Ringe und Körper	Basis und Dimension
Kombinatorik und Quotienten	Polynomringe	Darstellung linearer Abbildungen durch Matrizen
Ordnungsrelationen und Kardinalität	Matrixringe	Signatur und Determinante

Ausblick auf das Sommersemester: weiterer Aufbau

M006
Überblick

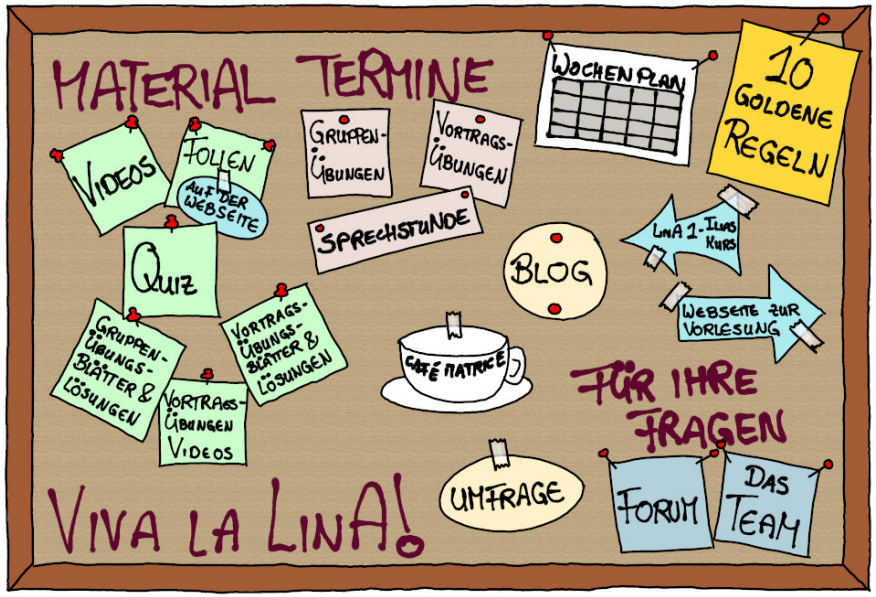
Normalformen für Endos	Bilineare Algebra	Euklidische Geometrie	Multilineare Algebra
Diagonalisierung	Bilinearformen	Skalarprodukte	Dualität
Jordanisierung	Quadriken	Spektralsatz	Tensorprodukt

Im Verlauf dieses Sommersemesters werden auch diese neuen Themen für Sie konkrete Gestalt annehmen. Weiterhin gilt: Die Mathematik ist wunderschön und nützlich, darauf dürfen Sie sich freuen!

Wo finden Sie Materialien und Unterstützung?

M007

Alle Angebote finden Sie in unserem liebevoll gestalteten Ilias-Kurs.



Ausblick auf das zweite Semester

M008

Wir unterstützen Sie auch digital bestmöglich beim Lernen.

- Lehrvideos mit Skript, ergänzend Lehrbücher
- Gut abgestimmte Vorlesung und Übungen
- Ein erfahrenes und hochmotiviertes Team

Sprechen Sie mit uns! Nutzen Sie die vielfältigen Kontaktmöglichkeiten!

Tipps zum aktiven Lernen mit Vorlesungsvideos:

- Nutzen Sie die Pausetaste. Justieren Sie Ihre Geschwindigkeit.
- Halten Sie Stift und Papier bereit. Machen Sie sich Notizen.
- Führen Sie Nebenrechnungen aus nach Ihrem Bedarf.

Studieren bereitet Freude und erfordert Disziplin!

Kanonische Darstellung einer linearen Abbildung

M101

Ziel: Wir wollen lineare Abbildungen möglichst einfach darstellen.

Sei K ein Körper und $m, n, r \in \mathbb{N}$ mit $r \leq \min\{m, n\}$.
Die **Modellmatrix** der Größe $m \times n$ vom Rang r ist

$$D = D^r_{m\times n} := \begin{bmatrix} 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} 1_{r\times r} & 0_{r\times n'} \\ 0_{m'\times r} & 0_{m'\times n'} \end{bmatrix}.$$

Die zugehörige K–lineare **Modellabbildung** ist

$$f_D : K^n \to K^m : (x_1, \ldots, x_r, \ldots, x_n) \mapsto (x_1, \ldots, x_r, 0, \ldots, 0).$$

Daran lesen wir insbesondere Bild und Kern ab:

$$\begin{aligned} \operatorname{im}(f_D) &= \operatorname{im}(D^r_{m\times n}) = \langle\, e_1, \ldots, e_r \,\rangle^!_K \leq K^m, \\ \ker(f_D) &= \ker(D^r_{m\times n}) = \langle\, e_{r+1}, \ldots, e_n \,\rangle^!_K \leq K^n. \end{aligned}$$

Kanonische Darstellung einer linearen Abbildung

M102

In geeigneten Basen sieht jede lineare Abbildung genau so aus:

$$\begin{array}{ccc} K^n & \xrightarrow{\quad f_D : (x_1,\ldots,x_r,\ldots,x_n) \mapsto (x_1,\ldots,x_r,0,\ldots,0) \quad} & K^m \\ \Phi_{\mathcal{B}} \downarrow \cong & & \Phi_{\mathcal{C}} \downarrow \cong \\ V & \xrightarrow{\quad f : \begin{cases} v_i \mapsto w_i & \text{für } i = 1,\ldots,r, \\ v_i \mapsto 0 & \text{für } i = r+1,\ldots,n \end{cases} \quad} & W \end{array}$$

♦ Satz K2C: kanonische Darstellung einer linearen Abbildung

Sei $f : V \to W$ eine lineare Abbildung von K–Vektorräumen endlicher Dimension $n := \dim_K(V)$ und $m := \dim_K(W)$ mit Rang $r := \operatorname{rang}_K(f)$.
Dann existieren Basen $\mathcal{B} = (v_1, \ldots, v_n)$ von V und $\mathcal{C} = (w_1, \ldots, w_m)$ von W mit $f(v_i) = w_i$ für $i = 1, \ldots, r$ und $f(v_i) = 0$ für $i = r+1, \ldots, n$.
Somit wird f dargestellt durch die Modellmatrix $D^r_{m\times n} = \mathrm{M}^{\mathcal{C}}_{\mathcal{B}}(f)$.

Diese Matrix ist so einfach und übersichtlich wie möglich. Das bringt uns zum allgemeinen Ziel dieses Kapitels: Wir wollen nun Endomorphismen $f : V \to V$ so einfach wie möglich durch eine „Normalform“ darstellen.

Gauß–Algorithmus zur kanonischen Darstellung

M103

Ausprobieren mit Gaël!

Mit Gauß wandeln wir jede Matrix $A \in K^{m\times n}$ zur Modellmatrix $D^r_{m\times n}$:

$$\begin{array}{ccc} A & \xleftrightarrow{\text{Zeilen-operationen}} & B = S^{-1}A \\ \Big\updownarrow \text{Spalten-operationen} & & \Big\updownarrow \text{Spalten-operationen} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ * & * & * & 0 & 0 \end{bmatrix} & \xleftrightarrow{\text{Zeilen-operationen}} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

$$A = \begin{bmatrix} 3 & 6 & -6 & -6 & -1 \\ -2 & -4 & 3 & 1 & 5 \\ -1 & -2 & 3 & 5 & 4 \\ 1 & 2 & 1 & 7 & 1 \end{bmatrix}, \quad B = S^{-1}A = \begin{bmatrix} 1 & 2 & 0 & 4 & 0 \\ 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$D = S^{-1}AT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

🙂 Wir haben $\operatorname{im} D = \langle\, e_1, \ldots, e_r \,\rangle^!_K$ und $\ker D = \langle\, e_{r+1}, \ldots, e_n \,\rangle^!_K$; dank $SD = AT$ folgt $\operatorname{im} A = \langle\, Se_1, \ldots, Se_r \,\rangle^!_K$ und $\ker A = \langle\, Te_{r+1}, \ldots, Te_n \,\rangle^!_K$.

Gauß–Algorithmus zur kanonischen Darstellung

M104
Erläuterung

Ausführlich haben wir hierzu das folgende, allgemeine Verfahren:

♦ Satz K2F: Gauß–Algorithmus zur kanonischen Darstellung

Sei $A \in K^{m\times n}$ eine Matrix über dem Körper K.

(1) Der Gauß–Algorithmus K2F liefert hierzu invertierbare Matrizen $S, S^{-1} \in \mathrm{GL}_m(K)$ und $T, T^{-1} \in \mathrm{GL}_n(K)$, sodass $AT = SD^r_{m\times n}$ gilt.

(2) Daraus folgt $\operatorname{rang}(A) = r$ und $\operatorname{def}(A) = n - r$ und explizit

$$\begin{aligned} \operatorname{im}(A) &= \langle\, Se_1, \ldots, Se_r \,\rangle^!_K, \\ \ker(A) &= \langle\, Te_{r+1}, \ldots, Te_n \,\rangle^!_K. \end{aligned}$$

🙂 Dies ist ein Basiswechsel: Wir lesen die Matrix $A \in K^{m\times n}$ in den richtigen Basen, und schon vereinfacht sich A zur Modellmatrix $D^r_{m\times n}$! Diese Gauß–Normalform (GNF) löst das Klassifikationsproblem K2H.

🙂 Die Bestimmung von Bild $\operatorname{im}(A)$ und Kern $\ker(A)$ haben wir bereits zuvor in Satz J1P gelöst. Mit Satz K2F sehen Sie hier nun eine elegante Umformulierung; beide Algorithmen tun im Wesentlichen dasselbe.

Matrixdarstellung eines Endomorphismus

M105

Wir betrachten einen Endomorphismus $f : V \to V$ über dem Körper K.

$$\begin{array}{ccc} K^n & \xrightarrow{\quad f_D \quad} & K^n \\ \Phi_{\mathcal{B}} \downarrow \cong & & \Phi_{\mathcal{B}} \downarrow \cong \\ V & \xrightarrow{\quad f \quad} & V \end{array}$$

Wir suchen eine Basis $\mathcal{B}$ von V, sodass die darstellende Matrix

$$D = \mathrm{M}_{\mathcal{B}}(f) := \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) \in K^{n \times n}$$

möglichst einfach wird. Die einfachsten Matrizen sind **diagonal**:

$$D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Zum Beispiel können wir die Potenzen von D leicht berechnen:

$$D^k = \operatorname{diag}(\lambda_1^k, \ldots, \lambda_n^k) = \begin{bmatrix} \lambda_1^k & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n^k \end{bmatrix}$$

Matrixdarstellung eines Endomorphismus

M106
Erläuterung

Strenger als im allgemeinen Fall $f : V \to W$ stimmen hier Startraum V und Zielraum W überein. Daher wollen wir statt zwei Basen $\mathcal{B}$ von V und $\mathcal{C}$ von W nur eine Basis $\mathcal{B} = \mathcal{C}$ von $V = W$ verwenden.

Das klingt auf den ersten Takt trügerisch einfacher: Statt *zwei* Basen müssen wir nur *eine* Basis wählen. Tatsächlich ist es schwieriger: Statt zwei Basen *dürfen* wir nur eine Basis wählen.

Damit haben wir weniger Möglichkeiten zur Anpassung unserer Basis, weniger Freiheitsgrade zur Problemlösung, nämlich nur „halb“ so viele! Weniger ist mehr: Weniger Spielraum bedeutet mehr Herausforderung.

Die Vereinfachung auf Diagonalform wird dadurch tatsächlich spürbar erschwert, und sie gelingt nicht immer. Auch das Klassifikationsproblem wird dadurch kniffliger. Genau darum geht es in diesem Kapitel!

Diese Problemstellung der **Diagonalisierung** tritt sehr häufig auf, und ihre Lösung ist ein vielseitiges Werkzeug der Linearen Algebra.

Matrixdarstellung eines Endomorphismus

M107
Erläuterung

Diagonalisierung ist nicht immer möglich. In diesem Falle weicht man notgedrungen auf die „nächstbeste“ Möglichkeit aus und sucht eine Darstellung als Blockdiagonalmatrix mit möglichst einfachen Blöcken:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} B_1 & 0 & 0 & 0 \\ 0 & B_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & B_k \end{bmatrix}$$

Diagonalisierung entspricht $k = n$ Blöcken $B_1, B_2, \ldots, B_k \in K = K^{1\times 1}$.
Das nächstbeste sind Jordan–Blöcke

$$B_i = J(n_i, \lambda) = \begin{bmatrix} \lambda_i & 1 & 0 & 0 \\ 0 & \lambda_i & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \lambda_i \end{bmatrix} \in K^{n_i \times n_i}.$$

Die Größen addieren sich hierbei gemäß $n = n_1 + n_2 + \cdots + n_k$.
Diese Jordan–Normalform (JNF) diskutieren wir im nächsten Kapitel.

Matrixdarstellung eines Endomorphismus

M108
Erläuterung

Der allgemeinste Fall ist die Frobenius–Normalform (FNF) mit Blöcken

$$B_i = C(P_i) = \begin{bmatrix} 0 & 0 & \ldots & 0 & -p_{n_i} \\ 1 & 0 & \ldots & 0 & -p_{n_i-1} \\ 0 & 1 & \ddots & \vdots & -p_{n_i-2} \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -p_1 \end{bmatrix} \in K^{n_i \times n_i}.$$

Diese Matrix ist nicht ganz so simpel wie zuvor, doch von übersichtlicher Struktur und mit erfreulich vielen Nullen. Dies ist die Begleitmatrix des Polynoms $P_i = X^{n_i} + p_1 X^{n_i-1} + \cdots + p_{n_i} X^0 \in K[X]_{n_i}^1$, siehe M2Q.

Jede lineare Abbildung $f : V \to V$ eines endlich-dimensionalen Vektorraums V lässt sich so möglichst übersichtlich darstellen.
Das ist zwar nicht so schön und einfach wie eine Diagonalmatrix, aber wie gesagt das nächstbeste und dafür universell einsetzbar.

Nach diesem kurzen Überblick beschäftigen wir uns nun in diesem Kapitel mit dem schönsten und einfachsten Fall: der Diagonalisierung.

Diagonalisierung eines Endomorphismus

Definition M1A: Diagonalisierung eines Endomorphismus

(1) Sei $f : V \to V$ linear über K. Eine **diagonalisierende Basis** zu f ist eine Basis $\mathcal{B}$ von V, für die die darstellende Matrix von f diagonal ist:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Hierzu sagen wir später kurz **Eigenbasis** in der Sprechweise von M1B.
Existiert eine solche Basis $\mathcal{B}$ von V, so nennen wir f **diagonalisierbar**.

(2) Sei $A \in K^{n\times n}$. Ein **diagonalisierender Basiswechsel** zu A über K ist eine invertierbare Matrix $T \in \mathrm{GL}_n(K)$, so dass $T^{-1}AT$ diagonal ist:

$$T^{-1}AT = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Existiert eine solche Matrix T, so nennen wir A **diagonalisierbar**.

Diagonalisierung eines Endomorphismus

(1) Wir interessieren uns besonders für den endlich-dimensionalen Fall $\dim_K(V) = n < \infty$. Dann hat jede Basis $\mathcal{B}$ von V Länge n, und wir können f durch eine Matrix darstellen, wenn möglich diagonal.

Im Allgemeinen suchen wir zu $f : V \to V$ eine Basis $\mathcal{B} = (v_i)_{i\in I}$ von V, mit der Eigenschaft $f(v_i) = \lambda_i v_i$ und $\lambda_i \in K$ für jeden Index $i \in I$.
Dies nennen wir eine diagonalisierende Basis zu f.

Je nach Anwendung darf diese Basis durchaus auch unendlich sein, also $\dim_K(V) = \sharp I = \infty$. Speziell für den endlichen Fall haben wir eine besonders schöne Theorie, Sätze und Techniken. Der unendliche Fall findet später in der Funktionalanalysis eine umfassende Behandlung.

(2) Die Spaltenvektoren der Transformationsmatrix $T = (v_1, \ldots, v_n)$ bilden eine Basis von K^n, und diese diagonalisiert die lineare Abbildung

$$f_A : K^n \to K^n : v \mapsto Av.$$

Aus $T^{-1}AT = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ folgt nämlich $T^{-1}ATe_i = \lambda_i e_i$, somit $A(Te_i) = \lambda_i(Te_i)$. Für $v_i = Te_i$ gilt also $Av_i = \lambda v_i$, wie gewünscht.

Diagonalisierung eines Endomorphismus

🙂 Die obige Definition M1A erklärt zunächst das angestrebte Ziel:
Wir wollen einen Endomorphismus $f : V \to V$ über K bzw.
eine quadratische Matrix $A \in K^{n\times n}$ über K diagonalisieren.

Im Folgenden erarbeiten wir uns nun die nötigen Werkzeuge:
präzise Begriffe (Definitionen) und wirksame Methoden (Sätze).
Wir wiederholen zunächst ein einfaches, aber illustratives Beispiel,
an dem Sie alle Techniken und das Vorgehen schon erkennen können.

Dieses unorthodoxe Vorgehen – Anwendung vor Theorie – hilft Ihnen zur Orientierung, zumindest möchte ich es so anbieten. Anschließend führen wir die Techniken sorgsam aus, also Definitionen und Beispiele, Sätze und Beweise, und schließlich schöne Anwendungsbeispiele, so wie Sie es im mathematisch-logischen Aufbau erwarten.

Diagonalisierung eines Endomorphismus

🙂 Beachten Sie die logische Trennung von Ziel und Weg. Es lohnt sich, zunächst das Ziel klar zu benennen, dann mögliche Wege zu suchen.
Es gibt im Allgemeinen mehrere alternative Lösungsmöglichkeiten,
die sollten Sie kennen, und darüber Ziel und Weg nicht verwechseln.

Manche wünschen sich sofort am Anfang ein fertiges Rezept wie das Standardverfahren zur Diagonalisierung (M2I). Das erscheint zunächst verlockend als entlastende Abkürzung, erweist sich anschließend jedoch als verwirrend und ineffizient, als erschwerender Umweg:

Allein durch Auswendiglernen versteht man weder den Sinn noch die Herleitung, weder nützliche Zusammenhänge noch korrekte Nutzung.
In realistischen Anwendungen benötigen Sie jedoch genau dies!
Daher lohnt sich ein gründlicher, umsichtiger Aufbau.

Erinnerung und Vorschau zur Diagonalisierung

Zu $v = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right] \in \mathbb{R}^2$ betrachten wir die $\mathbb{R}$–lineare Abbildung

$$f : \mathbb{R}^2 \to \mathbb{R}^2 : x \mapsto x - v \cdot v^\mathsf{T} \cdot x.$$

Aufgabe: (1) Finden Sie alle $\lambda \in \mathbb{R}$ mit nicht-trivialem **Eigenraum**

$$\mathrm{E}(\lambda) := \{\, x \in \mathbb{R}^2 \mid f(x) = \lambda x \,\} = \ker(f - \lambda\,\mathrm{id}).$$

(2) Bestimmen Sie die Eigenräume. (3) Diagonalisieren Sie f.

Lösung: (1) Zur Bestimmung von λ nutzen wir die **Determinante**:

$$\ker(f - \lambda\,\mathrm{id}) \neq \{0\} \quad \overset{\text{L3D}}{\Longleftrightarrow} \quad \det(f - \lambda\,\mathrm{id}) = 0$$

Zur Berechnung wählen wir eine Basis, etwa $\mathcal{E} = (e_1, e_2)$, und finden

$$A = \mathrm{M}_\mathcal{E}^\mathcal{E}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \det(A - \lambda I) = \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - 1.$$

Dies ist das **charakteristische Polynom** von A bzw. von f.
Seine Nullstellen sind in diesem Beispiel $\lambda = +1$ und $\lambda = -1$.
Dies sind die **Eigenwerte** der Matrix A bzw. der Abbildung f.

Erinnerung und Vorschau zur Diagonalisierung

(2) Wir bestimmen die Eigenräume $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$ wie folgt:

$$\mathrm{E}(+1) = \ker(f - \mathrm{id}) = \ker \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} = \mathbb{R}\, b_1 \quad \text{mit} \quad b_1 := \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\mathrm{E}(-1) = \ker(f + \mathrm{id}) = \ker \begin{bmatrix} +1 & 1 \\ 1 & +1 \end{bmatrix} = \mathbb{R}\, b_2 \quad \text{mit} \quad b_2 := \begin{bmatrix} -1 \\ 1 \end{bmatrix}$$

Für alle weiteren $\lambda \in \mathbb{R} \smallsetminus \{\pm 1\}$ gilt $\mathrm{E}(\lambda) = \{0\}$ dank Satz L3D,
denn hier ist $\det(A - \lambda I) \neq 0$, also $A - \lambda I$ in $\mathbb{R}^{2\times 2}$ invertierbar.

(3) Wir erhalten $\mathbb{R}^2 = \mathrm{E}(+1) \oplus \mathrm{E}(-1)$ und die Basis $\mathcal{B} = (b_1, b_2)$ von $\mathbb{R}^2$.
Nach Konstruktion gilt $f(b_1) = +1 \cdot b_1$ und $f(b_2) = -1 \cdot b_2$, und somit

$$\mathrm{M}_\mathcal{B}^\mathcal{B}(f) = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Auf Seite K237 haben wir bereits die Basiswechselmatrizen bestimmt:

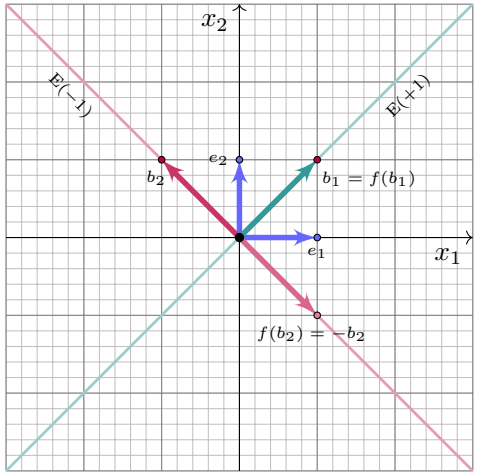
$$\mathrm{T}_\mathcal{B}^\mathcal{E} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \quad \text{und} \quad \mathrm{T}_\mathcal{E}^\mathcal{B} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

Erinnerung und Vorschau zur Diagonalisierung

☺ In der angepassten Basis $\mathcal{B} = (b_1, b_2)$ können wir die Abbildung f besonders einfach darstellen… Den Eigenräumen sei Dank!

$$\mathrm{M}_\mathcal{E}^\mathcal{E}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\mathrm{M}_\mathcal{B}^\mathcal{B}(f) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$ ist die Spiegelung an der Hauptdiagonalen.

Erinnerung und Vorschau zur Diagonalisierung

Eine solcherart angepasste Basis $\mathcal{B}$ zu f ist etwas ganz Besonderes:
Bezüglich $\mathcal{B}$ wird f durch eine Diagonalmatrix dargestellt, wie erhofft.

Wir nennen dies eine **diagonalisierende Basis** zu f, wie oben in Definition M1A vereinbart, oder auch kurz eine **Eigenbasis** zu f.

☺ Auf jedem Eigenraum $\mathrm{E}(\lambda)$ ist die Abbildung f besonders einfach:
Sie skaliert jeden Eigenvektor $v \in \mathrm{E}(\lambda)$ um den Eigenwert λ.
Glücklicherweise erhalten wir hier $\mathbb{R}^2 = \mathrm{E}(+1) \oplus \mathrm{E}(-1)$, wie erhofft.

Die Eigenräume unserer Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$ sind etwas Natürliches.
Die Wahl der jeweiligen Basen $b_1 \in \mathrm{E}(+1)$ und $b_2 \in \mathrm{E}(-1)$ ist hingegen etwas willkürlich; wir können auch Vielfache dieser Vektoren wählen.

☺ Die so gewonnene Eigenbasis $\mathcal{B}$ zeigt uns, was f eigentlich tut:
Hier offenbart die Abbildung f ihr wahres Wesen, ihren Charakter,
ihr Wirken, hier erkennen wir f sofort als Spiegelung.

Eigenwerte und Eigenvektoren eines Endomorphismus

M117

Definition M1B: Eigenwerte und Eigenvektoren

Sei $f : V \to V$ eine lineare Abbildung über dem Körper K.

(1) Zu jedem Skalar $\lambda \in K$ definieren wir den zugehörigen **Eigenraum**

$$\mathrm{E}(\lambda) = \mathrm{Eig}(f,\lambda) := \{\, v \in V \mid f(v) = \lambda v \,\} = \ker(f - \lambda\,\mathrm{id}_V) \leq V.$$

Im nicht-trivialen Fall $\mathrm{E}(\lambda) \neq \{0\}$ nennen wir λ einen **Eigenwert** von f.
Die Dimension $\dim_K \mathrm{E}(\lambda) \geq 1$ heißt **geometrische Vielfachheit** von λ.

(2) Die Menge aller Eigenwerte nennen wir das **(Eigenwert)Spektrum**

$$\sigma(f) = \sigma(f;K) := \{\, \lambda \in K \mid \exists v \in V \smallsetminus \{0\} : f(v) = \lambda v \,\}.$$

(3) Jedes Element $v \in \mathrm{E}(\lambda) \smallsetminus \{0\}$ heißt **Eigenvektor** zum Eigenwert λ.

(4) Eine **Eigenbasis** $\mathcal{B}$ ist eine Basis von V aus Eigenvektoren von f.
Im endlichen Fall heißt das, die darstellende Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f)$ ist diagonal.

Diese Begriffe nutzen wir ebenso für jede Matrix $A \in K^{n\times n}$ vermöge der zugehörigen K–linearen Abbildung $f = f_A : K^n \to K^n : v \mapsto Av$.

Eigenwerte und Eigenvektoren eines Endomorphismus

M118 Erläuterung

Zu $f \in \mathrm{End}_K(V)$ und $\lambda \in K$ definieren wir den zugehörigen Eigenraum

$$\mathrm{E}(\lambda) = \mathrm{Eig}(f,\lambda) := \{\, v \in V \mid f(v) = \lambda v \,\} = \ker(f - \lambda\,\mathrm{id}_V).$$

Die meisten Skalare $\lambda \in K$ erweisen sich dabei als uninteressant, denn meist ist der zugehörige Eigenraum trivial, also $\mathrm{E}(\lambda) = \{0\}$.

Wir betrachten daher nur die interessanten Werte $\lambda \in K$ mit $\mathrm{E}(\lambda) \neq \{0\}$.
Einen solchen Skalar $\lambda \in K$ mit $\mathrm{E}(\lambda) \neq \{0\}$ nennen wir zur Betonung einen **Eigenwert** von f, manche sagen **charakteristischer Wert**, engl. *eigenvalue* oder *proper value* oder *characteristic value*.

Aus demselben Grund verlangen wir von einem Eigenvektor stets $v \neq 0$.

⚠ Der Nullvektor erfüllt $f(0) = 0 = \lambda 0$ für alle $\lambda \in K$; diese Gleichung gilt immer und ist ohne jedes Interesse. Anders gesagt: Der Nullvektor gehört zu jedem Eigenraum $\mathrm{E}(\lambda)$, ist aber niemals ein Eigenvektor.

⚠ Der Skalar $\lambda = 0$ kann durchaus ein Eigenwert sein. Dies geschieht genau dann, wenn f nicht injektiv ist, denn es gilt $\mathrm{E}(0) = \ker(f)$.
Bitte lesen Sie die Definition aufmerksam durch und laut vor.

Eigenwerte und Eigenvektoren eines Endomorphismus

M119

Abkürzungen: EW = EWert = Eigenwert, EV = EVektor = Eigenvektor, ebenso ER = ERaum = Eigenraum, EB = EBasis = Eigenbasis, etc.

Beispiel: Sei $V \neq \{0\}$ und $f = \mathrm{id}_V$. Dann ist $\lambda = 1$ der einzige EW, $\mathrm{Eig}(f,1) = V$ ist der ER, die geometrische Vielfachheit ist $\dim_K(V)$.
Jeder Vektor $v \in V \smallsetminus \{0\}$ ist ein EV. Jede Basis von V ist eine EB zu f.

Beispiel M1C: eine Diagonalmatrix

Wir betrachten eine **Diagonalmatrix**

$$A = \mathrm{diag}(\lambda_1,\ldots,\lambda_n) = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix} \in K^{n\times n}.$$

Hier gilt $\ker(A - \lambda I) \neq \{0\}$ genau dann, wenn $\lambda \in \{\lambda_1,\ldots,\lambda_n\} = \sigma(A)$.
Der Vektor e_k ist EV zum EW λ_k, ebenso jedes Vielfache $v \in Ke_k \smallsetminus \{0\}$.
Die Standardbasis $(e_1,\ldots,e_n)$ des Raums K^n ist eine Eigenbasis zu A.

Zum Skalar $\lambda \in K$ gehört der Eigenraum $\mathrm{Eig}(f,\lambda) = \langle\, e_i \mid \lambda_i = \lambda \,\rangle_K^!$.
Gilt $\lambda_i \neq \lambda_j$ für $i \neq j$, so haben wir n Eigenräume $\mathrm{Eig}(f,\lambda_i) = \langle\, e_i \,\rangle_K^!$.

Eigenwerte und Eigenvektoren eines Endomorphismus

M120

Beispiel M1D: Jordan–Blöcke sind nicht-diagonalisierbar.

In jeder Dimension $n \geq 2$ betrachten wir den **Jordan–Block**:

$$B = \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix} \in K^{n\times n}, \quad B - \lambda I = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Hier gilt $\mathrm{Eig}(B,\lambda) = \langle\, e_1 \,\rangle_K^!$ und $\mathrm{Eig}(B,\mu) = \{0\}$ für $\mu \neq \lambda$,
also $\sigma(B) = \{\lambda\}$. Somit existiert zu B keine Eigenbasis.

Beispiel M1E: reelle Matrix ohne reelle Eigenwerte

Zu $a, b \in \mathbb{R}$ mit $b \neq 0$ betrachten wir die Matrix

$$C = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \quad \text{und} \quad \begin{vmatrix} a-\lambda & -b \\ b & a-\lambda \end{vmatrix} = (a-\lambda)^2 + b^2.$$

Für alle Skalare $\lambda \in \mathbb{R}$ gilt somit $\ker(C - \lambda I) = \{0\}$, kurz $\sigma(C;\mathbb{R}) = \emptyset$.
Hingegen ist $\lambda = a \pm \mathrm{i}b \in \mathbb{C}$ ein Eigenwert, genauer $\sigma(C;\mathbb{C}) = \{\, a \pm \mathrm{i}b \,\}$.

Lineare Unabhängigkeit von Eigenvektoren

M121

Satz M1F: lineare Unabhängigkeit von Eigenvektoren

Eigenvektoren zu verschiedenen Eigenwerten sind linear unabhängig.

Ausführlich: Sei $f : V \to V$ eine lineare Abbildung über dem Körper K.

1. Seien $v_0, \dots, v_r \in V \setminus \{0\}$ mit $f(v_i) = \lambda_i v_i$ und $\lambda_i \neq \lambda_j$ für $i \neq j$.
2. Es gelte $\mu_0 v_0 + \cdots + \mu_r v_r = 0$ mit Koeffizienten $\mu_0, \dots, \mu_r \in K$.

Dann folgt $\mu_0 = \cdots = \mu_r = 0$.

Beweis per Induktion über $r \in \mathbb{N}$:
Für $r = 0$ ist die Aussage klar, da wir $v_0 \neq 0$ voraussetzen (I1D).
Sei nun $r \geq 1$. Auf Gleichung (2) wenden wir $f - \lambda_0$ an und nutzen (1):

$$\mu_0(\lambda_0 - \lambda_0)v_0 + \mu_1(\lambda_1 - \lambda_0)v_1 + \cdots + \mu_r(\lambda_r - \lambda_0)v_r = 0$$

Nach Induktionsvoraussetzung folgt $\mu_i(\lambda_i - \lambda_0) = 0$ für $i = 1, \dots, r$.
Dank der Voraussetzung $\lambda_i \neq \lambda_0$ folgt $\mu_i = 0$ für alle $i = 1, \dots, r$.
Von Gleichung (2) bleibt schließlich nur $\mu_0 v_0 = 0$, also $\mu_0 = 0$. QED

Lineare Unabhängigkeit von Eigenvektoren

M122
Erläuterung

Beweis mit dem Vandermonde–Trick: Gegeben sind die Vektoren $u_i = \mu_i v_i \in \operatorname{Eig}(f, \lambda_i)$ mit $u_0 + u_1 + \cdots + u_r = 0$. Wir wenden f^k an:

$$\lambda_0^k u_0 + \lambda_1^k u_1 + \cdots + \lambda_r^k u_r = 0.$$

Für $k = 0, 1, \dots, r$ erhalten wir so das folgende Gleichungssystem:

$$\begin{bmatrix} \lambda_0^0 & \lambda_1^0 & \dots & \lambda_r^0 \\ \lambda_0^1 & \lambda_1^1 & \dots & \lambda_r^1 \\ \vdots & & \vdots & \\ \lambda_0^r & \lambda_1^r & \dots & \lambda_r^r \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_r \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Die Vandermonde–Matrix ist invertierbar dank Satz B3A:

$$\begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_r \end{bmatrix} = \begin{bmatrix} \lambda_0^0 & \lambda_1^0 & \dots & \lambda_r^0 \\ \lambda_0^1 & \lambda_1^1 & \dots & \lambda_r^1 \\ \vdots & & \vdots & \\ \lambda_0^r & \lambda_1^r & \dots & \lambda_r^r \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Daraus folgt $u_0 = u_1 = \cdots = u_r = 0$, wie behauptet. QED

Lineare Unabhängigkeit von Eigenvektoren

M123
Erläuterung

Zur Illustration nenne ich zwei einfache doch grundlegende Beispiele, die Lineare Algebra und Analysis elegant verbinden: die Eigenfolgen der Verschiebung (M1G) und die Eigenfunktionen der Ableitung (M1H).

Beispiel M1G: Eigenfolgen der Verschiebung

Über dem Körper K betrachten wir den Vektorraum $K^{\mathbb{N}}$ aller Folgen $f : \mathbb{N} \to K : n \mapsto f_n$, kurz $f = (f_n)_{n \in \mathbb{N}}$, mit dem Verschiebeoperator

$$\begin{aligned} s \;:\; K^{\mathbb{N}} \to K^{\mathbb{N}} \;:\; (f_n)_{n\in\mathbb{N}} &\mapsto (f_{n+1})_{n\in\mathbb{N}}, \\ (f_0, f_1, f_2, \dots) &\mapsto (f_1, f_2, f_3, \dots). \end{aligned}$$

Zu jeder Konstanten $\lambda \in K$ haben wir die Folge $e_\lambda = (\lambda^n)_{n\in\mathbb{N}}$.
Sie erfüllt $s(e_\lambda) = \lambda e_\lambda$, ist also eine Eigenfolge der Verschiebung.
Insbesondere ist die Familie $(e_\lambda)_{\lambda \in K}$ in $K^{\mathbb{N}}$ somit linear unabhängig.

Die lineare Unabhängigkeit ist nicht ganz leicht zu beweisen.
Alternativ gelingt dies direkt mit der Vandermonde–Matrix B3A.
Als Eigenfolgen erhalten wir Unabhängigkeit gratis dank Satz M1F.

Lineare Unabhängigkeit von Eigenvektoren

M124

Beispiel M1H: Eigenfunktionen der Ableitung

Sei $I =]a, b[\subseteq \mathbb{R}$ ein offenes Intervall der reellen Zahlen, etwa $I = \mathbb{R}$.

Über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ betrachten wir den Vektorraum $\mathscr{C}^\infty(I, \mathbb{K})$ aller beliebig oft differenzierbaren Funktionen $f : I \to \mathbb{K}$ mit dem Ableitungsoperator

$$\partial \;:\; \mathscr{C}^\infty \to \mathscr{C}^\infty \;:\; f \mapsto f'.$$

Zu jeder Konstanten $\lambda \in \mathbb{K}$ haben wir die Exponentialfunktion

$$e_\lambda \;:\; I \to \mathbb{K} \;:\; t \mapsto \mathrm{e}^{\lambda t}.$$

Sie erfüllt $\partial e_\lambda = \lambda e_\lambda$, ist also eine Eigenfunktion der Ableitung.
Insbesondere ist die Familie $(e_\lambda)_{\lambda \in \mathbb{K}}$ in $\mathscr{C}^\infty$ somit linear unabhängig.

Als Eigenfunktionen erhalten wir Unabhängigkeit gratis dank Satz M1F.
Versuchen Sie alternative Beweise zu formulieren (siehe etwa K143).

Dieses Beispiel ist eine nützliche Beobachtung, die wir später bei der Lösung von linearen Differentialgleichungen nutzen und weiterführen.

Eigenraumzerlegung und Diagonalisierung

Wie können wir effizient feststellen, ob $f : V \to V$ diagonalisierbar ist?

Satz M1I: Eigenraumzerlegung und Diagonalisierung

Vorgelegt sei eine lineare Abbildung $f : V \to V$ über dem Körper K.

(1) Die Summe $\mathrm{E} := \sum_{\lambda \in K} \mathrm{E}(\lambda) \leq V$ aller Eigenräume ist direkt, also

$$\mathrm{E} = \bigoplus_{\lambda \in K} \mathrm{E}(\lambda) = \bigoplus_{\lambda \in \sigma(f)} \mathrm{Eig}(f, \lambda).$$

(2) Genau dann ist $f : V \to V$ diagonalisierbar, wenn $\mathrm{E} = V$ gilt, also

$$\boxed{V = \bigoplus_{\lambda \in \sigma(f)} \mathrm{Eig}(f, \lambda).}$$

(3) Im Falle $\dim_K V < \infty$ ist dies äquivalent zur Dimensionsgleichung

$$\dim_K V = \sum_{\lambda \in \sigma(f)} \dim_K \mathrm{Eig}(f, \lambda).$$

Beweis: (1) Dies folgt aus der linearen Unabhängigkeit (Satz M1F).
(2) Es gibt genügend Eigenvektoren, um eine Eigenbasis zu bilden.
(3) Dies folgt dank Additivität der Dimension (Satz J2K und J2O). QED

Eigenraumzerlegung und Diagonalisierung

Aufgabe: Führen Sie den Beweis zu (1) detailliert aus.

Lösung: (1) Die Definition I2J zur direkten Summe verlangt:

$$\mathrm{E}(\lambda_0) \cap \left(\sum_{\lambda \neq \lambda_0} \mathrm{E}(\lambda) \right) = \{0\}$$

Gegeben seien also Vektoren $v_i \in \mathrm{E}(\lambda_i)$ mit $\lambda_1, \ldots, \lambda_r \in K \smallsetminus \{\lambda_0\}$.

Behauptung: Aus $v_0 = v_1 + \cdots + v_r$ folgt $v_0 = 0$.

Beweis: Wir führen Induktion über r. Für $r = 0$ ist die Aussage klar.
Sei nun $r \geq 1$. Wir wenden $f - \lambda_r$ an und erhalten nach Kürzung:

$$v_0 = \frac{\lambda_1 - \lambda_r}{\lambda_0 - \lambda_r} v_1 + \cdots + \frac{\lambda_{r-1} - \lambda_r}{\lambda_0 - \lambda_r} v_{r-1} + \frac{\lambda_r - \lambda_r}{\lambda_0 - \lambda_r} v_r$$

Nach Induktionsvoraussetzung für $r - 1$ folgt daraus $v_0 = 0$.

Zur Deutlichkeit wiederhole ich hier den raffinierten Induktionsbeweis von Satz M1F. Alternativ können Sie den Vandermonde–Trick nutzen oder auch direkt die Aussage von M1F anwenden. Sehen Sie wie?
Wir werden in Satz M3V einen weiteren Beweis kennenlernen.

Eigenraumzerlegung und Diagonalisierung

☺ Diagonalisierbarkeit bedeutet anschaulich vereinfacht formuliert:
Es gibt genügend Eigenvektoren, um eine Eigenbasis zu bilden.

Hierzu untersuchen wir auch die zweite Aussage noch etwas genauer:
(2) Genau dann ist f diagonalisierbar, wenn $V = \bigoplus_{\lambda \in K} \mathrm{Eig}(f, \lambda)$ gilt.

Aufgabe: Führen Sie den Beweis zu (2) detailliert aus.
Hierzu benötigen Sie keine Voraussetzung zur Dimension.

Lösung: Die Äquivalenz beweisen wir durch akribische Buchführung.

„⇐“: Zu jedem $\mathrm{E}(\lambda) \leq V$ wählen wir eine Basis $\mathcal{B}_\lambda = (v_i)_{i \in I_\lambda}$ (J2B).
Wir können $I_\lambda \cap I_\mu = \emptyset$ für $\lambda \neq \mu$ annehmen und setzen $I = \bigsqcup_{\lambda \in K} I_\lambda$.
Dank $V = \bigoplus_{\lambda \in K} \mathrm{E}(\lambda)$ erhalten wir eine Basis $\mathcal{B} = (v_i)_{i \in I}$ zu V (J2O).
Diese diagonalisiert $f : V \to V$, denn es gilt $f(v_i) = \lambda v_i$ für $i \in I_\lambda$.

Eigenraumzerlegung und Diagonalisierung

„⇒“: Sei $\mathcal{B} = (v_i)_{i \in I}$ eine diagonalisierende Basis zu f, das heißt $f(v_i) = \lambda_i v_i$ mit $\lambda_i \in K$ für alle $i \in I$. Wir zerlegen die Indexmenge $I = \bigsqcup_{\lambda \in K} I_\lambda$ in $I_\lambda = \{\, i \in I \mid \lambda_i = \lambda \,\}$. Dann gilt $\mathrm{E}(\lambda) = \langle\, v_i \mid i \in I_\lambda \,\rangle_K^!$.

(a) Die Inklusion „⊇“ ist klar: Für jede Linearkombination $v = \sum_{i \in I_\lambda} \mu_i v_i$ mit Koeffizienten $\mu_i \in K$ gilt $f(v) = \sum_{i \in I_\lambda} \mu_i f(v_i) = \sum_{i \in I_\lambda} \mu_i \lambda v_i = \lambda v$.

(b) Zum Beweis der Umkehrung „⊆“ sei $v \in \mathrm{E}(\lambda) \leq V$. Wir haben also $v = \sum_{i \in I} \mu_i v_i$ mit $\mu \in K^{(I)}$ und $0 = f(v) - \lambda v = \sum_{i \in I} (\mu_i \lambda_i - \lambda \mu_i) v_i$.
Da $\mathcal{B}$ linear unabhängig ist, folgt $(\lambda_i - \lambda)\mu_i = 0$ für jeden Index $i \in I$.
Daraus folgt $\lambda_i = \lambda$ oder $\mu_i = 0$ dank I1D, also $v \in \langle\, v_i \mid i \in I_\lambda \,\rangle_K^!$.

Wir erhalten somit $V = \bigoplus_{\lambda \in K} \langle\, v_i \mid i \in I_\lambda \,\rangle_K^! = \bigoplus_{\lambda \in K} \mathrm{E}(\lambda)$.
Das beweist die Äquivalenz (2) der Eigenraumzerlegung M1I.

Beispiel: Von der Eigenraumzerlegung zur Matrix

Aufgabe: (1) Sei $v_1 = \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]$ und $v_2 = \left[\begin{smallmatrix}-1\\1\end{smallmatrix}\right]$. Finden Sie alle $A \in \mathbb{R}^{2\times 2}$ mit

$$\mathrm{Eig}(A,-1) = \langle\, v_1 \,\rangle \quad \text{und} \quad \mathrm{Eig}(A,2) = \langle\, v_2 \,\rangle.$$

(2) Hat A noch weitere Eigenwerte? (3) Bestimmen Sie $\sigma(A)$.

Lösung: (1) Wir wissen $Av_1 = -v_1$ und $Av_2 = 2v_2$. Dank dem Prinzip der linearen Fortsetzung (K1B) gibt es genau eine solche Matrix A. Da $\mathcal{B} = (v_1, v_2)$ eine Basis von $\mathbb{R}^2$ ist, wird A durch $\mathcal{B}$ diagonalisiert:

$$T^{-1}AT = D = \begin{bmatrix}-1 & 0\\ 0 & 2\end{bmatrix} \in \mathbb{R}^{2\times 2} \text{ mit}$$

$$T = \mathrm{T}^{\mathcal{E}}_{\mathcal{B}} = \begin{bmatrix}2 & -1\\ 1 & 1\end{bmatrix} \quad \text{und} \quad T^{-1} = \mathrm{T}^{\mathcal{B}}_{\mathcal{E}} = \frac{1}{3}\begin{bmatrix}1 & 1\\ -1 & 2\end{bmatrix}, \text{ also}$$

$$A = TDT^{-1} = \frac{1}{3}\begin{bmatrix}2 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & 2\end{bmatrix}\begin{bmatrix}1 & 1\\ -1 & 2\end{bmatrix} = \begin{bmatrix}0 & -2\\ -1 & 1\end{bmatrix}.$$

(2) Wir haben $\mathbb{R}^2 = \mathrm{E}(-1) \oplus \mathrm{E}(2)$. Für $\lambda \in \mathbb{R} \smallsetminus \{-1, 2\}$ folgt dank M1I:

$$\mathrm{E}(\lambda) = \mathrm{E}(\lambda) \cap \mathbb{R}^2 = \mathrm{E}(\lambda) \cap \big(\mathrm{E}(-1) \oplus \mathrm{E}(2)\big) = \{0\}$$

(3) Das Spektrum der Matrix A ist demnach $\sigma(A) = \{-1, 2\}$.

Beispiel: Von der Eigenraumzerlegung zur Matrix

☺ In (2) nutzen wir geschickt die Eigenraumzerlegung aus Satz M1I. Für weitere nicht-triviale Eigenräume ist daher in $\mathbb{R}^2$ kein Platz mehr.

Das Eigenwertspektrum der Matrix A ist demnach $\sigma(A) = \{-1, 2\}$: Es gilt „$\supseteq$“ nach Konstruktion, und „$\subseteq$“ dank Satz M1I.

☹ Alternativ (aber umständlich) können Sie dies für jeden weiteren Kandidaten $\lambda \in \mathbb{R} \smallsetminus \{-1, 2\}$ einzeln explizit ausrechnen, indem Sie jeweils $\ker(A - \lambda I) = \{0\}$ bestimmen. Das ist möglich, aber mühselig.

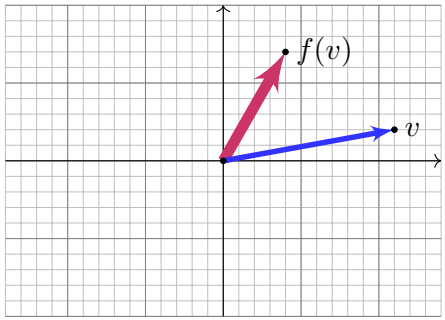
Zur Übung können Sie dies gerne ausprobieren und selbst spüren.

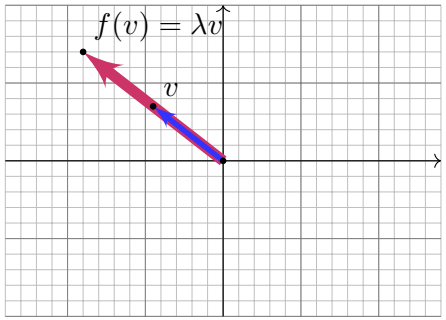
☺ Am besten sparen Sie sich unnötige Arbeit mit der zugehörigen Theorie, hier der Eigenraumzerlegung aus Satz M1I. Das kostet anfangs eine gewisse Investition, doch zahlt sich rasch aus.

Mit den passenden Werkzeugen arbeiten Sie effizienter.

Geometrische Bedeutung

Sei $f : V \to V$ linear über K. Was bedeuten EV und EW geometrisch?





Wir vergleichen einen Vektor $v \in V \smallsetminus \{0\}$ mit seinem Bild $w = f(v) \in V$.
Im Allgemeinen besteht keine Relation, beide sind linear unabhängig.

Im Fall $w = \lambda v$ mit $\lambda \in K$ sind sie linear abhängig, also parallel.
Der zugehörige Eigenwert λ ist der Streckfaktor von v zu w.

Algebraische Bedeutung

Für jeden Eigenvektor v mit $f(v) = \lambda v$ gilt

$$\boxed{f^n(v) = \lambda^n v.}$$

Dies folgt sofort per Induktion über $n \in \mathbb{N}$:

$$f^n(v) = f(f^{n-1}(v)) = f(\lambda^{n-1}v) = \lambda^{n-1}f(v) = \lambda^{n-1}\lambda v = \lambda^n v$$

Für jedes Polynom $P = \sum_{i=0}^{n} a_i X^i \in K[X]$ gilt demnach

$$\boxed{P(f)(v) = P(\lambda)\, v.}$$

Wir nutzen hier den Einsetzungshomomorphismus G3E:

$$\begin{aligned} P(f)(v) &= (a_0 + a_1 f + \cdots + a_n f^n)(v)\\ &= a_0 v + a_1 f(v) + \cdots + a_n f^n(v)\\ &= a_0 v + a_1 \lambda v + \cdots + a_n \lambda^n v\\ &= (a_0 v + a_1 \lambda + \cdots + a_n \lambda^n) v = P(\lambda)\, v \end{aligned}$$

Beispiel: Von der Matrix zur Eigenraumzerlegung

M133 Ausprobieren mit Gaël!

Aufgabe: Vorgelegt sei die Matrix

$$A = \begin{bmatrix} 0 & 4 & 2 \\ -2 & 6 & 2 \\ 4 & -8 & -2 \end{bmatrix}.$$

(1) Bestimmen Sie die Eigenräume $\mathrm{E}(\lambda)$ für $\lambda = 0, 1, 2, 3$.
(2) Ist A diagonalisierbar? Falls ja, diagonalisieren Sie A.
(3) Hat A noch weitere Eigenwerte? Bestimmen Sie $\sigma(A)$.

Lösung: (1) Für $\lambda = 0$ bestimmen wir $\mathrm{E}(0) = \ker(A - 0I) = \ker(A)$:

$$A = \begin{bmatrix} 0 & 4 & 2 \\ -2 & 6 & 2 \\ 4 & -8 & -2 \end{bmatrix} \xrightarrow[\text{RZSF}]{\text{Gauß}} \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 1 & 1/2 \\ 0 & 0 & 0 \end{bmatrix} \implies \mathrm{E}(0) = \left\langle \begin{bmatrix} 1 \\ 1 \\ -2 \end{bmatrix} \right\rangle^{!}$$

Für $\lambda = 1$ bestimmen wir $\mathrm{E}(1) = \ker(A - 1I)$ und finden:

$$A - 1I = \begin{bmatrix} -1 & 4 & 2 \\ -2 & 5 & 2 \\ 4 & -8 & -3 \end{bmatrix} \xrightarrow[\text{RZSF}]{\text{Gauß}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \implies \mathrm{E}(1) = \{0\}$$

Beispiel: Von der Matrix zur Eigenraumzerlegung

M134 Ausprobieren mit Gaël!

Für $\lambda = 2$ bestimmen wir $\mathrm{E}(2) = \ker(A - 2I)$ und finden:

$$\begin{bmatrix} -2 & 4 & 2 \\ -2 & 4 & 2 \\ 4 & -8 & -4 \end{bmatrix} \xrightarrow[\text{RZSF}]{\text{Gauß}} \begin{bmatrix} 1 & -2 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \implies \mathrm{E}(2) = \left\langle \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\rangle^{!}$$

Für $\lambda = 3$ wissen wir schon $\mathrm{E}(3) = \ker(A - 3I) = \{0\}$ dank M1I.

(2) Die Matrix A ist diagonalisierbar, etwa wie oben mit der Eigenbasis

$$\mathcal{B} = \left(\begin{bmatrix} 1 \\ 1 \\ -2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right).$$

Daraus erhalten wir den zugehörigen Basiswechsel zur Diagonalmatrix:

$$T = \mathrm{T}_{\mathcal{B}}^{\mathcal{E}} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix} \implies T^{-1}AT = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Beispiel: Von der Matrix zur Eigenraumzerlegung

M135 Erläuterung

☺ In diesem Beispiel hat der erste Eigenwert $\lambda = 0$ die algebraische Vielfachheit $\dim_{\mathbb{R}} \mathrm{E}(0) = 1$. Hingegen hat der zweite Eigenwert $\lambda = 2$ die algebraische Vielfachheit $\dim_{\mathbb{R}} \mathrm{E}(2) = 2$. Auch das kommt vor.

(3) Wir haben $\mathbb{R}^3 = \mathrm{E}(0) \oplus \mathrm{E}(2)$. Für $\lambda \in \mathbb{R} \smallsetminus \{0, 2\}$ folgt dank M1I:

$$\mathrm{E}(\lambda) = \mathrm{E}(\lambda) \cap \mathbb{R}^3 = \mathrm{E}(\lambda) \cap \big(\mathrm{E}(0) \oplus \mathrm{E}(2)\big) = \{0\}$$

☺ Für weitere nicht-triviale Eigenräume ist daher in $\mathbb{R}^3$ kein Platz. Das Eigenwertspektrum der Matrix A ist demnach $\sigma(A) = \{0, 2\}$. Es gilt „$\supseteq$“ nach Rechnung, und „$\subseteq$“ dank Satz M1I.

☺ Alternativ können Sie $\lambda = 3$ und weitere Beispiele explizit ausrechnen. Am besten sparen Sie sich unnötige Arbeit mit der passenden Theorie, hier der Eigenraumzerlegung aus Satz M1I.

Diese Aufgabe hat als mögliche Eigenwerte die Kandidaten $\lambda = 0, 1, 2, 3$ vorgegeben. Diese enge Fragestellung dient hier als didaktischer Kniff, um Ihre Aufmerksamkeit auf die grundlegenden Definitionen M1A und M1B sowie die omnipräsente Eigenraumzerlegung M1F zu fokussieren.

Beispiel: Von der Matrix zur Eigenraumzerlegung

M136 Erläuterung

Die Vorgabe von Eigenwerten kann manchmal durchaus sinnvoll sein, doch in den allermeisten Anwendungen ist sie eher unrealistisch. Oft haben Sie keine solche Anhaltspunkte oder Vorgaben. Dann müssen die möglichen Eigenwerte selbst finden.

Für das allgemeine Problem benötigen Sie daher weitere Werkzeuge. Dies gelingt uns im Folgenden mit dem charakteristischen Polynom.

⚠ Definition M1B und Satz M1F gelten unabhängig von der Dimension, egal ob endlich oder unendlich. Da wir nun Matrizen und Determinanten nutzen wollen, werden wir uns auf endliche Dimension konzentrieren. Das ist eine Weggabelung: Weniger Allgemeinheit, stärkere Werkzeuge.

Ausblick: Die Funktionalanalysis zweigt hier in die andere Richtung ab und betrachtet unendlich-dimensionale Vektorräume mit ihren eigenen, raffinierten Werkzeugen. Einfache Beispiele können wir jetzt bereits bewundern, in Ihrem Studium dürfen Sie sich auf noch viel mehr freuen.

Was bedeutet „Diagonalisieren Sie A“?

M137
Erläuterung

🙂 Diese Standardaufgabe ist typisch für Übungen und Klausuren. Dabei stellt sich jeweils die Frage, was genau gefordert ist: Welche Daten gehören zu einer vollständigen Antwort?

⚠ Je nach Aufgabe bzw. Anwendung sind verschiedene Stufen der Ausführung denkbar. Beginnen wir mit der maximalen Ausbaustufe:

Gegeben ist eine Matrix $A \in K^{n\times n}$ über dem Körper K.

Gesucht ist im Sinne einer vollständigen Analyse:

1. die Menge $\sigma(A) = \sigma(A;K)$ aller Eigenwerte,
2. die Dimension jedes Eigenraums $\operatorname{Eig}(A;\lambda)$ für M1ı,
3. eine Basis $\mathcal{B}_\lambda = (v_i)_{i\in I_\lambda}$ für jeden Eigenraum $\operatorname{Eig}(A;\lambda)$,
4. die daraus gebildete Basiswechselmatrix $T = (v_1,\dots,v_n) \in \mathrm{GL}_n K$,
5. die hierzu inverse Matrix T^{-1}, mit der Eigenschaft / Probe $T^{-1}T = I$,
6. die so gewonnene Diagonalmatrix $D = T^{-1}AT = \operatorname{diag}(\lambda_1,\dots,\lambda_n)$, mit der Eigenschaft / Probe $D = T^{-1}AT$ bzw. $AT = TD$.

Verschiedene Härtegrade

M138
Erläuterung

Neben der vollständigen Analyse gibt es mehrere kleinere **Varianten**:

Ist nur die **Diagonalisierbarkeit** von A gefragt, so genügen (1) und (2). Daran lässt sich die Diagonalisierbarkeit entscheiden und (6) D ablesen. Die fehlenden Daten (3,4,5) lassen sich anschließend ergänzen…

Ist ein **diagonalisierender Basiswechsel** gefragt, so genügen (4) T und (5) T^{-1} und (6) D. Damit lassen sich die Eigenschaften $T^{-1}T = I$ und $T^{-1}AT = D$ prüfen und die Daten (1,2,3) ablesen.

Ist nur eine **Eigenbasis** zu A gefragt, so genügen (4) T und (6) D. Damit lässt sich $AT = TD$ prüfen und die Daten (1,2,3) ablesen.

In Klausuren geben wir die Fragen kleinschrittig vor und sagen genau, was jeweils gefragt ist. Erfahrungsgemäß bereitet das keine Probleme.

Bei einer mündlichen Präsentation, etwa in Ihrer Gruppenübung, haben Sie mehr Freiheiten, Sie können nachfragen und ergänzen. In solchen Fällen ist eine offene Fragestellung meist sinnvoller.

Ergebnis und Zertifikat

M139
Erläuterung

Die algorithmische Sichtweise ist oft hilfreich. Hier geht es speziell um die Frage der Spezifikation: Was ist die Eingabe? Was ist die Ausgabe? Welche Eigenschaften müssen garantiert bzw. überprüft werden?

Spezifikation: Eigenbasis einer Matrix

Eingabe: eine Matrix $A \in K^{n\times n}$ über dem Körper K
Ausgabe: $D = \operatorname{diag}(\lambda_1,\dots,\lambda_n)$ und $T \in \mathrm{GL}_n(K)$ mit $AT = TD$ oder notfalls die Antwort „A ist nicht diagonalisierbar“

Allgemein gilt: Je mehr Daten die Spezifikation als Ausgabe verlangt, desto aufwändiger die Berechnung, doch umso leichter ist die Prüfung.

Umgekehrt: Wird von der Eingabe mehr verlangt, so ist dies schwerer für den Auftraggeber, doch umso leichter für den Auftragnehmer.

Spezifikation: Eigenbasis einer diagonalisierbaren Matrix

Eingabe: eine diagonalisierbare Matrix $A \in K^{n\times n}$ über K
Ausgabe: $D = \operatorname{diag}(\lambda_1,\dots,\lambda_n)$ und $T \in \mathrm{GL}_n(K)$ mit $AT = TD$

Was bedeutet „Diagonalisieren Sie f“?

M140
Erläuterung

Welche Daten gehören zu einer vollständigen Antwort?

⚠ Je nach Aufgabe bzw. Anwendung sind verschiedene Stufen der Ausführung denkbar. Beginnen wir mit der maximalen Ausbaustufe:

Gegeben ist $f \in \operatorname{End}_K(V)$ und $n = \dim_K(V) < \infty$.

Gesucht ist im Sinne einer vollständigen Analyse:

1. die Menge $\sigma(f) = \sigma(f;K)$ aller Eigenwerte,
2. die Dimension jedes Eigenraums $\operatorname{Eig}(f;\lambda)$ für M1ı,
3. eine Basis $\mathcal{B}_\lambda = (v_i)_{i\in I_\lambda}$ für jeden Eigenraum $\operatorname{Eig}(f;\lambda)$,
4. die durch $I = \bigsqcup_\lambda I_\lambda$ gebildete Eigenbasis $\mathcal{B} = (v_i)_{i\in I}$ von V,
5. die so gewonnene Diagonalmatrix $D = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) \in K^{n\times n}$.

Zur **Diagonalisierbarkeit** von f genügen (1) und (2). Daran lässt sich (5) ablesen und die fehlenden Daten (3,4) anschließend ergänzen…

Für eine **Eigenbasis** zu f genügen (4) und (5), daraus folgen (1,2,3). Selbst im Falle $\dim_K(V) = \infty$ bleiben (1,3,4) ebenso sinnvoll.

Wie finden wir alle Eigenwerte?

M201

Wie finden wir alle Eigenwerte einer vorgelegten Matrix $A \in K^{n\times n}$?

Satz M2A: Eigenwerte und Determinante

Sei K ein Körper, $A \in K^{n\times n}$ eine Matrix und $\lambda \in K$ ein Skalar.
Genau dann ist λ ein Eigenwert von A, wenn $\det(A-\lambda I)=0$ gilt.

Beweis: Wir setzen die Definition ein und formen sorgsam um:

$$
\begin{aligned}
& & \operatorname{Eig}(A,\lambda) &\neq \{0\} \\
&\overset{\text{Def M1B}}{\iff} & \exists v \in K^n,\ v\neq 0 :\quad Av &= \lambda v \\
&\overset{\text{Lin B1A}}{\iff} & \exists v \in K^n,\ v\neq 0 :\quad (A-\lambda I)v &= 0 \\
&\overset{\text{Def I1R}}{\iff} & \exists v \in K^n,\ v\neq 0 :\quad v &\in \ker(A-\lambda I) \\
&\overset{\text{Def I1R}}{\iff} & \ker(A-\lambda I) &\neq \{0\} \\
&\overset{\text{Det L2Q}}{\iff} & \det(A-\lambda I) &= 0
\end{aligned}
$$

Wie finden wir alle Eigenwerte?

M202
Erläuterung

☺ Die Eigenwerte der Matrix $A \in K^{n\times n}$ sind demnach die Nullstellen der **charakteristischen Funktion** $K \to K : \lambda \mapsto \det(A-\lambda I)$.

Sie ordnet jedem Skalar $\lambda \in K$ die Determinante $\det(A-\lambda I) \in K$ zu und zeigt an, ob der Kern von $A-\lambda I$ trivial ist oder nicht (Satz L2Q).

Diese Funktion wollen wir nun genauer untersuchen! Insbesondere werden wir sehen, dass dies eine Polynomfunktion ist. Somit können wir all unsere Werkzeuge zu Polynomen hier nutzbringend anwenden!

⚠ In Definition M1B haben wir zunächst erklärt, was Eigenwerte sind. Hier nun lernen Sie eine Rechenmethode mit der Determinante kennen. Um Matrizen und Determinanten überhaupt einsetzen zu können, werden wir uns auf endliche Dimension konzentrieren.

Bitte unterscheiden Sie Definition und Methoden, also Ziel und Wege! Eigenwerte und Eigenräume lassen sich auch in vielen Situationen erklären und nutzen, in denen die Determinante nicht anwendbar ist, insbesondere auch für unendlich-dimensionale Vektorräume.

Wie finden wir alle Eigenwerte?

M203

Wie finden wir alle Eigenwerte eines Endomorphismus $f : V \to V$?

$$
\begin{array}{ccc}
K^n & \xrightarrow{A : x\mapsto Ax} & K^n \\
{\scriptstyle \Phi_{\mathcal{B}}}\downarrow\cong & & {\scriptstyle \Phi_{\mathcal{B}}}\downarrow\cong \\
V & \xrightarrow{f : v\mapsto f(v)} & V
\end{array}
$$

Im Falle $\dim_K V = n < \infty$ wählen wir eine Basis $\mathcal{B} = (v_1,\dots,v_n)$ von V und stellen f dar durch die zugehörige Matrix $A = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) \in K^{n\times n}$.

Jeden Vektor $v \in V$ stellen wir eindeutig dar durch seine Koordinaten $x \in K^n$ mit $v = x_1v_1 + \cdots + x_nv_n$. Aus obigem Diagramm lesen wir ab:

Bemerkung: Genau dann gilt $f(v) = \lambda v$, wenn $Ax = \lambda x$.

⚠ Die entscheidende Voraussetzung ist hier $\dim_K V = n < \infty$.
In diesem Falle können wir Matrizen und die Determinante nutzen!

Auf unendlichen Vektorräumen ist die Sachlage schwieriger…
und weitaus interessanter (siehe Funktionalanalysis).

Wie finden wir alle Eigenwerte?

M204
Erläuterung

Damit wird das Problem berechenbar dank der Determinante und der charakteristischen Funktion von f bzw. A:

$$
\begin{aligned}
& \operatorname{Eig}(f,\lambda) \neq \{0\} \\
\iff\ & \operatorname{Eig}(A,\lambda) \neq \{0\} \\
\iff\ & \det(A-\lambda I) = 0 \\
\iff\ & \det(f-\lambda \operatorname{id}_V) = 0
\end{aligned}
$$

Zur Determinante eines Endomorphismus $f : V \to V$ siehe L3D:
Dies gelingt in einer Basis durch Darstellung als Matrix $A \in K^{n\times n}$.

Meist interessiert uns eigentlich die lineare Abbildung $f : V \to V$, doch mit der Matrix $A \in K^{n\times n}$ können wir besonders gut rechnen.

Notation: Hier ist $I = E = 1_{n\times n} = \operatorname{diag}(1,\dots,1)$ die Einheitsmatrix.
Da E schon für Eigenräume genutzt wird, schreibe ich hier lieber I.

Für $A-\lambda I$ schreiben wir kurz $A-\lambda$, und für $f-\lambda \operatorname{id}_V$ ebenso $f-\lambda$.
Diese Kurzschreibweise ist etwas nachlässig, aber manchmal bequem.

Das charakteristische Polynom

M205

Definition M2B: das charakteristische Polynom einer Matrix

Zur Matrix $A \in K^{n\times n}$ definieren wir das **charakteristische Polynom**

$$\tilde{P}_A(X) = \tilde{\chi}_A(X) := \det(A - XI) \in K[X].$$

Alternativ nutzen wir das **normierte charakteristische Polynom**

$$P_A(X) = \chi_A(X) := \det(XI - A) = (-1)^n \tilde{\chi}_A(X).$$

Dies ist tatsächlich ein Polynom, wie wir in Satz M2C nachrechnen.

⚠ Beide Konventionen sind in der Literatur üblich, aber uneinheitlich.
Das normierte Polynom hat immer Leitkoeffizient 1, das ist schöner.
Die unnormierte Variante ist in Rechnungen oft bequemer, da die Matrix A bereits vorliegt, und nur auf der Diagonalen jeweils X subtrahiert wird: Das ist per Hand leichter zu schreiben und vermeidet Vorzeichenfehler.
🙂 Beide Varianten unterscheiden sich nur in ungerader Dimension.
Für die Nullstellen (also Eigenwerte) spielt das Vorzeichen keine Rolle.
Auch für den Eigenraum gilt $\mathrm{Eig}(A,\lambda) = \ker(A - \lambda I) = \ker(\lambda I - A)$.

Das charakteristische Polynom

M206
Erläuterung

Zur Illustration betrachten wir ein einfaches Zahlenbeispiel:

$$A = \begin{bmatrix} 1 & 4 & 5 \\ 0 & 0 & 1 \\ 0 & 2 & 3 \end{bmatrix}$$

Der Übergang von A zu $A - XI$ ist etwas leichter auszuschreiben:

$$A - XI = \begin{bmatrix} 1-X & 4 & 5 \\ 0 & 0-X & 1 \\ 0 & 2 & 3-X \end{bmatrix}$$

Der Übergang von A zu $XI - A$ erfordert etwas mehr Änderungen:

$$XI - A = \begin{bmatrix} X-1 & -4 & -5 \\ -0 & X-0 & -1 \\ -0 & -2 & X-3 \end{bmatrix}$$

Für einen Computer ist der Unterschied unerheblich. Menschen jedoch machen (Schreib-)Fehler, daher biete ich Ihnen hier beide Varianten an.

Anwendungsbeispiel zum charakteristischen Polynom

M207

Aufgabe: (1) Berechnen Sie das charakteristische Polynom der Matrix

$$A = \begin{bmatrix} 1 & 4 & 5 \\ 0 & 0 & 1 \\ 0 & 2 & 3 \end{bmatrix} \in \mathbb{R}^{3\times 3}.$$

(2) Finden Sie damit alle Eigenwerte, also das Spektrum $\sigma(A;\mathbb{R})$.
(3) Ist A über $\mathbb{R}$ diagonalisierbar? (4) Falls ja, diagonalisieren Sie A.

Lösung: (1) Wir folgen der Definition und berechnen die Determinante:

$$\begin{aligned} \tilde{\chi}_A(X) = \begin{vmatrix} 1-X & 4 & 5 \\ 0 & -X & 1 \\ 0 & 2 & 3-X \end{vmatrix} &= (1-X)\big[-X(3-X) - 1\cdot 2\big] \\ &= (1-X)(X^2 - 3X - 2) \\ &= -X^3 + 4X^2 - X - 2 \end{aligned}$$

(2) Die Eigenwerte von A sind genau die Nullstellen von $\chi_A = -\tilde{\chi}_A$:

$$\sigma(A) = \{\, \lambda_1 = 1,\ \lambda_2 = \tfrac{1}{2}(3 - \sqrt{17}),\ \lambda_3 = \tfrac{1}{2}(3 + \sqrt{17}) \,\}$$

Anwendungsbeispiel zum charakteristischen Polynom

M208
Erläuterung

Summe von Monomen vs **Produkt von Linearfaktoren**

$$X^3 - 4X^2 + X + 2 \longleftarrow (X-1)(X^2 - 3X - 2) \longrightarrow (X-1)(X-\lambda_2)(X-\lambda_3)$$

Das Ausmultiplizieren (hier nach links) ist eine leichte Routineübung.
Das Faktorisieren (nach rechts) gelingt routiniert in kleinen Graden, ist im Allgemeinen jedoch eine schwieriges Problem.

In Frage (1) wollen wir das charakteristische Polynom bestimmen. Polynome können wir jedoch verschieden darstellen; implizit gemeint ist meist die Monomform, dazu multiplizieren wir alles geduldig aus.

Für die Frage (2) hingegen ist die Monomform nicht die beste Wahl! Wir suchen hier Nullstellen unseres Polynoms, also Linearfaktoren. Dazu geht das Ausmultiplizieren genau in die falsche Richtung; es ist schlauer, die bereits vorliegende partielle Faktorisierung zu nutzen.

⚠ In Klausuren ist das ein häufiger Fehler! Unnötige Umwege kosten Zeit und erhöhen die Wahrscheinlichkeit von Rechenfehlern. Sie sollten genau wissen, was Sie wollen und wie Sie es am besten erreichen.

Grad und Koeffizienten des char. Polynoms

Satz M2C: Grad und Koeffizienten des char. Polynoms

Zu $A \in K^{n\times n}$ ist $\tilde{\chi}_A(X) = \det(A - XI)$ ein Polynom von Grad n:

$$\tilde{\chi}_A(X) = a_0 - a_1 X \pm \cdots + (-1)^{n-1} a_{n-1} X^{n-1} + (-1)^n X^n$$

Normiert erhalten wir für $\chi_A(X) = \det(XI - A)$ demnach das Polynom:

$$\chi_A(X) = X^n - a_{n-1} X^{n-1} \pm \cdots + (-1)^{n-1} a_1 + (-1)^n a_0$$

Die extremen Koeffizienten erkennen wir wieder: $a_0 = \det(A)$ ist die **Determinante** und $a_{n-1} = \sum_{i=1}^{n} a_{ii} =: \operatorname{tr}(A)$ ist die **Spur** der Matrix A.

Beweis: Jeder Eintrag der Matrix $C = XI - A \in K[X]^{n\times n}$ hat Grad ≤ 1. Dank der Leibniz–Formel (L2G) hat $\chi_A = \det C$ den Grad $\leq n$ (G3B):

$$\chi_A = \det C = \textstyle\sum_{\tau\in S_n} \operatorname{sign}(\tau) \cdot c_{\tau(1),1} \cdot c_{\tau(2),2} \cdots c_{\tau(n),n}$$

Der Summand $(X - a_{11})(X - a_{22}) \cdots (X - a_{nn}) = X^n - X^{n-1} \operatorname{tr} A + \ldots$ für $\tau = \mathrm{id}$ hat Grad n. Alle weiteren Summanden haben Grad $\leq n - 2$, denn jede Permutation $\tau \neq \mathrm{id}$ hat höchstens $n - 2$ Fixpunkte. QED

Grad und Koeffizienten des char. Polynoms

Die Koeffizienten $a_0 = \det A$ und $a_{n-1} = \operatorname{tr} A$ haben eine besondere, klare Bedeutung, die anderen haben keine so leichte Interpretation.

⚠ Die charakteristische Matrix $XI - A \in K[X]^{n\times n}$ hat Koeffizienten im Polynomring $K[X]$. Wir rechnen also nicht mehr über dem Grundring K, sondern im Ring $K[X]$ der Polynome in der Variablen X über K.

🙂 Dazu ist alles vorbereitet, denn wir haben die Determinante wohlweislich gleich allgemein über kommutativen Ringen erklärt.

⚠ Manche Autoren arbeiten zunächst nur über einem Körper K, insbesondere für Matrizen und Determinanten, doch spätestens beim charakteristischen Polynom genügt dies genau genommen nicht mehr.

🙂 Man kann sich mit verschiedenen Tricks aus dieser misslichen Lage befreien, zum Beispiel können wir den Polynomring $K[X]$ einbetten in seinen Bruchkörper $K(X)$ der gebrochen-rationalen Funktionen (siehe Seite A139 und Satz E3L) und über diesem größeren Körper arbeiten.

Das Natürlichste scheint mir jedoch die allgemeine Betrachtung über kommutativen Ringen. Genau dafür haben wir alles sorgsam vorbereitet.

Konjugation und Ähnlichkeit von Matrizen

Wie ändert sich das charakteristische Polynom bei Basiswechsel?

Definition M2D: Konjugation und Ähnlichkeit von Matrizen

Sei K ein Ring und $n \in \mathbb{N}_{\geq 1}$. Die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$ operiert auf dem Matrizenring $K^{n\times n}$ durch Konjugation gemäß

$$K^{n\times n} \times \mathrm{GL}_n(K) \to K^{n\times n} : (A, T) \mapsto B = T^{-1} A T.$$

Zwei Matrizen $A, B \in K^{n\times n}$ heißen **ähnlich**, oder $\mathrm{GL}_n(K)$–konjugiert, falls es eine invertierbare Matrix $T \in \mathrm{GL}_n(K)$ mit $B = T^{-1}AT$ gibt.

Der Übergang von A zu B heißt auch **Ähnlichkeitstransformation** oder **Konjugation** vermöge T. Dies entspricht einem Basiswechsel.

Übung: Dies ist eine Äquivalenzrelation auf der Menge $K^{n\times n}$.

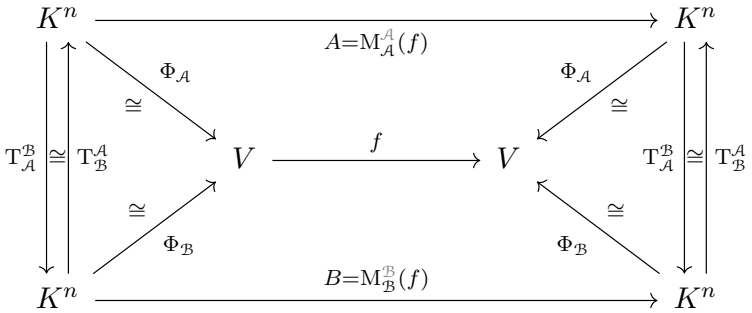
🙂 Diese Äquivalenzrelation wollen wir nutzen, um Matrizen soweit wie möglich zu vereinfachen: Wir wollen die vorgegebene Matrix A durch eine ähnliche, aber schönere Matrix B ersetzen. Im aktuellen Kontext geht es uns zunächst darum, dass B diagonal wird, falls möglich.

Konjugation und Ähnlichkeit von Matrizen

Lemma M2E: Ähnlichkeit und Basiswechsel

Seien $A, B \in K^{n\times n}$. Die folgenden Aussagen sind gleichbedeutend:

1. Die Matrizen A und B sind ähnlich, also $\mathrm{GL}_n(K)$–konjugiert.
2. Beide sind darstellende Matrizen eines Endomorphismus $f \in \mathrm{End}_K(V)$ bezüglich geeigneter Basis $\mathcal{A}$ und $\mathcal{B}$ von V.



In $K^{n\times n}$ haben wir $B = T^{-1} \cdot A \cdot T$ mit $T = \mathrm{T}_{\mathcal{B}}^{\mathcal{A}}$ und $T^{-1} = \mathrm{T}_{\mathcal{A}}^{\mathcal{B}}$.

Das charakteristische Polynom eines Endomorphismus

M213

Satz M2F: Invarianz und Wohldefiniertheit des char. Polynoms

Sei K ein Körper.

1. Sind A und B in $K^{n\times n}$ ähnlich, so folgt $\chi_A = \chi_B$ in $K[X]$.
2. Zu $f \in \mathrm{End}_K(V)$ wie oben ist $\chi_f := \chi_A = \chi_B$ wohldefiniert.

Beweis: (1) Wir haben $B = T^{-1}AT$ mit $T \in \mathrm{GL}_n(K)$. Daraus folgt:

$$\begin{aligned}
\chi_B(X) &\overset{\text{Def}}{=} \det(XI - B)\\
&\overset{\text{Vor}}{=} \det(XI - T^{-1}AT)\\
&\overset{\text{Com}}{=} \det\left[T^{-1}(XI - A)T\right]\\
&\overset{\text{L2N}}{=} \det(T^{-1}) \cdot \det(XI - A) \cdot \det(T)\\
&\overset{\text{Def}}{=} \chi_A(X)
\end{aligned}$$

(2) Für $A = \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f)$ und $B = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f)$ wie in M2E gilt $B = T^{-1}AT$. QED

🙂 Die implizite Definition (2) formulieren wir nun explizit aus.

Das charakteristische Polynom eines Endomorphismus

M214
Erläuterung

Definition M2G: das char. Polynom eines Endomorphismus

Sei K ein Körper und V ein K–Vektorraum mit $\dim_K(V) = n < \infty$.

Zu jedem Endomorphismus $f : V \to V$ über K definieren wir sein **charakteristisches Polynom** $\chi_f \in K[X]$ wie folgt.

Wir wählen eine Basis $\mathcal{A}$ von V und stellen f dar durch die zugehörige Matrix $A = \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f) \in K^{n\times n}$. Damit definieren wir das Polynom:

$$\boxed{\chi_f := \det(XI - A) \in K[X]}$$

Dank Satz M2F ist das Ergebnis χ_f wohldefiniert, da unabhängig von der willkürlich gewählten Basis $\mathcal{A}$.

🙂 Sie sehen hier sehr schön: Manchmal können wir eine Definition erst nach einem Satz aussprechen, der den Weg zum Begriff bereitet. Das geschieht immer dann, wenn die Wohldefiniertheit zu klären ist, bzw. Existenz und Eindeutigkeit des zu definierenden Gegenstands. So gesehen müsste ich auch Definition M2B und Satz M2C umdrehen.

Das char. Polynom ist keine vollständige Invariante.

M215

Je zwei ähnliche Matrizen haben dasselbe charakteristische Polynom. Somit ist $K^{n\times n} \to K[X]^1_n : A \mapsto \chi_A$ eine Invariante unter Ähnlichkeit.

Sie ist jedoch noch keine vollständige Invariante. Es gibt Matrizen, die dasselbe charakteristische Polynom haben, aber nicht ähnlich sind.

Aufgabe: Sind die folgenden Matrizen ähnlich?

$$A = \begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix} \quad \text{vs} \quad B = \begin{bmatrix}\lambda & 1\\ 0 & \lambda\end{bmatrix}$$

Lösung: (1) Die charakteristischen Polynome sind gleich:

$$\chi_A = \chi_B = (X - \lambda)^2$$

(2) Dennoch sind die Matrizen A und B nicht ähnlich:
A ist diagonal, doch B ist nicht diagonalisierbar (M1D).

Das char. Polynom ist keine vollständige Invariante.

M216
Erläuterung

🙂 Aus $\chi_A \neq \chi_B$ schließen wir, dass A und B nicht ähnlich sind. Das ist der klare, einfache Fall und gilt allgemein für jede Invariante: Sind χ_A und χ_B verschieden, so können A und B nicht ähnlich sein.

⚠ Die Umkehrung gilt nicht: Aus $\chi_A = \chi_B$ können wir im Allgemeinen noch nicht schließen, dass A und B ähnlich sind. Hierzu sind weitere Untersuchungen notwendig. Genau das zeigt dieses Beispiel!

Bemerkung: Für $\lambda = 0$ ist dies besonders augenfällig:

$$A = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix} \quad \text{vs} \quad B = \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$$

Auch der Rang einer Matrix ist invariant unter Ähnlichkeit $A \mapsto T^{-1}AT$, noch allgemeiner sogar unter Äquivalenz $A \mapsto S^{-1}AT$, siehe Satz K2H.

Hier gilt $\operatorname{rang} A = 0$ und $\operatorname{rang} B = 1$, also sind A und B nicht ähnlich, nicht einmal äquivalent: $B \neq S^{-1}AT$ für alle $S, T \in \mathrm{GL}_2\,\mathbb{K}$.

Das charakteristische Polynom eines Produkts

⚠ Für das charakteristische Polynom gilt schon aus Gradgründen:

$$\chi_{A\cdot B} \neq \chi_A \cdot \chi_B$$

🙂 Die Determinante ist multiplikativ (Satz L2N)

$$\det(A \cdot B) = \det(A) \cdot \det(B),$$

☹ die Spur jedoch nicht:

$$\operatorname{tr}(A \cdot B) \neq \operatorname{tr}(A) \cdot \operatorname{tr}(B)$$

Ein besonders einfaches, wahrhaft minimalistisches Gegenbeispiel ist

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{und} \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{mit} \quad AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Übung: Um sich gegen solch naiven Irrglauben zu immunisieren, erfinden und berechnen Sie selbst geeignete Gegenbeispiele!

Das charakteristische Polynom eines Produkts

Für die Determinante $\det : K^{n\times n} \to K$ gilt dank Multiplikativität L2N:

$$\det(A \cdot B) = \det(A) \cdot \det(B) = \det(B) \cdot \det(A) = \det(A \cdot B)$$

für alle $A, B \in K^{n\times n}$. Die Spur $\operatorname{tr} : K^{n\times n} \to K$ ist nicht multiplikativ, doch dank Satz B1J ebenfalls invariant unter zyklischer Vertauschung:

$$\operatorname{tr}(A \cdot B) = \operatorname{tr}(B \cdot A).$$

Frage: Gilt dies sogar für das gesamte charakteristische Polynom?

$$\chi_{AB} \overset{?}{=} \chi_{BA}$$

Teilantwort: Ist eine der beiden Matrizen A oder B invertierbar, so folgt dies aus der Invarianz M2F unter Konjugation / Ähnlichkeit:

$$\chi_{AB} = \chi_{A^{-1}(AB)A} = \chi_{BA}$$
$$\chi_{AB} = \chi_{B(AB)B^{-1}} = \chi_{BA}$$

🙂 Satz M2H verallgemeinert dies auf nicht-invertierbare Matrizen.

Das charakteristische Polynom eines Produkts

Satz M2H: das charakteristische Polynom eines Produkts

(0) Für je zwei rechteckige Matrizen $A \in K^{m\times n}$ und $B \in K^{n\times m}$ gilt

$$\chi_{AB} \cdot X^n = \chi_{BA} \cdot X^m.$$

(1) Für je zwei quadratische Matrizen $A, B \in K^{n\times n}$ gilt

$$\chi_{AB} = \chi_{BA}.$$

Aus (0) folgt (1) dank $m = n$ und Kürzung des Faktors $X^m = X^n$. Umgekehrt folgt (0) aus (1) durch Auffüllen mit Nullzeilen/spalten.

Für Determinante und Spur ist die Aussage klar, wie zuvor erklärt. Dies sind beiden extremen Koeffizienten des Polynoms (Satz M2C).

Die Koeffizienten zwischen Spur und Determinante in $\chi_{AB} = \chi_{BA}$ haben keine so leichte Interpretation, doch auch sie sind invariant unter zyklischer Vertauschung der Matrixfaktoren von AB zu BA.

Das charakteristische Polynom eines Produkts

Beweis: (0) Wir berechnen zunächst folgende Matrixprodukte:

$$\begin{bmatrix} XI_m & -A \\ 0 & I_n \end{bmatrix} \cdot \begin{bmatrix} I_m & A \\ B & XI_n \end{bmatrix} \overset{(a)}{=} \begin{bmatrix} XI_m - AB & 0 \\ B & XI_n \end{bmatrix}$$
$$\begin{bmatrix} XI_m & 0 \\ -B & I_n \end{bmatrix} \cdot \begin{bmatrix} I_m & A \\ B & XI_n \end{bmatrix} \overset{(b)}{=} \begin{bmatrix} XI_m & XA \\ 0 & XI_n - BA \end{bmatrix}$$

Dank Multiplikativität der Determinante L2N und Satz L2V folgt:

$$\det(XI_m - AB)X^n \overset{(a)}{=} \begin{vmatrix} I_m & A \\ B & XI_n \end{vmatrix} X^m \overset{(b)}{=} \det(XI_n - BA)X^m$$

Das ist trickreich-raffiniert. Rechnen Sie es nach! QED

Das ist eine gefürchtete Übungsaufgabe (oder Klausuraufgabe?) aus Paul Halmos, *Finite dimensional vector spaces* (1958), §53, exercise 13.

🙂 Ohne den Trick oder einen Hinweis ist es schwer, mit ist es leicht. Liegen die Formeln erst einmal vor uns, so genügt Nachrechnen.

Das Standardverfahren zur Diagonalisierung

M225

Verfahren M2I: Standardverfahren zur Diagonalisierung

Sei K ein Körper und V ein n–dimensionaler K–Vektorraum.
Gegeben sei ein Endomorphismus $f : V \to V$ über K.

(1) Wähle eine Basis $\mathcal{A}$ von V und bestimme $A = \mathrm{M}_{\mathcal{A}}(f) \in K^{n\times n}$.

(2) Berechne das charakteristische Polynom $\chi_f = \det(XI - A) \in K[X]$.

(3) Bestimme alle Nullstellen, $\sigma(f) = \sigma(f; K) = \{\, \lambda \in K \mid \chi_f(\lambda) = 0 \,\}$.

(4) Zu $\lambda \in \sigma(f)$ bestimme den Eigenraum $\mathrm{Eig}(f, \lambda) = \ker(f - \lambda)$.

Genau dann ist f diagonalisierbar, wenn $V = \bigoplus_{\lambda\in\sigma(f)} \mathrm{Eig}(f, \lambda)$ gilt, also die Dimensionsgleichung $n = \sum_{\lambda\in\sigma(f)} \dim_K \mathrm{Eig}(f, \lambda)$ erfüllt ist.

(5) In diesem Falle wähle eine Basis $\mathcal{B}$ von V aus Eigenvektoren und erhalte die ersehnte Darstellung $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$.

🙂 Schritte (1,2,4,5) sind Routineaufgaben der Linearen Algebra.
Hierzu kennen Sie effiziente Algorithmen (mit Aufwand $\le \mathrm{const} \cdot n^4$).

☹ Allein die Suche nach Nullstellen (3) ist im Allgemeinen schwierig.
Dieses Problem gehört zur (nicht-linearen!) Algebra bzw. Numerik.

Das Standardverfahren zur Diagonalisierung

M226
Erläuterung

Dieses Verfahren *können* Sie immer anwenden, insbesondere wenn keine weitere Information vorliegt. Zur Diagonalisierung *müssen* Sie nicht so vorgehen, manchmal sind auch geschickte Abkürzungen oder raffinierte Tricks möglich. Diese sollten Sie erkennen, um sich unnötige Arbeit und längliche Umwege zu ersparen, siehe Übungen (etwa M313).

Beispiel: Ist der Körper K klein doch die Matrix $A \in K^{n\times n}$ recht groß, etwa $\sharp K < n$, dann kann man Schritte (2) und (3) überspringen, und in (4) alle Kandidaten $\lambda \in K$ einsetzen und direkt $\ker(A - \lambda I)$ berechnen.

Das Standardverfahren verdeutlicht einige wichtige Eigenschaften:
Alle Schritte (bis auf Punkt 3) sind Routineaufgaben der Linearen Algebra. Diese können von einem Computer übernommen werden.
Der Rechenaufwand ist dabei polynomiell, höchstens $\mathrm{const} \cdot n^4$.

Kritisch ist und bleibt einzig der Punkt 3: die Bestimmung der Nullstellen. Wenn dieser gelingt, sei es durch günstige Umstände der gegebenen Daten oder durch zusätzliche Überlegungen zur vorliegenden Struktur, so ist das Diagonalisierungsproblem insgesamt gelöst.

Schnelle Berechnung des charakteristischen Polynoms

M227
Erläuterung

Wie schnell können wir das charakteristische Polynom berechnen?

Satz M2J: Berechnung des charakteristischen Polynoms

Sei K ein Körper mit Elementezahl $\sharp K \ge n$.

Zu jeder Matrix $A \in K^{n\times n}$ können wir das charakteristische Polynom $\chi_A \in K[X]_n^1$ berechnen mit $\le n^4$ arithmetischen Operationen in K.

Dies gelingt trickreich und genial-einfach durch Lagrange–Interpolation:

Algo M2J: Berechnung des charakteristischen Polynoms

Eingabe: eine Matrix $A \in K^{n\times n}$ über K, wobei $\sharp K \ge n$
Ausgabe: das charakteristische Polynom $\chi_A \in K[X]_n^1$

1: Wähle n verschiedene Stützstellen $x_1, \ldots, x_n \in K$.
2: Berechne die Werte $y_k = \det(x_k I - A)$ dank Gauß L2X.
3: Rekonstruiere $\chi_A \in K[X]_n^1$ dank Lagrange–Interpolation B3A.

Übung: Führen Sie die Details aus und beweisen Sie den Satz.

Schnelle Berechnung des charakteristischen Polynoms

M228
Erläuterung

In Übungsaufgaben und Klausuren berechnen Sie charakteristische Polynome meist für kleine Matrizen, etwa $n = 2, 3, 4$. Es gelingt auch noch für große, strukturierte Matrizen, etwa Begleitmatrizen M2Q.

🙂 Zur Behandlung von großen, unstrukturierten Matrizen nutzen Sie sinnvollerweise ein Computer-Algebra-System (CAS). Damit stellt sich die dringende Frage, auch für Sie als Nutzer/in, wie der Computer damit effizient umgehen soll, und welcher Rechenaufwand zu erwarten ist.

⚠ Die Leibniz–Formel L2G und die Laplace–Entwicklung L2Z erfordern schlimmstenfalls exponentiellen Aufwand, nämlich $n \cdot n!$ Operationen. Das überfordert selbst Supercomputer für moderate n, siehe L259.

🙂 Die Berechnung mit n^4 Operationen ist zwar immer noch aufwändig für sehr große n, aber effizient genug für viele Anwendungen mittlerer Größe, genau so wie Gauß: Für typische Laufzeiten siehe B216.

🙂 Der Algorithmus von Faddeev–LeVerrier erreicht dasselbe Ergebnis unter der Voraussetzung $\mathrm{char}\, K > n$. Für Details verweise ich auf `de.wikipedia.org/wiki/Algorithmus_von_Faddejew-Leverrier`.

Zerfällung von Polynomen in Linearfaktoren

Definition M2K: Zerfällung von Polynomen in Linearfaktoren

(0) Das Polynom $P \in K[X] \setminus \{0\}$ **zerfällt** über K in Linearfaktoren, falls

$$P(X) = c(X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n) \quad \text{mit } \lambda_1, \lambda_2, \ldots, \lambda_n \in K.$$

Wir sagen hierzu kurz, P zerfällt über K oder P ist K–zerfallend.

(1) Das Polynom P **zerfällt einfach** oder ist **einfach zerfallend**, falls alle Nullstellen einfach sind, also $\lambda_i \neq \lambda_j$ für alle $i \neq j$ gilt.

(2) Durch Zusammenfassen mehrfacher Nullstellen erhalten wir $P(X) = c(X-\mu_1)^{r_1}\cdots(X-\mu_k)^{r_k}$ mit Nullstellen $\mu_1, \ldots, \mu_k \in K$ und Vielfachheiten $r_1, \ldots, r_k \in \mathbb{N}_{\geq 1}$, wobei $\mu_i \neq \mu_j$ für $i \neq j$ gilt.

Der Exponent $r_i =: \operatorname{ord}(P, \mu_i)$ heißt (Nullstellen-)**Ordnung** oder (algebraische) **Vielfachheit** der Nullstelle μ_i im Polynom P.

Beispiele: $P = X^2 - 1 \in \mathbb{Q}[X]$ zerfällt gemäß $P = (X-1)(X+1)$.
$X^2 - 2 \in \mathbb{Q}[X]$ zerfällt nicht über $\mathbb{Q}$, aber über $\mathbb{R}$ in $(X-\sqrt{2})(X+\sqrt{2})$.
$X^2 + 1 \in \mathbb{Q}[X]$ zerfällt nicht über $\mathbb{R}$, aber über $\mathbb{C}$ in $(X-\mathrm{i})(X+\mathrm{i})$.

Zerfällung von Polynomen in Linearfaktoren

Alle bisherigen Begriffe und Verfahren der Linearen Algebra sind tatsächlich linear (im Sinne der mathematischen Struktur) und daher algorithmisch recht einfach (im Sinne der informatischen Komplexität).

Die Faktorisierung von Polynomen und speziell die Nullstellensuche verhalten sich dagegen spürbar anders, mathematisch und informatisch: Dieses Problem gehört zur (nicht-linearen!) Algebra bzw. Numerik.

Dieser Frage können wir nun nicht länger ausweichen. Alles weitere ist wieder originärer Bestandteil der Linearen Algebra, doch um überhaupt weiter arbeiten zu können, müssen wir uns um Nullstellen kümmern.

Definition M2K klärt zunächst die nötigen Begriffe und benennt das zu erreichende Ziel: Wir wollen jedes Polynom in Linearfaktoren zerlegen.

🙂 Über den komplexen Zahlen $\mathbb{C}$ lässt sich dies immer erreichen, genau dies ist die Aussage des Fundamentalsatzes der Algebra.

Algebraisch abgeschlossene Körper

♦ Satz A3C: Fundamentalsatz der Algebra

Jedes komplexe Polynom $P \in \mathbb{C}[X]$ zerfällt über $\mathbb{C}$. Ausführlich:

Zu jedem Polynom $P(X) = X^n + c_1 X^{n-1} + \cdots + c_n$ mit $c_1, \ldots, c_n \in \mathbb{C}$ existieren Nullstellen $z_1, \ldots, z_n \in \mathbb{C}$ sodass $P(X) = (X-z_1)\cdots(X-z_n)$.

Definition M2L: algebraischer Abschluss

Seien $C \geq K$ Körper, zum Beispiel $\mathbb{C} \geq \mathbb{R}$. Wir nennen C **algebraisch abgeschlossen**, falls jedes Polynom $P \in C[X]$ über C zerfällt.

Die Körpererweiterung $C \geq K$ ist **algebraisch**, falls jedes Element $a \in C$ Nullstelle eines geeigneten Polynoms $P \in K[X]$ ist.

Wir nennen $C \geq K$ einen **algebraischen Abschluss** der Körpers K, falls C algebraisch ist über K und zudem algebraisch abgeschlossen.

Beispiel: Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen, $\mathbb{R}$ jedoch nicht. Die Erweiterung $\mathbb{C} \geq \mathbb{R}$ ist ein algebraischer Abschluss des Körpers $\mathbb{R}$.

Algebraisch abgeschlossene Körper

🙂 Daher arbeiten wir meist lieber mit dem Körper $\mathbb{C}$ statt mit $\mathbb{R}$. Glücklicherweise ist solch ein Abschluss über jedem Körper möglich:

Satz M2M: Existenz und Eindeutigkeit

Zu jedem Körper K existiert ein algebraischer Abschluss $C \geq K$.
Je zwei algebraische Abschlüsse C und C' von K sind isomorph.

Ich zitiere dies hier vor allem zur Beruhigung und als schönen Ausblick: Diese und weitere Konstruktionen lernen Sie in der Vorlesung *Algebra*.

🙂 Es besteht also kein grundsätzliches mathematisches Problem: Wir können prinzipiell jedes Polynom in Linearfaktoren zerlegen, notfalls nutzen wir hierzu eine geeignete Körpererweiterung.

⚠ Die algorithmischen Fragen hingegen sind überaus anspruchsvoll und führen zu zwei wichtigen, modernen und tiefliegenden Themen: einerseits die Computeralgebra für exaktes, symbolisches Rechnen, andererseits die Numerik für effiziente Näherungslösungen.
Beide gehören zum mathematischen Werkzeugkasten.

Einfache Zerfällung impliziert Diagonalisierbarkeit.

Der folgende Spezialfall ist besonders einfach und sympathisch:

Satz M2N: Einfache Zerfällung impliziert Diagonalisierbarkeit.

Angenommen $f \in \mathrm{End}_K(V)$ hat ein einfach zerfallendes Polynom, also

$$\chi_f(X) = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n)$$

mit n Nullstellen $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$, wobei $\lambda_i \neq \lambda_j$ für alle $i \neq j$.

(1) In diesem Falle ist f diagonalisierbar, denn es gilt

$$V = \mathrm{Eig}(f,\lambda_1) \oplus \mathrm{Eig}(f,\lambda_2) \oplus \cdots \oplus \mathrm{Eig}(f,\lambda_n).$$

(2) Wir erhalten eine Eigenbasis $\mathcal{B} = (v_1, v_2, \ldots, v_n)$ durch Wahl von Eigenvektoren $v_i \in \mathrm{Eig}(f,\lambda_i) \smallsetminus \{0\}$. Somit wird f dargestellt durch

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n).$$

Beweis: Wegen $\dim_K \mathrm{E}(\lambda_i) \geq 1$ hat $\mathrm{E} = \bigoplus_{i=1}^n \mathrm{E}(\lambda_i) \leq V$ mindestens die Dimension n. Andererseits gilt $\dim_K V = n$, also $\mathrm{E} = V$. QED

Einfache Zerfällung impliziert Diagonalisierbarkeit.

Im allgemeinen Fall muss das char. Polynom $\chi_f \in K[X]$ nicht zerfallen, siehe etwa das Beispiel M1E. Selbst wenn $\chi_f \in K[X]$ über K zerfällt, kann es mehrfache Nullstellen haben, siehe Beispiele M1C und M1D. In diesem Falle ist zur Diagonalisierung noch kein Urteil möglich: f kann diagonalisierbar sein (M1C) oder auch nicht (M1D).

Im Falle mehrfacher Nullstellen hilft letztlich nur die Bestimmung der Eigenräume und insbesondere ihrer Dimension (Satz M1I):

Genau dann ist f diagonalisierbar, wenn $V = \bigoplus_{\lambda\in\sigma(f)} \mathrm{Eig}(f,\lambda)$ gilt, also die Dimensionsgleichung $n = \sum_{\lambda\in\sigma(f)} \dim_K \mathrm{Eig}(f,\lambda)$ erfüllt ist.

Das ist genau dann der Fall, wenn zu jedem Eigenwert $\lambda \in K$ die geometrische und die algebraische Vielfachheit übereinstimmen (M2O).

Hierzu zeigen wir die folgende nützliche Ungleichung: Die geometrische Vielfachheit ist immer kleiner oder gleich der algebraischen Vielfachheit. Das ist eine recht einfache, aber ebenso grundlegende Beobachtung, die wir anschließend in Theorie und Praxis überall nutzen werden.

Geometrische und algebraische Vielfachheit

Satz M2O: geometrische und algebraische Vielfachheit

(1) Für jeden Eigenwert $\lambda \in \sigma(f)$ gilt

$$1 \leq \dim_K \mathrm{Eig}(f,\lambda) \leq \mathrm{ord}(\chi_f,\lambda) \leq \dim V$$

(2) Genau dann ist f diagonalisierbar, wenn (a) χ_f über K zerfällt und (b) für jeden Eigenwert $\lambda \in \sigma(f)$ gilt $\dim_K \mathrm{Eig}(f,\lambda) = \mathrm{ord}(\chi_f,\lambda)$:

„Die geometrische Vielfachheit erreicht die algebraische.“

Beweis: (1) Wir ergänzen eine Basis $\mathcal{B} = (v_1, \ldots, v_k)$ von $\mathrm{Eig}(f,\lambda)$ zu einer Basis $\mathcal{A} = (v_1, \ldots, v_k, \ldots, v_n)$ von V und erhalten die Darstellung

$$A = \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f) = \begin{bmatrix} B & * \\ 0 & C \end{bmatrix} \quad \text{mit } B = \lambda \cdot I_k.$$

Somit gilt $\chi_A = \chi_B \cdot \chi_C = (X-\lambda)^k Q$ und $\dim_K \mathrm{Eig}(f,\lambda) \leq \mathrm{ord}(\chi_f,\lambda)$.

(2) Dies folgt aus der Eigenraumzerlegung M1I, dank der Gleichung $\sum_{\lambda\in\sigma(f)} \dim_K \mathrm{Eig}(f,\lambda) \overset{\text{(b)}}{=} \sum_{\lambda\in\sigma(f)} \mathrm{ord}(\chi_f,\lambda) \overset{\text{(a)}}{=} n = \dim V$. QED

Geometrische und algebraische Vielfachheit

(2a) Die rechte Gleichung $\sum_{\lambda\in\sigma(f)} \mathrm{ord}(\chi_f,\lambda) = n$ ist genau dann erfüllt, wenn das charakteristische Polynom χ_f zerfällt. Andernfalls enthält

$$\chi_f = (X-\lambda_1)^{r_1} \cdots (X-\lambda_k)^{r_k} Q$$

einen nicht-trivialen Faktor $Q \in K[X]$ ohne Nullstellen in K. Aus

$$\textstyle\sum_{\lambda\in\sigma(f)} \mathrm{ord}(\chi_f,\lambda) + \deg Q = n$$

mit $\deg Q > 0$ folgt somit $\sum_{\lambda\in\sigma(f)} \mathrm{ord}(\chi_f,\lambda) < n$.

(2b) Die linke Gleichung

$$\textstyle\sum_{\lambda\in\sigma(f)} \dim_K \mathrm{Eig}(f,\lambda) = \sum_{\lambda\in\sigma(f)} \mathrm{ord}(\chi_f,\lambda)$$

ist genau dann erfüllt, wenn summandenweise

$$\dim \mathrm{Eig}(f,\lambda) = \mathrm{ord}(\chi_f,\lambda)$$

für jeden Eigenwert λ gilt. Dank (1) gilt „$\leq$“ in jedem Summanden; gilt hierbei auch nur einmal die strikte Ungleichung „$<$“, so kann dies durch die anderen Summanden nicht mehr ausgeglichen werden.

Anwendungsbeispiel zur Diagonalisierung

Aufgabe: Ist A über $\mathbb{R}$ diagonalisierbar? Falls ja, diagonalisieren Sie A!

$$A = \begin{bmatrix} 1 & 4 & 5 \\ 0 & 0 & 1 \\ 0 & 2 & 3 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 4 & 5 \\ 0 & 0 & 2 \\ 0 & 2 & 3 \end{bmatrix}$$

Lösung: (1a) Wir bestimmen das charakteristische Polynom:

$$\begin{aligned} \tilde{\chi}_A(X) = \begin{vmatrix} 1-X & 4 & 5 \\ 0 & -X & 1 \\ 0 & 2 & 3-X \end{vmatrix} &= (1-X)\big[-X(3-X) - 1 \cdot 2\big] \\ &= (1-X)(X^2 - 3X - 2) \\ &= -X^3 + 4X^2 - X - 2 \end{aligned}$$

(1b) Die Nullstellen von $\chi_A = -\tilde{\chi}_A$ sind die Eigenwerte von A:

$$\sigma(A) = \{\, \lambda_1 = 1,\ \lambda_2 = \tfrac{1}{2}(3 - \sqrt{17}),\ \lambda_3 = \tfrac{1}{2}(3 + \sqrt{17}) \,\}$$

(1c) Da χ_A einfach zerfällt, schließen wir, dass A diagonalisierbar ist.

Anwendungsbeispiel zur Diagonalisierung

(1d) Die Diagonalisierung verläuft weiter nach Standardverfahren M2ı:

$$D = T^{-1}AT = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2}(3 - \sqrt{17}) & 0 \\ 0 & 0 & \frac{1}{2}(3 + \sqrt{17}) \end{bmatrix}$$

$$T = \begin{bmatrix} 1 & \frac{1}{8}(15 - \sqrt{17}) & \frac{1}{8}(15 + \sqrt{17}) \\ 0 & \frac{1}{4}(-3 - \sqrt{17}) & \frac{1}{4}(-3 + \sqrt{17}) \\ 0 & 1 & 1 \end{bmatrix}$$

$$T^{-1} = \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{9}{4} \\ 0 & -\frac{2}{\sqrt{17}} & \frac{1}{2} - \frac{3}{2\sqrt{17}} \\ 0 & +\frac{2}{\sqrt{17}} & \frac{1}{2} + \frac{3}{2\sqrt{17}} \end{bmatrix}$$

Die Rechnungen sind Routine, etwa für ein Computer-Algebra-System (CAS), doch für die Handrechnung nicht ganz kurz. Obwohl die Matrix A über $\mathbb{Q}$ gegeben ist, sind Rechnungen in der Körpererweiterung $\mathbb{Q}[\sqrt{17}]$ nötig. Auch das gelingt letztlich problemlos, wie wir in Kapitel A bereits gesehen haben. **Übung:** Machen Sie die Probe! Was ist zu prüfen?

Anwendungsbeispiel zur Diagonalisierung

Wir führen das Standardverfahren ebenso für die Matrix B aus.

Lösung: (2a) Wir bestimmen das charakteristische Polynom:

$$\begin{aligned} \tilde{\chi}_B(X) = \begin{vmatrix} 1-X & 4 & 5 \\ 0 & -X & 2 \\ 0 & 2 & 3-X \end{vmatrix} &= (1-X)\big[-X(3-X) - 2 \cdot 2\big] \\ &= (1-X)(X^2 - 3X - 4) \\ &= -X^3 + 4X^2 + X - 4 \end{aligned}$$

(2b) Die Nullstellen von $\chi_B = -\tilde{\chi}_B$ sind die Eigenwerte von B:

$$\sigma(B) = \{\, \lambda_1 = 1,\ \lambda_2 = -1,\ \lambda_3 = 4 \,\}$$

(2c) Da χ_B einfach zerfällt, schließen wir, dass B diagonalisierbar ist.

☺ Die Matrizen A und B unterscheiden sich nur an einer Stelle. Die Rechnungen für B sind dennoch spürbar einfacher.

Anwendungsbeispiel zur Diagonalisierung

(2d) Die Diagonalisierung verläuft weiter nach Standardverfahren M2ı:

$$D = T^{-1}BT = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$

$$T = \begin{bmatrix} 1 & 3 & 14 \\ 0 & -4 & 3 \\ 0 & 2 & 6 \end{bmatrix}$$

$$T^{-1} = \begin{bmatrix} 1 & -\frac{1}{3} & -\frac{16}{3} \\ 0 & -\frac{1}{5} & -\frac{1}{10} \\ 0 & -\frac{1}{15} & -\frac{2}{15} \end{bmatrix}$$

☺ Alle Eigenwerte liegen in $\mathbb{Q}$, das vereinfacht die Rechnung spürbar!

Übung: Machen Sie auch hier die Probe! Was ist zu prüfen?

Beispiel: symmetrische reelle Matrizen

Beispiel M2P: symmetrische reelle 2×2–Matrix

Zu $a, b, c \in \mathbb{R}$ betrachten wir die symmetrische Matrix

$$A = \begin{bmatrix} a & b \\ b & c \end{bmatrix} \in \mathbb{R}^{2\times 2}.$$

Ist A über $\mathbb{R}$ diagonalisierbar? Ihr charakteristisches Polynom ist

$$\chi_A = \begin{vmatrix} a-X & b \\ b & c-X \end{vmatrix} = X^2 - (a+c)X + (ac - b^2).$$

Die Diskriminante ist $D = (a+c)^2 - 4(ac-b^2) = (a-c) + 4b^2 \geq 0$.

Somit zerfällt $\chi_A = (X-\lambda_1)(X-\lambda_2)$ mit $\lambda_{1/2} = \frac{1}{2}(a+c \pm \sqrt{D}) \in \mathbb{R}$.

- Bei $D > 0$ zerfällt χ_A einfach, daher ist A diagonalisierbar (M2N).
- Bei $D = 0$ gilt $b = 0$ und $a = c$, somit ist A bereits diagonal.

☺ Jede symmetrische Matrix $A \in R^{2\times 2}$ ist $\mathbb{R}$–diagonalisierbar.

Beispiel: symmetrische reelle Matrizen

☺ Das ist ein sehr schönes, allgemeines und nützliches Ergebnis:
Wir betrachten eine symmetrische reelle Matrix $A \in \mathbb{R}^{n\times n}$, also $A^\intercal = A$.

Der erste interessante Fall ist die Dimension $n = 2$:
Das obige Beispiel zeigt, dass A diagonalisierbar ist.

Dies beweisen wir später allgemein in jeder Dimension $n \in \mathbb{N}$:
Jede symmetrische reelle Matrix ist über $\mathbb{R}$ diagonalisierbar!

Die Ausführung der Diagonalisierung erfordert wie immer die explizite Berechnung einer Eigenbasis. Im Falle $n = 2$ gelingt dies bereits jetzt ganz direkt. Im allgemeinen Fall werden wir dies später genauer noch untersuchen und hilfreiche Werkzeuge erarbeiten.

Übung: Diagonalisieren Sie die obige Matrix A im Falle $b > 0$.
(1) Untersuchen Sie einige konkrete Zahlenbeispiele.
(2) Entwickeln Sie eine allgemeine Formel.

Normiertes Polynom und seine Begleitmatrix

Tritt jedes normierte Polynom als charakteristisches Polynom auf? Ja!

Satz M2Q: normiertes Polynom und seine Begleitmatrix

Sei K ein Körper. Gegeben sei ein normiertes Polynom

$$P = X^n + p_1 X^{n-1} + \cdots + p_n X^0 \in K[X]_n^1.$$

Hierzu definieren wir die **Begleitmatrix** (engl. *companion matrix*):

$$C = C(P) := \begin{bmatrix} 0 & 0 & \dots & 0 & -p_n \\ 1 & 0 & \dots & 0 & -p_{n-1} \\ 0 & 1 & \ddots & \vdots & -p_{n-2} \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -p_1 \end{bmatrix} \in K^{n\times n}$$

(1) Ihr charakteristisches Polynom ist P. (2) Genau dann ist C über K diagonalisierbar, wenn $P = (X-\lambda_1)\cdots(X-\lambda_n)$ einfach zerfällt.

In diesem Falle gelingt die Diagonalisierung $VCV^{-1} = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ mit der Vandermonde–Matrix $V = (\lambda_i^j)_{i=1,\dots,n}^{j=0,\dots,n-1} \in \mathrm{GL}_n(K)$, siehe B3A.

Normiertes Polynom und Begleitmatrix

Einfache Zerfällung ist immer hinreichend für Diagonalisierbarkeit (M2N). Satz M2Q besagt speziell für die Begleitmatrix $C = C(P)$, dass einfache Zerfällung auch notwendig ist und gibt explizit eine Eigenbasis an.

Übung: (1) Berechnen Sie das Polynom, hier $\chi_C = P$, indem Sie die charakteristische Matrix $XI - C$ nach der letzten Spalte entwickeln.

(2a) Für jeden Skalar $\lambda \in K$ gilt $\dim \operatorname{Eig}(C, \lambda) \leq 1$,
denn die Matrix $\lambda I - C$ hat mindestens Rang $n-1$.

(2b) Wie folgt daraus das Diagonalisierbarkeitskriterium?
Warum ist es hier nicht nur hinreichend, sondern auch notwendig?

(2c) Die Eigenvektoren finden wir auf ganz natürliche Weise in den folgenden Untersuchungen zur linearen Rekursionen. Sie können es jetzt schon direkt versuchen, oder anschließend darauf zurückkommen.

☺ Die inverse Matrix V^{-1} ist mühsam, wie so oft. Für die Probe ist sie gar nicht nötig: Es genügt sicherzustellen, dass V invertierbar ist (B3A), und statt $VCV^{-1} = D$ die äquivalente Gleichung $VC = DV$ zu prüfen.

Anwendungsbeispiel: die Fibonacci–Folge

M245

Die Fibonacci–Folge $f : \mathbb{N} \to \mathbb{N} : n \mapsto f_n$ ist definiert durch die Startwerte $f_0 = 0$ und $f_1 = 1$ sowie für $n \in \mathbb{N}_{\geq 2}$ die **Rekursionsvorschrift**

$$f_n = f_{n-1} + f_{n-2}.$$

Die ersten Werte sind demnach:

n	0	1	2	3	4	5	6	7	8	9	...
f_n	0	1	1	2	3	5	8	13	21	34	...

Leonardo Fibonacci beschrieb damit im Jahr 1202 das Wachstum einer Kaninchenpopulation; in der Natur ist sie ein recht häufiges Muster.

Für alle $n \in \mathbb{N}$ gilt die phantastische **Binet–Formel**

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Übung: (1) Wie *beweisen* Sie die gegebene Formel? Induktion! (C443)
(2) Wie *finden* Sie eine solche Formel? Eigenwerte und Eigenvektoren!

Anwendungsbeispiel: die Fibonacci–Folge

M246
Erläuterung

Näherungswerte sind $\phi = \frac{1+\sqrt{5}}{2} \approx 1.618$ und $\psi = \frac{1-\sqrt{5}}{2} \approx -0.618$.

🙂 Die geschlossene Formel für f_n zeigt das Wachstumsverhalten:

- Der zweite Summand $(\frac{1-\sqrt{5}}{2})^n$ konvergiert rasch gegen Null.
- Die Fibonacci–Folge f_n wächst exponentiell, wie $(\frac{1+\sqrt{5}}{2})^n$.

🙂 Zunächst handelt die Fragestellung von Zahlenfolgen und Rekursion. Auf den ersten Blick hat das nichts mit Linearer Algebra, Matrizen oder gar Eigenvektoren zu tun. Es zeigt sich jedoch, dass diese universellen Werkzeuge auch hier wunderbar effizient angewendet werden können!

Das ist ein allgemeines und häufiges Phänomen: Die Problemstellung deutet meist noch nicht die möglichen oder nötigen Werkzeuge an. Zur Problemlösung braucht es daher Erfahrung und Kreativität.
Man erblickt nur, was man schon weiß und versteht. (Goethe)

🙂 Erfahrung sammeln Sie durch Übungen wie etwa der folgenden. Vielfältige Rechnungen und Erprobung der Werkzeuge übt die korrekte Anwendung und fördert Ihre Kreativität bei zukünftigen neuen Aufgaben.

Der Folgenraum $\mathbb{K}^{\mathbb{N}}$ mit Verschiebeoperator

M247

Sei $\mathbb{K}$ ein Körper, etwa $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Wir betrachten den Vektorraum $\mathbb{K}^{\mathbb{N}}$ aller Folgen $f : \mathbb{N} \to \mathbb{K} : n \mapsto f_n$ und hierauf den Verschiebeoperator

$$s \;:\; \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}} \;:\; (f_0, f_1, f_2, \dots) \mapsto (f_1, f_2, f_3, \dots).$$

Ausgeschrieben bedeutet das $s(f) = g$ mit $g_n = f_{n+1}$.
Dies ist offensichtlich eine $\mathbb{K}$–lineare Abbildung.

Aufgabe: Bestimmen Sie zu s alle Eigenwerte und Eigenräume.

Lösung: Sei $\lambda \in \mathbb{K}$. Die Gleichung $s(f) = \lambda f$ bedeutet ausgeschrieben

$$s(f) = (f_1, f_2, f_3, \dots) \overset{!}{=} (\lambda f_0, \lambda f_1, \lambda f_2, \dots) = \lambda f$$

Das entspricht der Rekursionsvorschrift $f_{n+1} = \lambda f_n$ für alle $n \in \mathbb{N}$.
Jede solche Folge $f : \mathbb{N} \to \mathbb{K}$ erfüllt somit $f_n = \lambda^n f_0$ für alle $n \in \mathbb{N}$.
Wir wählen den Eigenvektor $e_\lambda : \mathbb{N} \to \mathbb{K} : n \mapsto \lambda^n$ und erhalten:

$$\operatorname{Eig}(s, \lambda) = \langle\, e_\lambda \,\rangle_{\mathbb{K}}^{!}$$

Der Folgenraum $\mathbb{K}^{\mathbb{N}}$ mit Verschiebeoperator

M248
Erläuterung

🙂 Hier ist *jeder* Skalar $\lambda \in \mathbb{K}$ ein Eigenwert, also $\sigma(s; \mathbb{K}) = \mathbb{K}$.
Jeder Eigenraum ist eindimensional, das ist äußerst übersichtlich.
Die Eigenvektoren e_λ können wir bequem und explizit angeben.

⚠ Hier ist der Vektorraum $\mathbb{K}^{\mathbb{N}}$ unendlich-dimensional. Determinante und charakteristisches Polynom stehen uns daher nicht zur Verfügung. Dennoch können wir Eigenwerte und Eigenräume direkt berechnen.

Übung: Ist der Verschiebeoperator $s : \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$ diagonalisierbar? Auch wenn der Raum $\mathbb{K}^{\mathbb{N}}$ unendlich-dimensional ist, können wir uns dennoch eine diagonalisierende Basis wünschen. Ist dies hier erfüllbar? (Der endliche Fall $\sharp\mathbb{K} < \infty$ ist leicht, der allgemeine Fall etwas knifflig.)

Übung: Im Falle $\mathbb{K} = \mathbb{R}, \mathbb{C}$ betrachten wir die Menge $U = \ell^\infty(\mathbb{N}, \mathbb{K})$ der beschränkten Folgen. Dies ist ein Unterraum von $\mathbb{K}^{\mathbb{N}}$. Dieser Unterraum ist s–invariant, das heißt $s(U) \subseteq U$. Durch Einschränkung erhalten wir den Verschiebeoperator $s : U \to U$. Bestimmen Sie sein Spektrum.

Anwendungsbeispiel zu rekursiven Folgen

☺ Wir untersuchen nun die Fibonacci–Folge mit unseren Werkzeugen der Linearen Algebra, hier also mit Eigenwerten und Eigenvektoren.

Wir betrachten in $\mathbb{K}^{\mathbb{N}}$ den Kern von $s^2 - s - \mathrm{id}$, also den Unterraum

$$V = \left\{ f : \mathbb{N} \to \mathbb{K} \;\middle|\; \forall n \in \mathbb{N} : f_{n+2} = f_{n+1} + f_n \right\}.$$

Nach Konstruktion ist $V \leq \mathbb{K}^{\mathbb{N}}$ zudem s–invariant, das heißt $s(V) \subseteq V$.
Durch Einschränkung erhalten wir den Verschiebeoperator $s : V \to V$.

Aufgabe: (1) Welche Dimension hat V? (2) Stellen Sie s als Matrix dar.
(3) Bestimmen Sie Eigenwerte & Eigenräume. (4) Diagonalisieren Sie s.
(5) Linearkombinieren Sie die Fibonacci–Folge aus Eigenvektoren.

Lösung: (1) Wir betrachten die Projektion

$$q \;:\; \mathbb{K}^{\mathbb{N}} \geq V \to \mathbb{K}^2 \;:\; (f_0, f_1, f_2, \dots) \mapsto (f_0, f_1).$$

Zu beliebigen Startwerten $f_0, f_1 \in \mathbb{K}$ existiert genau eine Folge $f \in V$.
Somit ist $q : V \xrightarrow{\sim} \mathbb{K}^2$ ein Isomorphismus, insbesondere $\dim_{\mathbb{K}} V = 2$.

Anwendungsbeispiel zu rekursiven Folgen

(2) Als eine Basis $\mathcal{A} = (a_1, a_2)$ von V wählen wir $a_1 = (1, 0, 1, 1, 2, 3, \dots)$ und $a_2 = (0, 1, 1, 2, 3, 5, \dots)$. Es gilt $s(a_1) = a_2$ und $s(a_2) = a_1 + a_2$. Also:

$$A = \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(s) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

(3) Aus dieser Matrix gewinnen wir das charakteristische Polynom:

$$\chi_A = \begin{vmatrix} -X & 1 \\ 1 & 1 - X \end{vmatrix} = X^2 - X - 1$$

Die beiden Nullstellen sind $\phi = \frac{1}{2}(1 + \sqrt{5})$ und $\psi = \frac{1}{2}(1 - \sqrt{5})$.
Als Eigenvektoren erhalten wir $u = (\phi^n)_{n \in \mathbb{N}}$ und $v = (\psi^n)_{n \in \mathbb{N}}$ in V.

(4) Damit erhalten wir eine Eigenbasis $\mathcal{B} = (u, v)$ von $s : V \to V$ sowie

$$D = T^{-1} A T = \begin{bmatrix} \phi & 0 \\ 0 & \psi \end{bmatrix} \text{ mit } T = \begin{bmatrix} 1 & 1 \\ \phi & \psi \end{bmatrix} \text{ und } T^{-1} = \frac{1}{\sqrt{5}} \begin{bmatrix} -\psi & 1 \\ \phi & -1 \end{bmatrix}.$$

Obwohl die Matrix A über $\mathbb{Q}$ gegeben ist, sind Rechnungen in der Körpererweiterung $\mathbb{Q}[\sqrt{5}]$ nötig. **Übung:** Machen Sie die Probe!

Anwendungsbeispiel zu rekursiven Folgen

(5) Wir stellen die Fibonacci–Folge $f = (0, 1, 1, 2, 3, 5, 8, \dots) \in V$ dar als Linearkombination der Eigenvektoren $u = (\phi^n)_{n \in \mathbb{N}}$ und $v = (\psi^n)_{n \in \mathbb{N}}$:

$$f = au + bv \quad \Leftrightarrow \quad \left\{ \begin{matrix} 0 = a\phi^0 + b\psi^0 \\ 1 = a\phi^1 + b\psi^1 \end{matrix} \right\} \quad \Leftrightarrow \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} = T \begin{bmatrix} a \\ b \end{bmatrix}$$

Wir finden so die einzige Lösung für die gesuchten Koeffizienten:

$$\begin{bmatrix} a \\ b \end{bmatrix} = T^{-1} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Explizit ausgeschrieben ergibt dies die Binet–Formel:

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right]$$

☺ So lösen Sie Rekursionsgleichungen durch geschlossene Formeln.
Dies gelingt mit den Werkzeugen der Linearen Algebra: Eigenvektoren!

Übung: Prüfen Sie die so gefundene Gleichung per Induktion (C443).

Anwendungsbeispiel zu rekursiven Folgen

Das hier gezeigte Verfahren gilt allgemein für rekursive Folgen!

$$V = \left\{ f : \mathbb{N} \to \mathbb{K} \;\middle|\; \forall k \geq n \;:\; f_k + p_1 f_{k-1} + \cdots + p_n f_{k-n} = 0 \right\}$$

Dies entspricht der Rekursionsgleichung $P(s)(f) = 0$ mit dem Polynom

$$P = X^n + p_1 X^{n-1} + \cdots + p_n X^0 \in \mathbb{K}[X]_n^1.$$

Im Fibonacci–Beispiel haben wir $P = X^2 - X - 1$ betrachtet.

Allgemein ist $P \in \mathbb{K}[X]_n^1$ gegeben, wir haben also $V = \ker P(s)$.
Dieser Unterraum V in $\mathbb{K}^{\mathbb{N}}$ ist s–invariant, das heißt $s(V) \subseteq V$.
Wir wollen den Verschiebeoperator $s : V \to V$ diagonalisieren,
also eine Basis aus Eigenvektoren der Form $(\lambda^n)_{n \in \mathbb{N}}$ bestimmen.
Falls P über $\mathbb{K}$ einfach zerfällt, so gelingt dies wörtlich wie zuvor:
Zu beliebigen Anfangswerten finden wir so eine geschlossene Formel!

☺ Das ist das Standardverfahren M2I zur Diagonalisierung,
und es funktioniert auch für Rekursionsgleichungen wunderbar.

Satz M2R: lineare Rekursion und ihre Eigenfolgen

Sei $\mathbb{K}$ ein Körper. Vorgelegt sei ein beliebiges normiertes Polynom

$$P = X^n + p_1 X^{n-1} + \cdots + p_n X^0 \in \mathbb{K}[X]_n^1.$$

Wir betrachten den Folgenraum $\mathbb{K}^{\mathbb{N}}$ mit dem Verschiebeoperator

$$s : \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}} : (f_0, f_1, f_2, \dots) \mapsto (f_1, f_2, f_3, \dots).$$

Darin liegt der $\mathbb{K}$–Untervektorraum $V \leq \mathbb{K}^{\mathbb{N}}$ der P–rekursiven Folgen:
$V = \ker P(s) = \left\{ f : \mathbb{N} \to \mathbb{K} \;\middle|\; \forall k \geq n : f_k + p_1 f_{k-1} + \cdots + p_n f_{k-n} = 0 \right\}$
Dieser Unterraum ist s–invariant, $s(V) \subseteq V$, mit Dimension $\dim_{\mathbb{K}} V = n$.

Genau dann ist der (so eingeschränkte) Verschiebeoperator $s : V \to V$ über $\mathbb{K}$ diagonalisierbar, wenn das Polynom P über $\mathbb{K}$ einfach zerfällt,

$$P(X) = (X - \lambda_1) \cdots (X - \lambda_n) \quad \text{mit } \lambda_i \neq \lambda_j \text{ für } i \neq j.$$

Zu jedem Eigenwert λ haben wir die Eigenfolge $e_\lambda : \mathbb{N} \to \mathbb{K} : n \mapsto \lambda^n$.
Wir erhalten so die Eigenbasis $(e_{\lambda_1}, \dots, e_{\lambda_n})$ von V bezüglich s.

Einfache Zerfällung ist immer hinreichend für Diagonalisierbarkeit (M2N). Satz M2R besagt speziell für den Verschiebeoperator, dass einfache Zerfällung auch notwendig ist und gibt explizit eine Eigenbasis an.

Aufgabe: Beweisen Sie diesen allgemeinen Satz nach dem Vorbild des Fibonacci–Beispiels. Bestimmen Sie (1) die Dimension von V, (2) eine darstellende Matrix zu $s : V \to V$, (3) alle Eigenwerte und (4) Eigenräume, (5) eine Eigenbasis und (6) den Basiswechsel.

Lösung: (1) Wir betrachten die Projektion

$$q : \mathbb{K}^{\mathbb{N}} \geq V \to \mathbb{K}^n : f \mapsto (f_0, \dots, f_{n-1}).$$

Zu je n beliebig vorgegebenen Startwerten $f_0, \dots, f_{n-1} \in \mathbb{K}$ existiert genau eine P–rekursive Folge $f = (f_0, \dots, f_{n-1}, f_n, \dots)$.

Somit ist $q : V \xrightarrow{\sim} \mathbb{K}^n$ ein Isomorphismus, insbesondere $\dim_{\mathbb{K}} V = n$.
Diese einfache Vorgehensweise ist ebenso elegant wie effizient.

🙂 Durch diesen Isomorphismus q bestimmen wir die Dimension und erhalten nach Wunsch auch Basen, etwa $(q^{-1}(e_1), \dots, q^{-1}(e_n))$.

(2) Den Verschiebeoperator $s : V \to V$ können wir wie folgt darstellen:

$$\begin{array}{ccc} V & \xrightarrow{\;s\;} & V \\ {\scriptstyle q}\downarrow\cong & & {\scriptstyle q}\downarrow\cong \\ \mathbb{K}^n & \xrightarrow{\;A\;} & \mathbb{K}^n \end{array}$$

$$\begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_{n-1} \end{bmatrix} \mapsto \begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \\ -p_n & -p_{n-1} & -p_{n-2} & \dots & -p_1 \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_{n-1} \end{bmatrix}$$

Das charakteristische Polynom ist $\chi_A = P$, dank $A = C(P)^\intercal$ und M2Q.
Wir sehen $\dim \operatorname{Eig}(s, \lambda) \leq 1$ und können direkt Satz M1I anwenden:

(3) Genau dann ist $s : V \to V$ diagonalisierbar, wenn P einfach zerfällt, $P(X) = (X - \lambda_1) \cdots (X - \lambda_n)$ mit $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ und $\lambda_i \neq \lambda_j$ für $i \neq j$.

(4) Es gilt $\operatorname{Eig}(s, \lambda) = \langle\, e_\lambda \,\rangle_{\mathbb{K}}^!$ mit der Eigenfolge $e_\lambda : \mathbb{N} \to \mathbb{K} : n \mapsto \lambda^n$.
(5) Wir erhalten so die Eigenbasis $(e_{\lambda_1}, \dots, e_{\lambda_n})$ von V bezüglich s.
(6) Hierdurch wird der Verschiebeoperator $s : V \to V$ diagonalisiert:

$$T^{-1} A T = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{bmatrix} \quad \text{mit } T = \begin{bmatrix} \lambda_1^0 & \lambda_2^0 & \dots & \lambda_n^0 \\ \lambda_1^1 & \lambda_2^1 & \dots & \lambda_n^1 \\ \vdots & & \vdots & \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \dots & \lambda_n^{n-1} \end{bmatrix}$$

🙂 Die Basiswechselmatrix $T = \operatorname{VDM}(\lambda_1, \lambda_2, \dots, \lambda_n)^\intercal$ ist die berühmte Vandermonde–Matrix (siehe Satz B3A), hier transponiert. Alles ist gut.

Übung: Machen Sie die Probe $AT = TD$.

🙂 Die inverse Matrix T^{-1} ist mühsam, wie so oft. Für die Probe ist sie gar nicht nötig: Es genügt sicherzustellen, dass T invertierbar ist (B3A), und statt $T^{-1}AT = D$ die äquivalente Gleichung $AT = TD$ zu prüfen.

Trigonalisierung eines Endomorphismus

Definition M3A: Trigonalisierung eines Endomorphismus

Sei K ein Ring, wir denken insbesondere an Körper wie $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_p, \ldots$.

(1) Sei $f : V \to V$ linear über K. Eine **trigonalisierende Basis** zu f ist eine Basis $\mathcal{B}$ von V, für die die darstellende Matrix von f trigonal ist:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Existiert eine solche Basis $\mathcal{B}$ von V, so nennen wir f **trigonalisierbar**.

(2) Sei $A \in K^{n\times n}$. Ein **trigonalisierender Basiswechsel** zu A über K ist eine invertierbare Matrix $T \in \mathrm{GL}_n(K)$, so dass $T^{-1}AT$ trigonal ist:

$$T^{-1}AT = \begin{bmatrix} \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Existiert eine solche Matrix T, so nennen wir A **trigonalisierbar**.

Trigonalisierung und Zerfällung

Wie können wir feststellen, ob f bzw. A trigonalisierbar ist?

Satz M3B: Trigonalisierung $\Leftrightarrow$ Zerfällung

Sei $f : V \to V$ linear über dem Körper K mit $\dim_K V = n < \infty$.
Genau dann ist f über K trigonalisierbar, wenn χ_f über K zerfällt:

$$\chi_f(X) = (X - \lambda_1) \cdots (X - \lambda_n) \quad \text{mit } \lambda_1, \ldots, \lambda_n \in K$$

Dasselbe gilt für die Trigonalisierung einer Matrix $A \in K^{n\times n}$ über K.

Beispiel: Sei V ein endlich-dimensionaler Vektorraum über $\mathbb{C}$.
Dann ist jeder $\mathbb{C}$–Endomorphismus $f : V \to V$ trigonalisierbar.

Beweis: „$\Rightarrow$“: Zu f sei $\mathcal{B}$ eine trigonalisierende Basis von V:

$$B = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Demnach gilt $\chi_f = \chi_B = \det(XI - B) = (X - \lambda_1) \cdots (X - \lambda_n)$.

Trigonalisierung und Zerfällung

„$\Leftarrow$“: Wir führen Induktion über n. Für $n = 1$ ist die Aussage trivial.
Sei nun $n \geq 2$, und die Behauptung für $n - 1$ sei bereits bewiesen.

Zum Eigenwert $\lambda_1 \in K$ existiert ein Eigenvektor $v_1 \in \mathrm{Eig}(f, \lambda_1) \leq V$.
Diesen ergänzen wir zu einer Basis $\mathcal{A} = (v_1, u_2, \ldots, u_n)$ von V. (J2B)

$$A = \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f) = \begin{bmatrix} \lambda_1 & * & * & * \\ 0 & & & \\ 0 & & A' & \\ 0 & & & \end{bmatrix} \quad \Longrightarrow \quad B = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} \lambda_1 & * & * & * \\ 0 & \lambda_2 & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & \lambda_n \end{bmatrix}$$

Wir zerlegen $V = U \oplus V'$ in $U = \langle\, v_1 \,\rangle_K^!$ und $V' = \langle\, u_2, \ldots, u_n \,\rangle_K^!$.
Einschränkung und Projektion ergibt $f' = p_{V'} \circ f \circ \iota_{V'} : V' \to V'$.
In der Basis $\mathcal{A}' = (u_2, \ldots, u_n)$ gilt $A' = \mathrm{M}_{\mathcal{A}'}^{\mathcal{A}'}(f')$ wie oben gezeigt.
Wir haben $\chi_f = (X - \lambda_1) \cdot \chi_{f'}$, also zerfällt auch das Polynom $\chi_{f'}$.
Dank $\dim V' = n - 1$ greift nun unsere Induktionsvoraussetzung:
Zu f' existiert eine trigonalisierende Basis $\mathcal{B}' = (v_2, \ldots, v_n)$ von V'.
Die Basis $\mathcal{B} = (v_1, v_2, \ldots, v_n)$ von V trigonalisiert $f : V \to V$. QED

Trigonalisierung und Zerfällung

🙂 Um Induktion über die Dimension führen zu können, müssen wir die Dimension reduzieren. Der entscheidende Konstruktionsschritt ist hier die Projektion auf den strikt kleineren Teilraum $V' < V$:

$$\begin{array}{ccc} V & \xrightarrow{\quad f \quad} & V \\ {\scriptstyle \iota_{V'}}\uparrow & & \downarrow{\scriptstyle p_{V'}} \\ V' & \xrightarrow{\quad f' \quad} & V' \end{array}$$

Konkret bedeutet das: Zu jedem $v' = \sum_{k=2}^n \alpha_k u_k \in V'$ betrachten wir $f(v') = \beta_1 v_1 + \sum_{k=2}^n \beta_k u_k$ und setzen $f'(v') := \sum_{k=2}^n \beta_k u_k \in V'$.
Wir ignorieren also ganz dreist-naiv den Störterm $\beta_1 v_1 \in U$.

🙂 Dass $f' : V' \to V'$ linear ist, sehen wir an $f' = p_{V'} \circ f \circ \iota_{V'}$.

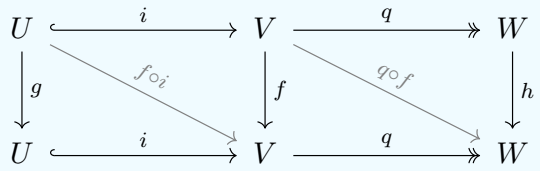
🙂 In der Zerlegung $V = U \oplus V'$ als direkte Summe ist die Wahl des Komplements V' willkürlich. Mit dem Quotienten $W = V/U$ gelingt dies natürlich und elegant, aber auch abstrakter. Dies führen wir nun aus.

Trigonalisierung: der Quotiententrick

Lemma M3C: Endomorphismus einer kurzen exakten Sequenz

Sei $f : V \to V$ linear über K und $U \leq V$ ein invarianter Unterraum.

(1) Wir haben die Einschränkung $g = f_U^U$ und auf dem Quotienten $W = V/U$ die lineare Abbildung $h : W \to W : x + U \mapsto f(x) + U$.



(2) Aus je zwei Basen $\mathcal{A}$ von U und $\mathcal{C}$ von W erhalten wir eine Basis $\mathcal{B}$ von V gemäß Satz J2M. Für die darstellenden Matrizen gilt dann:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(g) & * \\ 0 & \mathrm{M}_{\mathcal{C}}^{\mathcal{C}}(h) \end{bmatrix}$$

Für die charakteristischen Polynome folgt somit $\chi_f = \chi_g \cdot \chi_h$.

Trigonalisierung: der Quotiententrick

Aufgabe: Beweisen Sie Lemma M3C und damit erneut Satz M3B.

Beweis von Lemma M3C: (1) Wir erhalten $g : U \to U$ und $h : W \to W$ durch lineare Faktorisierung über eine Injektion I2F bzw. Surjektion I2E.
(2) Die Matrixdarstellung folgt aus (1) und der Konstruktion der Basis $\mathcal{B}$.

Beweis von Satz M3B: Wir zeigen hier nur die Rückrichtung „⇐“:
Wir führen Induktion über $n = \dim V$. Für $n = 1$ ist die Aussage trivial.
Sei nun $n \geq 2$, und die Behauptung für $n - 1$ sei bereits bewiesen.

Zum Eigenwert $\lambda_1 \in K$ existiert ein Eigenvektor $v_1 \in \mathrm{Eig}(f, \lambda_1) \leq V$.
Der Unterraum $U = \langle\, v_1 \,\rangle_K^! < V$ ist f–invariant. Lemma M3C beschert uns die lineare Abbildung $h : W \to W$ auf dem Quotienten $W = V/U$.
Dabei gilt $\chi_f = (X - \lambda_1) \cdot \chi_h$, also zerfällt auch das Polynom χ_h.

Dank $\dim W = \dim V - \dim U < n$ greift die Induktionsvoraussetzung:
Zu $h : W \to W$ existiert eine trigonalisierende Basis $\mathcal{C} = (w_2, \ldots, w_n)$.
Wir wählen Urbilder $v_2, \ldots, v_n \in V$ mit $q(v_i) = w_i$. Dank Lemma M3C wird f durch die Basis $\mathcal{B} = (v_1, v_2, \ldots, v_n)$ trigonalisiert. QED

Trigonalisierung: Fahne von Unterräumen

Definition M3D: Fahne von Unterräumen

(1) Sei V ein K–Vektorraum der Dimension n. Eine **Fahne** ist eine Kette

$$\{0\} = V_0 < V_1 < \cdots < V_\ell = V$$

von Unterräumen. Dabei gilt $0 = \dim V_0 < \dim V_1 < \cdots < \dim V_\ell = n$.
Eine **vollständige Fahne** erfüllt $\ell = n$ und $\dim V_i = i$ für $i = 0, 1, \ldots, n$.

Die ersten Teilräume $V_0 < V_1 < V_2$ mit $\dim V_i = i$ entsprechen Punkt, Gerade, Ebene; daher der geometrisch anschauliche Name „Fahne“.

Beispiel: Ist $(v_1, \ldots, v_n)$ eine Basis von V über K, so definieren die aufgespannten Unterräume $V_i = \langle\, v_1, \ldots, v_i \,\rangle_K$ für $i = 0, 1, \ldots, n$ eine vollständige Fahne $\{0\} = V_0 < V_1 < \cdots < V_n = V$.

Definition M3D: invariante Fahne von Unterräumen

(2) Sei $f : V \to V$ eine K–lineare Abbildung.
Ein Unterraum $U \leq V$ heißt *f–invariant*, wenn $f(U) \subseteq U$ gilt.
Eine Fahne $(V_i)_i$ heißt *f–invariant*, wenn $f(V_i) \subseteq V_i$ für alle i gilt.

Trigonalisierung: Fahne von Unterräumen

Lemma M3E: Trigonalisierung ⇔ invariante Fahne

Genau dann ist $f : V \to V$ trigonalisierbar, wenn eine vollständige, f–invariante Fahne $\{0\} = V_0 < V_1 < \cdots < V_n = V$ existiert.

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} \lambda_1 & * & * & * \\ 0 & \lambda_2 & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & \lambda_n \end{bmatrix}$$

Aufgabe: Beweisen Sie dieses Lemma.

Lösung: „⇒“: Angenommen, zu f existiert eine trigonalisierende Basis $(v_1, \ldots, v_n)$ von V. Die Unterräume $V_i = \langle\, v_1, \ldots, v_i \,\rangle_K$ für $i = 0, 1, \ldots, n$ sind eine vollständige Fahne und zudem f–invariant, denn $f(V_i) \subseteq V_i$.

„⇐“: Durch schrittweise Ergänzung erhalten wir eine Basis $(v_1, \ldots, v_i)$ von V_i. Die Basis $\mathcal{B} = (v_1, v_2, \ldots, v_n)$ von V trigonalisiert $f : V \to V$.

Spur und Determinante aus Eigenwerten

Satz M3F: Spur und Determinante

Sei $A \in K^{n\times n}$ eine Matrix mit zerfallendem charakteristischen Polynom

$$\chi_A(X) = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n).$$

(1) Die Spur von A ist die Summe der Eigenwerte:

$$\boxed{\operatorname{tr}(A) = \lambda_1 + \lambda_2 + \cdots + \lambda_n}$$

(2) Die Determinante ist das Produkt der Eigenwerte:

$$\boxed{\det(A) = \lambda_1 \cdot \lambda_2 \cdots \lambda_n}$$

🙂 Die Spur $\operatorname{tr}(A)$ der Matrix A ist besonders leicht zu berechnen. Wenn wir also $n-1$ Eigenwerte kennen, so ist der letzte gratis!

🙂 Über $\mathbb{C}$ zerfällt jedes Polynom, die Voraussetzung ist also erfüllt. Dasselbe gilt über jedem algebraisch abgeschlossenen Körper.

Aufgabe: Beweisen Sie diesen Satz! (Zwei Wege sind möglich.)

Spur und Determinante aus Eigenwerten

Erster Beweis: Wir multiplizieren zur Monomform aus:

$$\begin{aligned}\chi_A(X) &= (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n)\\ &= X^n - a_{n-1}X^{n-1} \pm \cdots + (-1)^n a_0\end{aligned}$$

Dank Satz M2C kennen wir die extremen Koeffizienten:

$$\begin{aligned}\operatorname{tr}(A) &\overset{\text{M2C}}{=} a_{n-1} &&= \lambda_1 + \lambda_2 + \cdots + \lambda_n,\\ \det(A) &\overset{\text{M2C}}{=} a_0 &&= \lambda_1 \cdot \lambda_2 \cdots \lambda_n.\end{aligned}$$

Zweiter Beweis: Dank M3B können wir A trigonalisieren zu

$$B = T^{-1}AT = \begin{bmatrix}\lambda_1 & * & *\\ 0 & \ddots & *\\ 0 & 0 & \lambda_n\end{bmatrix}$$

Dank Satz M2F gilt dabei $\chi_A = \chi_B$, also insbesondere

$$\begin{aligned}\operatorname{tr}(A) &\overset{\text{M2F}}{=} \operatorname{tr}(B) &&= \lambda_1 + \lambda_2 + \cdots + \lambda_n,\\ \det(A) &\overset{\text{M2F}}{=} \det(B) &&= \lambda_1 \cdot \lambda_2 \cdots \lambda_n.\end{aligned}$$

🙂 Der zweite Beweis ist noch schöner, dank stärkerer Werkzeuge.

Elementarsymmetrische Polynome

Der obige Satz M3F erklärt die Spur $\operatorname{tr}(A) = \lambda_1 + \lambda_2 + \cdots + \lambda_n$ und die Determinante $\det(A) = \lambda_1\lambda_2\cdots\lambda_n$ aus den Eigenwerten. Allgemein:

Definition M3G: elementarsymmetrische Polynome

Im Polynomring $\mathbb{Z}[T, X_1, \ldots, X_n]$ betrachten wir das Produkt

$$(T+X_1)(T+X_2)\cdots(T+X_n) = T^n + \sigma_1 T^{n-1} + \sigma_2 T^{n-2} + \cdots + \sigma_n.$$

Der hier auftretende Koeffizient $\sigma_k \in \mathbb{Z}[X_1, \ldots, X_n]$ für $k = 1, 2, \ldots, n$ ist das **elementarsymmetrische Polynom** vom Grad k in $X_1, X_2, \ldots, X_n$:

$$\begin{aligned}\sigma_1(X_1, X_2, \ldots, X_n) &= X_1 + X_2 + \cdots + X_n\\ &\cdots\\ \sigma_k(X_1, X_2, \ldots, X_n) &= \textstyle\sum_{i_1<i_2<\cdots<i_k} X_{i_1}X_{i_2}\cdots X_{i_k}\\ &\cdots\\ \sigma_n(X_1, X_2, \ldots, X_n) &= X_1X_2\cdots X_n\end{aligned}$$

Das Polynom σ_k ist die Summe von $\binom{n}{k}$ Monomen, jedes vom Grad k.

Elementarsymmetrische Polynome

Satz M3H: Wurzelsatz von Vieta

Vorgelegt sei ein normiertes Polynom $P \in K[X]_n^1$, einerseits als Summe von Monomen und andererseits als Produkt von Linearfaktoren:

$$P = X^n + a_1X^{n-1} + \cdots + a_n = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n)$$

Dann gilt $a_k = (-1)^k\sigma_k(\lambda_1, \lambda_2, \ldots, \lambda_n)$, also ausgeschrieben

$$a_k = (-1)^k \textstyle\sum_{i_1<i_2<\cdots<i_k} \lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_k}.$$

Dies gilt insb. für das charakteristische Polynom und die Eigenwerte!

Aus den Nullstellen $\lambda_1, \ldots, \lambda_n \in K$ von P können wir also ganz leicht die Koeffizienten $a_1, \ldots, a_n \in K$ bestimmen: Ausmultiplizieren genügt.

Umgekehrt bestimmen die Koeffizienten $a_1, \ldots, a_n \in K$ von P eindeutig die Nullstellen $\lambda_1, \ldots, \lambda_n$ bis auf die Reihenfolge.

Die Faktorisierung ist wesentlich schwieriger als das Ausmultiplizieren!

Die Spur lesen: Der letzte Eigenwert ist gratis!

M313

Aufgabe: Gegeben ist die Matrix $A \in \mathbb{R}^{4\times4}$ mit vier Vektoren:

$$A = \begin{bmatrix} -18 & -50 & 10 & 10 \\ 4 & 11 & -1 & -3 \\ -12 & -32 & 10 & 4 \\ 2 & 2 & 2 & -2 \end{bmatrix}, \quad b = \begin{bmatrix} 0 \\ 1 \\ 4 \\ 0 \end{bmatrix}, \quad c = \begin{bmatrix} -3 \\ 1 \\ 0 \\ -1 \end{bmatrix}, \quad d = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix}, \quad e = \begin{bmatrix} -1 \\ 0 \\ -1 \\ -1 \end{bmatrix}$$

(1) Welche davon sind Eigenvektoren von A? Zu welchen Eigenwerten?
(2) Bestimmen Sie alle Eigenwerte, (3) Eigenräume, (4) eine Eigenbasis.

Lösung: (1) Wir setzen die Definition $Av = \lambda v$ ein und rechnen:

$$Ab = A\begin{bmatrix} 0 \\ 1 \\ 4 \\ 0 \end{bmatrix} = \begin{bmatrix} -10 \\ 7 \\ 8 \\ 10 \end{bmatrix} \notin \mathbb{R}b, \qquad Ac = A\begin{bmatrix} -3 \\ 1 \\ 0 \\ -1 \end{bmatrix} = \begin{bmatrix} -6 \\ 2 \\ 0 \\ -2 \end{bmatrix} = 2c,$$

$$Ad = A\begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 0d, \qquad Ae = A\begin{bmatrix} -1 \\ 0 \\ -1 \\ -1 \end{bmatrix} = \begin{bmatrix} -2 \\ 0 \\ -2 \\ -2 \end{bmatrix} = 2e$$

Die Spur lesen: Der letzte Eigenwert ist gratis!

M314
Erläuterung

🙂 Teil (1) ist eine leichte Fingerübung: Um zu prüfen, ob $v \in K^n$ ein Eigenvektor der Matrix $A \in K^{n\times n}$ ist, genügt es, die Definition $Av = \lambda v$ einzusetzen… und im günstigen Fall den Eigenwert λ abzulesen.

⚠ Es lohnt sich, die wertvollen Informationen aus Teil (1) zu nutzen! Die hier angebotenen Daten sind nicht zufällig, sondern mit Bedacht vorbereitet; in einer Klausur sind sie eine gezielte Hilfestellung. Auch außerhalb von Klausuren kann diese Situation entstehen.

☹ Alternativ, aber ungeschickt, kann man die hilfreichen Daten aus Teil (1) ignorieren und für (2–4) stur das Standardverfahren einsetzen: Das charakteristische Polynom entwickeln und seine Nullstellen finden, Eigenräume berechnen und eine Eigenbasis wählen. Das ist mühsam.

🙂 Sie arbeiten umso effizienter, je genauer Sie verstehen, was Sie tun! … insbesondere, was Sie schon haben und was Sie noch suchen. Sie können dann geschickt vom Standardverfahren abweichen, je nach konkretem Bedarf und möglichen Abkürzungen.

Die Spur lesen: Der letzte Eigenwert ist gratis!

M315

$$A = \begin{bmatrix} -18 & -50 & 10 & 10 \\ 4 & 11 & -1 & -3 \\ -12 & -32 & 10 & 4 \\ 2 & 2 & 2 & -2 \end{bmatrix}, \quad b = \begin{bmatrix} 0 \\ 1 \\ 4 \\ 0 \end{bmatrix}, \quad c = \begin{bmatrix} -3 \\ 1 \\ 0 \\ -1 \end{bmatrix}, \quad d = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix}, \quad e = \begin{bmatrix} -1 \\ 0 \\ -1 \\ -1 \end{bmatrix}$$

(2) Dank (1) wissen wir $\operatorname{Eig}(A,0) \geq \langle\, d \,\rangle^!_{\mathbb{R}}$ und $\operatorname{Eig}(A,2) \geq \langle\, c,e \,\rangle^!_{\mathbb{R}}$.
Damit kennen wir drei der vier Eigenwerte: $\lambda_1 = 0$, $\lambda_2 = 2$, $\lambda_3 = 2$.
Dank $\operatorname{tr}(A) = 1$ bekommen wir den vierten gratis: $\lambda_4 = -3$.
Ohne weitere Mühe schließen wir $\chi_A = X(X-2)^2(X+3)$.

(3) Wir berechnen den Eigenraum $\operatorname{Eig}(A,-3)$ wie üblich mit Gauß:

$$A + 3I = \begin{bmatrix} -15 & -50 & 10 & 10 \\ 4 & 14 & -1 & -3 \\ -12 & -32 & 13 & 4 \\ 2 & 2 & 2 & 1 \end{bmatrix} \xrightarrow[\text{RZSF}]{\text{Gauß}} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1/2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Demnach gilt $\operatorname{Eig}(A,-3) = \langle\, f \,\rangle^!_{\mathbb{R}}$ mit $f = (-2,1,0,2)^\intercal$.
(4) Damit haben wir zu A unsere Eigenbasis (d,c,e,f) gefunden.

Die Spur lesen: Der letzte Eigenwert ist gratis!

M316
Erläuterung

🙂 Dank der Informationen aus (1) sind unsere Rechnungen (2–4) in dieser Anwendung wesentlich effizienter als das Standardverfahren!

Vielleicht erscheint Ihnen die obige Aufgabenstellung etwas künstlich, das will ich gar nicht bestreiten. Ganz unrealistisch ist das Vorgehen jedoch auch nicht, denn in Anwendungen verfügen Sie manchmal über Teilinformationen, und diese sollten Sie geschickt nutzen.

Das Standardverfahren M2ı zur Diagonalisierung hat natürlich trotzdem seine Berechtigung: Wenn Sie keine weiteren Daten oder Ideen haben, dann bietet es Ihnen eine allgemeine und verlässliche Methode, um das Diagonalisierungsproblem zu lösen.

Variantenreiche Beispiele wie das vorige zeigen Ihnen jedoch ebenso, dass Sie sich nicht stur auf vorgefertigte Rezepte verlassen sollten. Manchmal sind geschickte Abkürzungen oder raffinierte Tricks möglich. Diese sollten Sie erkennen, um sich unnötige Arbeit zu ersparen.

🙂 Denken hilft!

Das lokale Minimalpolynom

M317

Sei $f : V \to V$ linear über dem Körper K und $\dim_K(V) = n < \infty$.

(1) Jeder Vektor $v \in V$ erzeugt seinen **f–zyklischen Unterraum**

$$Z := \langle\, f^k(v) \mid k \in \mathbb{N} \,\rangle_K \leq V.$$

Wegen $\dim_K(Z) \leq n$ sind $f^0(v), f^1(v), \ldots, f^n(v)$ linear abhängig (J2K).

(2) Sei $m \in \mathbb{N}$ minimal, sodass $f^0(v), \ldots, f^m(v)$ linear abhängig sind.
Somit ist die Familie $f^0(v), \ldots, f^{m-1}(v)$ noch linear unabhängig,
und wir erhalten $a_0 f^0(v) + \ldots + a_{m-1} f^{m-1}(v) + f^m(v) = 0$
mit eindeutigen Koeffizienten $a_0, \ldots, a_{m-1} \in K$.

Definition M3I: das lokale Minimalpolynom

Wir nennen $\mu = \mu_f^v := a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m \in K[X]$ das **lokale Minimalpolynom** von $f : V \to V$ bezüglich des Vektors $v \in V$.

Das Polynom $P = \mu_f^v$ ist normiert und annulliert v gemäß $P(f)(v) = 0$.
Unter allen Polynomen in $K[X]$ mit diesen beiden Eigenschaften hat es den kleinsten Grad, daher der Name **Minimalpolynom** von f bzgl. v.

Das lokale Minimalpolynom

M318
Erläuterung

Allgemein gilt $f^0 = \mathrm{id}_V$ und $f^1 = f$ sowie rekursiv $f^{k+1} = f \circ f^k$.
Dies sind die Potenzen von $f : V \to V$ im Endomorphismenring

$$(\mathrm{End}_K(V), +, 0, \circ, \mathrm{id}_V).$$

Für $v \in V$ gilt $f^0(v) = v$ und $f^1(v) = f(v)$ sowie $f^{k+1}(v) = f(f^k(v))$.
Die Familie $f^0(v), f^1(v), f^2(v), \ldots$ in V entsteht demnach aus dem Startvektor $v \in V$ durch wiederholte Anwendung von $f : V \to V$.

🙂 Die obige Definition M3I erklärt zugleich einen Algorithmus:

Algo M3I: Berechnung des lokalen Minimalpolynoms

Eingabe: ein Endomorphismus $f : V \to V$ und ein Vektor $v \in V$
Ausgabe: das lokale Minimalpolynom $\mu_f^v \in K[X]$

1: Wähle eine Basis von V und schreibe $f^0(v), f^1(v), \ldots, f^m(v)$ als Spalten in eine Matrix M bis der Rang stagniert bei $\operatorname{rang} M = m$.
2: Bestimme den Kern $\ker M = \langle\, (a_0, a_1, \ldots, a_{m-1}, 1)^\intercal \,\rangle$.
3: return $\mu_f^v = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m$

Der Satz von Cayley–Hamilton

M319

Lemma M3J: Cayley–Hamilton

Das lokale Minimalpolynom μ_f^v teilt das charakteristische Polynom χ_f.

Aufgabe: Beweisen Sie dieses Lemma nach folgender Anleitung:
(1) Berechnen Sie zu $g = f|_Z^Z$ das charakteristische Polynom χ_g.
(2) Vergleichen Sie dies mit dem charakteristischen Polynom χ_f.

Lösung: (1) Wir nutzen weiterhin die obigen Bezeichnungen (M3I).
Wir haben $Z = \langle\, f^k(v) \mid k < m \,\rangle_K^! \leq V$ mit der Basis $\mathcal{B} = (f^k(v))_{k=0}^{m-1}$.
Nach Konstruktion gilt $f(Z) \subseteq Z$, das heißt, der Raum Z ist f–invariant.
Die Einschränkung $g = f|_Z^Z$ wird dargestellt durch die **Begleitmatrix**

$$B := \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(g) = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -a_{m-1} \end{bmatrix} =: \mathrm{C}(\mu_f^v).$$

Das charakteristische Polynom ist $\chi_g = \det(XI - B) = \mu_f^v$ dank M2Q.

Der Satz von Cayley–Hamilton

M320

(2) Wir ergänzen die Basis $\mathcal{B}$ von Z zu einer Basis $\mathcal{A}$ von V.
Bezüglich dieser Basis wird $f : V \to V$ dargestellt durch die Matrix

$$A := \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f) = \begin{bmatrix} B & * \\ 0 & C \end{bmatrix}.$$

Für diese Block-Dreiecksmatrix gilt (dank L2V)

$$\chi_f = \det(XI - A) = \det(XI - B) \det(XI - C) = \chi_g \cdot Q.$$

In Worten ausformuliert ist das genau die Behauptung: Das lokale Minimalpolynom $\mu_f^v = \chi_g$ teilt das charakteristische Polynom χ_f. QED

Satz M3K: Cayley–Hamilton

Sei $f \in \mathrm{End}_K(V)$ und $\dim_K(V) < \infty$. Dann gilt $\chi_f(f) = 0$ in $\mathrm{End}_K(V)$:
Das charakteristische Polynom von f annulliert den Endomorphismus f.

Beweis: Sei $v \in V$. Dank obigem Lemma gilt $\chi_f = Q \cdot \mu_f^v$ mit $Q \in K[X]$,
also $\chi_f(f)(v) = Q(f)\mu_f^v(f)(v) = 0$. Wir schließen $\chi_f(f) = 0$. QED

Cayley–Hamilton für Matrizen: falscher Beweis

Der Satz M3K von Cayley–Hamilton für Endomorphismen ist äquivalent zu folgender Formulierung für quadratische Matrizen:

Satz M3K: Cayley–Hamilton für Matrizen

Für jede Matrix $A \in K^{n\times n}$ und $\chi_A \in K[X]^1_n$ gilt $\chi_A(A) = 0$ in $K^{n\times n}$:
Das charakteristische Polynom von A annulliert die Matrix A.

⚠ Verlockend simpel, aber unsinnig, ist folgendes Scheinargument:
Das charakteristische Polynom ist definiert als die Determinante

$$\chi_A(X) := \det(XI - A) \in K[X].$$

Wenn wir formal X durch A ersetzen, so erhalten wir scheinbar

$$\chi_A(A) \overset{?}{=} \det(AI - A) = \det(A - A) = \det(0) = 0.$$

Aufgabe: Bitte schützen Sie sich gegen solcherart (Selbst)Betrug!
Warum ist das kein Beweis von Cayley–Hamilton, sondern Unsinn?

Cayley–Hamilton für Matrizen: falscher Beweis

Lösung: Links ist $\chi_A(A) \in K^{n\times n}$ eine Matrix: Diese entsteht, indem wir in das Polynom $\chi_A(X) = X^n - a_{n-1}X^{n-1} \pm \cdots + (-1)^n a_0$ die Matrix einsetzen, ausgeschrieben $\chi_A(A) = A^n - a_{n-1}A^{n-1} \pm \cdots + (-1)^n a_0 A^0$.
Rechts hingegen ist $\det(AI - A) = \det(0) = 0 \in K$ ein Skalar.

Das obige Scheinargument behauptet, naiv oder frech, nach obskurer Rechnung „Matrix = Skalar“ und ist deshalb offensichtlich unsinnig.

⚠ Schon die rein syntaktische Typen-Prüfung schlägt hier fehl!
Auf der linken und der rechten Seite stehen verschiedene Objekte.
Die frech-naiv behauptete Gleichung „$\overset{?}{=}$“ gilt ganz sicher nicht.

🙂 Erstaunlicherweise lässt sich dieses unsinnige Scheinargument reparieren zu einem Beweis (nach S. Lang: *Algebra.* 2002, §XIV.3):

Aufgabe: (1) Was erhalten Sie tatsächlich, wenn Sie in der Matrix $C(X) = (XI - A)^\intercal$ die Variable X durch die Matrix A ersetzen?
(2) Multiplizieren Sie die Matrix $C(A)$ mit dem Vektor $(e_1, \ldots, e_n)^\intercal$.
(3) Multiplikation mit der Adjunkten $B(A) = \operatorname{adj} C(A)$ zeigt $\chi_A(A) = 0$.

Cayley–Hamilton für Matrizen: reparierter Beweis

Lösung: (1) Wir betrachten die Matrix $C(X) = (XI - A)^\intercal$, also

$$C(X) = \begin{bmatrix} X - a_{11} & \ldots & -a_{n1} \\ \vdots & & \vdots \\ -a_{1n} & \ldots & X - a_{nn} \end{bmatrix} \in K[X]^{n\times n}.$$

Wir ersetzen die Variable X korrekt durch die Matrix A und erhalten

$$C(A) = \begin{bmatrix} A - a_{11}I & \ldots & -a_{n1}I \\ \vdots & & \vdots \\ -a_{1n}I & \ldots & A - a_{nn}I \end{bmatrix} \in K[A]^{n\times n}.$$

(2) Angewendet auf die Standardbasis $e_1, \ldots, e_n \in K^n$ gilt:

$$C(A) \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} Ae_1 - a_{11}e_1 - \ldots - a_{n1}e_n \\ \vdots \\ -a_{1n}e_1 - \ldots + Ae_n - a_{nn}e_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Wir arbeiten hier über dem kommutativen Ring $K[A] \leq K^{n\times n}$.
Der Ring $K[A]$ operiert von links auf dem Raum $K^n = K^{n\times 1}$.

Cayley–Hamilton für Matrizen: reparierter Beweis

(3) Aus der Gleichung (2) folgern wir nun $\det C(A) = 0$.
Für die adjunkte Matrix $B(X) = \operatorname{adj} C(X)$ gilt dank L2S:

$$B(X) \cdot C(X) = \det C(X) \cdot I = \begin{bmatrix} \chi_A(X) & & 0 \\ & \ddots & \\ 0 & & \chi_A(X) \end{bmatrix} \in K[X]^{n\times n}$$

Wir ersetzen wieder X durch A und erhalten:

$$\begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = C(A) \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = B(A) \cdot C(A) \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} \chi_A(A) & & 0 \\ & \ddots & \\ 0 & & \chi_A(A) \end{bmatrix} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix}$$

Somit gilt $\chi_A(A)\, e_i = 0$ in K^n für alle i, also $\chi_A(A) = 0$ in $K^{n\times n}$. QED

🙂 Diese Rechnung folgt der naiven Eingebung „ersetze X durch A“.
Die korrekte Ausführung erfordert allerdings extrem genaue Notation.

🙂 Determinante und Adjunkte haben wir über jedem kommutativen Ring, insbesondere also über unserem Matrixunterring $K[A] \leq K^{n\times n}$.

Das (globale) Minimalpolynom

M325

Sei $f : V \to V$ linear über dem Körper K und $\dim_K(V) = n < \infty$.

(1) Der Endomorphismenring $\mathrm{End}_K(V) \cong K^{n\times n}$ ist ein K–Vektorraum der Dimension $d = n^2$ (K1I). Demnach sind in $\mathrm{End}_K(V)$ die Potenzen $f^0, f^1, f^2, \ldots, f^d$ linear abhängig über K (J2K).

(2) Sei $m \in \mathbb{N}$ minimal, sodass $f^0, f_1, \ldots, f^m$ linear abhängig sind. Somit ist die Familie $f^0, f_1, \ldots, f^{m-1}$ noch linear unabhängig, und wir erhalten $a_0 f^0 + a_1 f^1 + \ldots + a_{m-1} f^{m-1} + f^m = 0$ mit eindeutigen Koeffizienten $a_0, a_1, \ldots, a_{m-1} \in K$.

Definition M3L: das (globale) Minimalpolynom

Wir nennen $\mu = \mu_f := a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m \in K[X]$ das **(globale) Minimalpolynom** des Endomorphismus $f : V \to V$.

Das Polynom $P = \mu_f$ ist normiert und annulliert f gemäß $P(f) = 0$. Unter allen Polynomen in $K[X]$ mit diesen beiden Eigenschaften hat es den kleinsten Grad, daher der Name **Minimalpolynom**.

🙂 Diese Definition erklärt zugleich einen Algorithmus!

Das (globale) Minimalpolynom

M326
Erläuterung

Algo M3L: Berechnung des (globalen) Minimalpolynoms

Eingabe: ein Endomorphismus $f : V \to V$, wobei $\dim V = n < \infty$
Ausgabe: das (globale) Minimalpolynom $\mu_f \in K[X]$

1: Wähle eine Basis $V \cong K^n$ und somit $\mathrm{End}_K(V) \cong K^{n^2}$.
2: Schreibe $f^0, f^1(v), \ldots, f^m(v) \in \mathrm{End}_K(V)$ so als Spalten in eine Matrix M bis der Rang stagniert bei $\operatorname{rang} M = m$.
3: Bestimme den Kern $\ker M = \langle\, (a_0, a_1, \ldots, a_{m-1}, 1)^\intercal \,\rangle$.
4: return $\mu_f = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m$

Bemerkung: Der Gauß–Algorithmus zeigt: Das Minimalpolynom ändert sich nicht, wenn wir es in einem Erweiterungskörper $\bar{K} \geq K$ berechnen.

☹ Die Spalten haben hier die Länge n^2; das ist spürbar aufwändiger als die Dimension $n = \dim_K V$ beim lokalen Minimalpolynom (M3I).

Für den Polynomgrad haben wir zunächst die grobe Schranke $m \leq n^2$.

🙂 Der folgende Satz M3O zeigt $\mu_f \mid \chi_f$ und reduziert dies zu $m \leq n$. Diese Schranke ist eine enorme Verbesserung und scharf (M3M, M3N).

Zahlenbeispiele zum Minimalpolynom

M327

Aufgabe: Berechnen Sie das Minimalpolynom zu

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \text{ und } B = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \text{ und } C = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}.$$

Lösung: Wir finden direkt nach Definition:

$$A^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A^1 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \implies \mu_A = X - 2$$

$$B^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B^1 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}, B^2 = \begin{bmatrix} 4 & 4 \\ 0 & 4 \end{bmatrix} \implies \mu_B = X^2 - 4X + 4$$

$$C^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, C^1 = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}, C^2 = \begin{bmatrix} 7 & 4 \\ 12 & 7 \end{bmatrix} \implies \mu_C = X^2 - 4X + 1$$

Für 2×2–Matrizen wie A, B, C sind die Rechnungen allzu einfach, dennoch können wir hieran schön die Definition M3L anwenden und den zugehörigen Algorithmus M3L als allgemeines Verfahren illustrieren.

Zahlenbeispiele zum Minimalpolynom

M328
Erläuterung

Um das Minimalpolynom von $C \in K^{n\times n}$ zu bestimmen, suchen wir die erste nicht-triviale Relation der Potenzen $C^0, C^1, C^2, \ldots \in K^{n\times n}$.

Hierzu füllen wir die Koeffizienten der ersten $m+1$ Matrizen $C^0, \ldots, C^m$ spaltenweise in die Matrix M bis der Rang stagniert bei $\operatorname{rang} M = m$:

$$M = \begin{bmatrix} 1 & 2 & 7 \\ 0 & 3 & 12 \\ 0 & 1 & 4 \\ 1 & 2 & 7 \end{bmatrix} \implies \ker M = K \begin{bmatrix} 1 \\ -4 \\ 1 \end{bmatrix} \implies \mu_C = X^2 - 4X + 1$$

Allgemein nutzen wir Gauß $M \to SM$ zur RZFS. Gilt $\operatorname{rang} M = m + 1$, so erweitere zu $M' = (M, v) \to (SM, Sv)$, reduziere $M' \to S'M'$, usw.

Für $C \in K^{n\times n}$ erwarten wir $M \in K^{n^2 \times m}$ mit $m \leq n^2$, besser nur $m \leq n$ dank M3O. Für große n ist das aufwändig, aber es ist immer möglich.

Die folgenden Beispiele zeigen willkommene Vereinfachungen für Jordan–Blöcke M3M, Diagonalmatrizen M3N und Begleitmatrizen M3P.

Bemerkung: Das Minimalpolynom ist invariant unter Ähnlichkeit (M3Q).

Strukturbeispiel: ein Jordan–Block

M329

Beispiel M3M: ein Jordan–Block

In Dimension $n \in \mathbb{N}$ betrachten wir den nilpotenten Jordan–Block

$$B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \in K^{n \times n}.$$

In diesem Falle gilt $\mu_B = X^n$, und dies stimmt mit $\chi_B = X^n$ überein.

Beweis: (a) Das Polynom $P = X^n$ annulliert B, denn es gilt $B^n = 0$.
(b) Für jedes Polynom $Q = a_0 + \cdots + a_{n-1}X^{n-1}$ kleineren Grades gilt:

$$Q(B) = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ 0 & a_0 & \ddots & \vdots \\ 0 & 0 & \ddots & a_1 \\ 0 & 0 & 0 & a_0 \end{bmatrix}$$

Demnach ist $Q(B) = 0$ und $\deg Q < n$ nur für $Q = 0$ möglich.
Somit ist $P = X^n$ tatsächlich das Minimalpolynom von B. QED

Strukturbeispiel: ein diagonalisierbarer Endomorphismus

M330

Beispiel M3N: ein diagonalisierbarer Endomorphismus

Sei $f : V \to V$ diagonalisierbar mit charakteristischem Polynom

$$\chi_f = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k}$$

wobei $\lambda_i \neq \lambda_j$ für $i \neq j$. Für das Minimalpolynom gilt dann

$$\mu_f = (X - \lambda_1) \cdots (X - \lambda_k).$$

Beweis: (a) Für $P = (X - \lambda_1) \cdots (X - \lambda_k)$ zeigen wir $P(f) = 0$, also $P(f)(v) = 0$ für alle $v \in V$. Wir haben $V = \bigoplus_{i=1}^{k} \operatorname{Eig}(f, \lambda_i)$.
Es genügt also, Eigenvektoren $v_i \in \operatorname{Eig}(f, \lambda_i)$ zu betrachten:

$$P(f)(v_i) = P(\lambda_i)\, v_i = 0$$

(b) Jedes Polynom $Q \neq 0$ vom Grad $d < k$ hat höchstens d Nullstellen dank Satz G3K. Demnach gilt $Q(\lambda_i) \neq 0$ für ein $i \in \{1, \dots, k\}$, also

$$Q(f)(v_i) = Q(\lambda_i)\, v_i \neq 0.$$

Somit ist P tatsächlich das Minimalpolynom von f. QED

Das Minimalpolynom teilt das charakteristische Polynom.

M331

🙂 Minimalität bezüglich Teilbarkeit und Grad stimmen überein:

Satz M3O: μ_f^v teilt μ_f teilt χ_f, kurz $\mu_f^v \mid \mu_f \mid \chi_f$

Sei $f : V \to V$ eine K–lineare Abbildung und $\dim_K V = n < \infty$.
Sei $v \in V$ ein Vektor und $P \in K[X]$ ein Polynom über K.

(1) Genau dann gilt $P(f) = 0$, wenn P ein Vielfaches von μ_f ist.

$$P(f) = 0 \quad \Longleftrightarrow \quad \exists Q \in K[X] \,:\, P = Q \cdot \mu_f$$

(2) Das Minimalpolynom μ_f teilt das charakteristische Polynom χ_f.
Für den Polynomgrad gilt insbesondere $m = \deg \mu_f \leq \deg \chi_f = n$.

(3) Genau dann gilt $P(f)(v) = 0$, wenn P ein Vielfaches von μ_f^v ist.

$$P(f)(v) = 0 \quad \Longleftrightarrow \quad \exists Q \in K[X] \,:\, P = Q \cdot \mu_f^v$$

(4) Das globale Minimalpolynom μ_f ist das kleinste gemeinsame Vielfache im Ring $K[X]$ aller lokalen Minimalpolynome μ_f^v für $v \in V$.
Zur Berechnung genügt ein $K[f]$–Erzeugendensystem $(v_i)_{i \in I}$ von V.

Das Minimalpolynom teilt das charakteristische Polynom.

M332

Beweis: (1) Sei $P(f) = 0$. Euklidische Division (G3H) von P durch μ_f ergibt $P = \mu_f \cdot Q + R$ mit $Q, R \in K[X]$ und $\deg R < \deg \mu_f = m$.
Daraus folgt $0 = P(f) = \mu_f(f)Q(f) + R(f) = R(f)$, da $\mu_f(f) = 0$.
Da $\mu_f \in K[X]_m^1$ minimalen Grad hat, bleibt nur $R = 0$.

(2) Dank Cayley–Hamilton (M3K) gilt $\chi_f(f) = 0$. Dank (1) folgt $\mu_f \mid \chi_f$.

(3) Sei $P(f)(v) = 0$. Wie in (1) folgt $\mu_f^v \mid P$ durch euklidische Division.

(4a) Aus $\mu_f(f) = 0$ folgt $\mu_f(f)(v_i) = 0$ für $i \in I$, dank (3) also $\mu_f^{v_i} \mid \mu_f$.
Das bedeutet, μ_f ist ein gemeinsames Vielfaches von $(\mu_f^v)_{v \in V}$.
(4b) Sei $P \in K[X]$ mit $\mu_f^{v_i} \mid P$ für alle $i \in I$. Dank (3) gilt $P(f)(v_i) = 0$, somit $P(f)(v) = 0$ für alle $v \in V$, also $P(f) = 0$. Dank (1) folgt $\mu_f \mid P$.
Somit ist μ_f ein kleinstes gemeinsames Vielfaches von $(\mu_f^{v_i})_{i \in I}$. QED

🙂 Das Minimalpolynom μ_f ist zudem normiert, wir sprechen daher von *dem* (normierten) kgV der lokalen Minimalpolynome $(\mu_f^{v_i})_{i \in I}$.

Strukturbeispiel: eine Begleitmatrix

Beispiel M3P: eine Begleitmatrix

(1) Sei $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]_n^1$ ein normiertes Polynom und $C = C(P)$ seine Begleitmatrix (M2Q). Dann gilt $\mu_C = \chi_C$.

(2) Sei $f : V \to V$ linear über K mit $\dim_K V = n < \infty$. Ist V zudem f–zyklisch, also $V = \langle\, f^k(v) \mid k < n \,\rangle_K^!$ für ein $v \in V$, so folgt $\mu_f = \chi_f$.

Aufgabe: Beweisen Sie dies nach dem Vorbild von Lemma M3J.

Lösung: (2) Bezüglich der Basis $\mathcal{B} = (f^k(v))_{k=0}^{n-1}$ von V haben wir

$$B := \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{bmatrix} =: \mathrm{C}(P).$$

(a) Das charakteristische Polynom ist $\chi_f = \det(XI - B) = P$ dank M2Q.
(b) Das lokale Minimalpolynom von f bezüglich v ist ebenfalls $\mu_f^v = P$.
(c) Dank M3O gilt $\mu_f^v \mid \mu_f \mid \chi_f$, mit (a) und (b) folgt $\mu_f^v = \mu_f = \chi_f = P$.

Das Minimalpolynom ist invariant unter Ähnlichkeit.

Lemma M3Q: Das Minimalpolynom ist invariant unter Ähnlichkeit.

(1) Für jedes Polynom $P \in K[X]$ sowie $A \in K^{n\times n}$ und $T \in \mathrm{GL}_n K$ gilt:

$$\boxed{P\big(T^{-1}AT\big) = T^{-1}\,P(A)\,T}$$

(2) Aus $P(A) = 0$ folgt $P(B) = 0$ für alle ähnlichen Matrizen $B \sim A$.

(3) Das Minimalpolynom ist invariant unter Ähnlichkeit, also $\mu_A = \mu_B$.

Beweis: (1) Wir setzen die konjugierte Matrix $B = T^{-1}AT$ in unser Polynom $P(X) = \sum_{i=0}^n p_i X^i$ ein und erhalten:

$$\begin{aligned} P(T^{-1}AT) &= \textstyle\sum_{i=0}^n p_i (T^{-1}AT)^i = \sum_{i=0}^n p_i (T^{-1}A^iT) \\ &= \textstyle\sum_{i=0}^n T^{-1}(p_iA^i)T = T^{-1}(\sum_{i=0}^n p_iA^i)T = T^{-1}P(A)T \end{aligned}$$

Daraus folgt (2) und daraus wiederum (3) nach Definition M3L. QED

🙂 Der Algorithmus M3L ist demnach unabhängig von der Basiswahl. Die Definition M3L ist ohnehin schon basisunabhängig formuliert.

Die Nullstellen des Minimalpolynoms

Satz M3R: Nullstellen des Minimalpolynoms

Sei $f : V \to V$ eine K–lineare Abbildung und $\dim_K V = n < \infty$.

(1) Falls χ_f über K in Linearfaktoren zerfällt, so gilt

$$\boxed{\begin{aligned} \chi_f &= (X-\lambda_1)^{r_1} \cdots (X-\lambda_k)^{r_k} \quad \text{mit } \lambda_i \neq \lambda_j \text{ für } i \neq j \text{ und} \\ \mu_f &= (X-\lambda_1)^{s_1} \cdots (X-\lambda_k)^{s_k} \quad \text{mit } 1 \leq s_i \leq r_i \text{ für alle } i. \end{aligned}}$$

(2) Das Minimalpolynom μ_f teilt das charakteristische Polynom χ_f, und umgekehrt teilt χ_f eine hinreichend hohe Potenz $(\mu_f)^a$ mit $a \in \mathbb{N}$.
Beide Polynome haben dieselben Nullstellen: die Eigenwerte von f.

(3) Allgemein gilt demnach

$$\begin{aligned} \chi_f &= (X-\lambda_1)^{r_1} \cdots (X-\lambda_k)^{r_k}\, Q, \\ \mu_f &= (X-\lambda_1)^{s_1} \cdots (X-\lambda_k)^{s_k}\, P, \end{aligned}$$

wobei $P, Q \in K[X]$ keine Nullstellen in K haben und $P \mid Q \mid P^a$ erfüllen.

Die Nullstellen des Minimalpolynoms

Beweis: (1) Dank M3O gilt $\mu_f \mid \chi_f$. Daraus folgt $s_i \leq r_i$ für alle i.
Zu jedem Eigenwert λ_i existiert ein Eigenvektor $v_i \in \mathrm{Eig}(f, \lambda_i) \smallsetminus \{0\}$.
Aus $v_i \neq 0$ und $f(v_i) = \lambda_i v_i$ erhalten wir das lokale Minimalpolynom $\mu_f^{v_i} = X - \lambda_i$. Dank M3O gilt $\mu_f^{v_i} \mid \mu_f$, also tatsächlich $s_i \geq 1$.

Aus (1) folgt (2), falls das charakteristische Polynom χ_f über K zerfällt.
Falls χ_f über K nicht zerfällt, so behelfen wir uns mit folgendem Trick:

Allgemein betrachten wir ohne Einschränkung $f : K^n \to K^n : x \mapsto Ax$.
Es existiert eine Körpererweiterung $\bar{K} \geq K$, sodass χ_f über $\bar{K}$ zerfällt.
Wir betrachten nun die lineare Abbildung $\bar{f} : \bar{K}^n \to \bar{K}^n : x \mapsto Ax$ über $\bar{K}$.
Für diese gilt Aussage (1) und somit Teilbarkeit (2) $\mu_{\bar{f}} \mid \chi_{\bar{f}} \mid \mu_{\bar{f}}^a$ in $\bar{K}[X]$.
Es gilt $\chi_f = \chi_{\bar{f}}$ und $\mu_f = \mu_{\bar{f}}$ in $K[X] \leq \bar{K}[X]$, also $\mu_f \mid \chi_f \mid \mu_f^a$ in $K[X]$.
(Für χ ist das klar, für μ siehe die Bemerkung nach Algorithmus M3L.)
Somit gilt gegenseitige Teilbarkeit (2) tatsächlich über jedem Körper K.

Aus der Teilbarkeit (2) folgt sofort die Aussage (3). QED

Die Nullstellen des Minimalpolynoms

M337 Erläuterung

Aufgabe: Beweisen Sie Satz M3R(2) ohne Erweiterungskörper:

Es gilt $\mu_f \mid \chi_f \mid (\mu_f)^a$ für ein $a \in \mathbb{N}$.

Anleitung: Führen Sie Induktion über die Dimension $n = \dim_K V$ und folgen Sie dem Vorbild von Lemma M3J zu Cayley–Hamilton.

🙂 Warum sollten wir einen Satz wie M3R zweimal beweisen?

Im vorliegenden Fall ist der erste Beweis elegant-schön-trickreich, beruht jedoch auf einem recht starken Hilfsmittel: der Existenz eines Erweiterungskörpers $\bar{K} \geq K$, über dem χ_f in Linearfaktoren zerfällt.

🙂 Der nachfolgende Beweis hingegen kommt ohne diesen Trick aus, das ist zwar etwas länger, dafür aber elementar – und eine gute Übung!

Lösung: Für $n = 0$ gilt $\chi_f = \mu_f = 1$. Für $n \geq 1$ existiert $v \in V \setminus \{0\}$.
Wir betrachten den f–zyklischen Unterraum $Z := \langle\, f^k(v) \mid k \in \mathbb{N} \,\rangle_K$.
Für $m := \dim_K Z$ gilt $1 \leq m \leq n$ und $Z = \langle\, f^k(v) \mid k < m \,\rangle_K^!$,
das heißt, die Familie $\mathcal{B} = (f^k(v))_{k=0}^{m-1}$ ist eine Basis von Z.

Die Nullstellen des Minimalpolynoms

M338 Erläuterung

Die Einschränkung $g = f|_Z^Z$ wird dargestellt durch die **Begleitmatrix**

$$B := \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(g) = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_{m-1} \end{bmatrix}.$$

Hier wissen wir bereits $\mu_B = \chi_B$ aus Beispiel M3P, also $\mu_B \mid \chi_B \mid \mu_B^1$.
Wir ergänzen die Basis $\mathcal{B}$ von Z zu einer Basis $\mathcal{A}$ von V und erhalten

$$A := \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f) = \begin{bmatrix} B & * \\ 0 & C \end{bmatrix}.$$

Nach Induktionsvoraussetzung gilt hier $\mu_C \mid \chi_C \mid \mu_C^\gamma$ für ein $\gamma \in \mathbb{N}$.
Das Minimalpolynom μ_A annulliert B und C, also $\mu_B \mid \mu_A$ und $\mu_C \mid \mu_A$.
Für das charakteristische Polynom folgt $\chi_A = \chi_B \cdot \chi_C \mid \mu_B \cdot \mu_C^\gamma \mid \mu_A^{\gamma+1}$.
Die grundlegende Teilbarkeit $\mu_A \mid \chi_A$ verdanken wir Satz M3O.
Gleiches gilt für den Endomorphismus f, also $\mu_f \mid \chi_f \mid \mu_f^{\gamma+1}$.

Minimalpolynom in un/endlicher Dimension

M339 Erläuterung

🙂 Die folgenden Aussagen erfordern keine endliche Dimension.
In günstigen Fällen kann dies unsere Rechnungen vereinfachen.

Satz M3S: Minimalpolynom in un/endlicher Dimension

Sei $f : V \to V$ eine lineare Abbildung über dem Körper K.
Angenommen wir finden ein Polynom $P \in K[X]_n^1$ mit $P(f) = 0$.

(1) Das Minimalpolynom $\mu_f \in K[X]_m^1$ existiert und erfüllt $\mu_f \mid P$.

(2) Weiterhin ist μ_f das kgV aller lokalen Minimalpolynome μ_f^v.

(3) Jeder Eigenwert von f ist eine Nullstelle des Polynoms P.

(4) Das Spektrum ist $\sigma(f; K) = \{\, \lambda \in K \mid \mu_f(\lambda) = 0 \,\}$.

(1) Im Falle $\dim_K V = n < \infty$ erfüllt das charakteristische Polynom $P = \chi_f \in K[X]_n^1$ diese Rolle, denn $\chi_f(f) = 0$ dank Cayley–Hamilton.

(3) Nicht alle Nullstellen von P müssen tatsächlich Eigenwerte sein, doch die Kenntnis von P schränkt die möglichen Kandidaten stark ein.

(4) Beim Minimalpolynom hingegen ist jede Nullstelle ein Eigenwert.

Minimalpolynom in un/endlicher Dimension

M340 Erläuterung

Beweis: (1) Existenz und Eindeutigkeit folgen wie zuvor in M3L.

(2) Satz M3O(3,4) gilt weiterhin, unabhängig von der Dimension.

(1) Angenommen $v \in V \setminus \{0\}$ und $\lambda \in K$ erfüllen $f(v) = \lambda v$.
Aus $P(f) = 0$ folgt $0 = P(f)(v) = P(\lambda)\, v$, also $P(\lambda) = 0$.

(2) Die Inklusion „$\subseteq$“ folgt aus (1), „$\supseteq$“ folgt aus M3O. QED

Aufgabe: Sei $A \in K^{n\times n}$ und $\{\chi_A, \mu_A\} \ni P = a_0 + a_1 X + \cdots + a_m X^m$.
Genau dann ist A in $K^{n\times n}$ invertierbar, wenn a_0 in K invertierbar ist;
in diesem Falle gilt $A^{-1} = B := -a_0^{-1}(a_1 + a_2 A + \cdots + a_m A^{m-1})$.

Lösung: Wir haben folgende Äquivalenzen:

$$A \in \mathrm{GL}_n K \overset{\text{B2D}}{\iff} \ker A = \{0\} \overset{\text{M1B}}{\iff} 0 \notin \sigma(f) \overset{\text{M3R}}{\iff} a_0 \neq 0$$

Im Falle $a_0 \neq 0$ gilt $AB = I - a_0^{-1} P(A) = I$ dank $P(A) = 0$ (M3K, M3L).

🙂 Wir können so die Inverse A^{-1} als ein Polynom in A ausdrücken.
Hierzu genügt jedes annullierende Polynom P mit $P(A) = 0$ und $a_0 \neq 0$.

Anwendungsbeispiel: Nilpotenz und Minimalpolynom

Sei V ein Vektorraum. Ein Endomorphismus $f : V \to V$ heißt **nilpotent**, falls $f^k = 0$ für einen (hinreichend großen) Exponenten $k \in \mathbb{N}$ gilt.
Der kleinste Exponent $m \in \mathbb{N}$ mit $f^m = 0$ heißt **Nilpotenzindex** von f.

Beispiel M3T: ein nilpotenter Endomorphismus

Für $f \in \mathrm{End}_K(V)$ und $\dim_K(V) = n < \infty$ gilt:

$$f \text{ ist nilpotent} \iff \mu_f = X^m \iff \chi_f = X^n \implies \mathrm{tr}(f) = \det(f) = 0$$

Die letzte Bedingung ist notwendig, aber für $n \geq 3$ nicht hinreichend.
Speziell in Dimension $n = 2$ gilt $\chi_f = X^2 - \mathrm{tr}(f)X + \det(f)$,
die Bedingung $\mathrm{tr}(f) = \det(f) = 0$ ist hier auch hinreichend.

Beweis: „⇒“: Ist f nilpotent, so gilt $f^k = 0$ für einen Exponenten $k \in \mathbb{N}$.
Dank M3O gilt $\mu_f \mid X^k$, also $\mu_f = X^m$ mit dem Nilpotenzindex $m \leq k$.
Dank M3R gilt $\chi_f \mid (\mu_f)^a$ für ein $a \in \mathbb{N}$, und somit folgt $\chi_f = X^n$.
„⇐“: Die Umkehrung ist klar, dank Cayley–Hamilton (M3K). QED

Anwendungsbeispiel: Nilpotenz und Minimalpolynom

Aufgabe: Sei $f : V \to V$ ein nilpotenter Endomorphismus.
Unter welcher Bedingung ist f diagonalisierbar?

Lösung: Nilpotenz bedeutet $\mu_f = X^m$ mit $m \in \mathbb{N}$ dank M3T.
Diagonalisierbarkeit ist dann äquivalent zu $m \leq 1$ nach M3N
Das bedeutet $m = 0$: $V = \{0\}$, oder $m = 1$: $V \neq \{0\}$ und $f = 0$.
Jeder nilpotente Endomorphismus $f \neq 0$ ist nicht diagonalisierbar.

Aufgabe: Sei $f \in \mathrm{End}_K(V)$ nilpotent vom Index m. Zeigen Sie (ohne M3T), dass $f^0, \ldots, f^{m-1}$ über K linear unabhängig sind.

Lösung: Wir wissen $f^m = 0$ und $f^{m-1} \neq 0$. Gegeben sei $0 \leq r < m$ und Koeffizienten $a_r, \ldots, a_{m-1} \in K$ mit $a_r f^r + \cdots + a_{m-1} f^{m-1} = 0$.
Komposition mit f^{m-r-1} ergibt $a_r f^{m-1} = 0$, also $a_r = 0$.
So fortfahrend schließen wir $a_r = \cdots = a_{m-1} = 0$.

Anwendungsbeispiel: Idempotenz und Eigenraumzerlegung

Beispiel M3U: Idempotenz und Eigenraumzerlegung

Sei $f : V \to V$ eine K–lineare Abbildung mit $f^2 = f$.
Das Minimalpolynom μ_f teilt demnach $X^2 - X = X(X-1)$:

0. Im Falle $\mu_f = 1$ ist $V = 0$ der Nullraum.
1. Im Falle $\mu_f = X$ ist $f = 0$ die Nullabbildung.
2. Im Falle $\mu_f = X - 1$ ist $f = \mathrm{id}_V$ die Identität.
3. Im Falle $\mu_f = X(X-1)$ haben wir die Eigenraumzerlegung I2L:

$$V = \mathrm{Eig}(f,0) \oplus \mathrm{Eig}(f,1) \text{ mit}$$
$$\mathrm{Eig}(f,0) = \ker(f - 0) = \mathrm{im}(f - 1) \neq \{0\},$$
$$\mathrm{Eig}(f,1) = \ker(f - 1) = \mathrm{im}(f - 0) \neq \{0\}.$$

Anwendungsbeispiel: Idempotenz und Eigenraumzerlegung

Idempotenz $f^2 = f$ bedeutet $P(f) = 0$ für $P = X^2 - X = X(X-1)$.
Aus dieser Faktorisierung folgt die Kernzerlegung

$$V = \ker(f^2 - f) = \ker(f) \oplus \ker(f - 1).$$

🙂 Die Eigenraumzerlegung $V = \mathrm{Eig}(f,0) \oplus \mathrm{Eig}(f,1)$ haben wir in I2L explizit ausgerechnet durch die Projektoren $\varphi_1 = f$ und $\varphi_2 = \mathrm{id}_V - f$.
Diese Beobachtung werden wir im folgenden Satz M3V optimieren zu einem möglichst allgemeinen Zerlegungssatz.

🙂 Beispiel M3U gilt unabhängig von der Dimension $\dim_K(V)$, egal ob endlich oder unendlich. Das ist bemerkenswert: Das charakteristische Polynom steht uns bei $\dim_K(V) = \infty$ zwar nicht mehr zur Verfügung, aber ein Minimalpolynom ist in glücklichen Fällen dennoch möglich.

Teilerfremde Faktorisierung und Kernzerlegung

Satz M3v: teilerfremde Faktorisierung und Kernzerlegung

Sei $P = P_1 \cdots P_n$ mit $P_1, \ldots, P_n \in K[X]$ und $\operatorname{ggT}(P_i, P_j) = 1$ für $i \neq j$.
(1) Für jeden K–Endomorphismus $f : V \to V$ mit $P(f) = 0$ gilt

$$V = \ker P(f) = \ker P_1(f) \oplus \cdots \oplus \ker P_n(f).$$

(2) Jeder Summand dieser Zerlegung ist f–invariant und erfüllt zudem
(3) $\ker P_i(f) = \operatorname{im} P_i^*(f)$ mit dem Cofaktor $P_i^* = P_1 \cdots P_{i-1} P_{i+1} \cdots P_n$.
(4) Bézout liefert $Q_i, Q_i^* \in K[X]$ mit $Q_i P_i + Q_i^* P_i^* = \operatorname{ggT}(P_i, P_i^*) = 1$,
(5) und $\varphi_i := Q_i^*(f) P_i^*(f) : V \to V$ projiziert auf den $i$ten Summanden.

Paradebeispiel: Zerfällt $P = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_k)$ über K mit $\lambda_i \neq \lambda_j$ für $i \neq j$, so erhalten wir aus $P(f) = 0$ die Eigenraumzerlegung

$$V = \operatorname{Eig}(f, \lambda_1) \oplus \operatorname{Eig}(f, \lambda_2) \oplus \cdots \oplus \operatorname{Eig}(f, \lambda_k)$$

mit den expliziten Lagrange–Projektoren $\varphi_i = \prod_{j \neq i} (f - \lambda_j)/(\lambda_i - \lambda_j)$.

Teilerfremde Faktorisierung und Kernzerlegung

Bemerkung: Ohne die Voraussetzung $P(f) = 0$ gilt entsprechend nur

$$V \geq \ker P(f) = \ker P_1(f) \oplus \cdots \oplus \ker P_n(f).$$

Der Unterraum $U = \ker P(f)$ ist nämlich f–invariant, also $f(U) \subseteq U$.
Somit können wir $f : V \to V$ einschränken zu $g : U \to U$ mit $P(g) = 0$.
Der Satz zerlegt dann $\ker P(g) = \ker P(f) = U$ als direkte Summe der Unterräume $\ker P_i(f) = \ker P_i(g) \leq U$ wie oben angegeben.

Das ist eine bemerkenswerte Zerlegung, ebenso einfach wie elegant:
Aus jeder Produktzerlegung $P = P_1 \cdots P_n$ in teilerfremde Faktoren $P_1, \ldots, P_n \in K[X]$ erhalten wir die Summenzerlegung des Kerns!

Zudem erhalten wir jeden Projektor φ_i von $U = \ker P(g)$ auf $\ker P_i(g)$ als Polynom in g, durch eine explizite Formel wie im Satz angegeben.
Im Beispiel ist dies besonders schön und einfach. Rechnen Sie es nach!

Der Beweis ist nicht minder elegant: Es handelt sich um eine genial effiziente Anwendung des Satzes von Beźout für Polynome in $K[X]$.
Alle Daten liegen explizit vor, wir müssen es nur noch nachrechnen.

Kernzerlegung: teile und herrsche… mit Bézout!

Beweis: (3a) Es gilt $0 = P(f) = P_i(f) P_i^*(f)$, also $\operatorname{im} P_i^*(f) \subseteq \ker P_i(f)$.
(3b) Wir nutzen (4) $Q_i P_i + Q_i^* P_i^* = 1$. Angewendet auf f und $v \in V$ gilt

$$v = Q_i(f) P_i(f)(v) + P_i^*(f) Q_i^*(f)(v).$$

Für $v \in \ker P_i(f)$ folgt $v = P_i^*(f) Q_i^*(f)(v)$, also $\ker P_i(f) \subseteq \operatorname{im} P_i^*(f)$.

(2) Für $v \in \ker P_i(f)$ gilt $f(v) \in \ker P_i(f)$, denn

$$P_i(f) \circ f(v) = f \circ P_i(f)(v) = 0.$$

(1a) Wir haben $Q_i P_i + Q_i^* P_i^* = 1$. Für jeden Vektor $v \in V$ gilt

$$v = P_i(f) Q_i(f)(v) + P_i^*(f) Q_i^*(f)(v).$$

Somit erhalten wir die Summe

$$V = \operatorname{im} P_i(f) + \operatorname{im} P_i^*(f) \overset{(3)}{=} \ker P_i(f) + \ker P_i^*(f).$$

Hierzu nutzen wir (3) für die Zerlegung $P = P_i P_i^*$.

Kernzerlegung: teile und herrsche… mit Bézout!

(1b) Für $v \in \ker P_i(f) \cap \ker P_i^*(f)$ gilt

$$v = Q_i(f) P_i(f)(v) + Q_i^*(f) P_i^*(f)(v) = 0.$$

Wir erhalten so die Zerlegung als direkte Summe

$$V = \ker P_i(f) \oplus \ker P_i^*(f).$$

Der Projektor $\varphi_i := Q_i^*(f) P_i^*(f) : V \to V$ schickt $v_i + v_i^*$ auf v_i.

(1c) Der Unterraum $V^* = \ker P_i^*(f) \leq V$ ist f–invariant dank (2).
Wir können daher f einschränken zu $f^* : V^* \to V^*$ mit $P_i^*(f^*) = 0$.
Per Induktion über n gilt $V^* = \bigoplus_{j \neq i} \ker P_j(f)$, also insgesamt

$$V = \ker P_1(f) \oplus \ker P_2(f) \oplus \cdots \oplus \ker P_n(f).$$

Der Projektor $\varphi_i := Q_i^*(f) P_i^*(f)$ schickt $v_1 + \cdots + v_n$ auf v_i. QED

Insbesondere gilt $\varphi_i^2 = \varphi$ mit $\operatorname{im} \varphi_i = \ker P_i(f)$ und $\ker \varphi_i = \ker P_i^*(f)$ sowie $\varphi_1 + \cdots + \varphi_n = \mathrm{id}_V$ und $\varphi_i \circ \varphi_j = 0$ für $i \neq j$ siehe Satz I2K.

Diagonalisierung: notwendige und hinreichende Kriterien

Satz M3W: Kriterien zur Diagonalisierbarkeit

Sei $f : V \to V$ eine K–lineare Abbildung und $\dim_K V = n < \infty$.

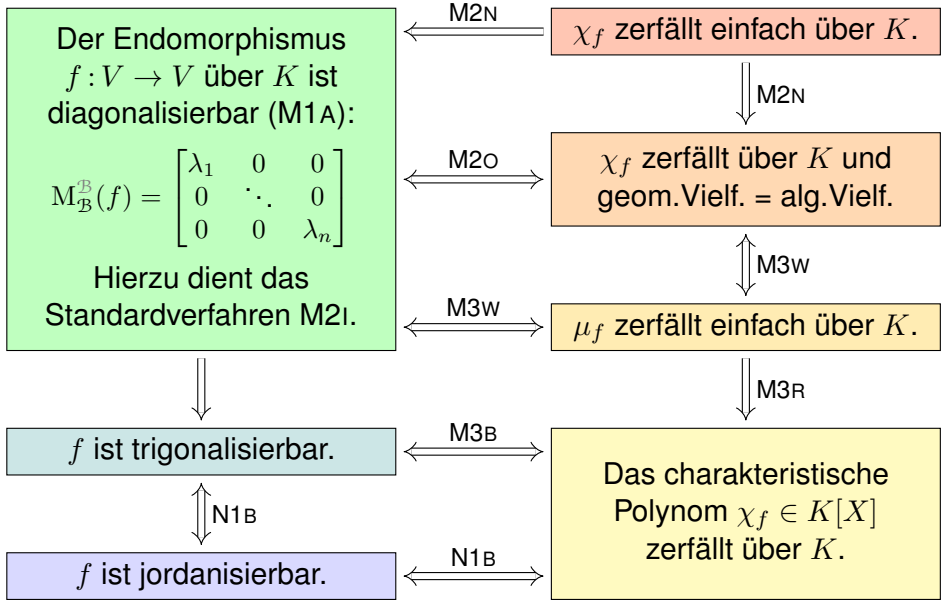
Dann sind die folgenden Bedingungen äquivalent:

1. Der Endomorphismus $f : V \to V$ ist diagonalisierbar.
2. Es gilt die Eigenraumzerlegung $V = \bigoplus_{\lambda \in \sigma(f)} \operatorname{Eig}(f, \lambda)$.
3. Es gilt die Dimensionsformel $n = \sum_{\lambda \in \sigma(f)} \dim_K \operatorname{Eig}(A, \lambda)$.
4. Das charakteristische Polynom χ_f zerfällt über K in Linearfaktoren und für jeden Eigenwert $\lambda \in \sigma(f)$ gilt $\dim_K \operatorname{Eig}(f, \lambda) = \operatorname{ord}(\chi_f, \lambda)$.
5. Das Minimalpolynom μ_f zerfällt einfach über K, ausgeschrieben $\mu_f = \prod_{\lambda \in \sigma(f)} (X - \lambda)$.

Beweis: Die Äquivalenz „(1) ⇔ (2) ⇔ (3)“ ist die Aussage von Satz M1I. Die Äquivalenz zu (4) ist Satz M2O. Neu ist nur die Äquivalenz zu (5):

Die Implikation „(1) ⇒ (5)“ haben wir in Beispiel M3N nachgerechnet. Die Umkehrung „(5) ⇒ (2)“ verdanken wir Satz M3V. QED

Diagonalisierung: notwendige und hinreichende Kriterien



Zusammenfassung zur Diagonalisierung

Grundlegende Begriffe und Techniken zur Diagonalisierung:

- Diagonalisierung (M1A), Eigenvektor, Eigenwert, Eigenraum, geometrische Vielfachheit, Eigenbasis, Spektrum (M1B)
- Jordan–Blöcke sind nicht-diagonalisierbar. (M1D)
- lineare Unabhängigkeit von Eigenvektoren (M1F)
- Eigenraumzerlegung und Diagonalisierung (M1I)
- Eigenwerte (M2A) und charakteristisches Polynom (M2C)
- Ähnlichkeit von Matrizen (M2D) und Invarianz (M2F)
- Standardverfahren zur Diagonalisierung (M2I)
- Einfache Zerfällung impliziert Diagonalisierbarkeit. (M2N)
- geometrische und algebraische Vielfachheit (M2O)
- Begleitmatrix (M2Q) und lineare Rekursion (M2R)

Zusammenfassung zur Diagonalisierung

Diagonalisierung hat zwei Bedingungen: (a) Das char. Polynom zerfällt und (b) die geometrische Vielfachheit erreicht die algebraische (M2O).

Letzteres ist nicht immer gegeben, statt Diagonalisierung begnügen wir uns dann mit einer Trigonalisierung; das ist wenig, aber immerhin etwas:

- Trigonalisierung (M3A) und Zerfällung (M3B)
- Spur und Determinante aus Eigenwerten (M3F)

Schließlich bündeln Minimalpolynome nützliche Informationen:

- lokales Minimalpolynom (M3I) und Cayley–Hamilton (M3K)
- das (globale) Minimalpolynom eines Endomorphismus (M3L)
- Teilbarkeit (M3O) und Nullstellen (M3R) der beiden Polynome
- teilerfremde Faktorisierung und Kernzerlegung (M3V)
- äquivalente Kriterien zur Diagonalisierbarkeit (M3W)

Aufgabe: Zu untersuchen ist die reelle Matrix

$$A = \begin{bmatrix} 0 & -1 & 1 \\ 1 & 2 & -1 \\ 1 & 1 & 0 \end{bmatrix} \in \mathbb{R}^{3\times 3}.$$

(1) Bestimmen und zerlegen Sie die Polynome χ_A und μ_A in $\mathbb{R}[X]$.
(2) Warum ist A diagonalisierbar? Bestimmen Sie eine Eigenbasis zu A.
(3) Beschreiben Sie die Wirkung von A auf $\mathbb{R}^3$ geometrisch / in Worten.

Lösung: (1a) Für das charakteristische Polynom finden wir

$$\chi_A(X) := \det(XI - A) \quad = \quad X^3 - 2X^2 + X \quad = \quad X(X-1)^2.$$

(1b) Das Minimalpolynom von A ist die erste nicht-triviale Relation der Potenzen A^0, A^1, A^2, A^3. Wir berechnen $A^2 = A$ und schließen

$$\mu_A \quad = \quad X^2 - X \quad = \quad X(X-1).$$

(2a) Allein aus χ_A können wir auf Trigonalisierbarkeit schließen (M3B). Da zudem μ_A einfach zerfällt, ist die Matrix A diagonalisierbar (M3W).

(2b) Wir bestimmen die zugehörigen Eigenräume:

$$A - 0I = \begin{bmatrix} 0 & -1 & 1 \\ 1 & 2 & -1 \\ 1 & 1 & 0 \end{bmatrix} \xrightarrow[\text{RZSF}]{\text{Gauß}} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix}$$

Daraus lesen wir $\operatorname{Eig}(A,0) = \langle\, v_1 = (-1,1,1)^\intercal \,\rangle =: U$ ab.

$$A - 1I = \begin{bmatrix} -1 & -1 & 1 \\ 1 & 1 & -1 \\ 1 & 1 & -1 \end{bmatrix} \xrightarrow[\text{RZSF}]{\text{Gauß}} \begin{bmatrix} 1 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Daraus folgt $\operatorname{Eig}(A,1) = \langle\, v_2 = (-1,1,0)^\intercal,\ v_3 = (1,0,1)^\intercal \,\rangle := V$
Wie in (2a) vorhergesagt, gilt $\mathbb{R}^3 = \operatorname{Eig}(A,0) \oplus \operatorname{Eig}(A,1)$.

Mit $\mathcal{B} = (v_1, v_2, v_3)$ haben wir eine Eigenbasis von $\mathbb{R}^3$ zu A.
Für $T = (v_1, v_2, v_3) \in \mathrm{GL}_3\,\mathbb{R}$ gilt $T^{-1}AT = \operatorname{diag}(0,1,1)$.

(3) Die Abbildung $p : \mathbb{R}^3 \to \mathbb{R}^3 : x \mapsto Ax$ ist die Projektion auf die Ebene V parallel zur Geraden U: Es gilt $p^2 = p$ mit $\ker(p) = U$ und $\operatorname{im}(p) = V$.

Aufgabe: Sei $\mathbb{K} = \mathbb{R}, \mathbb{C}$ sowie $A \in \mathbb{K}^{n\times n}$ und $m \in \mathbb{N}_{\geq 1}$ mit $A^m = I$.
Ist A diagonalisierbar? Geben Sie einen Beweis oder ein Gegenbeispiel.

Lösung: (1) Wir betrachten zunächst den reellen Fall $\mathbb{K} = \mathbb{R}$.

(1a) Das einfachste Gegenbeispiel ist die Vierteldrehung der Ebene $\mathbb{R}^2$:

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \mathbb{R}^{2\times 2}$$

Für diese Matrix gilt $A^4 = I$, doch $\chi_A = X^2 + 1$ zerfällt nicht über $\mathbb{R}$, also ist A nicht diagonalisierbar, nicht einmal trigonalisierbar (M3B).

(1b) Wir betrachten eine Drehung der Ebene $\mathbb{R}^2$ um den Winkel $\theta \in \mathbb{R}$:

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in \mathbb{R}^{2\times 2}$$

Speziell $A = R(\theta)$ mit $\theta = \pi k/n$ und $k \in \{1, \ldots, n-1\}$ erfüllt $A^{2n} = I$.
Das char. Polynom $\chi_A = (X - \cos\theta)^2 + (\sin\theta)^2$ zerfällt nicht über $\mathbb{R}$.
Das einfachste Beispiel erhalten wir für $\theta = \pi/2$, wie in (1a) gezeigt.

(2) Der komplexe Fall $\mathbb{K} = \mathbb{C}$ ist wesentlich sympathischer, wie so oft:

(2a) Das Polynom $P = X^m - 1$ annulliert A, denn $P(A) = A^m - I = 0$.
Die Gleichung $z^m = 1$ hat in $\mathbb{C}$ die Lösungen $z_k = \mathrm{e}^{2\pi \mathrm{i} k/m}$. Demnach gilt

$$X^m - 1 = \textstyle\prod_{k=0}^{m-1}(X - \mathrm{e}^{2\pi \mathrm{i} k/m}).$$

Die komplexen Zahlen $z_0, z_1, \ldots, z_{m-1}$ sind die $m$ten Einheitswurzeln.
Über $\mathbb{R}$ zerfällt $X^m - 1$ nur für $m \leq 2$, dank $X^2 - 1 = (X-1)(X+1)$.

(2b) Das Minimalpolynom μ_A teilt das Polynom P gemäß Satz M3O.
Also zerfällt auch μ_A einfach, und A ist diagonalisierbar dank M3W.

Beispiel: Die Drehmatrix $A = R(\theta) \in \mathbb{R}^{2\times 2}$ aus (1b) hat zwei echt komplexe Eigenwerte, $\sigma(A;\mathbb{R}) = \emptyset$ und $\sigma(A;\mathbb{C}) = \{\, \cos\theta \pm \mathrm{i}\sin\theta \,\}$.
Über $\mathbb{C}$ zerfällt χ_A einfach, und A ist diagonalisierbar dank M2N.
Über $\mathbb{R}$ jedoch ist A nicht einmal trigonalisierbar wegen M3B.

Bemerkung: Das Argument (2) gilt über jedem Körper $\mathbb{K}$, über dem $X^m - 1$ zerfällt, zum Beispiel $\mathbb{K} = \mathbb{F}_p$ mit $p = nm + 1$ prim. Dank G3N gilt $X^{p-1} - 1 = (X^m - 1)(X^{(n-1)m} + \cdots + X^m + 1) = \prod_{a\in\mathbb{F}_p^*}(X - a)$.

Definition M4A: simultane Diagonalisierung von Endomorphismen

(1) Seien $f_1, \dots, f_\ell : V \to V$ lineare Abbildungen über K. Hierzu ist eine **diagonalisierende Basis** $\mathcal{B} = (v_i)_{i \in I}$ eine Basis von V, sodass $f_k(v_i) = \lambda_i^{(k)} v_i$ und $\lambda_i^{(k)} \in K$ für jeden Index $i \in I$ und alle $k = 1, \dots, \ell$.

Wir nennen $\mathcal{B}$ eine **(simultane) Eigenbasis** der Familie $(f_1, \dots, f_\ell)$.

Existiert zur Familie $(f_1, \dots, f_\ell)$ eine simultane Eigenbasis $\mathcal{B}$ von V, so nennen wir $(f_1, \dots, f_\ell)$ **simultan diagonalisierbar**.

(2) Seien $A_1, \dots, A_\ell \in K^{n \times n}$ quadratische Matrizen derselben Größe über K. Hierzu ist ein **(simultan) diagonalisierender Basiswechsel** eine invertierbare Matrix $T \in \mathrm{GL}_n(K)$, so dass die konjugierten Matrizen $T^{-1}A_1T, \dots, T^{-1}A_\ell T \in K^{n \times n}$ allesamt diagonal sind.

Existiert eine solche Matrix T, so nennen wir die Familie $(A_1, \dots, A_r)$ in $K^{n \times n}$ **simultan diagonalisierbar** über K.

Im Falle $\ell = 1$ ist dies die vorige Definition M1A zur Diagonalisierung.

Wann ist simultane Diagonalisierung möglich? Der folgende Satz gibt hierzu ein einfaches Kriterium, sowohl notwendig als auch hinreichend:

Satz M4B: simultane Diagonalisierung von Endomorphismen

Seien $f_1, \dots, f_\ell : V \to V$ lineare Abbildungen über K. Äquivalent sind:

1. Die Familie $(f_1, \dots, f_\ell)$ ist simultan diagonalisierbar.
2. Jeder Endomorphismus $f_1, \dots, f_\ell$ ist einzeln diagonalisierbar und je zwei kommutieren, also $f_j \circ f_k = f_k \circ f_j$ für alle $j, k \in \{1, \dots, \ell\}$.

Die im Beweis geführte Konstruktion „(2) ⇒ (1)“ erklärt zugleich einen Algorithmus zur simultanen Diagonalisierung.

Beweis: „(1) ⇒ (2)“: Sei $\mathcal{B} = (v_i)_{i \in I}$ eine simultan diagonalisierende Basis, also $f_k(v_i) = \lambda_i^{(k)} v_i$ für jeden Index $i \in I$ und alle $k = 1, \dots, \ell$. Dann gilt $f_j \circ f_k = f_k \circ f_j$ auf der Basis $\mathcal{B}$ und somit auf ganz V:

$$f_j(f_k(v_i)) = f_j(\lambda_i^{(k)} v_i) = \lambda_i^{(k)} f_j(v_i) = \lambda_i^{(k)} \lambda_i^{(j)} v_i,$$
$$f_k(f_j(v_i)) = f_j(\lambda_i^{(j)} v_i) = \lambda_i^{(j)} f_k(v_i) = \lambda_i^{(j)} \lambda_i^{(k)} v_i.$$

„(2) ⇒ (1)“: Wir führen Induktion über ℓ. Der Fall $\ell = 1$ ist trivial. Sei also $\ell \geq 2$. Der Endomorphismus $f_\ell : V \to V$ ist diagonalisierbar, also gilt $V = \bigoplus_{\lambda \in K} \mathrm{Eig}(f_\ell, \lambda)$. Die entscheidende Beobachtung ist: Jeder Eigenraum $U = \mathrm{Eig}(f_\ell, \lambda)$ ist f_k–invariant: Für $v \in \mathrm{Eig}(f_\ell, \lambda)$ gilt

$$f_\ell(f_k(v)) = f_k(f_\ell(v)) = f_k(\lambda v) = \lambda f_k(v),$$

also $f_k(v) \in \mathrm{Eig}(f_\ell, \lambda)$. Wir können also $f_k : V \to V$ einschränken zu $g_k = f_k|_U^U$. Die Endomorphismen $g_1, \dots, g_{\ell-1}$ kommutieren weiterhin und sind einzeln diagonalisierbar dank dem nachfolgenden Lemma.

Nach Induktionsvoraussetzung existiert eine diagonalisierende Basis $\mathcal{B}_\lambda = (v_i)_{i \in I_\lambda}$ von U zu der Familie $(g_1, \dots, g_{\ell-1})$. Zudem gilt $g_\ell = \lambda \, \mathrm{id}_U$. Zusammengesetzt zu $I = \bigsqcup_{\lambda \in K} I_\lambda$ erhalten wir die diagonalisierende Basis $\mathcal{B} = (v_i)_{i \in I}$ von V zu der Familie $(f_1, \dots, f_{\ell-1}, f_\ell)$. QED

🙂 Dieser Beweis ist konstruktiv: Das Vorgehen erklärt zugleich einen Algorithmus zur simultanen Diagonalisierung.

⚠ Die Basis $\mathcal{B}_\lambda$ des Eigenraums $\mathrm{Eig}(f_\ell, \lambda)$ bestimmen wir nicht allein mit f_ℓ, sondern auch mit den anderen Endomorphismen $f_1, \dots, f_{\ell-1}$.

⚠ Satz M4B sagt nicht allgemein: „Kommutierende Endomorphismus sind diagonalisierbar.“ Der Satz sagt korrekt genau: „Kommutierende diagonalisierbare Endomorphismus sind simultan diagonalisierbar.“

Beispiel: Alle Matrizen $\left[\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right]$ mit $a \in K^*$ kommutieren untereinander, aber keine davon ist diagonalisierbar. (Übung: Rechnen Sie es nach.)

🙂 Angenommen, die Basis $\mathcal{B}$ diagonalisiert $f_1, \dots, f_\ell$ in $\mathrm{End}_K(V)$. Dann gilt dies für alle Endomorphismen in dem hiervon erzeugten kommutativen Unterring $K[f_1, \dots, f_\ell] \leq \mathrm{End}_K(V)$.

Beispiel: Ohne Kommutativität bleibt Diagonalisierbarkeit nicht erhalten unter Summen und Produkten. Zum Beispiel sind die Matrizen $A = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right]$ und $B = \left[\begin{smallmatrix} 0 & 1 \\ 0 & -1 \end{smallmatrix}\right]$ einzeln diagonalisierbar, nicht jedoch $A + B = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. (Übung: Finden Sie ähnliche Gegenbeispiele für Produkte.)

Lemma M4C: Diagonalisierbarkeit und Einschränkung

Sei $f : V \to V$ diagonalisierbar und $U \leq V$ ein f–invarianter Unterraum. Dann ist auch die Einschränkung $g = f|_U^U : U \to U$ diagonalisierbar:

$$U = \bigoplus_{\lambda \in K} \operatorname{Eig}(g, \lambda) \quad \text{mit} \quad \operatorname{Eig}(g, \lambda) = \operatorname{Eig}(f, \lambda) \cap U$$

Beweis in endlicher Dimension: Genau dann ist f diagonalisierbar, wenn das Minimalpolynom μ_f einfach zerfällt (M3W). Zudem gilt $\mu_g \mid \mu_f$, denn $\mu_f(g) = \mu_f(f)|_U^U = 0$ (M3O). Daher zerfällt μ_g ebenfalls einfach, und somit ist auch g diagonalisierbar (M3W). QED

Allgemein: Es gilt $V = \bigoplus_{\lambda \in K} \operatorname{Eig}(f, \lambda)$. Jeder Vektor $u \in U$ schreibt sich $u = v_0 + \cdots + v_n$ mit $v_i \in \operatorname{Eig}(f, \lambda_i)$, wobei $\lambda_i \neq \lambda_j$ für $i \neq j$ gelte. Wir zeigen $v_0, \ldots, v_n \in U$ und schließen daraus die obige Zerlegung.

Beweis per Induktion über n: Der Fall $n = 0$ ist klar. Sei also $n \geq 1$. Anwendung von $f - \lambda_0$ ergibt $u' = (\lambda_1 - \lambda_0)v_1 + \cdots + (\lambda_n - \lambda_0)v_n \in U$. Per Induktion folgt daraus $v_1, \ldots, v_n \in U$, also auch $v_0 \in U$. QED

Beweis mit dem Vandermonde–Trick: Da U invariant unter f ist, gilt $u_k := f^k(u) \in U$ für alle $k \in \mathbb{N}$. Wir haben $f^k(u) = \lambda_0^k v_0 + \cdots + \lambda_n^k v_n$. Für $k = 0, 1, \ldots, r$ erhalten wir so das folgende Gleichungssystem:

$$\begin{bmatrix} \lambda_0^0 & \lambda_1^0 & \ldots & \lambda_n^0 \\ \lambda_0^1 & \lambda_1^1 & \ldots & \lambda_n^1 \\ \vdots & & \vdots & \\ \lambda_0^n & \lambda_1^n & \ldots & \lambda_n^n \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix}$$

Die Vandermonde–Matrix ist invertierbar dank Satz B3A:

$$\begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} \lambda_0^0 & \lambda_1^0 & \ldots & \lambda_n^0 \\ \lambda_0^1 & \lambda_1^1 & \ldots & \lambda_n^1 \\ \vdots & & \vdots & \\ \lambda_0^n & \lambda_1^n & \ldots & \lambda_n^n \end{bmatrix}^{-1} \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix}$$

Somit ist jeder Vektor $v_0, \ldots, v_n$ eine Linearkombination von $u_0, \ldots, u_n$, insbesondere gilt demnach $v_0, \ldots, v_n \in U$, wie behauptet. QED

Beweis mit Lagrange–Projektoren: Wir nutzen die Endomorphismen

$$\varphi_i = \prod_{j \neq i} (f - \lambda_j)/(\lambda_i - \lambda_j) \; : \; U \to U.$$

Damit gilt $v_i = \varphi_i(u) \in U$, und genau das war zu zeigen. QED

🙂 Warum sollten wir ein Lemma wie M4C mehrfach beweisen?

Rein logisch gesehen genügt selbstverständlich ein einziger Beweis. Wenn sich mehrere anbieten, wählen wir je nach Bedarf den kürzesten, schönsten, nützlichsten, etc. Im vorliegenden Fall fällt die Wahl schwer, denn jeder unserer Beweise illustriert ein anderes schönes Werkzeug: Minimalpolynom, Induktion, Vandermonde oder Projektoren.

Aus didaktischen Gründen und zur Übung dieser Techniken halte ich es daher für sinnvoll, mehrere Beweise zu präsentieren. So sehen Sie ihre jeweiligen Vorzüge und können sich den für Sie schönsten aussuchen. Das bietet zudem eine breite Grundlage für zukünftige Anwendungen und vielfältige Erfahrung für eigene Rechnungen und Beweise.

Auch in der Physik treten Eigenwerte und Eigenvektoren häufig auf. In der Quantenmechanik werden physikalische Größen durch lineare Operatoren beschrieben. Eigenvektoren sind besonders einfache Basiszustände, ihre Eigenwerte entsprechen möglichen Messwerten.

Auf diese Weise erklärte Heisenberg seine Unschärferelation durch Begriffe der Linearen Algebra: Ortsoperator und Impulsoperator kommutieren nicht und haben keine gemeinsame Eigenbasis, sie können nicht beide gleichzeitig genau gemessen werden.

Die „Atom-Orbitale“, die Sie aus dem Chemie-Unterricht kennen, sind die Eigenfunktionen der zugehörigen Schrödinger–Gleichung. Auch hier entsprechen Messungen linearen Operatoren, Messwerte sind Eigenwerte, und gleichzeitige Messung entspricht simultaner Diagonalisierung. Letzteres gelingt nur bei Kommutativität.

Eigenvektoren spielen in vielen weiteren Anwendungen eine wichtige Rolle, etwa in der Graphentheorie, speziell beim PageRank–Verfahren, mit dem Google die Relevanz von Internetseiten bewertet.

Anwendungsbeispiel zur simultanen Diagonalisierung

Aufgabe: (1) Welche der folgenden Matrizen sind $\mathbb{R}$–diagonalisierbar?

$$A = \begin{bmatrix} -10 & -8 & -2 \\ 11 & 9 & 2 \\ 22 & 16 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} -9 & -8 & -2 \\ 18 & 15 & 3 \\ -6 & -4 & 2 \end{bmatrix}, \quad C = \begin{bmatrix} -10 & -8 & -2 \\ 14 & 11 & 2 \\ 10 & 8 & 5 \end{bmatrix}$$

(2) Welche Teilfamilien von (A, B, C) sind simultan diagonalisierbar?
(3) Finden Sie jeweils eine simultane Eigenbasis, soweit möglich.
(4) Finden Sie jeweils alle simultanen Eigenbasen, soweit möglich.

Lösung: (1a) Wir berechnen $\chi_A = (X-1)^2(X-2)$. Das allein lässt die Frage der Diagonalisierbarkeit noch offen. Zur Klärung berechnen wir entweder zuerst $\mu_A = (X-1)(X-2)$ oder gleich die Eigenräume:

$$\operatorname{Eig}(A,1) = \left\langle\, (-8,11,0)^\intercal,\ (-2,0,11)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$
$$\operatorname{Eig}(A,2) = \left\langle\, (-1,1,2)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$

Machen Sie die Probe! Somit ist die Matrix A über $\mathbb{R}$ diagonalisierbar.
(Bonus: Die Eigenräume liefern erneut χ_A und μ_A wie angegeben.)

Anwendungsbeispiel zur simultanen Diagonalisierung

(1b) Wir berechnen $\chi_B = (X-2)^2(X-3)$. Das allein lässt die Frage der Diagonalisierbarkeit vorerst noch offen. Zur Klärung berechnen wir entweder zuerst $\mu_B = (X-2)(X-3)$ oder gleich die Eigenräume:

$$\operatorname{Eig}(B,2) = \left\langle\, (2,-3,1)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$
$$\operatorname{Eig}(B,3) = \left\langle\, (-2,3,0)^\intercal,\ (-1,0,6)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$

Machen Sie die Probe! Somit ist die Matrix B über $\mathbb{R}$ diagonalisierbar.
(Bonus: Die Eigenräume liefern erneut χ_B und μ_B wie angegeben.)

(1c) Wir berechnen $\chi_C = (X-1)(X-2)(X-3)$. Somit ist die Matrix C über $\mathbb{R}$ diagonalisierbar. Explizit berechnen wir hierzu die Eigenräume:

$$\operatorname{Eig}(C,1) = \left\langle\, (2,-3,1)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$
$$\operatorname{Eig}(C,2) = \left\langle\, (1,-2,2)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$
$$\operatorname{Eig}(C,3) = \left\langle\, (0,-1,4)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$

Machen Sie die Probe! Dies zeigt erneut $\chi_C = (X-1)(X-2)(X-3)$.

Anwendungsbeispiel zur simultanen Diagonalisierung

(2) Jede Matrix A, B, C ist *einzeln* diagonalisierbar. Zur *simultanen* Diagonalisierbarkeit prüfen wir die Kommutativität (M4B) und finden:

$$AB = BA \quad \text{und} \quad BC = CB \quad \text{aber} \quad AC \neq CA$$

Die Teilfamilien (A, B) und (B, C) sind also simultan diagonalisierbar, die Teilfamilien (A, C) und (A, B, C) hingegen sind es nicht!

(3a) Wir können auf (A, B) den Algorithmus M4B anwenden oder aus den berechneten Eigenräumen eine gemeinsame Eigenbasis wählen:

$$\operatorname{Eig}(A,1) = \left\langle\, (-8,11,0)^\intercal,\ (-2,0,11)^\intercal \,\right\rangle_{\mathbb{R}}^{!}, \quad \operatorname{Eig}(A,2) = \left\langle\, (-1,1,2)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$
$$\operatorname{Eig}(B,2) = \left\langle\, (2,-3,1)^\intercal \,\right\rangle_{\mathbb{R}}^{!}, \quad \operatorname{Eig}(B,3) = \left\langle\, (-2,3,0)^\intercal,\ (-1,0,6)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$

$$S = \begin{bmatrix} 2 & 0 & -1 \\ -3 & -1 & 1 \\ 1 & 4 & 2 \end{bmatrix}, \quad S^{-1}AS = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \quad S^{-1}BS = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

(4a) Das ist die einzige gemeinsame Eigenbasis des Paares (A, B), wie immer bis auf Vielfache und Vertauschung der Basisvektoren.

Anwendungsbeispiel zur simultanen Diagonalisierung

(3b) Wir können auf (B, C) den Algorithmus M4B anwenden oder aus den berechneten Eigenräumen eine gemeinsame Eigenbasis wählen:

$$\operatorname{Eig}(B,2) = \left\langle\, (2,-3,1)^\intercal \,\right\rangle_{\mathbb{R}}^{!}, \quad \operatorname{Eig}(B,3) = \left\langle\, (-2,3,0)^\intercal,\ (-1,0,6)^\intercal \,\right\rangle_{\mathbb{R}}^{!}$$
$$\operatorname{Eig}(C,\{1,2,3\}) = \left\{ \left\langle\, (2,-3,1)^\intercal \,\right\rangle_{\mathbb{R}}^{!}, \ \left\langle\, (1,-2,2)^\intercal \,\right\rangle_{\mathbb{R}}^{!}, \ \left\langle\, (0,-1,4)^\intercal \,\right\rangle_{\mathbb{R}}^{!} \right\}$$

$$T = \begin{bmatrix} 2 & 1 & 0 \\ -3 & -2 & -1 \\ 1 & 2 & 4 \end{bmatrix}, \quad T^{-1}BT = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}, \quad T^{-1}CT = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

(4b) Das ist die einzige Eigenbasis von C und somit auch von (B, C), wie immer bis auf Vielfache und Vertauschung der Basisvektoren.

Bemerkung: In den Eigenbasen zu (A, B) bzw. (B, C) gilt jeweils

$$S^{-1}CS = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 2 \end{bmatrix} \quad \text{bzw.} \quad T^{-1}AT = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -1 & 1 \end{bmatrix}.$$

Dies zeigt eindrücklich, dass die jeweils dritte Matrix nicht gleichzeitig diagonalisiert wird, auch nicht kann, wie wir aus (2) bereits wissen.

Anwendungsbeispiel zur simultanen Diagonalisierung

Aufgabe: Wir betrachten weiterhin die drei reellen Matrizen

$$A = \begin{bmatrix} -10 & -8 & -2 \\ 11 & 9 & 2 \\ 22 & 16 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} -9 & -8 & -2 \\ 18 & 15 & 3 \\ -6 & -4 & 2 \end{bmatrix}, \quad C = \begin{bmatrix} -10 & -8 & -2 \\ 14 & 11 & 2 \\ 10 & 8 & 5 \end{bmatrix}.$$

(5) Sind $A,\ B,\ A+B,\ A\cdot B$ diagonalisierbar? einzeln? simultan?
(6) Sind $B,\ C,\ B+C,\ B\cdot C$ diagonalisierbar? einzeln? simultan?
(7) Sind $A,\ C,\ A+C,\ A\cdot C$ diagonalisierbar? einzeln? simultan?

Lösung: (5) Wir haben das Paar (A,B) bereits simultan diagonalisiert:

$$S = \begin{bmatrix} 2 & 0 & -1 \\ -3 & -1 & 1 \\ 1 & 4 & 2 \end{bmatrix} \implies \begin{cases} S^{-1}AS & = \operatorname{diag}(1,1,2) \\ S^{-1}BS & = \operatorname{diag}(2,3,3) \\ S^{-1}(A+B)S & = \operatorname{diag}(3,4,5) \\ S^{-1}(A\cdot B)S & = \operatorname{diag}(2,3,6) \end{cases}$$

Durch S wird somit auch $(\,A,\ B,\ A+B,\ A\cdot B\,)$ simultan diagonalisiert.

Anwendungsbeispiel zur simultanen Diagonalisierung

(6) Wir haben das Paar (B,C) bereits simultan diagonalisiert:

$$T = \begin{bmatrix} 2 & 1 & 0 \\ -3 & -2 & -1 \\ 1 & 2 & 4 \end{bmatrix} \implies \begin{cases} T^{-1}BT & = \operatorname{diag}(2,3,3) \\ T^{-1}CT & = \operatorname{diag}(1,2,3) \\ T^{-1}(B+C)T & = \operatorname{diag}(3,5,6) \\ T^{-1}(B\cdot C)T & = \operatorname{diag}(2,6,9) \end{cases}$$

Durch T wird somit auch $(\,B,\ C,\ B+C,\ B\cdot C\,)$ simultan diagonalisiert.

(7) Wegen $AC \neq CA$ lässt sich (A,C) nicht simultan diagonalisieren. Über die Diagonalisierbarkeit von $A+C$ und $A\cdot C$ lässt sich daraus allein leider noch nichts schließen; beide Fälle sind noch möglich.

Um dies zu klären, müssen wir die Matrizen genauer untersuchen.
Langer Weg: Wir können das Standardverfahren M2I anwenden.
Abkürzung: Wir nutzen geschickt unsere Ergebnisse (1–4).

Anwendungsbeispiel zur simultanen Diagonalisierung

Zur Vereinfachung nutzen wir unsere Diagonalisierung von A:

$$S = \begin{bmatrix} 2 & 0 & -1 \\ -3 & -1 & 1 \\ 1 & 4 & 2 \end{bmatrix}, \quad S^{-1}AS = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \quad S^{-1}CS = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 2 \end{bmatrix}$$

Daraus lesen wir Summe und Produkt ab:

$$S^{-1}(A+C)S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{bmatrix}, \quad S^{-1}(A\cdot C)S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 4 \end{bmatrix}$$

Das zeigt uns, $A\cdot C$ ist (zufällig) diagonalisierbar, $A+C$ jedoch nicht.
Ausführlich gilt $\chi_{A+C} = \mu_{A+C} = (X-1)(X-4)^2$, also greift Satz M3W:
Somit sind zwar A und C diagonalisierbar, $A+C$ jedoch nicht.

Ebenso gilt $\chi_{AC} = \mu_{AC} = (X-1)(X-3)(X-4)$, also greift Satz M2N:
Somit sind A und C und AC diagonalisierbar, jedoch nicht simultan,
denn es gilt $AC \neq CA$ sowie $A(AC) \neq (AC)A$ und $C(AC) \neq (AC)C$.

Anwendungsbeispiel zur simultanen Diagonalisierung

Dieses Zahlenbeispiel zeigt erneut sehr eindrücklich:

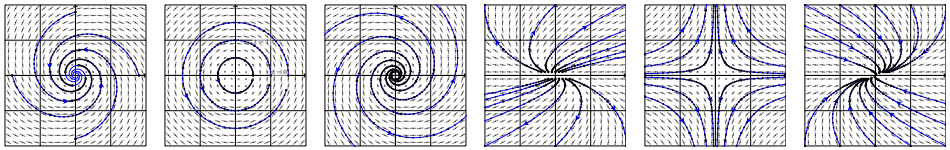
☺ Starke theoretische Grundlagen liefern praktische Werkzeuge.
Diese strukturieren und vereinfachen die Rechnungen spürbar.

☺ Gute Notation und Standardverfahren erleichtern das Vorgehen.
Oft hilft es, vorige Informationen geschickt wiederzuverwenden.

☺ Sie arbeiten umso effizienter, je genauer Sie verstehen, was Sie tun!
. . . insbesondere, was Sie schon haben und was Sie noch suchen.
Sie können dann geschickt vom Standardverfahren abweichen,
je nach konkretem Bedarf und möglichen Abkürzungen.

Kapitel N

Hauptvektoren und Jordanisierung



To learn to succeed,
you must first learn to fail.

Michael Jordan (1963–)

Inhalt dieses Kapitels N

Kanonische Darstellung eines Endomorphismus

Worum geht es bei der kanonischen Darstellung von Endomorphismen? Vorgelegt sei eine lineare Abbildung $f : V \to V$ über einem Körper K. Unser Ziel ist eine möglichst einfache und übersichtliche Darstellung von f als Matrix bezüglich einer Basis von V – geschickt zu f angepasst!

Im vorigen Kapitel M haben wir zuerst die Diagonalisierung geklärt: Bezüglich einer Eigenbasis $\mathcal{B} = (v_i)_{i\in I}$ gilt $f(v_i) = \lambda_i v_i$ für alle $i \in I$. Das ist der Idealfall: In endlicher Dimension ist die darstellende Matrix dann diagonal, also $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$. Einfacher geht es nicht.

Leider ist nicht jeder Endomorphismus $f : V \to V$ diagonalisierbar!

Wir konzentrieren uns auf endliche Dimension $\dim_K V = n < \infty$. Notwendig ist, dass das charakteristische Polynom $\chi_f \in K[X]_n^1$ über K in Linearfaktoren zerfällt. Hinreichend wird dies jedoch erst, wenn die geometrische Vielfachheit die algebraische erreicht (M3W).

In diesem Kapitel N lösen wir alle verbleibenden Fälle, in denen zwar χ_f über K zerfällt, aber dennoch zu wenige Eigenvektoren zu f existieren.

Naturwissenschaftlich-technische Anwendungen

Die Jordan–Form ist ein grundlegendes Ergebnis der Linearen Algebra und zugleich ein Universalwerkzeug in ihren zahlreichen Anwendungen. Sie ist benannt nach dem französischen Mathematiker Camille Jordan (1838–1921), der sie 1870 veröffentlichte. Karl Weierstraß (1815–1897) hatte kurz zuvor bereits 1868 ein äquivalentes Ergebnis vorgestellt.

Genutzt wird die Jordan–Form nicht nur in der Algebra, sondern auch in der Analysis. Anwendern in den Natur- und Ingenieurwissenschaften ist sie höchst willkommen zur Lösung von linearen Differentialgleichungssystemen $\dot{u} = Au$ mit $A \in \mathbb{C}^{n\times n}$. Der Ingenieur Yvon Villarceau löste 1870 den Fall von $n = 2$ Variablen, doch fehlten ihm die algebraischen Werkzeuge für das allgemeine Problem. Jordan antwortete ihm 1871, wie die Normalform dieses Problem löst, und übernahm diese Lösung in die zweite Auflage seines Lehrwerks *Cours d'analyse* von 1887.

Auch diese wichtigen Anwendungen will ich hier gebührend beleuchten. Zeit und Mühe sind gut investiert, denn dadurch werden Motivation, Anwendungen und Techniken wesentlich besser verständlich.

Ist jede quadratische Matrix trigonalisierbar?

N005
Erinnerung

Welche quadratischen Matrizen $A \in K^{n\times n}$ sind trigonalisierbar?

Hindernis: Zerfällt das charakteristische Polynom χ_A in $K[X]$?

Für $n \geq 2$ gilt dies i.A. nicht, typisches Gegenbeispiel über $\mathbb{R}$:

$$A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in \mathbb{R}^{2\times 2} \quad \Rightarrow \quad \chi_A = (X-a)^2 + b^2 \in \mathbb{R}[X]_2^1$$

In $\mathbb{C}[X]$ gilt $\chi_A(X) = (X-\lambda)(X-\bar{\lambda})$ mit $\sigma(A;\mathbb{C}) = \{\lambda, \bar{\lambda}\} = \{a \pm \mathrm{i}b\}$.

Für $b \neq 0$ hat χ_A keine reelle Nullstelle, zerfällt also nicht in $\mathbb{R}[X]$.

☹ Somit ist A für $b \neq 0$ über $\mathbb{R}$ nicht trigonalisierbar, $A \not\sim \left[\begin{smallmatrix} \lambda_1 & * \\ 0 & \lambda_2 \end{smallmatrix}\right]$.

🙂 Zur Trigonalisierung ist dies bereits das einzige Hindernis:

♦ Satz M3B: Trigonalisierung ⇔ Zerfällung

Genau dann ist eine Matrix $A \in K^{n\times n}$ über K trigonalisierbar, wenn ihr charakteristisches Polynom $\chi_A \in K[X]$ über K zerfällt.

⚠ Das hängt sowohl von der Matrix A als auch von dem Körper K ab.

Ist jede quadratische Matrix trigonalisierbar?

N006
Erinnerung

🙂 Über einem algebraisch abgeschlossenen Körper K, etwa $\mathbb{C}$ (A3C), zerfällt jedes Polynom in Linearfaktoren (M2L), dieses erste Hindernis tritt über K demnach nie auf, und jede Matrix ist über K trigonalisierbar.

🙂 Im Allgemeinen ist der Körper K nicht algebraisch abgeschlossen. Notfalls, wenn χ_f über K nicht zerfällt, können wir in einer geeigneten Körpererweiterung $\bar{K} \geq K$ arbeiten, sodass χ_f über $\bar{K}$ zerfällt.

Beispiel: Bei der Untersuchung der Fibonacci–Folge in $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$ tritt die folgende Matrix A auf als Darstellung des Verschiebeoperators:

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \Longrightarrow \quad \chi_A = X^2 - X - 1$$

Das charakteristische Polynom zerfällt nicht über $\mathbb{Q}$, dies gelingt jedoch über der Körpererweiterung $\mathbb{Q}[\sqrt{5}]$: Die beiden Nullstellen von χ_A sind $\phi = \frac{1}{2}(1+\sqrt{5})$ und $\psi = \frac{1}{2}(1-\sqrt{5})$. Somit lässt sich die Matrix A über dem Körper $\mathbb{Q}[\sqrt{5}]$ diagonalisieren und so die Fibonacci–Folge durch die einfache geschlossene Formel $f_n = (\phi^n - \psi^n)/(\phi - \psi)$ darstellen.

Ist jede trigonalisierbare Matrix diagonalisierbar?

N007
Erinnerung

Welche quadratischen Matrizen $A \in K^{n\times n}$ sind diagonalisierbar?

1. Hindernis: Zerfällt das charakteristische Polynom χ_A in $K[X]$?

2. Hindernis: Erreicht die geometrische Vielfachheit die algebraische?

♦ Satz M3W: Kriterien für Diagonalisierbarkeit

Sei $f : V \to V$ eine K–lineare Abbildung und $\dim_K V = n < \infty$.

Dann sind die folgenden Bedingungen äquivalent:

1. Der Endomorphismus $f : V \to V$ ist diagonalisierbar.
2. Es gilt die Eigenraumzerlegung $V = \bigoplus_{\lambda\in\sigma(f)} \operatorname{Eig}(f,\lambda)$.
3. Es gilt die Dimensionsformel $n = \sum_{\lambda\in\sigma(f)} \dim_K \operatorname{Eig}(A,\lambda)$.
4. Das charakteristische Polynom χ_f zerfällt über K in Linearfaktoren und für jeden Eigenwert $\lambda \in \sigma(f)$ gilt $\dim_K \operatorname{Eig}(f,\lambda) = \operatorname{ord}(\chi_f,\lambda)$.
5. Das Minimalpolynom μ_f zerfällt einfach über K, ausgeschrieben $\mu_f = \prod_{\lambda\in\sigma(f)}(X-\lambda)$.

Übung: Beweisen Sie diesen Satz zur Wiederholung.

Ist jede trigonalisierbare Matrix diagonalisierbar?

N008
Erinnerung

🙂 Das erste Hindernis tritt über einem algebraisch abgeschlossenen Körper wie $\mathbb{C}$ nie auf. Über jedem nicht-abgeschlossenen Körper K lässt es sich durch eine geeignete Körpererweiterung $\bar{K} \geq K$ lösen.

⚠ Das zweite Hindernis ist noch ernster und lässt sich nicht umgehen. Typisches Gegenbeispiel ist ein **Jordan–Block** der Dimension $n \geq 2$:

$$B = \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix} \in K^{n\times n} \quad \Rightarrow \quad B - \lambda I = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Aufgabe: Bestimmen Sie zu B das Spektrum und die Eigenräume.

Lösung: Für $\mu \neq \lambda$ ist $B - \mu I$ invertierbar, also $\operatorname{Eig}(B,\mu) = \{0\}$.
Es bleibt nur $\operatorname{Eig}(B,\lambda) = Ke_1$, also erlaubt B keine Eigenbasis.

Das Polynom $\chi_B(x) = (X-\lambda)^n$ hat die Nullstelle λ mit Vielfachheit n.
Der zugehörige Kern $\ker(B-\lambda I) = Ke_1$ hat aber nur Dimension 1:
Die geometrische Vielfachheit ist hier kleiner als die algebraische!

Jordan–Blöcke und Hauptvektorketten

🙂 Über einem algebraisch abgeschlossenen Körper K, etwa $K = \mathbb{C}$, zerfällt jedes Polynom. Somit ist jede Matrix in $K^{n\times n}$ trigonalisierbar.

☹ Leider ist dennoch nicht jede Matrix in $K^{n\times n}$ diagonalisierbar:

$$B = J(n,\lambda) := \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix} \in K^{n\times n}$$

☹ Es gibt nicht genug **Eigenvektoren** zu B für eine Basis von K^n.

🙂 Wir nutzen das Nächstbeste, die **Hauptvektorkette** $(e_1, e_2, \ldots, e_n)$:

$$0 \xleftarrow{B-\lambda} e_1 \xleftarrow{B-\lambda} e_2 \xleftarrow{B-\lambda} \ldots \xleftarrow{B-\lambda} e_n$$

Definition N1A: Hauptvektoren

Sei $f \in \mathrm{End}_K(V)$ und $\lambda \in K$. Eine **Hauptvektorkette** / **Jordan–Kette**

$$0 \xleftarrow{f-\lambda} v_1 \xleftarrow{f-\lambda} v_2 \xleftarrow{f-\lambda} \ldots \xleftarrow{f-\lambda} v_\ell$$

besteht aus Vektoren $v_0 = 0 \neq v_1, \ldots, v_\ell \in V$ mit $(f-\lambda)(v_k) = v_{k-1}$.

Jordan–Blöcke und Hauptvektorketten

Wir schreiben kurz $B - \lambda$ für $B - \lambda I$ und $f - \lambda$ für $f - \lambda\,\mathrm{id}_V$.
Wir nennen v_k einen **Hauptvektor $k$ter Stufe**. Das bedeutet:

$$(f-\lambda)^k(v_k) = 0 \quad \text{aber} \quad v_1 = (f-\lambda)^{k-1}(v_k) \neq 0$$

Die Eigenvektoren v_1 von f sind genau die **Hauptvektoren 1. Stufe**:

$$(f-\lambda)^1(v_1) = 0 \quad \text{aber} \quad v_1 = (f-\lambda)^0(v_1) \neq 0$$

Jeder Vektor v_2 mit $(f-\lambda)(v_2) = v_1$ ist ein **Hauptvektor 2. Stufe**.
Jeder Vektor v_3 mit $(f-\lambda)(v_3) = v_2$ ist ein **Hauptvektor 3. Stufe**, usw.
Daher heißen Hauptvektoren auch **verallgemeinerte Eigenvektoren**.

Jordan–Blöcke spielen im Folgenden die zentrale Rolle: Sie zeigen einfach und eindrücklich, dass nicht jede Matrix diagonalisierbar ist. Die gute Nachricht: Jordan–Blöcke sind auch schon das Schlimmste, was uns passieren kann (wie immer vorausgesetzt, χ_f zerfällt über K).

Jeder Jordan–Block der Größe $n \times n$ entspricht einer Hauptvektorkette der Länge n und umgekehrt. Der folgende Satz N1B besagt, dass wir zu $f : V \to V$ eine Basis aus Hauptvektorketten konstruieren können.

Jordan–Basen und Jordan–Normalform

Beim Diagonalisierungsproblem sind Jordan–Blöcke unvermeidlich. Müssen wir zudem noch mit schlimmeren Komplikationen rechnen? Nein, glücklicherweise sind sie bereits alles, was passieren kann:

Satz N1B: Jordan–Basis eines Endomorphismus

Sei $f \in \mathrm{End}_K(V)$ mit $\dim_K V = n < \infty$ und $\chi_f \in K[X]$ zerfalle über K.

(1) Dann existiert zu f eine Basis $\mathcal{B}$ von V aus Hauptvektorketten.
Wir nennen jede solche Basis $\mathcal{B}$ von V eine **Jordan–Basis** zu f.

So wird f dargestellt als Diagonalmatrix von **Jordan–Blöcken**:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} B_1 & 0 & 0 & 0 \\ 0 & B_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & B_k \end{bmatrix} \quad \text{mit} \quad B_i = \begin{bmatrix} \lambda_i & 1 & 0 & 0 \\ 0 & \lambda_i & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \lambda_i \end{bmatrix} \in K^{n_i \times n_i}$$

(2) Wir nennen diese Darstellung die **Jordan–(Normal)Form** von f, kurz JNF; sie ist eindeutig bis auf die Reihenfolge der Jordan–Blöcke.

Jordan–Basen und Jordan–Normalform

Für jeden Endomorphismus f über $\mathbb{C}$ zerfällt das charakteristische Polynom, also $\chi_f(X) = (X-\lambda_1)\cdots(X-\lambda_n)$ mit $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$.
Sind alle Nullstellen verschieden, so ist f diagonalisierbar (M2N).

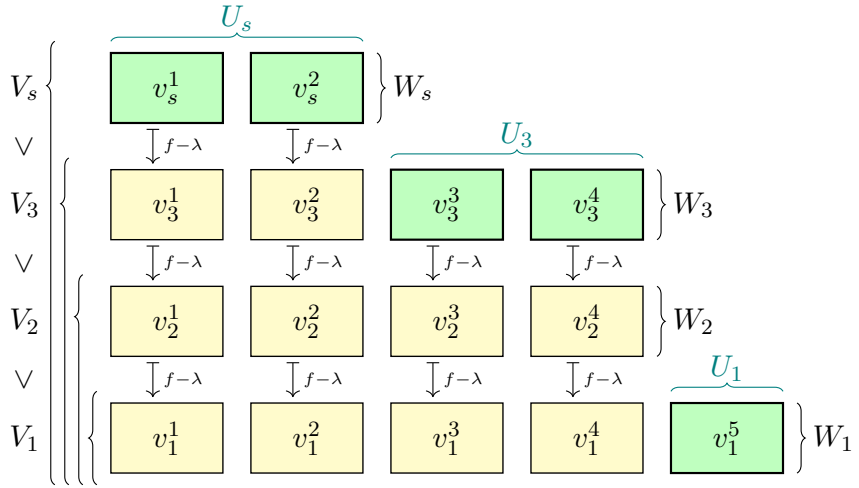
⚠ Bei mehrfachen Nullstellen müssen wir genauer hinschauen: Möglicherweise ist f diagonalisierbar (M1C) oder auch nicht (M1D).

Gegenbeispiel: Für die Matrix B existieren nicht genug Eigenvektoren, um eine Basis zu bilden. Mit der Verallgemeinerung zu Hauptvektoren können wir dieses Problem allgemein lösen. Die Matrix kommt zwar nicht in Diagonalform, wird aber immerhin so einfach wie möglich.

Jeder r–fache Eigenwert λ erlaubt mindestens einen und höchstens r linear unabhängige Eigenvektoren; alle Möglichkeiten können auftreten. Hingegen existieren zu λ immer r linear unabhängige Hauptvektoren! Genauer besagt Satz N1B: Es gibt eine Basis aus Hauptvektorketten.

Die nächsten Folien erklären das Standardverfahren zur Jordanisierung; der Beweis arbeitet die nötigen Argumente anschließend sorgfältig aus.

Standardverfahren zur Jordanisierung: Hauptraum-Sudoku!



Kurzfassung: Zu jedem Eigenwert λ von $f : V \to V$ konstruieren wir ein solches Young–Diagramm und lesen daraus die Jordan–Form ab.

Langfassung: Wir füllen die Kästchen geschickt mit Hauptvektorketten und erhalten daraus wie ersehnt eine Jordan–Basis von V zu f.

Standardverfahren zur Jordanisierung: Hauptraum-Sudoku!

Sei K ein Körper, V ein K–Vektorraum mit $n = \dim V < \infty$ und $f : V \to V$ ein Endomorphismus. Nach folgendem Verfahren finden wir eine Jordan–Basis von V zu f und somit die Jordan–Form von f.

(Einzige Voraussetzung ist, dass das charakteristische Polynom χ_f über K in Linearfaktoren zerfällt. Der Beweis von Satz N1B ist nichts anderes als dieser Algorithmus plus Nachweis der Korrektheit aller Schritte.)

Zunächst benötigen wir alle Eigenwerte von f:

1. Bestimme das charakteristische Polynom $\chi_f \in K[X]$.
2. Bestimme die Eigenwerte $\lambda_i \in K$ mit Vielfachheiten $r_i \in \mathbb{N}_{\geq 1}$.

Abbruch: Falls χ_f nicht zerfällt, so ist f nicht jordanisierbar (M3B).

Vereinfachung: Falls χ_f einfach zerfällt, so ist f diagonalisierbar (M2N), also $V = \bigoplus_i \operatorname{Eig}(f, \lambda_i)$. In diesem Falle genügt das Standardverfahren zur Diagonalisierung (M2I). Allgemein jedoch müssen wir jordanisieren.

(Keine Sorge: Das folgende Standardverfahren zur Jordanisierung beinhaltet die Diagonalisierung als besonders einfachen Spezialfall.)

Standardverfahren zur Jordanisierung: Hauptraum-Sudoku!

Für jeden Eigenwert λ mit Vielfachheit r setze $g := f - \lambda \operatorname{id}_V : V \to V$ und führe die folgenden Schritte (3) und (4) sowie bei Bedarf (5) aus:

3. Für $i = 0, 1, \ldots, s$ setze $V_i := \ker g^i = \ker(f - \lambda \operatorname{id}_V)^i$ und bestimme die Dimension $k_i := \dim V_i$ bis schließlich $k_s = r$ gilt (dank N1M).

Visualisierung: Diese Daten stellen wir wie oben als Young–Diagramm übersichtlich dar; die Zeile $i = 1, \ldots, s$ enthält $z_i := k_i - k_{i-1}$ Kästchen. Dabei gilt $z_1 \geq z_2 \geq \cdots \geq z_s$: Kein Kästchen hängt in der Luft (N1J).

4. Lies die Jordan–Form $\operatorname{diag}(B_1, \ldots, B_t)$ ab: Die $j$te Spalte der Höhe ℓ zum Eigenwert λ steht für eine Hauptvektorkette der Länge ℓ und somit für den Jordan–Block $B_j = J(\ell, \lambda)$. Diese Jordan–Form ist eindeutig bis auf die willkürliche Reihenfolge der Eigenwerte.

Kurzfassung: Wenn zu f nur die Jordan–Form $J = \mathrm{M}_{\mathcal{J}}^{\mathcal{J}}(f)$ gefragt ist, so sind wir an dieser Stelle schon fertig.

Langfassung: Falls zudem eine explizite Jordan–Basis $\mathcal{J}$ gesucht ist, so gelingt uns dies wie folgt: In den grünen Kästchen stehen die Startvektoren der Hauptvektorketten. Diese suchen wir!

Standardverfahren zur Jordanisierung: Hauptraum-Sudoku!

5. Für $i = s, \ldots, 1$ wähle in V_i zu $V_{i-1} \oplus g(W_{i+1})$ ein Komplement U_i, sodass $V_i = V_{i-1} \oplus g(W_{i+1}) \oplus U_i$ gilt, und setze $W_i = g(W_{i+1}) \oplus U_i$. Anfangs gilt $W_{s+1} = 0$, also $U_s = W_s$. Wähle eine Basis von U_i und lasse diese Startvektoren zu Hauptvektorketten runterrieseln (N1J).

Konkrete Rechnung mit Basisvektoren: In jeder Schicht $i = s, \ldots, 1$ konstruieren wir eine Basis von W_i. Zuvor berechnet ist eine Basis $w_1, \ldots, w_q$ der darüberliegenden Schicht W_{i+1}. (Anfangs $W_{s+1} = 0$.) Runterrieseln liefert eine Basis $g(w_1), \ldots, g(w_q)$ des Bildes $g(W_{i+1})$. Wähle eine Hilfsbasis $v_1, \ldots, v_p$ von V_{i-1} und setzte diese zur Basis $v_1, \ldots, v_p, g(w_1), \ldots, g(w_q)$ von $V_{i-1} \oplus g(W_i)$ zusammen. Ergänze diese schließlich zu einer Basis $v_1, \ldots, v_p, g(w_1), \ldots, g(w_q), u_1, \ldots, u_h$ von V_i. Trage die Startvektoren $u_1, \ldots, u_h$ in die grünen Kästchen ein und lasse runterrieseln. Unsere Basis von W_i ist nun $g(w_1), \ldots, g(w_q), u_1, \ldots, u_h$. Mit diesen Daten gehen wir weiter zur darunterliegenden Schicht $i - 1$.

6. Lies die Jordan–Basis $\mathcal{J}$ zu f ab: Alle Spalten von links nach rechts, jede Spalte von unten nach oben (in der Konvention von Satz N1B). Füge diese Jordan–Ketten für alle Eigenwerte zur Jordan–Basis $\mathcal{J}$.

Beispiele: Welche Jordan–Formen sind möglich?

Aufgabe: Gegeben sei eine Matrix $A \in \mathbb{R}^{n\times n}$ mit charakteristischem Polynom $\chi_A \in \mathbb{R}[X]_n^1$. Welche Jordan–Normalformen sind möglich?

(1) $\chi_A = (X-1)(X-2)(X-3)$ sowie (2) $\chi_A = (X-1)(X-2)^2(X-3)$, (3) $\chi_A = (X-2)^2(X-3)^2$, (4) $\chi_A = (X-2)^3(X-3)$, (5) $\chi_A = (X-\lambda)^4$

Lösung: (1) Die Matrix A ist diagonalisierbar (M2N). Durch die Wahl einer Eigenbasis (v_1, v_2, v_3) von $\mathbb{R}^3$ zu A erhalten wir $T \in \mathrm{GL}_3\,\mathbb{R}$ mit

$$A \sim T^{-1}AT = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

(2) Die Matrix A ist eventuell diagonalisierbar… oder sie ist es nicht:

$$A \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} \quad \text{oder} \quad A \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

🙂 Diese beiden Normalformen sind die einzigen Möglichkeiten (N1B).

Beispiele: Welche Jordan–Formen sind möglich?

🙂 Der einfachste Fall sind n paarweise verschiedene Eigenwerte. Hier greift Satz M2N und garantiert uns die Diagonalisierbarkeit:

$$V = \mathrm{Eig}(f, \lambda_1) \oplus \mathrm{Eig}(f, \lambda_2) \oplus \cdots \oplus \mathrm{Eig}(f, \lambda_n).$$

☹ Leider ist nicht jede Matrix so einfach zu durchschauen, es können mehrfache Eigenwerte auftreten. Dann steht die Diagonalisierbarkeit in Frage (M3W): Erreicht die geometrische Vielfachheit die algebraische?

🙂 Dank der Jordan–Normalform (N1B) können wir alle möglichen Fälle einfach und übersichtlich darstellen, egal ob diagonalisierbar oder nicht. Das ist eine enorme Vereinfachung und sehr nützliche Struktur.

Im vorliegenden Beispiel (2) gibt es genau zwei Möglichkeiten: Dank Satz N1B ist jede Matrix A mit charakteristischem Polynom $\chi_A = (X-1)(X-2)^2(X-3)$ entweder ähnlich zur Diagonalmatrix links oder ähnlich zur hier gezeigten Jordan–Matrix rechts.

Auch in den folgenden Beispielen gibt es jeweils nur endlich viele Möglichkeiten, und wir können diese leicht vollständig aufzählen.

Beispiele: Welche Jordan–Formen sind möglich?

(3) Bei $\chi_A = (X-2)^2(X-3)^2$ sind vier Normalformen möglich:

$$A \sim \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

(4) Bei $\chi_A = (X-2)^3(X-3)$ sind genau drei Normalformen möglich:

$$A \sim \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

(5) Bei $\chi_A = (X-\lambda)^4$ sind genau fünf Normalformen möglich:

$$\begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix}$$

Beispiele: Welche Jordan–Formen sind möglich?

⚠ Die Reihenfolge der Eigenwerte $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ ist dabei beliebig; in $(\mathbb{R}, \leq)$ können wir sie zum Beispiel der Größe nach anordnen. Im Allgemeinen jedoch gibt es hierzu keine sinnvolle Konvention.

Die Konstruktion aller möglichen Jordan–Matrizen ist denkbar einfach. Dank Satz N1B haben wir neben der Existenz auch die Eindeutigkeit!

Zu jedem Eigenwert $\lambda \in \mathbb{K}$ mit Vielfachheit $r \geq 1$ überlegen wir uns, wie wir die gegebene Dimension r in Jordan–Blöcke aufteilen können. Das entspricht den Zahlpartitionen, wie anschließend in N1C erklärt.

Zu jedem Eigenwert sortieren wir die Jordan–Blöcke nach ihrer Größe, und zwar absteigend wie im Young–Diagram. Diese übliche Konvention ist zwar etwas willkürlich, aber doch sehr nützlich und übersichtlich.

Übung: Umordnung der Jordan–Blöcke führt zu einer ähnlichen Matrix.

🙂 Da wir aus jeder Ähnlichkeitsklasse genau einen Repräsentanten auswählen wollen, verhelfen uns die hier erklärten Konventionen zur (weitgehenden) Eindeutigkeit, wie in den Beispielen (3–5) zu sehen.

Kombinatorik: Wie viele Jordan–Formen gibt es?

Aufgabe: Gegeben sei eine Matrix $A \in K^{n\times n}$ mit charakteristischem Polynom $\chi_A = (X-\lambda)^n$. Wie viele Jordan–Formen gibt es hierzu?

Lösung: Zur systematischen Aufzählung zerlegen wir $n \in \mathbb{N}$ in eine Summe $n = n_1 + \cdots + n_k$ mit $n_1, \ldots, n_k \in \mathbb{N}_{\geq 1}$. Da die Reihenfolge keine Rolle spielt, können wir die Summanden absteigend ordnen:

Definition N1C: (ungeordnete) Zahlpartition

Eine **Partition** der Zahl $n \in \mathbb{N}$ als Summe von $k \in \mathbb{N}$ (ungeordneten, umsortierbaren) Summanden ist ein Tupel $(n_1, n_2, \ldots, n_k) \in \mathbb{N}^k$ mit

$$n = n_1 + n_2 + \cdots + n_k \quad \text{und} \quad n_1 \geq n_2 \geq \cdots \geq n_k \geq 1.$$

Ihre Menge bezeichnen wir mit $P(n,k)$ und $P(n) = \bigsqcup_{k=0}^{n} P(n,k)$, ihre Anzahl mit $p(n,k) = \sharp P(n,k)$ und $p(n) = \sharp P(n) = \sum_{k=0}^{n} p(n,k)$.

So zählt $P(n,k)$ die Young–Diagramme mit n Kästchen und k Spalten. Mit dieser hilfreichen Notation können wir auch für große n die Anzahl der möglichen Jordan–Formen übersichtlich darstellen und berechnen.

Kombinatorik: Wie viele Jordan–Formen gibt es?

Partitionen spielen in Kombinatorik und Informatik eine wichtige Rolle. Auch in der Linearen Algebra treten sie ganz natürlich auf, wie hier bei der Aufzählung von Jordan–Normalformen. Zur Betonung sagen wir **Zahlpartition** in N1C im Gegensatz zu **Mengenpartition** in E2K.

Beispiele: Für $n = 2, 3, 4, 5$ erhalten wir die folgenden Zahlpartitionen:

$$\begin{aligned}
n = 2 &= 1+1 \\
n = 3 &= 2+1 = 1+1+1 \\
n = 4 &= 3+1 = 2+2 = 2+1+1 = 1+1+1+1 \\
n = 5 &= 4+1 = 3+2 = 3+1+1 = 2+2+1 \\
&= 2+1+1+1 = 1+1+1+1+1
\end{aligned}$$

Im letzten Beispiel finden wir also $P(5,0) = \emptyset$, $P(5,1) = \{(5)\}$, $P(5,2) = \{(4,1),(3,2)\}$, $P(5,3) = \{(3,1,1)),(2,2,1)\}$, $P(5,4) = \{(2,1,1,1)\}$, $P(5,5) = \{(1,1,1,1,1)\}$.

Wir suchen nun eine möglichst effiziente Methode, um die Anzahlen $p(n,k)$ und auch die Mengen $P(n,k)$ systematisch zu konstruieren.

Kombinatorik: Wie viele Jordan–Formen gibt es?

Für die ersten Partitionszahlen erhalten wir somit folgende Werte:

n	$p(n)$	$p(n,k)$							
		$k=0$	1	2	3	4	5	6	…
0	1	1	0	0	0	0	0	0	…
1	1	0	1	0	0	0	0	0	…
2	2	0	1	1	0	0	0	0	…
3	3	0	1	1	1	0	0	0	…
4	5	0	1	2	1	1	0	0	…
5	7	0	1	2	2	1	1	0	…
6	11	0	1	3	3	2	1	1	…

Hierbei gilt $P(n) = \bigsqcup_{k=0}^{n} P(n,k)$, also $p(n) = \sharp P(n) = \sum_{k=0}^{n} p(n,k)$.
Für $k = n$ gilt $P(n,n) = \{(1,1,\ldots,1)\}$, und somit $p(n,n) = 1$.
Für $k > n$ gilt $P(n,k) = \emptyset$, und somit $p(n,k) = 0$.

Bemerkung: Für alle k mit $n/2 \leq k \leq n$ gilt zudem $p(n,k) = p(n-k)$: Wenn wir zunächst jeden Summanden mit 1 belegen, so bleibt noch $n-k \leq k$ zu verteilen. Hierfür gibt es genau $p(n-k)$ Möglichkeiten.

Kombinatorik: Wie viele Jordan–Formen gibt es?

Wie berechnen wir die Partitionszahlen $p(n,k)$ und $p(n)$ geschickt? Eine Möglichkeit ist die explizite Konstruktion von $P(n,k)$. Effizienter:

Satz N1D: Rekursionsformel für Partitionszahlen

(0) Für $k = 0$ gilt $p(0,0) = 1$ sowie $p(n,0) = 0$ für alle $n \in \mathbb{N}_{\geq 1}$.
(1) Für alle $1 \leq k \leq n$ gilt $p(n,k) = p(n-1,k-1) + p(n-k,k)$

Aufgabe: Beweisen Sie die Rekursionsformeln des Satzes.

Lösung: (0) Nach Definition N1C gilt $P(0,0) = \{()\}$ und $P(n,0) = \{\}$.

(1) Wir zerlegen $P(n,k) = P_1(n,k) \sqcup P_2(n,k)$ in disjunkte Teilmengen

- $P_1(n,k) := \{\, (n_1,\ldots,n_k) \in P(n,k) \mid n_k = 1 \,\} \cong P(n-1,k-1)$, vermöge der Bijektion $(n_1,\ldots,n_{k-1},1) \leftrightarrows (n_1,\ldots,n_{k-1})$, und
- $P_2(n,k) := \{\, (n_1,\ldots,n_k) \in P(n,k) \mid n_k \geq 2 \,\} \cong P(n-k,k)$, vermöge der Bijektion $(n_1,\ldots,n_k) \leftrightarrows (n_1-1,\ldots,n_k-1)$.

Übung: Füllen Sie damit die Tabelle für $0 \leq k \leq n \leq 10$ aus! Zur Probe:

n	0	1	2	3	4	5	6	7	8	9	10	…
$p(n)$	1	1	2	3	5	7	11	15	22	30	42	…

Minimalpolynom aus der Jordan–Form

Aufgabe: Bestimmen Sie das Minimalpolynom der Matrizen

$$A = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad C = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}.$$

Lösung: Das char. Polynom ist $\chi_A = \chi_B = \chi_C = (X-2)^3(X-3)^2$.
Das Minimalpolynom folgt aus der max. Größe der Jordan–Blöcke:

$$\mu_A = (X-2)^1(X-3)^1,$$
$$\mu_B = (X-2)^2(X-3)^2,$$
$$\mu_C = (X-2)^3(X-3)^1.$$

Aufgabe: Setzen Sie A, B, C in $(X-2)^k(X-3)^\ell$ ein und bestimmen Sie die minimalen Exponenten k und ℓ, für die Matrix annulliert wird.

Aufgabe: Formulieren Sie hierzu eine allgemeine, einfache Merkregel: Wie extrahieren Sie das Minimalpolynom aus der Jordan–Form?

Minimalpolynom aus der Jordan–Form

Satz N1E: charakteristisches Polynom und Minimalpolynom

Sei $f : V \to V$ eine K–lineare Abbildung und $\dim_K V = n < \infty$.

(1) Angenommen, χ_f zerfällt in Linearfaktoren über K. Dann gilt

$$\chi_f = (X-\lambda_1)^{r_1} \cdots (X-\lambda_k)^{r_k} \quad \text{mit } \lambda_i \neq \lambda_j \text{ für } i \neq j \text{ und}$$
$$\mu_f = (X-\lambda_1)^{s_1} \cdots (X-\lambda_k)^{s_k} \quad \text{mit } 1 \leq s_i \leq r_i \text{ für alle } i.$$

(2) Der Exponent s_i ist die maximale Größe aller Jordan–Blöcke zu λ_i. Der Exponent r_i ist die Summe der Größen aller Jordan–Blöcke zu λ_i.

(3) Genau dann ist der Endomorphismus f über K diagonalisierbar, wenn sein Minimalpolynom $\mu_f \in K[X]$ über K einfach zerfällt.

Beweis: Diese Zusammenfassung ist eine unmittelbare Anwendung der zuvor erarbeiteten Sätze (1) M3R und (2) M3O und (3) M3W. QED

Übung: Führen Sie zur Wiederholung die Aussage (2) sorgfältig aus: Warum hat das Minimalpolynom genau diese schöne einfache Form?

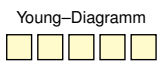
Jordan–Formen zu gegebenem Minimalpolynom

Aufgabe: Welche Jordan–Formen sind möglich mit charakteristischem Polynom $\chi_A = (X-\lambda)^5$ und Minimalpolynom $\mu_A = (X-\lambda)^s$?

Lösung: (1) Im Falle $\mu_A = (X-\lambda)^1$ ist A diagonalisierbar:

$$A \sim T^{-1}AT = \begin{bmatrix} \lambda & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}$$

Young–Diagramm



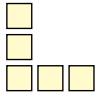
In diesem Fall ist A selbst diagonal, denn $A = T(\lambda I)T^{-1} = \lambda I$.

(2) Im Falle $\mu_A = (X-\lambda)^2$ gibt es genau zwei Möglichkeiten:

$$A \sim \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix} \quad \text{oder} \quad A \sim \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}$$

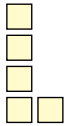
Jordan–Formen zu gegebenem Minimalpolynom

(3) Im Falle $\mu_A = (X-\lambda)^3$ gibt es genau zwei Möglichkeiten:



$$A \sim \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix} \quad \text{oder} \quad A \sim \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}$$

(4) Im Falle $\mu_A = (X-\lambda)^4$ bzw. $\mu_A = (X-\lambda)^5$ bleibt nur



$$A \sim \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix} \quad \text{bzw.} \quad A \sim \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}.$$

☺ Das Minimalpolynom bündelt nützliche Informationen zur Größe der Jordan–Blöcke und damit insbesondere zur Diagonalisierbarkeit.

Die Zerlegung $J = D + N$ in diagonal plus nilpotent

Bemerkung N1F: Potenzen der Jordan–Form $J = D + N$

Die Jordan–Form $T^{-1}AT = J = D + N$ ist Summe der Diagonalmatrix D und der nilpotenten Matrix N, und beide kommutieren: $DN = ND$.

Angenommen $N^s = 0$. Dank binomischem Lehrsatz E2J gilt dann:

$$J^n = (D+N)^n = \sum_{k=0}^{s-1} \binom{n}{k} D^{n-k} N^k$$

Aus $A = TJT^{-1}$ folgt dann $A^n = TJ^nT^{-1}$ für jeden Exponenten $n \in \mathbb{N}$. Dies ergibt eine geschlossene Formel für jeden Koeffizienten von A^n.

Beweis: Jeder Jordan–Block operiert auf seinem zyklischen Unterraum. Dank der Zerlegung als direkte Summe kommutieren sie untereinander. In jedem einzelnen Jordan–Block $D + N$ gilt $D = \lambda I$, also $DN = ND$.

Induktion über n: Für $n = 0$ gilt $A^0 = I$ und $TJ^0T^{n-1} = TIT^{-1} = I$.
Für $n \geq 1$ gilt $A^n = A \cdot A^{n-1} = TJT^{-1} \cdot TJ^{n-1}T^{n-1} = TJ^nT^{-1}$. QED

Die Zerlegung $J = D + N$ in diagonal plus nilpotent

Illustrative Beispiele:

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}^n = \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \binom{n}{3}\lambda^{n-3} & \binom{n}{4}\lambda^{n-4} \\ 0 & \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \binom{n}{3}\lambda^{n-3} \\ 0 & 0 & \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} \\ 0 & 0 & 0 & \lambda^n & n\lambda^{n-1} \\ 0 & 0 & 0 & 0 & \lambda^n \end{bmatrix}$$

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \mu \end{bmatrix}^n = \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \binom{n}{3}\lambda^{n-3} & 0 \\ 0 & \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & 0 \\ 0 & 0 & \lambda^n & n\lambda^{n-1} & 0 \\ 0 & 0 & 0 & \lambda^n & 0 \\ 0 & 0 & 0 & 0 & \mu^n \end{bmatrix}$$

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \mu & 1 \\ 0 & 0 & 0 & 0 & \mu \end{bmatrix}^n = \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & 0 & 0 \\ 0 & \lambda^n & n\lambda^{n-1} & 0 & 0 \\ 0 & 0 & \lambda^n & 0 & 0 \\ 0 & 0 & 0 & \mu^n & n\mu^{n-1} \\ 0 & 0 & 0 & 0 & \mu^n \end{bmatrix}$$

Der Spezialfall $A = \lambda I + N$ mit N nilpotent

Bemerkung N1G: Speziallfall $A = \lambda I + N$

Angenommen, für $A \in K^{r\times r}$ gilt $\mu_A = (X - \lambda)^r$. Dann folgt $A = \lambda I + N$ mit $N^s = 0$ für ein $s \in \{1, \ldots, r\}$. Dank binomischem Lehrsatz E2J gilt:

$$A^n = (\lambda I + N)^n = \sum_{k=0}^{s-1} \binom{n}{k} \lambda^{n-k} N^k$$

Dies ergibt eine geschlossene Formel für jeden Koeffizienten von A^n.

Beweis: Aus der Jordan–Form $T^{-1}AT = J = \lambda I + M$ mit $M^s = 0$ folgt $A = TJT^{-1} = \lambda I + N$ mit $N = TMT^{-1}$, also ebenso $N^s = 0$. QED

$$A = \begin{bmatrix} 1 & 2 & -5 \\ 14 & 10 & -18 \\ 11 & 9 & -17 \end{bmatrix}$$

Aufgabe: Für die obige Matrix $A \in \mathbb{R}^{3\times 3}$ gilt $\mu_A = (X - \lambda)^3$. Bestimmen Sie eine geschlossene Formel für jeden Koeffizienten von $A^n = (a_{ij}^{(n)})$.

Der Spezialfall $A = \lambda I + N$ mit N nilpotent

Standardverfahren: Bestimme die Jordan–Form $T^{-1}AT = J = D + N$.
Rücktransformation ergibt $A^n = TJ^nT^{-1} = T\left[\sum_{k=0}^{s-1} \binom{n}{k} D^{n-k}N^k\right]T^{-1}$.

☺ Allgemein und gelingt immer: Wir berechnen J sowie T und T^{-1}.

☹ Die Berechnung ist aufwändig. Geht es vielleicht auch kürzer?

$$A = \begin{bmatrix} 1 & 2 & -5 \\ 14 & 10 & -18 \\ 11 & 9 & -17 \end{bmatrix}$$

Im Spezialfall haben wir den kurzen Weg: $A = \lambda I + N$ mit N nilpotent. Aus $\operatorname{tr}(A) = -6$ lesen wir $\lambda = -2$ (M3F). Somit ist $N = A + 2I$ nilpotent:

$$N = \begin{bmatrix} 3 & 2 & -5 \\ 14 & 12 & -18 \\ 11 & 9 & -15 \end{bmatrix} \implies N^2 = \begin{bmatrix} -18 & -15 & 24 \\ 12 & 10 & -16 \\ -6 & -5 & 8 \end{bmatrix} \implies N^3 = 0$$

☺ Damit ist auch die Annahme $\mu_A = (X - \lambda)^3$ nachträglich bewiesen.

☺ Wir erhalten so $A^n = \lambda^n N^0 + n\lambda^{n-1}N^1 + \binom{n}{2}\lambda^{n-2}N^2$ für alle $n \in \mathbb{N}$.
Das ist eine einfache geschlossene Formel für die Koeffizienten von A^n.

Zum Beweis: Jordanisierung gelingt!

Warum können wir jeden Endomorphismus $f : V \to V$ über K jordanisieren, vorausgesetzt $\dim_K V < \infty$ und χ_f zerfällt über K?

Zum Konstruktion einer Jordan–Basis benötigen wir zwei Bausteine:

1. Der Vektorraum V ist die direkte Summe der Haupträume (N1M).
2. Jeder Hauptraum erlaubt eine Basis aus Hauptvektorketten (N1L).

Es gibt nicht immer genug Eigenvektoren, um eine Basis zu bilden.
Aussage (1) garantiert, dass es immer genug Hauptvektoren gibt.

Dank (2) können wir diese sogar zu Hauptvektorketten anordnen.
So finden wir eine Jordan–Basis, bestehend aus Hauptvektorketten.

Das Standardverfahren zur Jordanisierung haben wir als Algorithmus erklärt (ab Seite N106). Wir wollen nun seine Korrektheit beweisen.

Zum Beweis: Jordanisierung gelingt!

Wir beweisen den Satz von Jordan (N1B) wie folgt:

Zuerst halten wir fest: Hauptvektorketten sind linear unabhängig (N1H).
Das ist für konkrete Rechnungen eine hilfreiche Gewissheit.

Anschließend erklären wir die Haupträume (N1I) von $f : V \to V$ als verallgemeinerte Eigenräume und klären ihre interne Struktur (N1J).

Daraus folgt sofort die Eindeutigkeit der Jordan–Form (N1K)
und die Jordanisierung für nilpotente Endomorphismen (N1L).

Die Hauptraumzerlegung (N1M) vollendet schließlich den Beweis:
Existenz einer Jordan–Basis und Eindeutigkeit der Jordan–Form.

Erst in diesem letzten Schritt benötigen wir, dass das charakteristische Polynom χ_f über K zerfällt. Über $K = \mathbb{C}$ ist dies immer garantiert.

Hauptvektorketten sind linear unabhängig.

Satz N1H: Hauptvektorketten sind linear unabhängig.

Sei $f : V \to V$ eine lineare Abbildung über K und $\lambda \in K$ ein Skalar.

(1) Jede Hauptvektorkette $\mathcal{F} = (v_1, \dots, v_\ell)$ zu λ ist linear unabhängig.

$$0 \xleftarrow{f-\lambda} v_1 \xleftarrow{f-\lambda} v_2 \xleftarrow{f-\lambda} \dots \xleftarrow{f-\lambda} v_\ell$$

(2) Eine Familie von Hauptvektorketten $\mathcal{F} = (v_1^1, \dots, v_{\ell_1}^1; \dots; v_1^k, \dots, v_{\ell_k}^k)$ zu λ ist genau dann linear unabhängig, wenn die zugrundeliegenden Eigenvektoren $\mathcal{E} = (v_1^1, \dots, v_1^k)$ linear unabhängig sind.

$$\begin{aligned} 0 &\xleftarrow{f-\lambda} v_1^1 \xleftarrow{f-\lambda} v_2^1 \xleftarrow{f-\lambda} \dots \xleftarrow{f-\lambda} v_{\ell_1}^1 \\ &\vdots \\ 0 &\xleftarrow{f-\lambda} v_1^k \xleftarrow{f-\lambda} v_2^k \xleftarrow{f-\lambda} \dots \xleftarrow{f-\lambda} v_{\ell_k}^k \end{aligned}$$

🙂 Alle Vektoren in einem korrekt ausgefüllten Young–Diagramm, wie auf Seite N105 dargestellt, sind demnach linear unabhängig.

Hauptvektorketten sind linear unabhängig.

Beweis: (1) Wir führen Induktion über die Länge ℓ der Hauptvektorkette.
Der Fall $\ell = 1$ ist klar (I1D), denn es gilt $v_1 \neq 0$ nach Definition N1A.
Sei also $\ell \geq 2$. Gegeben seien Koeffizienten $a_1, \dots, a_{\ell-1}, a_\ell \in K$ mit $a_1 v_1 + \dots + a_{\ell-1} v_{\ell-1} + a_\ell v_\ell = 0$. Wir zeigen $0 = a_1 = \dots = a_{\ell-1} = a_\ell$.
Die Anwendung von $(f - \lambda)^{\ell-1}$ ergibt zunächst $a_\ell v_1 = 0$, also gilt $a_\ell = 0$.
Die reduzierte Familie $\mathcal{F}' = (v_1, \dots, v_{\ell-1})$ ohne v_ℓ ist linear unabhängig nach Induktionsvoraussetzung. Wir schließen $0 = a_1 = \dots = a_{\ell-1} = a_\ell$.

(2) Wir führen Induktion über die maximale Länge $\ell = \max\{\ell_1, \dots, \ell_k\}$.
Der Fall $\ell = 1$ ist trivial, denn hier ist $\mathcal{F} = \mathcal{E}$ linear unabhängig.
Wir können $\ell = \ell_1 = \dots = \ell_r > \ell_{r+1} \geq \dots \geq \ell_k \geq 1$ annehmen.
Gegeben seien Koeffizienten $a_j^i \in K$ mit $\sum_{i=1}^{k} \sum_{j=1}^{\ell_k} a_j^i v_j^i = 0$.
Die Anwendung von $(f - \lambda)^{\ell-1}$ reduziert dies zu $\sum_{i=1}^{r} a_\ell^i v_1^i = 0$.
Da die Familie $\mathcal{E}$ linear unabhängig ist, folgt $a_\ell^1 = \dots = a_\ell^r = 0$.
Die Familie $\mathcal{F}'$ entsteht aus $\mathcal{F}$ durch Löschung von $v_\ell^1, \dots, v_\ell^r$.
Nach Induktionsvoraussetzung ist $\mathcal{F}'$ linear unabhängig,
also gilt $a_j^i = 0$ für alle i, j. Das war zu zeigen. QED

Haupträume eines Endomorphismus

Definition N1ı: Haupträume eines Endomorphismus

Sei $f : V \to V$ eine K–lineare Abbildung und $\lambda \in K$ ein Skalar.

(1) Der **Hauptraum der Stufe** $s = 0, 1, 2, \dots$ von f zu λ ist

$$V_s := \ker(f - \lambda \operatorname{id}_V)^s.$$

(2) Wir erhalten so eine aufsteigende Kette f–invarianter Unterräume:

$$\{0\} = V_0 \leq V_1 \leq V_2 \leq V_3 \leq \cdots \leq V \quad \text{und} \quad f(V_i) \subseteq V_i$$

Hierbei ist $V_1 = \ker(f - \lambda \operatorname{id}_V)$ der **Eigenraum** von f zu λ,
und V_s heißt auch **verallgemeinerter Eigenraum** der Stufe s.

(3) Der **Hauptraum** von f zu λ (ohne Einschränkung der Stufe) ist

$$\operatorname{Hau}(f, \lambda) := \bigcup_{s \in \mathbb{N}} \ker(f - \lambda \operatorname{id}_V)^s.$$

(4) Dank (2) ist $\operatorname{Hau}(f, \lambda)$ ein f–invarianter Unterraum von V. Er besteht aus allen Vektoren $v \in V$ mit $(f - \lambda \operatorname{id}_V)^s(v) = 0$ für einen hinreichend großen Exponenten $s \in \mathbb{N}$, der im Allgemeinen von v abhängen wird.

Haupträume eines Endomorphismus

Aufgabe: Zeigen Sie die Aussagen (2) und (4). (Streng genommen sollte eine Definition keine Behauptungen enthalten, doch hier will ich davon abweichen und sofort die grundlegenden Eigenschaften nennen.)

Lösung: (2) Wir setzen abkürzend $g := f - \lambda$, genauer $g = f - \lambda \operatorname{id}_V$.
Sei $v \in V_s$. Daraus folgt $g^{s+1}(v) = g(g^s(v)) = g(0) = 0$, also $v \in V_{s+1}$.
Dank $g \circ f = f \circ g$ folgt $g^s(f(v)) = f(g^s(v)) = f(0) = 0$, also $f(v) \in V_s$.
(4) Ist $V_0 \leq V_1 \leq V_2 \leq \cdots \leq V$ eine Kette von Unterräumen in V,
dann ist ihre Vereinigung $\bigcup_{s \in \mathbb{N}} V_s$ ebenfalls ein Unterraum in V.
Beweisen Sie dies als Übung, oder konsultieren Sie Satz I1z.

Bemerkung: Ist V endlich-dimensional, so auch jeder Unterraum

$$V_0 \leq V_1 \leq V_2 \leq \cdots \leq V,$$

und diese Kette stabilisiert, das heißt es existiert ein Index $s \in \mathbb{N}$,
sodass $V_s = V_r$ für alle $r \geq s$ gilt, also $\operatorname{Hau}(f, \lambda) = \ker(f - \lambda \operatorname{id}_V)^s$.
Der folgende Satz klärt die interne Struktur des Hauptraumes $\operatorname{Hau}(f, \lambda)$,
so wie wir sie im Standardverfahren zur Jordanisierung (N106) nutzen.

Interne Struktur eines Hauptraums

Satz N1ȷ: interne Struktur eines Hauptraums

Sei $f : V \to V$ linear über K sowie $\lambda \in K$ ein Skalar und $g = f - \lambda \operatorname{id}_V$.

(0) Für die Haupträume $V_i := \ker g^i$ der Stufe $i = 0, 1, 2, \dots$ gilt

$$\{0\} = V_0 \leq V_1 \leq V_2 \leq \cdots \leq V.$$

Für die Dimensionen $k_i := \dim V_i$ folgt somit $0 = k_0 \leq k_1 \leq k_2 \leq \dots$.
Für alle $i \geq 1$ wählen wir eine Basis von V_{i-1}, ergänzen diese zu einer Basis von V_i und erhalten so eine Summenzerlegung $V_i = V_{i-1} \oplus W_i$.

(1) Dann ist g injektiv auf W_{i+1}. Zudem gilt $V_{i-1} \cap g(W_{i+1}) = \{0\}$, also

$$g : W_{i+1} \xrightarrow{\sim} g(W_{i+1}) \quad \text{und} \quad V_{i-1} \oplus g(W_{i+1}) \leq V_i.$$

Insbesondere folgt daraus $\dim W_{i+1} \leq \dim W_i$.

(2) Sei zudem $k_1 = \dim V_1 = \dim W_1$ endlich. Per Induktion über $i \in \mathbb{N}$ folgt aus (1), dass auch $\dim W_i \leq k_1$ und $\dim V_i \leq i k_1$ endlich sind.

Für die Zuwächse $z_i = k_i - k_{i-1} = \dim W_i$ gilt $z_1 \geq z_2 \geq z_3 \geq \dots$.

Interne Struktur eines Hauptraums

Beweis: Aussage (0) haben wir bereits zuvor in N1ı geklärt.
Durch Basiswahl und Ergänzung erhalten wir $V_i = V_{i-1} \oplus W_i$.

(1) Für $w \in W_{i+1} \smallsetminus \{0\}$ gilt $w \notin V_i$, also $0 \neq g^i(w) = g^{i-1}(g(w))$.
Das bedeutet $g(w) \neq 0$ und $g(w) \notin V_{i-1}$, also $g : W_{i+1} \xrightarrow{\sim} g(W_{i+1})$
und $V_{i-1} \oplus g(W_{i+1}) \leq V_i$. Daraus folgt $\dim W_{i+1} \leq \dim W_i$.

(2) Dies folgt sofort per Induktion über $i \in \mathbb{N}$. QED

☺ Dies rechtfertigt die Darstellung als Young–Diagramm (Seite N105).
Jede Zeile $i = 1, \dots, s$ enthält $z_i := k_i - k_{i-1} = \dim W_i$ Kästchen.
Dabei gilt $z_1 \geq z_2 \geq \cdots \geq z_s$: Kein Kästchen hängt in der Luft.

☺ Zudem präzisiert Satz N1ȷ auch die Stabilisierung:
Gilt $V_s = V_{s+1}$ für ein $s \in \mathbb{N}$, so folgt $V_s = V_r$ für alle $r \geq s$.

☺ Unser Satz N1ȷ gilt auch für unendliche Dimension.
Im Falle $k_1 < \infty$ erhalten wir die lineare Schranke $k_i \leq i k_1$.

Satz N1K: Eindeutigkeit der Jordan–Form

Vorgelegt seien in $K^{n\times n}$ zwei Jordan–Matrizen

$$B = \begin{bmatrix} B_1 & 0 & 0 & 0 \\ 0 & B_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & B_\ell \end{bmatrix} \quad \text{und} \quad C = \begin{bmatrix} C_1 & 0 & 0 & 0 \\ 0 & C_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & C_m \end{bmatrix}$$

mit Jordan–Blöcken $B_i = J(\ell_i, \lambda_i)$ und $C_j = J(m_j, \mu_j)$ für alle i und j.

(1) Sind B und C ähnlich, also $C = T^{-1}BT$ für ein $T \in \mathrm{GL}_n K$, dann gilt $\ell = m$ und nach Umordnung $B_i = C_i$ für alle $i = 1, \ldots, \ell$.

(2) Genauer: Die Anzahl $n(B;\ell,\lambda)$ der Blöcke $J(\ell,\lambda)$ der Matrix B ist

$$n(B;\ell,\lambda) = 2\dim\ker(B-\lambda)^\ell - \dim\ker(B-\lambda)^{\ell-1} - \dim\ker(B-\lambda)^{\ell+1}.$$

Diese Anzahl ist eine Invariante unter Ähnlichkeit $B \sim C$ von Matrizen: Aus $C = T^{-1}BT$ folgt $n(C;\ell,\lambda) = n(B;\ell,\lambda)$ für alle $\lambda \in K$ und $\ell \in \mathbb{N}_{\geq 1}$.

Beweis: (2) Jeder Jordan–Block $J(\ell,\lambda)$ der Größe $\ell \times \ell$ entspricht einer Hauptvektorkette der Länge ℓ, und umgekehrt. Zur Matrix B definieren wir $k_\ell := \dim\ker(B-\lambda)^\ell$ und setzen $z_\ell := k_\ell - k_{\ell-1}$ wie in Satz N1J.

Die Zahl $z_\ell \in \mathbb{N}$ ist die Breite der Zeile ℓ im Young–Diagramm (N105) zum Hauptvektorraum $\mathrm{Hau}(B,\lambda)$. Dies ist zugleich die Anzahl der Hauptvektorketten der Länge $\geq \ell$. Somit ist $n(B;\ell,\lambda) = z_\ell - z_{\ell+1}$ die gesuchte Anzahl der Hauptvektorketten der Länge genau ℓ.

Aus $C = T^{-1}BT$ folgt $(C-\lambda)^\ell = (T^{-1}BT-\lambda)^\ell = T^{-1}(B-\lambda)^\ell T$, also $\dim\ker(C-\lambda)^\ell = \dim\ker(B-\lambda)^\ell$ für alle $\lambda \in K$ und $\ell \in \mathbb{N}$. Nach obiger Rechnung folgt demnach $n(C;\ell,\lambda) = n(B;\ell,\lambda)$. Daraus schließen wir Aussage (1). QED

☺ Für alle jordanisierbaren Matrizen haben wir damit das Klassifikationsproblem bis auf Ähnlichkeit gelöst.

☺ Über jedem algebraisch abgeschlossenen Körper wie $\mathbb{C}$ ist jede Matrix jordanisierbar, wie wir nun zeigen werden.

Satz N1L: Jordanisierung eines nilpotenten Endomorphismus

(1) Sei $g : V \to V$ linear über K und nilpotent, $g^s = 0$. Dann existiert zu g eine Jordan–Basis von V, also eine Basis aus Hauptvektorketten.

Beweis: Die Konstruktion haben wir ab Seite N106 ausgeführt.

- Für $i = 0, 1, \ldots, s$ setze $V_i := \ker g^i$ und bestimme die Dimension $k_i := \dim V_i$. Den Struktursatz N1J mit diesen Daten visualisieren wir als Young–Diagramm, wie auf Seite N105 gezeigt.
- Für $i = s, \ldots, 1$ wähle in V_i zu $V_{i-1} \oplus g(W_{i+1})$ ein Komplement U_i, sodass $V_i = V_{i-1} \oplus g(W_{i+1}) \oplus U_i$ gilt, und setze $W_i = g(W_{i+1}) \oplus U_i$. Anfangs gilt $W_{s+1} = 0$, also $U_s = W_s$. Wähle eine Basis von U_i und lasse diese Startvektoren zu Hauptvektorketten runterrieseln.

Das Gelingen dieser Konstruktion verdanken wir dem Struktursatz N1J. Das so ausgefüllte Young–Diagramm liefert eine Basis von V. QED

Satz N1L: Jordanisierung eines nilpotenten Endomorphismus

(2) Sei $f : V \to V$ linear über K. Dann erlaubt jeder Hauptraum $\mathrm{Hau}(f,\lambda)$ eine Jordan–Basis, also eine Basis aus Hauptvektorketten.

Beweis: Wir betrachten die Abbildung $g = f - \lambda_i$ auf dem Hauptraum $\mathrm{Hau}(f,\lambda)$. Dieser Endomorphismus ist nilpotent. Dank (1) können wir eine Jordan–Basis zu g konstruieren, und damit zu f. QED

☺ Damit können wir jeden nilpotenten Endomorphismus g jordanisieren, und allgemein f auf jedem Hauptraum $\mathrm{Hau}(f,\lambda)$.

Es bleibt schließlich noch die Hauptraumzerlegung zu klären. Das ist der Inhalt des folgenden, abschließenden Satzes.

Erst in diesem letzten Schritt benötigen wir, dass das charakteristische Polynom χ_f über K zerfällt. Über $K = \mathbb{C}$ ist dies immer garantiert.

Satz N1M: Hauptraumzerlegung

Vorgelegt sei $f : V \to V$ linear über K mit $n = \dim_K(V) < \infty$.
Das charakteristische Polynom von f zerfalle über K gemäß

$$\chi_f(X) = (X - \lambda_1)^{r_1}(X - \lambda_2)^{r_2} \cdots (X - \lambda_k)^{r_k}$$

wobei $\lambda_1, \lambda_2, \ldots, \lambda_k \in K$ und $\lambda_i \neq \lambda_j$ für $i \neq j$ gelte.

(1) Dann haben wir die Summenzerlegung in Haupträume:

$$\boxed{V = \operatorname{Hau}(f, \lambda_1) \oplus \operatorname{Hau}(f, \lambda_2) \oplus \cdots \oplus \operatorname{Hau}(f, \lambda_k)}$$

Dabei gilt $\operatorname{Hau}(f, \lambda_i) = \ker(f - \lambda_i \operatorname{id}_V)^{r_i}$ und $\dim_K \operatorname{Hau}(f, \lambda_i) = r_i$.

🙂 Das erinnert uns an die Eigenraumzerlegung aus Satz M1I.
Der entscheidende Vorteil gegenüber Eigenräumen $\operatorname{Eig}(f, \lambda_i)$ ist, dass die Haupträume $\operatorname{Hau}(f, \lambda_i)$ *immer* eine Summenzerlegung von ganz V ergeben. Insbesondere hat jeder Hauptraum $\operatorname{Hau}(f, \lambda_i)$ *immer* die richtige Dimension, nämlich genau die algebraische Vielfachheit r_i.

Aufgabe: Beweisen Sie dies mit dem Satz M3K von Cayley–Hamilton und der Kernzerlegung M3V dank Bézout wie in Kapitel M vorbereitet.

Lösung: Dank Cayley–Hamilton M3K gilt $\chi_f(f) = 0$. Wir setzen voraus, dass χ_f über K zerfällt. Die zugehörige Kernzerlegung M3V ergibt

$$V = \ker(f - \lambda_1)^{r_1} \oplus \ker(f - \lambda_2)^{r_2} \oplus \cdots \oplus \ker(f - \lambda_k)^{r_k}.$$

Für $i \in \{1, \ldots, k\}$ betrachten wir den Summanden $H_i := \ker(f - \lambda_i)^{r_i}$ und seine Dimension $s_i = \dim H_i$. Auf H_i ist $f - \lambda_i$ nilpotent, also hat $f_i := f|_{H_i}^{H_i} : H_i \to H_i$ das charakteristische Polynom $(X - \lambda_i)^{s_i}$ (M3T).

Auf der direkten Summe $V = \bigoplus_i H_i$ gilt somit $\chi_f = \prod_i (X - \lambda_i)^{s_i}$.
Der Polynomvergleich zeigt $s_i = r_i$ für alle i, also $\dim H_i = r_i$.

Wir haben somit $H_i = \ker(f - \lambda_i)^{r_i} \leq \bigcup_{s \in \mathbb{N}} \ker(f - \lambda_i)^s = \operatorname{Hau}(f, \lambda_i)$.
Auf H_j mit $j \neq i$ ist $f - \lambda_i$ ein Isomorphismus, also gilt $\operatorname{Hau}(f, \lambda_i) \leq H_i$.

Damit ist die ersehnte Hauptraumzerlegung $V = \bigoplus_i H_i$ bewiesen,
mit $H_i := \ker(f - \lambda_i)^{r_i} = \operatorname{Hau}(f, \lambda_i)$ und $\dim H_i = r_i$. QED

Satz N1M: Hauptraumzerlegung

(2) Sei $\mathcal{A}_i$ eine Basis von $\operatorname{Hau}(f, \lambda_i)$. Zusammengesetzt erhalten wir eine Basis $\mathcal{A}$ von V. Die Abbildung f wird dann dargestellt durch

$$A = \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f) = \begin{bmatrix} A_1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & A_k \end{bmatrix}.$$

Hierbei gilt $A_i = \lambda_i E_{r_i} + N_i$ mit einer nilpotenten Matrix $N_i \in K^{r_i \times r_i}$.
Somit erhalten wir die Zerlegung $A = D + N$ mit $D, N \in K^{n \times n}$,
wobei D diagonal und N nilpotent ist und zudem $DN = ND$ gilt.

(3) Für jeden Hauptraum können wir eine Jordan–Basis wählen.
So wird f dargestellt als Diagonalmatrix von Jordan–Blöcken:

$$A_i = \operatorname{diag}(J(r_{i,1}, \lambda_i), J(r_{i,2}, \lambda_i), \ldots, J(r_{i,k_i}, \lambda_i))$$

mit $r_{i,1} \geq r_{i,2} \geq \cdots \geq r_{i,k_i}$ und $r_i = r_{i,1} + r_{i,2} + \cdots + r_{i,k_i}$.

🙂 Damit haben wir den Satz von Jordan (N1B) bewiesen, also die Existenz einer Jordan–Basis und die Eindeutigkeit der Jordan–Form.

Die sorgsame Ausführung des Beweises beschert uns ein genaues Verständnis und darüber hinaus als Bonus noch weitere Erkenntnisse:

🙂 Zugleich haben wir das Standardverfahren zur Jordanisierung als Algorithmus erklärt (ab Seite N106) und seine Korrektheit bewiesen.

Das beweist insbesondere die Existenz einer Jordan–Basis
und ist zudem eine Anleitung für die konkrete Berechnung.

🙂 Jordan–Basen gibt es viele, doch die Jordan–Form ist eindeutig (bis auf Umordnung der Jordan–Blöcke). Dies folgt aus den Invarianten $n(f; \ell, \lambda)$ aus Satz N1K, diese zählen die Jordan–Blöcke $J(\ell, \lambda)$ von f.

Diese Invarianten ermöglichen insbesondere die Kurzfassung des Standardverfahrens, wenn nur die Jordan–Form ohne Basis gefragt ist.

Kern und Defekt einer Komposition

N201

Lemma N2A: Defekt-Ungleichung

(1) Für jeden Endomorphismus $f : V \to V$ über K gilt

$$\dim_K \ker(f^r) \leq r \cdot \dim_K \ker(f).$$

(2) Allgemein seien $f : U \to V$ und $g : V \to W$ lineare Abbildungen,

$$U \xrightarrow{\ f\ } V \xrightarrow{\ g\ } W.$$

(2a) Daraus erhalten wir die kurze exakte Sequenz

$$0 \longrightarrow \ker(f) \xrightarrow{\ \text{inc}\ } \ker(g \circ f) \xrightarrow[u \mapsto f(u)]{f'} \operatorname{im}(f) \cap \ker(g) \xrightarrow[v \mapsto g(v)]{g'} 0.$$

(2b) Insbesondere gilt für die Dimensionen:

$$\begin{aligned} \dim_K \ker(g \circ f) &= \dim_K \ker(f) + \dim_K \big[\operatorname{im}(f) \cap \ker(g)\big] \\ &\leq \dim_K \ker(f) + \dim_K \ker(g) \end{aligned}$$

Kern und Defekt einer Komposition

N202

Aufgabe: Treten alle numerisch möglichen Fälle tatsächlich auf?

Ausführlich: Gegeben seien $k, \ell, m \in \mathbb{N}$ mit $k \leq m \leq k + \ell$. Finden Sie

$$\begin{aligned} f : U \to V \quad &\text{mit} \quad \dim \ker(f) = k, \\ g : V \to W \quad &\text{mit} \quad \dim \ker(g) = \ell, \\ h = g \circ f \quad &\text{mit} \quad \dim \ker(h) = m. \end{aligned}$$

Das zeigt: Die Abschätzung des Lemmas lässt sich nicht verbessern.

Bemerkung: Das ist eine offene Frage. Gesucht ist eine Konstruktion, möglichst einfach und elegant. Hier können und sollen Sie kreativ sein! Bitte machen Sie sich die Freude und versuchen Sie es zunächst selbst.

Lösung: Für $n := k + \ell - m$ gilt $0 \leq n \leq \ell$. Wir betrachten die Matrizen

$$A = \begin{bmatrix} 1_{\ell \times \ell} & 0_{\ell \times k} \\ 0_{n \times \ell} & 0_{n \times k} \end{bmatrix}, \quad B = \begin{bmatrix} 1_{n \times n} & 0_{n \times \ell} \end{bmatrix}, \quad BA = \begin{bmatrix} 1_{n \times n} & 0_{n \times m} \end{bmatrix}.$$

Diese definieren lineare Abbildungen $f : K^{\ell+k} \to K^{\ell+n} : u \mapsto Au$ und $g : K^{n+\ell} \to K^n : v \mapsto Bv$ mit $h = g \circ f : K^{\ell+k} \to K^n$ wie gewünscht.

Kern und Defekt einer Komposition

N203
Erläuterung

Zur Erinnerung: Die Dimension des Kerns heißt abkürzend auch Defekt. Daher nenne ich die Aussagen (1) und (2b) griffig *Defekt-Ungleichung*. Aussage (2a) formuliert dies bequem und präzise als *exakte Sequenz*.

Aufgabe: Beweisen Sie die Defekt-Ungleichungen des Lemmas.

Bemerkung: Das ist eine geschlossene Frage. Gesucht ist ein Beweis, möglichst einfach und elegant. Hier können und sollen Sie akribisch die Begriffe einüben und die nötigen Argumente sorgsam ausführen. Bitte machen Sie sich die Freude und versuchen Sie es selbst.

Lösung: (1) Anschaulich, in endlicher Dimension $\dim V < \infty$:
Wir nutzen das Young–Diagramm des Hauptraums zum Eigenwert 0.
Das Fundament der Breite $z_1 = \dim_K \ker(f)$ erlaubt weitere Schichten der Breite $z_1 \geq z_2 \geq \cdots \geq z_r$, somit $\dim_K \ker(f^r) = z_1 + \cdots + z_r \leq r z_1$.

☺ Den allgemeinen Fall (1) entnehmen wir Satz N1J.

☺ Alternativ folgt (1) aus Aussage (2), die wir nun beweisen.

Kern und Defekt einer Komposition

N204
Erläuterung

(2a) Zunächst ist die Sequenz wie angegeben tatsächlich wohldefiniert:
Für $u \in \ker(f)$ gilt $g(f(u)) = g(0) = 0$, somit $\ker(f) \leq \ker(g \circ f)$.
Für $u \in \ker(g \circ f)$ gilt $f(u) \in \operatorname{im}(f) \cap \ker(g)$, denn $g(f(u)) = 0$.

Zur Erinnerung, Exaktheit bedeutet „Bild gleich Kern“ an jeder Stelle:
Das Bild von links ist gleich dem Kern nach rechts. (Definition I2H)

Exaktheit links ist klar, denn die Inklusion $\ker(f) \hookrightarrow \ker(g \circ f)$ ist injektiv.

Die Exaktheit rechts entspricht der Surjektivität der Abbildung f'.
Jedes Element $v \in \operatorname{im}(f) \cap \ker(g)$ hat die Form $v = f(u)$ mit $g(v) = 0$.
Somit existiert $u \in \ker(g \circ f)$ mit $v = f'(u)$. Das heißt, f' ist surjektiv.

Die Exaktheit in der Mitte bedeutet $\ker(f') = \ker(f)$:
Dies gilt, denn $\ker(f) \leq \ker(g \circ f)$, und f' ist die Einschränkung von f auf den Startraum $\ker(g \circ f)$ und den Zielraum $\operatorname{im}(f) \cap \ker(g)$.

Die Aussage (2b) folgt aus (2a) dank der Dimensionsformel J2M.

Aus (2b) schließlich folgt (1) mit $g = f^{r-1}$ und Induktion über r.

Die diskrete Ableitung und ihre Hauptfolgen

Sei $\mathbb{K}$ ein Körper, etwa $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Wir arbeiten im Vektorraum $\mathbb{K}^{\mathbb{N}}$ aller Folgen $f : \mathbb{N} \to \mathbb{K} : n \mapsto f(n)$ mit Indexmenge $\mathbb{N}$ und Werten in $\mathbb{K}$.

Wir betrachten den Differenzenoperator (aka die diskrete Ableitung):

$$\Delta : \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}} : f \mapsto \Delta f \quad \text{mit} \quad (\Delta f)(n) = f(n+1) - f(n).$$

Aufgabe: (1) Bestimmen Sie $V_r = \ker \Delta^r$ und $V = \bigcup_{r\in\mathbb{N}} V_r$ in $\mathbb{K}^{\mathbb{N}}$.
(2) Nennen Sie eine Basis aus Hauptvektorketten von V_r und V.

🙂 Hier haben wir eine aufsteigende Kette von Untervektorräumen $V_0 \leq V_1 \leq V_2 \leq \dots$ in $\mathbb{K}^{\mathbb{N}}$, daher ist ihre Vereinigung $V = \bigcup_{r\in\mathbb{N}} V_r$ ebenfalls ein Untervektorraum von $\mathbb{K}^{\mathbb{N}}$. (Warum? Übung!)

Lösung: (1a) Für $r = 0$ haben wir $\Delta^0 = \mathrm{id}$, also $V_0 = \{0\}$.

(1b) Die Gleichung $\Delta f = 0$ bedeutet $f(n+1) - f(n) = 0$ für alle $n \in \mathbb{N}$. Somit gilt $V_1 = \ker \Delta = \langle\, 1 \,\rangle^!_{\mathbb{K}}$ mit der konstanten Funktion $1 = \mathrm{const}^1_{\mathbb{N}}$.

(1c) Aus $\dim_{\mathbb{K}} \ker \Delta = 1$ folgt $\dim_{\mathbb{K}} \ker \Delta^r \leq r$ für alle $r \in \mathbb{N}$. (N1J/N2A)

Die diskrete Ableitung und ihre Hauptfolgen

(1d) Wir erinnern uns an die Binomialkoeffizienten und betrachten

$$f_k : \mathbb{N} \to \mathbb{K} : f_k(n) = \binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

Hier gilt $f_0(n) = 1$ und $f_1(n) = n$ und $f_2(n) = n(n-1)/2$ usw.
Für die diskrete Ableitung finden wir:

$$\Delta f_k(n) \overset{\text{Def}}{=} f_k(n+1) - f_k(n) \overset{\text{Def}}{=} \binom{n+1}{k} - \binom{n}{k} \overset{\text{E229}}{=} \binom{n}{k-1} \overset{\text{Def}}{=} f_{k-1}(n)$$

(1e) Wir haben also eine (unendlich lange) Hauptvektorkette

$$0 \xleftarrow{\Delta} f_0 \xleftarrow{\Delta} f_1 \xleftarrow{\Delta} f_2 \xleftarrow{\Delta} f_3 \xleftarrow{\Delta} \dots$$

Jede Hauptvektorkette ist linear unabhängig.

(2) Somit erhalten wir die ersehnten Basen aus Hauptvektorketten:

$$V_r = \ker \Delta^r = \langle\, f_0, \dots, f_{r-1} \,\rangle^!_{\mathbb{K}},$$
$$V = \textstyle\bigcup_{r\in\mathbb{N}} V_r = \langle\, f_k \mid k \in \mathbb{N} \,\rangle^!_{\mathbb{K}}$$

Die diskrete Ableitung und ihre Hauptfolgen

$\binom{n}{k}$	n=0	1	2	3	4	5	6	7	8	9	10
k=0	1	1	1	1	1	1	1	1	1	1	1
1	0	1	2	3	4	5	6	7	8	9	10
2	0	0	1	3	6	10	15	21	28	36	45
3	0	0	0	1	4	10	20	35	56	84	120
4	0	0	0	0	1	5	15	35	70	126	210

Satz N2B

Wir betrachten den Differenzenoperator / die diskrete Ableitung

$$\Delta : \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}} : f \mapsto \Delta f \quad \text{mit} \quad (\Delta f)(n) = f(n+1) - f(n).$$

Zum Eigenwert 0 sind die Haupträume der Stufe $r = 1, 2, 3, \dots$ dann

$$\ker(\Delta^r) = \left\langle\, f_k \;\middle|\; k < r \,\right\rangle^!_{\mathbb{K}} \quad \text{mit} \quad f_k(n) = \binom{n}{k} \quad \text{und}$$
$$0 \xleftarrow{\Delta} f_0 \xleftarrow{\Delta} f_1 \xleftarrow{\Delta} f_2 \xleftarrow{\Delta} f_3 \xleftarrow{\Delta} f_4 \xleftarrow{\Delta} \dots$$

Die diskrete Ableitung und ihre Hauptfolgen

🙂 Wir sehen an diesem Zahlenbeispiel sehr schön, warum der Differenzenoperator auch als „diskrete Ableitung“ betrachtet wird: Die Folge $f = \Delta F$ mit $f(n) = F(n+1) - F(n)$ gibt in jedem Punkt die „Steigung“ von F an, also die Differenz zum nächsten Wert.

🙂 Umgekehrt entsteht F aus f durch „diskrete Integration“: Wir geben die Folge $f : \mathbb{N} \to \mathbb{K}$ sowie den Startwert $F(0) = 0$ vor und erhalten alle weiteren Werte $F(n)$ für $n = 1, 2, 3, \dots$ rekursiv durch Aufsummieren gemäß $F(n+1) = F(n) + f(n)$ für alle $n \in \mathbb{N}$.

Genau dies ist die Definition der Summe $F(n) = \sum_{k=0}^{n-1} f(k)$.

🙂 Die so entstehende Tabelle ist gerade das Pascalsche Dreieck! Die Darstellung haben wir der vorliegenden Situation angepasst: In jeder Zeile halten wir $k \in \mathbb{N}$ fest und lassen $n \in \mathbb{N}$ laufen. (Üblicherweise ist $n \in \mathbb{N}$ die Zeile und $k \in \{0, \dots, n\}$ läuft.)

🙂 Eine Art diskrete Ableitung macht im Young–Diagramm aus $\dim V_k$ die Breite $\dim W_k = \dim V_k - \dim V_{k-1}$ der Schichten und daraus schließlich die Anzahl der Startvektoren, $\dim U_k = \dim W_k - \dim W_{k+1}$.

Der Verschiebeoperator und seine Hauptfolgen

Auf dem Folgenraum $\mathbb{K}^{\mathbb{N}}$ betrachten wir den Verschiebeoperator

$$s : \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}} : f \mapsto sf \quad \text{mit} \quad (sf)(n) = f(n+1).$$

Aufgabe: Bestimmen Sie alle Haupträume $V_r = \ker(s-\lambda)^r$ der Stufe $r = 1, 2, 3, \ldots$. Nennen Sie eine Basis aus Hauptvektorketten.

Lösung: (a) Sei $\lambda \in \mathbb{K}$. Stufe $r = 1$ ist der Eigenraum (M247):

$$\operatorname{Eig}(s, \lambda) = \left\langle\, f_0 \,\right\rangle_{\mathbb{K}}^{!} \quad \text{mit} \quad f_0 : \mathbb{N} \to \mathbb{K} : n \mapsto \lambda^n$$

(b) Aus $\dim_{\mathbb{K}} \ker(s-\lambda) = 1$ folgt $\dim_{\mathbb{K}} \ker(s-\lambda)^r \leq r$ dank N1J/N2A.

(c) Wir inspirieren uns an der vorigen Aufgabe und N1F und betrachten

$$f_k : \mathbb{N} \to \mathbb{K} : n \mapsto \tbinom{n}{k} \lambda^{n-k}.$$

Dank Rekursionsformel der Binomialkoeffizienten E229 finden wir:

$$(s-\lambda) f_k(n) = \tbinom{n+1}{k} \lambda^{n+1-k} - \tbinom{n}{k} \lambda^{n+1-k} = \tbinom{n}{k-1} \lambda^{n-(k-1)} = f_{k-1}(n)$$

(d) Wir erhalten also auch hier eine unendlich lange Hauptvektorkette:

$$0 \xleftarrow{s-\lambda} f_0 \xleftarrow{s-\lambda} f_1 \xleftarrow{s-\lambda} f_2 \xleftarrow{s-\lambda} f_3 \xleftarrow{s-\lambda} \ldots$$

Anwendung: lineare Rekursionsgleichungen

☺ Das ist ein sehr effizientes und elegantes Vorgehen:
Wir bestimmen zunächst den Eigenraum $V_1 = \operatorname{Eig}(s, \lambda)$.
Daraus folgt die Abschätzung $\dim_{\mathbb{K}} \ker(s-\lambda)^r \leq r$ für alle $r \in \mathbb{N}$.
Durch explizite Konstruktion finden wir eine Hauptvektorkette,
somit eine Basis von V_r, und daraus folgt $\dim_{\mathbb{K}} \ker(s-\lambda)^r = r$.

☺ Ich zelebriere diese Anwendung hier betont ausführlich, da es sich um allgemein wichtige Operatoren handelt, und all unsere Werkzeuge der Linearen Algebra hier zur Blüte kommen und Früchte tragen.
Die Formel (c) fällt nicht vom Himmel, siehe Bemerkung N1F.

Übung: Was genau passiert im interessanten Sonderfall $\lambda = 0$?
Wie ist die Formel $f_k(n) = \binom{n}{k} \lambda^{n-k}$ hier zu interpretieren?

☺ Zusammenfassend formuliere ich hierzu den folgenden Satz zum Verschiebeoperator und den Lösungen von Rekursionsgleichungen.
Anschließend werden wir dieses erfolgreiche Rezept genauso auf die Ableitung und Differentialgleichungen anwenden.

Der Verschiebeoperator und seine Hauptfolgen

Satz N2C: Hauptfolgen des Verschiebeoperators

Auf dem Folgenraum $\mathbb{K}^{\mathbb{N}}$ betrachten wir den Verschiebeoperator

$$s : \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}} : f \mapsto sf \quad \text{mit} \quad (sf)(n) = f(n+1).$$

(1) Zum Eigenwert λ sind die Haupträume der Stufe $r = 1, 2, 3, \ldots$ dann

$$\ker(s-\lambda)^r = \left\langle\, f_k \,\middle|\, k < r \,\right\rangle_{\mathbb{K}}^{!} \quad \text{mit} \quad f_k(n) = \tbinom{n}{k} \lambda^{n-k} \quad \text{und}$$
$$0 \xleftarrow{s-\lambda} f_0 \xleftarrow{s-\lambda} f_1 \xleftarrow{s-\lambda} f_2 \xleftarrow{s-\lambda} f_3 \xleftarrow{s-\lambda} f_4 \xleftarrow{s-\lambda} \ldots$$

(2) Vorgelegt sei ein normiertes Polynom

$$P = X^r + a_{r-1} X^{r-1} + \cdots + a_0 X^0 = (X-\lambda_1)^{r_1} \cdots (X-\lambda_k)^{r_k}.$$

Dann hat $L = \ker P(s) \leq \mathbb{K}^{\mathbb{N}}$ eine Basis aus Hauptvektorketten:

$$L = \ker(s-\lambda_1)^{r_1} \oplus \cdots \oplus \ker(s-\lambda_k)^{r_k}$$

Damit können wir jede lineare Rekursionsgleichung $P(s) f = 0$ lösen.

Der Verschiebeoperator und seine Hauptfolgen

Satz N2C: Hauptfolgen des Verschiebeoperators

(3) Die Auswertung stiftet den $\mathbb{K}$–Isomorphismus

$$q : L \xrightarrow{\sim} \mathbb{K}^r : f \mapsto \big(\, f(0),\, f(1),\, f(2), \ldots, f(r-1) \,\big).$$

Damit können wir jedes Anfangswertproblem lösen, das heißt,
die eindeutige Lösung als einfache, geschlossene Formel darstellen.

☺ Damit können Sie lineare Rekursionsgleichungen $P(s) f = 0$ lösen, nun für alle Polynome $P \in \mathbb{K}[X]_r^1$, auch mit mehrfachen Eigenwerten!

☺ Dasselbe gilt entsprechend für die diskrete Ableitung $\Delta = s - \mathrm{id}$:
Nur die Eigenwerte verschieben sich, denn $\Delta - \lambda = s - (1+\lambda)$.

Beweis: (1) Die Haupträume kennen wir aus der vorigen Aufgabe.

(2) Diese direkte Summe ist die Kernzerlegung aus Satz M3V.

(3) Auswertung und Dimension kennen wir aus Satz M2R:
Zu je r beliebig vorgegebenen Startwerten $f_0, \ldots, f_{r-1} \in \mathbb{K}$
existiert genau eine P–rekursive Folge $f = (f_0, \ldots, f_{r-1}, f_r, \ldots)$. QED

Aufgabe: Wie lösen Sie mit Satz N2c lineare Rekursionsgleichungen?
Erklären Sie hierzu das Standardverfahren (ohne & mit Anfangswerten).

Die Ableitung auf Polynomen und ihre Hauptfunktionen

N217

Über dem Körper $\mathbb{K}$ betrachten wir die Ableitung auf Polynomen:

$$\partial : \mathbb{K}[X] \to \mathbb{K}[X] : P = \textstyle\sum_{i=0}^{n} p_i X^i \mapsto \partial P = \sum_{i=1}^{n} i p_i X^{i-1}$$

Aufgabe: Bestimmen Sie alle Haupträume $V_r = \ker(\partial - \lambda)^r$ der Stufe $r = 1, 2, 3, \ldots$. Nennen Sie eine Basis aus Hauptvektorketten.

Lösung: Wir betrachten die Eigenvektorgleichung $\partial P = \lambda P$.
Sei $\lambda \neq 0$. Für $P \neq 0$ gilt $\deg(\partial P) < \deg(\lambda P)$, also $\operatorname{Eig}(\partial, \lambda) = \{0\}$.
Somit bleibt nur $\lambda = 0$ als einzig möglicher Eigenwert von ∂.

(0a) Charakteristik $\operatorname{char} \mathbb{K} = 0$: Wir finden $\ker(\partial) = \langle\, X^0 \,\rangle_{\mathbb{K}}^{!}$.

(0b) Aus $\dim_{\mathbb{K}} \ker(\partial) = 1$ folgt $\dim_{\mathbb{K}} \ker(\partial^r) \leq r$ für $r \in \mathbb{N}$. (N1J/N2A)

(0c) Die Polynome $F_k = X^k/k! \in \mathbb{K}[X]$ bilden eine Hauptvektorkette:

$$0 \xleftarrow{\partial} F_0 \xleftarrow{\partial} F_1 \xleftarrow{\partial} F_2 \xleftarrow{\partial} F_3 \xleftarrow{\partial} \ldots$$

(0d) Dank linearer Unabhängigkeit finden wir so:

$$\ker(\partial^r) = \mathbb{K}[X]_{<r} = \left\langle\, F_k \;\middle|\; k < r \,\right\rangle_{\mathbb{K}}^{!}$$

Die Ableitung auf Polynomen und ihre Hauptfunktionen

N218

(1a) Charakteristik $\operatorname{char} \mathbb{K} = p > 0$ verhält sich anders!

$$\ker(\partial) = \langle\, X^0, X^p, X^{2p}, X^{3p}, \ldots \,\rangle_{\mathbb{K}}^{!}$$

(1b) Für die Polynome $F_{m,k} = X^{mp+k}/k!$ mit $k = 0, 1, \ldots, p-1$ gilt:

$$\begin{array}{ccccccccc}
0 & \xleftarrow{\partial} & F_{0,0} & \xleftarrow{\partial} & F_{0,1} & \xleftarrow{\partial} & \ldots & \xleftarrow{\partial} & F_{0,p-1} \\
0 & \xleftarrow{\partial} & F_{1,0} & \xleftarrow{\partial} & F_{1,1} & \xleftarrow{\partial} & \ldots & \xleftarrow{\partial} & F_{1,p-1} \\
\vdots & & & & & & & & \\
0 & \xleftarrow{\partial} & F_{m,0} & \xleftarrow{\partial} & F_{m,1} & \xleftarrow{\partial} & \ldots & \xleftarrow{\partial} & F_{m,p-1} \\
\vdots & & & & & & & &
\end{array}$$

(1c) Wir finden hier eine Basis aus mehreren Hauptvektorketten:

$$\ker(\partial^r) = \left\langle\, F_{m,k} \;\middle|\; m \in \mathbb{N},\ k < r \,\right\rangle_{\mathbb{K}}^{!}$$

Dies gilt für $r = 0, 1, \ldots, p$, wobei $\ker \partial^0 = \{0\}$ und $\ker \partial^p = \mathbb{K}[X]$.

⚠ Die Ableitung von Polynomen definieren wir über jedem Körper $\mathbb{K}$. In positiver Charakteristik verhält sie sich jedoch recht ungewohnt. Umso erfreulicher ist es, auch hier einfache Strukturen zu finden.

Lineare Differentialgleichung und Exponentialfunktion

N219

Zu lösen sei die folgende **Differentialgleichung mit Anfangswert**:

$$u'(t) = a\,u(t) \quad \text{mit} \quad u(0) = v$$

Diese Aufgabenstellung nennt man **Anfangswertproblem**, kurz AWP, oder auch **Cauchy–Problem**. Wir arbeiten über dem Körper $\mathbb{K} = \mathbb{R}, \mathbb{C}$.

Gegeben ist die Konstante $a \in \mathbb{K}$ und der Anfangswert $v \in \mathbb{K}$.

Gesucht sind alle differenzierbaren Funktionen $u : \mathbb{R} \to \mathbb{K} : t \mapsto u(t)$, die $u(0) = v$ und die Gleichung $u'(t) = a\,u(t)$ für alle $t \in \mathbb{R}$ erfüllen.

Aufgabe: (1) Existenz: Finden Sie eine Lösung $u : \mathbb{R} \to \mathbb{K} : t \mapsto u(t)$.
(2) Eindeutigkeit: Finden Sie alle Lösungen des Anfangswertproblems.

Lösung: (1) Die Funktion $u : \mathbb{R} \to \mathbb{K} : u(t) = \mathrm{e}^{ta} v$ ist eine Lösung.
(2) Sei $\tilde{u} : \mathbb{R} \to \mathbb{K}$ eine weitere Lösung. Wir betrachten $w(t) = \mathrm{e}^{-ta}\tilde{u}(t)$.
Dank Produktregel erhalten wir $w'(t) = -a\,\mathrm{e}^{-ta} \cdot \tilde{u}(t) + \mathrm{e}^{-ta} \cdot a\tilde{u}(t) = 0$.
Dank Mittelwertsatz ist $w : \mathbb{R} \to \mathbb{K}$ konstant v, also $\tilde{u}(t) = \mathrm{e}^{ta} v = u(t)$.
🙂 Es gibt genau eine Lösung $u : \mathbb{R} \to \mathbb{K}$, nämlich $u(t) = \mathrm{e}^{ta} v$.

Lineare Differentialgleichung und Exponentialfunktion

N220
Erläuterung

☹ Aus der vorigen Aufgabe wissen wir, dass Polynomfunktionen nicht zur Lösung der Differentialgleichung $u'(t) = a\,u(t)$ mit $a \neq 0$ taugen.

🙂 Die Exponentialfunktion erweitert unser Arsenal ganz wesentlich:

$$\exp : \mathbb{K} \to \mathbb{K} : x \mapsto \exp(x) = \textstyle\sum_{k=0}^{\infty} x^k/k!$$

Analysis: Diese Potenzreihe konvergiert absolut in jedem Punkt $x \in \mathbb{K}$. Wir dürfen termweise ableiten, wie Polynome, und erhalten $\exp' = \exp$. Dank Kettenregel ist die Ableitung von $t \mapsto \exp(ta)$ dann $t \mapsto a \exp(ta)$.

🙂 Neben der Existenz erhalten wir auch die Eindeutigkeit der Lösung. Damit ist dieses grundlegende Problem gelöst, darauf bauen wir auf.

Wir gehen genauso vor wie in der Rechnung zur diskreten Ableitung und bestimmen alle Haupträume durch eine explizite Konstruktion.

Lineare Algebra: Ausgestattet mit diesen grundlegenden Daten lösen wir routiniert jede Differentialgleichung höherer Ordnung (gemeint ist: homogen lineare Differentialgleichung mit konstanten Koeffizienten).

Der Ableitungsoperator und seine Hauptfunktionen

Auf $\mathscr{C}^\infty = \mathscr{C}^\infty(\mathbb{R},\mathbb{K})$ über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ haben wir den Ableitungsoperator

$$\partial : \mathscr{C}^\infty \to \mathscr{C}^\infty : f \mapsto f'.$$

Aufgabe: Bestimmen Sie alle Haupträume $V_r = \ker(\partial - \lambda)^r$ der Stufe $r = 1, 2, 3, \ldots$. Nennen Sie eine Basis aus Hauptvektorketten.

Lösung: (a) Sei $\lambda \in \mathbb{K}$. Stufe $r = 1$ ist der Eigenraum (N219):

$$\operatorname{Eig}(s,\lambda) = \big\langle\, f_0 \,\big\rangle^!_{\mathbb{K}} \quad \text{mit} \quad f_0 : \mathbb{R} \to \mathbb{K} : t \mapsto \mathrm{e}^{t\lambda}$$

(b) Aus $\dim_{\mathbb{K}} \ker(\partial - \lambda) = 1$ folgt $\dim_{\mathbb{K}} \ker(\partial - \lambda)^r \leq r$ dank N1J/N2A.

(c) Wir inspirieren uns an vorigen Beispielen und betrachten

$$f_k : \mathbb{R} \to \mathbb{K} : t \mapsto \tfrac{t^k}{k!}\,\mathrm{e}^{t\lambda}.$$

Dank Produktregel der Ableitung finden wir:

$$(\partial - \lambda) f_k(t) \;=\; \tfrac{t^{k-1}}{(k-1)!}\,\mathrm{e}^{t\lambda} + \lambda\,\tfrac{t^k}{k!}\,\mathrm{e}^{t\lambda} \;-\; \lambda\,\tfrac{t^k}{k!}\,\mathrm{e}^{t\lambda} \;=\; f_{k-1}(t)$$

(d) Wir erhalten also auch hier eine unendlich lange Hauptvektorkette:

$$0 \xleftarrow{\partial-\lambda} f_0 \xleftarrow{\partial-\lambda} f_1 \xleftarrow{\partial-\lambda} f_2 \xleftarrow{\partial-\lambda} f_3 \xleftarrow{\partial-\lambda} \ldots$$

Der Ableitungsoperator und seine Hauptfunktionen

Satz N2D: Hauptfunktionen des Ableitungsoperator

Auf $\mathscr{C}^\infty = \mathscr{C}^\infty(\mathbb{R},\mathbb{K})$ über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ haben wir den Ableitungsoperator

$$\partial : \mathscr{C}^\infty \to \mathscr{C}^\infty : f \mapsto f'.$$

(1) Zum Eigenwert λ sind die Haupträume der Stufe $r = 1, 2, 3, \ldots$ dann

$$\ker(\partial - \lambda)^r = \big\langle\, f_k \,\big|\, k < r \,\big\rangle^!_{\mathbb{K}} \quad \text{mit} \quad f_k(t) = \mathrm{e}^{t\lambda}\, t^k/k! \quad \text{und}$$
$$0 \xleftarrow{\partial-\lambda} f_0 \xleftarrow{\partial-\lambda} f_1 \xleftarrow{\partial-\lambda} f_2 \xleftarrow{\partial-\lambda} f_3 \xleftarrow{\partial-\lambda} f_4 \xleftarrow{\partial-\lambda} \ldots$$

(2) Vorgelegt sei ein normiertes Polynom

$$P = X^r + a_{r-1}X^{r-1} + \cdots + a_0 X^0 = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k}.$$

Dann hat $L = \ker P(\partial) \leq \mathscr{C}^\infty$ eine Basis aus Hauptvektorketten:

$$L = \ker(\partial - \lambda_1)^{r_1} \oplus \cdots \oplus \ker(\partial - \lambda_k)^{r_k}$$

Damit können wir jede lineare Differentialgleichung $P(\partial) f = 0$ lösen.

Der Ableitungsoperator und seine Hauptfunktionen

Satz N2D: Hauptfunktionen des Ableitungsoperator

(3) Die Auswertung zum Zeitpunkt $t = 0$ stiftet den $\mathbb{K}$–Isomorphismus

$$q : L \xrightarrow{\sim} \mathbb{K}^r : f \mapsto \big(\, f(0),\, f'(0),\, f''(0), \ldots, f^{(r-1)}(0) \,\big).$$

Damit können wir jedes Anfangswertproblem lösen, das heißt,
die eindeutige Lösung als einfache, geschlossene Formel darstellen.

(4) Für jede Hauptfunktion f_k zu λ gilt $f_k^{(n)}(0) = \binom{n}{k}\lambda^{n-k}$ für alle $n \in \mathbb{N}$.

Beweis: (1) Die Haupträume kennen wir aus der vorigen Aufgabe.

(2) Diese direkte Summe ist die Kernzerlegung M3V.

(3) Dank (4) und Satz N2C bildet $q : L \to \mathbb{K}^r$ eine Basis von L
auf eine Basis von $\mathbb{K}^r$ ab. Somit ist q ein Isomorphismus. QED

Aufgabe: Berechnen Sie $f_k^{(n)}(t)$ mit Auswertung $f_k^{(n)}(0) = \binom{n}{k}\lambda^{n-k}$
zunächst für kleine Beispiele und dann allgemein per Induktion.

Der Ableitungsoperator und seine Hauptfunktionen

Lösung: Wir wissen $\partial f_k = \lambda f_k + f_{k-1}$. Per Induktion zeigen wir:

$$\partial^n f_k = \sum_{i\in\mathbb{Z}} \binom{n}{i} \lambda^{n-i} f_{k-i} = \sum_{i=0}^{n} \binom{n}{i} \lambda^{n-i} f_{k-i}$$

Zu einfacheren Schreibweise setzen wir $f_k := 0$ für $k \in \mathbb{Z}_{<0}$.
Die Aussage gilt für $n = 0$. Induktionsschritt von $n-1$ auf n:

$$\partial^n f_k = \partial(\partial^{n-1} f_k) = \partial\Big[\sum_{i\in\mathbb{Z}} \binom{n-1}{i} \lambda^{n-1-i} f_{k-i} \Big]$$

$$= \sum_{i\in\mathbb{Z}} \binom{n-1}{i} \lambda^{n-i} f_{k-i} + \sum_{j\in\mathbb{Z}} \binom{n-1}{j} \lambda^{n-1-j} f_{k-j-1}$$

$$= \sum_{i\in\mathbb{Z}} \binom{n-1}{i} \lambda^{n-i} f_{k-i} + \sum_{i\in\mathbb{Z}} \binom{n-1}{i-1} \lambda^{n-i} f_{k-i} = \sum_{i\in\mathbb{Z}} \binom{n}{i} \lambda^{n-i} f_{k-i}$$

Wir nutzen die Indexverschiebung $i = j + 1$ bzw. $j = i - 1$. Schließlich
gilt $f_0(0) = 1$ und $f_k(0) = 0$ für alle $k \neq 0$, also $(\partial^n f_k)(0) = \binom{n}{k}\lambda^{n-k}$.

Konjugiert-komplexe Lösungen

⚠ Anwendungen erfordern oft **reelle Lösungen** $u : \mathbb{R} \to \mathbb{R}$.

Zu lösen sei über $\mathbb{R}$ die homogene lineare Differentialgleichung

$$P(\partial)\, u(t) = 0.$$

Hierzu sei $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{R}[X]$ ein **reelles Polynom**.

Ist $\lambda = \sigma + \mathrm{i}\omega$ mit $\sigma, \omega \in \mathbb{R}$ eine Nullstelle von P, dann auch $\overline{\lambda} = \sigma - \mathrm{i}\omega$.

Unsere DG hat dann die beiden **konjugiert-komplexen Lösungen**

$$z_1(t) = \mathrm{e}^{\lambda t} = \mathrm{e}^{\sigma t}\, \mathrm{e}^{+\mathrm{i}\omega t} = \mathrm{e}^{\sigma t}\big(\cos(\omega t) + \mathrm{i}\sin(\omega t)\big),$$
$$z_2(t) = \mathrm{e}^{\overline{\lambda} t} = \mathrm{e}^{\sigma t}\, \mathrm{e}^{-\mathrm{i}\omega t} = \mathrm{e}^{\sigma t}\big(\cos(\omega t) - \mathrm{i}\sin(\omega t)\big).$$

Basiswechsel: Hieraus kombinieren wir die beiden **reellen Lösungen**

$$u_1(t) = \mathrm{Re}\big[z_1(t)\big] = \tfrac{1}{2}\big[z_1(t) + z_2(t)\big] = \mathrm{e}^{\sigma t}\cos(\omega t),$$
$$u_2(t) = \mathrm{Im}\big[z_1(t)\big] = \tfrac{1}{2\mathrm{i}}\big[z_1(t) - z_2(t)\big] = \mathrm{e}^{\sigma t}\sin(\omega t).$$

Im Falle $\omega \neq 0$ sind diese beiden Lösungen linear unabhängig.

Anwendungsbeispiel: komplex vs reell

Aufgabe: Lösen Sie (a) allgemein und (b) das Anfangswertproblem

$$u''(t) + 2u'(t) + 5u(t) = 0 \quad \text{mit} \quad u(0) = 1,\ u'(0) = 3$$

Lösung: (a) Das charakteristische Polynom ist $P(X) = X^2 + 2X + 5$.
Die Nullstellen $\lambda_{1/2} = -1 \pm \sqrt{1-5} = -1 \pm 2\mathrm{i}$ sind komplex-konjugiert.

Komplexes Fundamentalsystem: $\mathrm{e}^{(-1+2\mathrm{i})t},\ \mathrm{e}^{(-1-2\mathrm{i})t}$
Komplexe Lösungen: $z(t) = c_1\, \mathrm{e}^{(-1+2\mathrm{i})t} + c_2\, \mathrm{e}^{(-1-2\mathrm{i})t}$ mit $c_1, c_2 \in \mathbb{C}$
Reelles Fundamentalsystem: $\mathrm{e}^{-t}\cos(2t),\ \mathrm{e}^{-t}\sin(2t)$
Reelle Lösungen: $u(t) = \alpha_1\, \mathrm{e}^{-t}\cos(2t) + \alpha_2\, \mathrm{e}^{-t}\sin(2t)$ mit $\alpha_1, \alpha_2 \in \mathbb{R}$

(b) Die Anfangsdaten bestimmen eindeutig die freien Konstanten:

$$\left.\begin{aligned} u(0) &= \alpha_1 &&= 1 \\ u'(0) &= -\alpha_1 + 2\alpha_2 &&= 3 \end{aligned}\right\} \quad \Rightarrow \quad \begin{cases} \alpha_1 = 1 \\ \alpha_2 = 2 \end{cases}$$

Probe! Die eindeutige Lösung des Anfangswertproblems ist demnach

$$u(t) = \mathrm{e}^{-t}\big(\cos(2t) + 2\sin(2t)\big).$$

☺ Über die komplexe Lösung kommt man zur selben Lösung des AWP.

Mehrfache konjugiert-komplexe Lösungen

Zu lösen sei über $\mathbb{R}$ die homogene lineare Differentialgleichung

$$P(\partial)\, u(t) = 0.$$

Hierzu sei $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{R}[X]$ ein **reelles Polynom**.

Ist $\lambda = \sigma + \mathrm{i}\omega$ mit $\sigma, \omega \in \mathbb{R}$ und $\omega \neq 0$ eine k–fache Nullstelle von P, dann auch die komplex-konjugierte Zahl $\overline{\lambda} = \sigma - \mathrm{i}\omega$.

Unsere DG hat dann die $2k$ **konjugiert-komplexen Lösungen**

$$\mathrm{e}^{\lambda t},\ \mathrm{e}^{\lambda t}\, t, \ldots,\ \mathrm{e}^{\lambda t}\, \tfrac{t^{k-1}}{(k-1)!},$$
$$\mathrm{e}^{\overline{\lambda} t},\ \mathrm{e}^{\overline{\lambda} t}\, t, \ldots,\ \mathrm{e}^{\overline{\lambda} t}\, \tfrac{t^{k-1}}{(k-1)!}.$$

Basiswechsel: Hieraus kombinieren wir die $2k$ **reellen Lösungen**

$$\mathrm{e}^{\sigma t}\cos(\omega t),\ \mathrm{e}^{\sigma t}\cos(\omega t)\, t, \ldots,\ \mathrm{e}^{\sigma t}\cos(\omega t)\, \tfrac{t^{k-1}}{(k-1)!},$$
$$\mathrm{e}^{\sigma t}\sin(\omega t),\ \mathrm{e}^{\sigma t}\sin(\omega t)\, t, \ldots,\ \mathrm{e}^{\sigma t}\sin(\omega t)\, \tfrac{t^{k-1}}{(k-1)!}.$$

Dank $\omega \neq 0$ sind diese $2k$ Lösungen linear unabhängig.

Anwendungsbeispiel: komplex vs reell

Aufgabe: Finden Sie ein reelles Fundamentalsystem der Gleichung

$$u^{(4)}(t) + 8u''(t) + 16u(t) = 0.$$

Lösung: Das char. Polynom unserer Gleichung $P(\partial)\, u = 0$ ist

$$P(X) = X^4 + 8X^2 + 16 = (X^2 + 4)^2 = (X - 2\mathrm{i})^2 (X + 2\mathrm{i})^2.$$

Doppelte Nullstellen $2\mathrm{i}$, $-2\mathrm{i}$. Ein komplexes Fundamentalsystem ist

$$\mathrm{e}^{2\mathrm{i}t}, \quad \mathrm{e}^{-2\mathrm{i}t}, \quad t\, \mathrm{e}^{2\mathrm{i}t}, \quad t\, \mathrm{e}^{-2\mathrm{i}t}.$$

Probe! Hieraus gewinnen wir das reelle Fundamentalsystem

$$\cos(2t), \quad \sin(2t), \quad t\cos(2t), \quad t\sin(2t).$$

Basiswechsel! Jede reelle Lösung hat demnach die Form

$$u(t) = \cos(2t)(\alpha_1 + \alpha_2 t) + \sin(2t)(\alpha_3 + \alpha_4 t)$$

mit eindeutig bestimmten Konstanten $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}$.

☺ Wie immer gilt: **Anfangswerte** $u(t_0), u'(t_0), u''(t_0), u'''(t_0) \in \mathbb{R}$ zu einem Startzeitpunkt t_0 können beliebig vorgegeben werden; sie legen die freien Konstanten $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}$ eindeutig fest.

Aufgabe: Wie lösen Sie mit Satz N2D lineare Differentialgleichungen?
Erklären Sie hierzu das Standardverfahren (ohne & mit Anfangswerten).

Inhomogene lineare Differentialgleichungen

N233

Wir betrachten eine **lineare Differentialgleichung** über $\mathbb{K} = \mathbb{R}, \mathbb{C}$:

$$u^{(n)}(t) + a_{n-1}\, u^{(n-1)}(t) + \cdots + a_1\, u'(t) + a_0\, u(t) = b(t)$$

Gegeben sind die **konstanten Koeffizienten** $a_0, a_1, \ldots, a_{n-1} \in \mathbb{K}$ und als **rechte Seite** die stetige Funktion $b : \mathbb{R} \supset I \to \mathbb{K}$ auf einem Intervall.

Mit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ bündeln wir dies zu

$$P(\partial)\, u(t) = b(t).$$

Gesucht sind als **Lösungen** alle Funktionen $u : I \to \mathbb{K}$ in $\mathscr{C}^n(I, \mathbb{K})$, die die Gleichung $P(\partial)\, u(t) = b(t)$ in jedem Punkt $t \in I$ erfüllen.

Beim **Anfangswertproblem** sind zudem die Anfangswerte in $t_0 \in I$ vorgegeben durch $u(t_0) = v_0$, $u'(t_0) = v_1$, …, $u^{(n-1)}(t_0) = v_{n-1} \in \mathbb{K}$.

Für $b = 0$ erhalten wir die **homogene Differentialgleichung**

$$P(\partial)\, u(t) = 0.$$

🙂 Letztere können wir bereits vollständig und explizit lösen (N2D).

Inhomogene lineare Differentialgleichungen

N234
Erläuterung

Übliche Bezeichnung in den Anwendungen und in der Mathematik:

Gleichung	Bezeichnung	Struktur
$P(\partial)\, u(t) = 0$	homogene lineare DG	linear
$P(\partial)\, u(t) = b(t)$	inhomogene lineare DG	affin-linear

Bezeichnung und Struktur entsprechen linearen Gleichungssystemen:

$Ax = 0$	homogenes LGS	linear
$Ax = b$	inhomogenes LGS	affin-linear

⚠ Der Funktionenraum $\mathscr{C}^n(I, \mathbb{K})$ ist unendlich-dimensional, wir können daher nicht direkt auf die Matrizenrechnung zurückgreifen! Schade.

🙂 Homogene Differentialgleichungen $P(\partial)\, u(t) = 0$ können wir bereits allgemein, vollständig und explizit lösen durch Hauptfunktionen (N2D).

Wie lösen wir inhomogene Differentialgleichungen $P(\partial)\, u(t) = b(t)$?

🙂 Satz N2G zeigt eine systematische Lösungsformel durch Integration. Für spezielle rechte Seiten gibt es einfache Lösungsformeln (N2E) bzw. Lösungsansätze (N2F), die meist leichter und schneller zum Ziel führen.

Lösungsformel für exponentielle rechte Seiten

N235

Satz N2E: Lösungsformel für exponentielle rechte Seiten

Sei $P \in \mathbb{K}[X]$ ein Polynom. Zu lösen sei die Differentialgleichung

$$P(\partial)\, u(t) = \mathrm{e}^{\mu t}.$$

(0) Gilt $P(\mu) \neq 0$, so haben wir die **kanonische Lösung**

$$u_0(t) = \mathrm{e}^{\mu t} / P(\mu).$$

(1) Ist μ eine k–fache Nullstelle des Polynoms P, so sprechen wir von **k–facher Resonanz** und erhalten die **modifizierte Lösung**

$$u_0(t) = \mathrm{e}^{\mu t}\, t^k / P^{(k)}(\mu).$$

(2) Dank **Superposition** lösen wir damit auch rechte Seiten der Form

$$\mathrm{e}^{\sigma t}\cos(\omega t) = \tfrac{1}{2}\left[\mathrm{e}^{(\sigma+\mathrm{i}\omega)t} + \mathrm{e}^{(\sigma-\mathrm{i}\omega)t}\right],$$
$$\mathrm{e}^{\sigma t}\sin(\omega t) = \tfrac{1}{2\mathrm{i}}\left[\mathrm{e}^{(\sigma+\mathrm{i}\omega)t} - \mathrm{e}^{(\sigma-\mathrm{i}\omega)t}\right].$$

Lösungsformel für exponentielle rechte Seiten

N236
Erläuterung

Aufgabe: Rechnen Sie die Lösungsformeln des Satzes sorgsam nach.

Lösung: (0) Wir haben $\partial^k \mathrm{e}^{\mu t} = \mu^k \mathrm{e}^{\mu t}$ und somit $P(\partial)\, \mathrm{e}^{\mu t} = P(\mu)\, \mathrm{e}^{\mu t}$.
Im Falle $P(\mu) \neq 0$ erhalten wir die kanonische Lösung $u_0(t) = \mathrm{e}^{\mu t}/P(\mu)$.

(1) Wir zerlegen $P(X) = \tilde{P}(X)(X-\mu)^k$ mit $\tilde{P}(\mu) \neq 0$ und erhalten

$$P(\partial)\left[\mathrm{e}^{\mu t}\, t^k\right] = \tilde{P}(\partial)(\partial-\mu)^k\left[\mathrm{e}^{\mu t}\, t^k\right] = \tilde{P}(\partial)\, \mathrm{e}^{\mu t}\, k! = \tilde{P}(\mu)\, \mathrm{e}^{\mu t}\, k!$$
$$P^{(k)}(t) = \textstyle\sum_{j=0}^{k} \binom{k}{j} \partial^j \tilde{P}(t) \cdot \partial^{k-j}(t-\mu)^k \quad \Longrightarrow \quad P^{(k)}(\mu) = \tilde{P}(\mu)\, k!$$

Wir erhalten so die modifizierte Lösung $u_0(t) = \mathrm{e}^{\mu t}\, t^k / P^{(k)}(\mu)$.

(2) Dank (0) und (1) finden wir Lösungen $u_\pm$ mit $P(\partial)\, u_\pm(t) = \mathrm{e}^{(\sigma\pm\mathrm{i}\omega)t}$.
Dank Linearität des Operators $P(\partial)$ erhalten wir

$$P(\partial)\, \tfrac{1}{2}\left[u_+(t) + u_-(t)\right] = \tfrac{1}{2}\left[\mathrm{e}^{(\sigma+\mathrm{i}\omega)t} + \mathrm{e}^{(\sigma-\mathrm{i}\omega)t}\right] = \mathrm{e}^{\sigma t}\cos(\omega t),$$
$$P(\partial)\, \tfrac{1}{2\mathrm{i}}\left[u_+(t) - u_-(t)\right] = \tfrac{1}{2\mathrm{i}}\left[\mathrm{e}^{(\sigma+\mathrm{i}\omega)t} - \mathrm{e}^{(\sigma-\mathrm{i}\omega)t}\right] = \mathrm{e}^{\sigma t}\sin(\omega t).$$

🙂 All diese rechten Seiten können wir somit leicht und explizit lösen!

Lösungsansatz für spezielle rechte Seiten

Satz N2F: Lösungsansatz für spezielle rechte Seiten

Seien $P, R \in \mathbb{K}[X]$ Polynome. Zu lösen sei die Differentialgleichung

$$\boxed{P(\partial)\, u(t) = \mathrm{e}^{\mu t}\, R(t).}$$

(1) Ist μ eine k–fache Nullstelle von P, so existiert eine Lösung

$$\boxed{u_0(t) = \mathrm{e}^{\mu t}\, t^k\, Q(t)}$$

mit einem eindeutigen Polynom $Q \in \mathbb{K}[X]$ vom Grad $\deg Q = \deg R$.
(2) Speziell $P(\partial)\, u(t) = \mathrm{e}^{\mu t}$ wird gelöst durch $u_0(t) = \mathrm{e}^{\mu t}\, t^k / P^{(k)}(\mu)$.

☺ Wir berechnen Q leicht durch Einsetzen und Koeffizientenvergleich.
Hier ist $k = 0$ erlaubt; bei $k > 0$ sprechen wir von k–facher **Resonanz**.

☺ Dieser Ansatz gelingt ebenso für rechte Seiten $\mathrm{e}^{0t}\, R(t) = R(t)$ sowie

$$\mathrm{e}^{\sigma t} \cos(\omega t)\, R(t) = \tfrac{1}{2}\left[\mathrm{e}^{(\sigma+\mathrm{i}\omega)t} + \mathrm{e}^{(\sigma-\mathrm{i}\omega)t}\right] R(t),$$
$$\mathrm{e}^{\sigma t} \sin(\omega t)\, R(t) = \tfrac{1}{2\mathrm{i}}\left[\mathrm{e}^{(\sigma+\mathrm{i}\omega)t} - \mathrm{e}^{(\sigma-\mathrm{i}\omega)t}\right] R(t).$$

Lösungsansatz für spezielle rechte Seiten

Vorbereitung: Wir wollen Differentialoperatoren geschickt nutzen.
Dank Leibniz–Regel für Produkte $\partial(f \cdot g) = (\partial f) \cdot g + f \cdot (\partial g)$ gilt:

$$\partial \left[\mathrm{e}^{\mu t}\, g(t)\right] = \mathrm{e}^{\mu t} \left[(\partial + \mu)\, g(t)\right]$$
$$\partial^k \left[\mathrm{e}^{\mu t}\, g(t)\right] = \mathrm{e}^{\mu t} \left[(\partial + \mu)^k\, g(t)\right]$$

Für jedes Polynom $P \in \mathbb{K}[X]$ und jede Konstante $\mu \in \mathbb{K}$ gilt somit:

$$\boxed{P(\partial) \left[\mathrm{e}^{\mu t}\, g(t)\right] = \mathrm{e}^{\mu t} \left[P(\partial + \mu)\, g(t)\right]}$$

Als typisches Beispiel haben wir insbesondere:

$$(\partial - \lambda)^k \left[\mathrm{e}^{\mu t}\, g(t)\right] = \mathrm{e}^{\mu t} \left[(\partial - \lambda + \mu)^k\, g(t)\right]$$

Diese hilfreiche **Verschiebungsregel** vereinfacht unsere Rechnungen:

$$\boxed{P(\partial)\ \mathrm{e}^{\mu t} = \mathrm{e}^{\mu t}\, P(\partial + \mu)}$$

Lösungsansatz für spezielle rechte Seiten

Beweis des Satzes: Der Satz erklärt ein Lösungsrezept: „Wenn das Problem soundso gegeben ist, dann sieht die Lösung soundso aus.“

Wir zeigen, dass der genannte Ansatz tatsächlich immer gelingt.
Hierzu betrachten wir die Menge aller Polynome in t vom Grad $< n$:

$$\mathbb{K}[t]_{<n} = \left\{ a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} \;\middle|\; a_0, a_1, \ldots, a_{n-1} \in \mathbb{K} \right\}.$$

Dies ist ein $\mathbb{K}$–Vektorraum der Dimension n. Die k–fache Ableitung $\partial^k : \mathbb{K}[t]_{<n} \to \mathbb{K}[t]_{<n-k}$ ist surjektiv. Ihr Kern ist der Unterraum $\mathbb{K}[t]_{<k}$.

Für $\lambda \neq 0$ hingegen ist $(\partial - \lambda) : \mathbb{K}[t]_{<n} \xrightarrow{\sim} \mathbb{K}[t]_{<n}$ ein Isomorphismus: Dieser Operator erhält den Grad, hat trivialen Kern, ist somit injektiv, dank endlicher Dimension auch surjektiv. Alternative und konkretere Sichtweise: Bezüglich der Monombasis $t^0, t^1, \ldots, t^{n-1}$ schreibt sich $\partial - \lambda$ als obere Dreiecksmatrix mit Determinante $(-\lambda)^n \neq 0$.

Nach Voraussetzung gilt $P(X) = \tilde{P}(X)\,(X - \mu)^k$ mit $\tilde{P}(\mu) \neq 0$, also

$$P(\partial) \left[\mathrm{e}^{\mu t}\, t^k\, Q(t)\right] = \mathrm{e}^{\mu t}\, P(\partial + \mu) \left[t^k\, Q(t)\right] = \mathrm{e}^{\mu t}\, \tilde{P}(\partial + \mu)\, \partial^k \left[t^k\, Q(t)\right].$$

Zunächst senkt ∂^k den Grad um k, sodann erhält $\tilde{p}(\partial + \mu)$ den Grad.

Lösungsansatz für spezielle rechte Seiten

Zusammenfassend erhalten wir also Vektorraumisomorphismen

$$\partial^k : \quad t^k\, \mathbb{K}[t]_{<n} \quad \xrightarrow{\sim} \quad \mathbb{K}[t]_{<n},$$
$$P(\partial) : \mathrm{e}^{\mu t}\, t^k\, \mathbb{K}[t]_{<n} \quad \xrightarrow{\sim} \quad \mathrm{e}^{\mu t}\, \mathbb{K}[t]_{<n}.$$

Für unsere Differentialgleichung bedeutet das ausführlich folgendes:
Zu jedem Polynom $R(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1} \in \mathbb{K}[x]_{<n}$ existiert genau ein Polynom $Q(x) = q_0 + q_1 x + \ldots q_{n-1} x^{n-1} \in \mathbb{K}[x]_{<n}$,
das unsere Differentialgleichung $P(\partial) \left[\mathrm{e}^{\mu x}\, x^k\, Q(x)\right] = \mathrm{e}^{\mu x}\, R(x)$ löst.

☺ Die praktische Berechnung gelingt durch Koeffizientenvergleich:
Die lineare Abbildung $Q \mapsto R$ können wir leicht ausrechnen, für ihre Umkehrung $R \mapsto Q$ nutzen wir die Methoden der Linearen Algebra.

Dies gelingt besonders leicht im wichtigen Spezialfall $P(\partial)\, u(t) = \mathrm{e}^{\mu t}$:

$$P(\partial) \left[\mathrm{e}^{\mu t}\, t^k\right] = \tilde{P}(\partial)(\partial - \mu)^k \left[\mathrm{e}^{\mu t}\, t^k\right] = \tilde{P}(\partial)\ \mathrm{e}^{\mu t}\, k! = \tilde{P}(\mu)\ \mathrm{e}^{\mu t}\, k!$$
$$P^{(k)}(t) = \textstyle\sum_{j=0}^{k} \binom{k}{j} \partial^j \tilde{P}(t) \cdot \partial^{k-j} (t - \mu)^k \quad \Longrightarrow \quad P^{(k)}(\mu) = \tilde{P}(\mu)\, k!$$

☺ Somit wird $P(\partial)\, u(t) = \mathrm{e}^{\mu t}$ gelöst durch $u_0(t) = \mathrm{e}^{\mu t}\, t^k / P^{(k)}(\mu)$. QED

Greensche Lösungsformel für beliebige rechte Seiten

N241

Satz N2G: Greensche Fundamentallösung und Lösungsformel

Sei $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$ ein Polynom und $b : \mathbb{R} \supset I \to \mathbb{K}$ stetig. Zu lösen ist die Differentialgleichung

$$P(\partial)\, x(t) = b(t).$$

Die homogene Gleichung $P(\partial)\, u = 0$ hat genau eine Lösung $u : \mathbb{R} \to \mathbb{K}$ mit den Anfangswerten $u(0) = \cdots = u^{(n-2)}(0) = 0$ und $u^{(n-1)}(0) = 1$.

Wir nennen u die **Greensche Fundamentallösung**. Hieraus erhalten wir eine Lösung der inhomogenen Gleichung $P(\partial)\, x = b$ durch **Faltung**:

$$x(t) = \int_{\tau=t_0}^{t} u(t-\tau)\, b(\tau)\, \mathrm{d}\tau.$$

Genauer ist $x : I \to \mathbb{K}$ die eindeutige Lösung der Gleichung $P(\partial)\, x = b$ mit verschwindenden Anfangswerten $x(t_0) = \cdots = x^{(n-1)}(t_0) = 0$.

🙂 Weitere erhalten wir durch Addition homogener Lösungen (N2H).

Greensche Lösungsformel für beliebige rechte Seiten

N242 Erläuterung

Aufgabe: Zu lösen sei, für $-\pi/2 < t < \pi/2$, die Differentialgleichung

$$\ddot{x}(t) + x(t) = \frac{1}{\cos t} \quad \text{mit} \quad x(0) = \dot{x}(0) = 0.$$

Lösung: Die allgemeine homogene Lösung ist $u(t) = c_1 \cos t + c_2 \sin t$, Fundamentallösung mit $u(0) = 0$ und $\dot{u}(0) = 1$ ist $u(t) = \sin t$. Wir falten:

$$\begin{aligned} x(t) &= \int_{\tau=0}^{t} \sin(t-\tau)\frac{1}{\cos\tau}\,\mathrm{d}\tau = \int_{\tau=0}^{t} \big(\sin t\cos\tau - \cos t\sin\tau\big)\frac{1}{\cos\tau}\,\mathrm{d}\tau \\ &= \int_{\tau=0}^{t} \sin t - \cos t\cdot\frac{\sin\tau}{\cos\tau}\,\mathrm{d}\tau = \Big[\tau\sin t + \cos t\cdot\ln\cos\tau\Big]_{\tau=0}^{t} \\ &= t\sin t + \cos t\cdot\ln\cos t \end{aligned}$$

🙂 Die Probe ist wie immer leicht und lohnend! Geduldig ausrechnen:

$$\begin{aligned} \dot{x}(t) &= \sin t + t\cos t - \sin t\cdot\ln\cos t - \sin t \\ \ddot{x}(t) &= \cos t - t\sin t - \cos t\cdot\ln\cos t + \sin(t)^2/\cos t \end{aligned}$$

Einsetzen: $\ddot{x}(t) + x(t) = \cos t + \sin(t)^2/\cos t = 1/\cos t$. Alles passt!

Greensche Lösungsformel für beliebige rechte Seiten

N243 Erläuterung

Aufgabe: Beweisen Sie Greens Lösungsformel durch Nachrechnen.

Lösung: (a) Für die Ableitung nutzen wir die Leibniz–Regel:

$$\frac{\mathrm{d}}{\mathrm{d}t}\int_{\tau=t_0}^{h(t)} f(t,\tau)\,\mathrm{d}\tau = h'(t)\, f\big(t,h(t)\big) + \int_{\tau=t_0}^{h(t)} \frac{\partial f}{\partial t}(t,\tau)\,\mathrm{d}\tau$$

Angewendet auf $h(t) = t$ und $f(t,\tau) = u(t-\tau)\, b(\tau)$ erhalten wir

$$\begin{aligned} x'(t) &= \underbrace{u(0)}_{=0}\, b(t) + \int_{\tau=t_0}^{t} u'(t-\tau)\, b(\tau)\,\mathrm{d}\tau, \\ x''(t) &= \underbrace{u'(0)}_{=0}\, b(t) + \int_{\tau=t_0}^{t} u''(t-\tau)\, b(\tau)\,\mathrm{d}\tau, \\ &\vdots \\ x^{(n-1)}(t) &= \underbrace{u^{(n-2)}(0)}_{=0}\, b(t) + \int_{\tau=t_0}^{t} u^{(n-1)}(t-\tau)\, b(\tau)\,\mathrm{d}\tau, \\ x^{(n)}(t) &= \underbrace{u^{(n-1)}(0)}_{=1}\, b(t) + \int_{\tau=t_0}^{t} u^{(n)}(t-\tau)\, b(\tau)\,\mathrm{d}\tau. \end{aligned}$$

Greensche Lösungsformel für beliebige rechte Seiten

N244 Erläuterung

Einsetzen dieser Ableitungen in unsere Differentialgleichung ergibt:

$$\begin{aligned} &x^{(n)}(t) + a_{n-1}\, x^{(n-1)}(t) + \cdots + a_1\, x'(t) + a_0\, x(t) \\ &= b(t) + \int_{\tau=t_0}^{t} \underbrace{\big[u^{(n)} + a_{n-1}\, u^{(n-1)} + \cdots + a_1\, u' + a_0\, u\big]}_{=0,\ \text{da } u \text{ eine Lösung der homogenen DG ist}}(t-\tau)\, b(\tau)\,\mathrm{d}\tau \end{aligned}$$

Somit ist x eine Lösung der inhomogenen Gleichung $P(\partial)\, x = b$.

(b) Die Anfangswerte $x(t_0) = x'(t_0) = \cdots = x^{(n-2)}(t_0) = x^{(n-1)}(t_0) = 0$ folgen sofort aus der Berechnung der Ableitungen (a) im Punkt $t = t_0$.

Anschauliche Erklärung wie sie in der Physik beliebt ist: Für alle $t < 0$ sei das System in Ruhelage $u(t) = 0$. Zum Zeitpunkt $t = 0$ gilt $u(0) = u'(0) = \cdots = u^{(n-2)}(0) = 0$, und es wird abrupt beschleunigt durch $u^{(n-1)}(0) = 1$. Man stellt sich dies als „Hammerschlag“ vor. Das System vollführt als sogenannte **Impulsantwort** die Bewegung $u(t)$ für alle Zeit $t \geq 0$.

Entsprechend verschoben ist $u(t-\tau)\, b(\tau)$ ein Hammerschlag zum Zeitpunkt τ mit Stärke $b(\tau)$. Das Integral über τ ist die Summe dieser Beiträge: Wir nutzen **Superposition** dank Linearität und erhalten so $x(t) = \int_{\tau=t_0}^{t} u(t-\tau)\, b(\tau)\,\mathrm{d}\tau$ als Summe kleiner Hammerschläge $b(\tau)\,\mathrm{d}\tau$. Diese Intuition liefert tatsächlich eine korrekte Lösung: Wir haben es nachgerechnet!

Affin-lineare Struktur des Lösungsraumes

Satz N2H: Struktursatz für lineare Differentialgleichungen

Gegeben seien $P \in \mathbb{K}[X]^1_n$ und $b : I \to \mathbb{K}$ stetig auf dem Intervall $I \subseteq \mathbb{R}$. Wir untersuchen die Lösungsmenge $L = \{\, u \in \mathscr{C}^n(I,\mathbb{K}) \mid P(\partial)\, u = b \,\}$.

(0) **Globale Existenz und Eindeutigkeit**: Zu jedem Anfangsdatum $(t_0, v_0, \ldots, v_{n-1}) \in I \times \mathbb{K}^n$ existiert genau eine Lösung $u \in L$ mit $u(t_0) = v_0, \ldots, u^{(n-1)}(t_0) = v_{n-1}$. Wir haben also eine Bijektion:

$$\Psi_{t_0} : L \xrightarrow{\sim} \mathbb{K}^n : u \mapsto \big(u(t_0), u'(t_0), \ldots, u^{(n-1)}(t_0)\big)$$

(1) $L_0 = \{\, u \mid P(\partial)\, u = 0 \,\}$ ist ein **Vektorraum** der Dimension n über $\mathbb{K}$. Wir finden ein **Fundamentalsystem** $u_1, \ldots, u_n \in L_0$, also eine Basis:

$$L_0 = \big\{\, c_1 u_1 + \cdots + c_n u_n \;\big|\; c_1, \ldots, c_n \in \mathbb{K} \,\big\} \;\cong\; \mathbb{K}^n$$

(2) $L = \{\, u \mid P(\partial)\, u = b \,\}$ ist ein **affiner Raum** der Dimension n über $\mathbb{K}$. Für jede **Partikulärlösung** $u_0 \in L$ gilt $L = u_0 + L_0$, ausgeschrieben:

$$L = u_0 + L_0 = \big\{\, u_0 + c_1 u_1 + \cdots + c_n u_n \;\big|\; c_1, \ldots, c_n \in \mathbb{K} \,\big\}$$

Affin-lineare Struktur des Lösungsraumes

☺ „Allgemeine Lösungen = partikuläre Lösung + homogene Lösungen“ Sie kennen diese Strukturaussagen von linearen Gleichungssystemen! Diese gilt allgemein für lineare Abbildungen, also auch $P(\partial) : \mathscr{C}^n \to \mathscr{C}^0$.

⚠ Die Menge $\mathscr{C}^n(I,\mathbb{K})$ aller n–mal stetig diff'baren Funktionen ist ein $\mathbb{K}$–Vektorraum. Allerdings ist er unendlich-dimensional; daher greifen die so erfolgreichen Methoden der Matrizenrechnung wie etwa der Gauß–Algorithmus hier nicht. Wir müssen genauer hinsehen!

☺ Glücklicherweise ist unser Lösungsraum L endlich-dimensional, und wir können allgemein die Dimension $\dim_{\mathbb{K}}(L_0) = n$ bestimmen. Bei jeder konkreten Berechnung wissen wir daher genau, wie viele Lösungen wir suchen müssen und wann wir alle gefunden haben!

⚠ Die Dimension $\dim_{\mathbb{K}}(L_0) = n$ besagt $L_0 \cong \mathbb{K}^n$. Darüber hinaus sind die konkreten Isomorphismen interessant, insbesondere $\Psi_{t_0} : L_0 \xrightarrow{\sim} \mathbb{K}^n$.

☺ Zu Verständnis und Lösung von Differentialgleichungen arbeiten Analysis und Lineare Algebra wunderbar zusammen. Hier wie überall lohnt sich Ihre Investition in solide mathematische Grundlagen.

Affin-lineare Struktur des Lösungsraums

☺ In der Analysis lernen Sie diesen Satz von anderer Seite kennen, meist über den Existenz- und Eindeutigkeitssatz von Picard–Lindelöf.

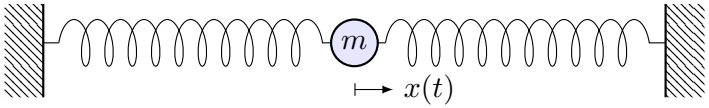
☺ Wir kommen hier (beinahe) ausschließlich mit Linearer Algebra aus, benötigen lediglich die Exponentialfunktion (N2D) und die Greensche Lösungsformel (N2G). Auch das ist raffiniert, prüfen Sie die Argumente!

Aufgabe: Wiederholen Sie gewissenhaft die bisher bewiesenen Sätze zu Differentialgleichungen und zeigen Sie damit den Struktursatz N2H.

Affin-lineare Struktur des Lösungsraums

Beispiel: mechanische Schwingung

Schwingung einer Masse an einer Feder:



Zeit $t \in \mathbb{R}$, Auslenkung $x(t)$ aus Ruhelage, Rückstellkraft $F_1 = -k\,x$, zusätzlich noch Reibung / viskoser Strömungswiderstand $F_2 = -c\,\dot{x}$.
Newtons Bewegungsgesetz $m\,\ddot{x} = F_1 + F_2$, also $m\,\ddot{x} + c\,\dot{x} + k\,x = 0$.
Dies führt zu einer **linearen Differentialgleichung zweiter Ordnung**

$$\ddot{x}(t) + 2\delta\,\dot{x}(t) + \omega_0^2\,x(t) = 0$$

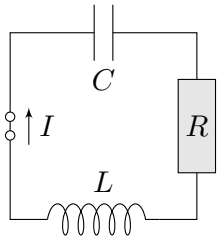
mit konstanten Koeffizienten $\delta = c/2m \geq 0$ und $\omega_0^2 = k/m$, $\omega_0 \geq 0$.
Bei äußerer Anregung durch eine Kraft $F(t) = m\,f(t)$ gilt:

$$\ddot{x}(t) + 2\delta\,\dot{x}(t) + \omega_0^2\,x(t) = f(t)$$

Allgemein suchen wir alle möglichen Lösungen $x : \mathbb{R} \to \mathbb{R} : t \mapsto x(t)$, speziell die Lösung x zu vorgegebenen Anfangswerten $x(t_0)$ und $\dot{x}(t_0)$.

Beispiel: elektrischer Schwingkreis

Diese Differentialgleichung begegnet uns in sehr vielen Situationen.
Sie ist daher grundlegend wichtig in Naturwissenschaft und Technik.



Elektrischer Schwingkreis (RLC), Radioempfänger:
Beziehungen zwischen Strom I und Spannung U:

- Ohmscher Widerstand: $U_R = R\,I$,
- Selbstinduktivität der Spule: $U_L = L\,\dot{I}$,
- Kapazität des Kondensators: $I = C\,\dot{U}_C$.

In der Reihenschaltung summieren sich diese Spannungen zu Null:
$U_L + U_R + U_C = 0$. Wir erhalten $L\,\ddot{I}(t) + R\,\dot{I}(t) + \frac{1}{C} I(t) = 0$, also

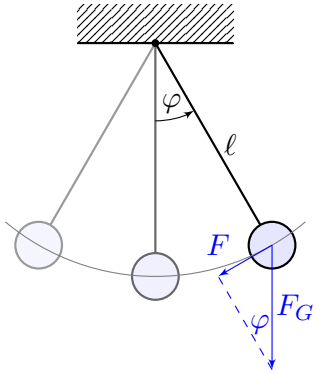
$$\ddot{x}(t) + 2\delta\,\dot{x}(t) + \omega_0^2\,x(t) = 0$$

mit $x(t) = I(t)$ sowie $\delta = \frac{R}{2L}$ und $\omega_0^2 = \frac{1}{LC}$. Bei äußerer Anregung gilt:

$$\ddot{x}(t) + 2\delta\,\dot{x}(t) + \omega_0^2\,x(t) = f(t)$$

Wir suchen Lösungen $x(t)$, speziell zu Anfangswerten $x(0)$ und $\dot{x}(0)$.

Beispiel: das mathematische Pendel



Die Rückstellkraft ist hier nicht-linear:

$$F(t) = -m \cdot g \cdot \sin\varphi(t)$$

m = Masse des Pendelkörpers
$g = 9.81\mathrm{m/s}^2$ Erdbeschleunigung
$F_G = mg$ Gravitationskraft zur Masse m
ℓ = Länge des Pendelstabes
$\varphi(t)$ = Winkelauslenkung
$\ell\,\varphi(t)$ = Auslenkung

Newtons Bewegungsgesetz $F(t) = m\,\ell\,\ddot{\varphi}(t)$ führt zu

$$\ddot{\varphi}(t) = -\frac{g}{\ell}\,\sin\varphi(t).$$

Anders als vorige ist dies eine **nicht-lineare Differentialgleichung**.
Gegeben sind die anfängliche Position $\varphi(0)$ und Geschwindigkeit $\dot{\varphi}(0)$.
Fragen: Wie sieht die Trajektorie aus? Wie lang dauert eine Periode?

Beispiel: Pendel bei kleinen Amplituden

⚠ Wir vereinfachen etwas: punktförmige Masse des Pendelkörpers, vernachlässigbare Masse des Stabes, reibungsfreie Aufhängung, etc.
Für kleine Auslenkungen gilt $\sin(\varphi) \approx \varphi$. (Faustregel für $|\varphi| < 5°$)
Dies führt uns zur **linearisierten Differentialgleichung**:

$$\ddot{\varphi}(t) = -\frac{g}{\ell}\,\varphi(t)$$

Diese Differentialgleichung ist viel einfacher, denn sie ist linear in φ:

$$\ddot{\varphi}(t) = -\omega^2\varphi(t) \quad \text{mit} \quad \omega = \sqrt{\frac{g}{\ell}}$$

Dies ist die Bewegungsgleichung eines **harmonischen Oszillators**:

$$\varphi(t) = \varphi_0\cos(\omega t + \alpha), \quad \ddot{\varphi}(t) = -\varphi_0\,\omega^2\cos(\omega t + \alpha).$$

Für kleine Auslenkungen ist demnach die Periodendauer $T = 2\pi\sqrt{\ell/g}$.
Die Anfangsdaten bestimmen die Auslenkung φ_0 und die Phase α.
⚠ Für große Auslenkungen brauchen wir eine genauere Rechnung!
Die Lösung ist schwieriger und wird im nächsten Abschnitt diskutiert.

Freie harmonische Schwingung

Aufgabe: Finden Sie alle Lösungen $u : \mathbb{R} \to \mathbb{R}$ der Differentialgleichung

$$\ddot{u}(t) + 2\delta\,\dot{u}(t) + \omega_0^2\,u(t) = 0.$$

Wir nennen dies die Gleichung des **harmonischen Oszillators** mit **Dämpfung** $\delta \geq 0$ und **ungedämpfter Eigenfrequenz** $\omega_0 > 0$.

Dies ist eine lineare DG zweiter Ordnung mit konstanten Koeffizienten. In diesem einfachen aber sehr wichtigen Spezialfall zeigen sich bereits alle Techniken dieses Kapitels, wenn auch erst in embryonaler Form.

Lösung: Der Exponentialansatz $u(t) = \mathrm{e}^{\lambda t}$ führt zur char. Gleichung

$$\underbrace{\left(\lambda^2 + 2\delta\lambda + \omega_0^2\right)}_{\text{charakteristisches Polynom}} \mathrm{e}^{\lambda t} = 0 \qquad \Longleftrightarrow \qquad \lambda = \underbrace{-\delta \pm \sqrt{\delta^2 - \omega_0^2}}_{\text{Eigenwerte des Systems}} \in \mathbb{C}.$$

Je nach Diskriminante beobachten wir verschiedene Reaktionen:
$\delta < \omega_0$: **schwache Dämpfung**, zwei komplex-konjugierte Nullstellen
$\delta > \omega_0$: **starke Dämpfung**, zwei reelle Nullstellen $\lambda_1 < -\delta < \lambda_2 < 0$
$\delta = \omega_0$: **kritische Dämpfung**, doppelte reelle Nullstelle $\lambda_1 = \lambda_2 = -\delta$

Freie harmonische Schwingung

Physikalische Anwendungen fordern meist **reelle Lösungen** $u : \mathbb{R} \to \mathbb{R}$. Oft vereinfachen sich Rechnungen und Formulierungen von Sätzen, wenn wir allgemeiner auch **komplexe Lösungen** $u : \mathbb{R} \to \mathbb{C}$ zulassen und anschließend in reelle Lösungen umrechnen.

Die Bewegung $u(t)$ wird durch die Startwerte $u(0)$ und $\dot{u}(0)$ festgelegt. Die Anfangswerte sind beliebig, wir haben daher **zwei Freiheitsgrade**.

Als Lösungsraum erwarten wir einen **Vektorraum der Dimension** 2: Diese mathematische Aussage haben wir oben im Struktursatz N2H zusammengefasst und zuvor explizit und konstruktiv hergeleitet.

Das **charakteristische Polynom** der DG ist $P(X) = X^2 + 2\delta X + \omega_0^2$. Die Lösungsformel beschert uns die **Eigenwerte** $\lambda_{1/2} = -\delta \pm \sqrt{\delta^2 - \omega_0^2}$ und so **linear unabhängige Lösungen** $u_1(t) = \mathrm{e}^{\lambda_1 t}$ und $u_2(t) = \mathrm{e}^{\lambda_2 t}$. Hierbei unterscheiden wir den komplexen Fall $\delta < \omega_0$ und den reellen Fall $\delta > \omega_0$; anschließend lösen wir auch den kritischen Fall $\delta = \omega$.

Wir diskutieren zunächst die homogenen Gleichung: rechte Seite $f = 0$, anschließend eine harmonische Anregung der Form $f(t) = \cos(\omega t)$.

Schwache Dämpfung: $\delta < \omega_0$

Im Fall $0 \leq \delta < \omega_0$ gibt es **zwei komplex-konjugierte Nullstellen**

$$\lambda_{1/2} = -\delta \pm \mathrm{i}\,\omega \quad \text{mit} \quad \omega = \sqrt{\omega_0^2 - \delta^2}, \quad 0 < \omega \leq \omega_0.$$

Die komplexen Lösungen $u : \mathbb{R} \to \mathbb{C}$ der Differentialgleichung sind

$$u(t) = c_1\,\mathrm{e}^{\lambda_1 t} + c_2\,\mathrm{e}^{\lambda_2 t} \quad \text{mit} \quad c_1, c_2 \in \mathbb{C}.$$

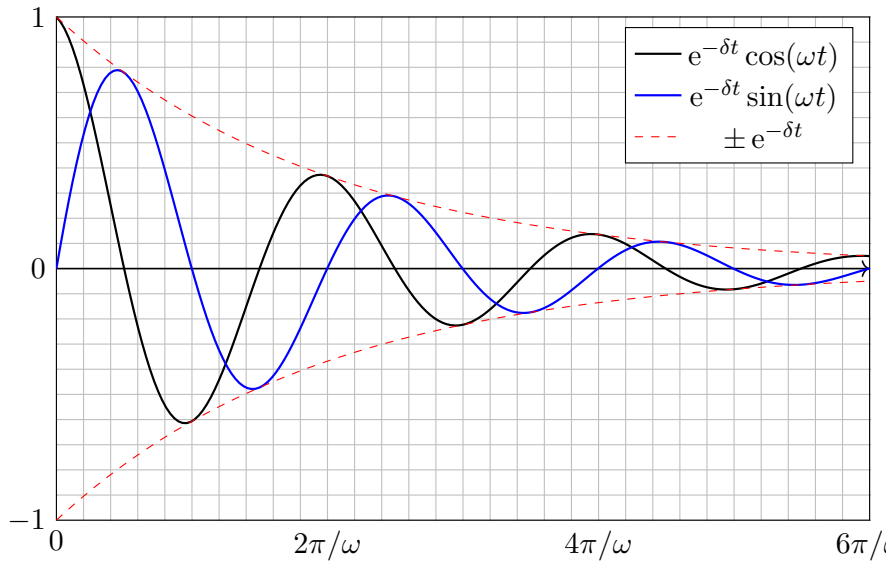
☺ Diese Lösungen bilden einen zweidimensionalen $\mathbb{C}$–Vektorraum.
☺ Über den komplexen Zahlen ist die Rechnung leicht. Physikalische Anwendungen fordern meist die Umrechnung in reelle Lösungen:
Die reellen Lösungen $u : \mathbb{R} \to \mathbb{R}$ der Differentialgleichung sind

$$u(t) = \mathrm{e}^{-\delta t}\left[\alpha_1 \cos(\omega t) + \alpha_2 \sin(\omega t)\right] \quad \text{mit} \quad \alpha_1, \alpha_2 \in \mathbb{R}.$$

☺ Diese Lösungen bilden einen zweidimensionalen $\mathbb{R}$–Vektorraum.
☺ Sie entsprechen Real- und Imaginärteil der komplexen Lösungen.
Für $\delta = 0$ haben wir eine **ungedämpfte Schwingung** mit $\omega = \omega_0$.

Schwache Dämpfung: $\delta < \omega_0$

Die Masse wird durch die Federkraft zur Ruhelage zurückgezogen, aufgrund ihrer Trägheit schwingt die Masse jedoch darüber hinaus.



Starke Dämpfung: $\delta > \omega_0$

Im Fall $\delta > \omega_0$ gibt es **zwei reelle Nullstellen** $\lambda_1 < \lambda_2 < 0$, nämlich

$$\lambda_1 = -\delta - \sqrt{\delta^2 - \omega_0^2} \;<\; -\delta \;<\; \lambda_2 = -\delta + \sqrt{\delta^2 - \omega_0^2} \;<\; 0.$$

Hierzu gehören die Lösungen $\mathrm{e}^{\lambda_1 t}$ und $\mathrm{e}^{\lambda_2 t}$ als Eigenfunktionen.
Die allgemeine Lösung erhalten wir durch Linearkombination:

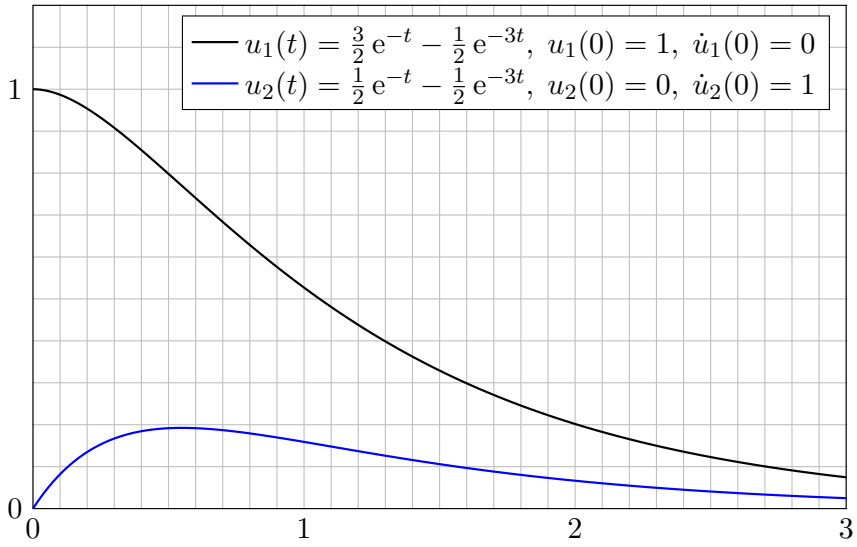
$$u(t) = c_1\,\mathrm{e}^{\lambda_1 t} + c_2\,\mathrm{e}^{\lambda_2 t}$$

☺ Diese Lösungen bilden einen zweidimensionalen $\mathbb{K}$–Vektorraum:
Für reelle Lösungen $u : \mathbb{R} \to \mathbb{R}$ dürfen wir die Konstanten $c_1, c_2 \in \mathbb{R}$ frei wählen, für komplexe Lösungen $u : \mathbb{R} \to \mathbb{C}$ entsprechend $c_1, c_2 \in \mathbb{C}$.

Zahlenbeispiel: Die Differentialgleichung $\ddot{u}(t) + 4\,\dot{u}(t) + 3\,u(t) = 0$ führt zur Gleichung $\lambda^2 + 4\lambda + 3 = 0$, also $\lambda_1 = -3$ und $\lambda_2 = -1$.
Linearfaktorzerlegung $(\partial_t + 3)(\partial_t + 1)\,u(t) = 0$, Lösungen e^{-3t}, e^{-t}.
Die DG hat als reelle Lösungen $u(t) = c_1\,\mathrm{e}^{-3t} + c_2\,\mathrm{e}^{-t}$ mit $c_1, c_2 \in \mathbb{R}$.
Anfangswerte $u(0) = 1$ und $\dot{u}(0) = 0$ führen zu $u(t) = \frac{3}{2}\,\mathrm{e}^{-t} - \frac{1}{2}\,\mathrm{e}^{-3t}$.
Anfangswerte $u(0) = 0$ und $\dot{u}(0) = 1$ führen zu $u(t) = \frac{1}{2}\,\mathrm{e}^{-t} - \frac{1}{2}\,\mathrm{e}^{-3t}$.

Starke Dämpfung: $\delta > \omega_0$

Dies nennt man auch den **Kriechfall:** Es gibt keine Schwingung, das System kriecht nach einer Auslenkung zur Ruhelage zurück.



Kritische Dämpfung: $\delta = \omega_0$

Im Fall $\delta = \omega_0$ gibt es eine **doppelte reelle Nullstelle** $\lambda = -\delta$.
Wir finden die Lösung $\mathrm{e}^{\lambda t}$ und zusätzlich $t\,\mathrm{e}^{\lambda t}$ als Hauptfunktionen.
Die allgemeine Lösung der Differentialgleichung ist in diesem Fall:

$$u(t) = \mathrm{e}^{\lambda t}(c_1 + c_2 t)$$

☺ Diese Lösungen bilden einen zweidimensionalen Vektorraum:
Für reelle Lösungen $u : \mathbb{R} \to \mathbb{R}$ dürfen wir die Konstanten $c_1, c_2 \in \mathbb{R}$ frei wählen, für komplexe Lösungen $u : \mathbb{R} \to \mathbb{C}$ entsprechend $c_1, c_2 \in \mathbb{C}$.

Nachrechnen: Zu lösen ist hier $\ddot{u}(t) - 2\lambda\,\dot{u}(t) + \lambda^2\,u(t) = 0$.
Linearfaktorzerlegung $(\partial_t - \lambda)(\partial_t - \lambda)\,u(t) = 0$. Einsetzen:

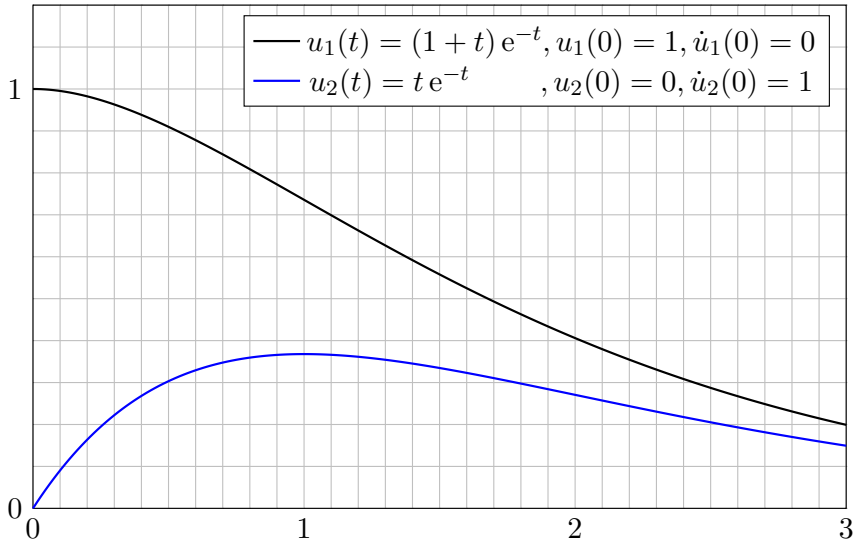
$$\begin{aligned}(\partial_t - \lambda)(\partial_t - \lambda)\left[\mathrm{e}^{\lambda t}\right] &= (\partial_t - \lambda)\left[\lambda\,\mathrm{e}^{\lambda t} - \lambda\,\mathrm{e}^{\lambda t}\right] \\ &= (\partial_t - \lambda)\left[0\right] &= 0\end{aligned}$$

$$\begin{aligned}(\partial_t - \lambda)(\partial_t - \lambda)\left[t\,\mathrm{e}^{\lambda t}\right] &= (\partial_t - \lambda)\left[\mathrm{e}^{\lambda t} + \lambda t\,\mathrm{e}^{\lambda t} - \lambda t\,\mathrm{e}^{\lambda t}\right] \\ &= (\partial_t - \lambda)\left[\mathrm{e}^{\lambda t}\right] &= 0\end{aligned}$$

☺ Damit sind zwei linear unabhängige Lösungen gefunden.

Kritische Dämpfung: $\delta = \omega_0$

Dies nennt man den **aperiodischen Grenzfall**: Er liegt genau auf der Grenze zwischen gedämpfter Schwingung und Kriechfall.



Erzwungene harmonische Schwingung

Aufgabe: Bei Anregung durch $f(t) = a\cos(\omega_1 t)$ ist als DG zu lösen

$$\ddot{u}(t) + 2\delta\,\dot{u}(t) + \omega_0^2\,u(t) = a\cos(\omega_1 t).$$

Gesucht ist eine reelle Lösung der Form $u(t) = A\cos(\omega t - \varphi)$, zu bestimmen sind hierbei die Amplitude A und die Phase φ.

Lösung: Dies ist der Realteil der komplexen Differentialgleichung

$$\ddot{z}(t) + 2\delta\,\dot{z}(t) + \omega_0^2\,z(t) = a\,\mathrm{e}^{\mathrm{i}\omega_1 t}.$$

Der Exponentialansatz $z(t) = c\,\mathrm{e}^{\mathrm{i}\omega t}$ führt uns zur Gleichung

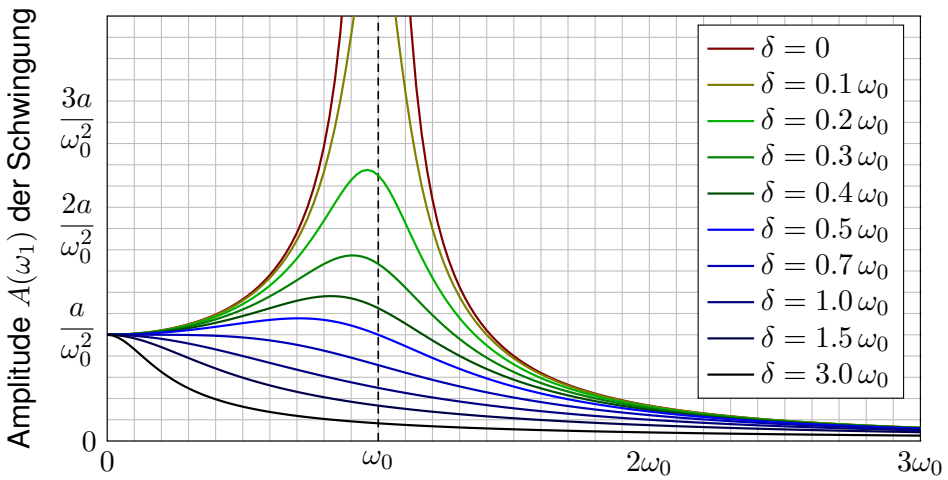
$$\left[-\omega^2 + 2\delta\,\mathrm{i}\omega + \omega_0^2\right] c\,\mathrm{e}^{\mathrm{i}\omega t} \stackrel{!}{=} a\,\mathrm{e}^{\mathrm{i}\omega_1 t}.$$

Damit finden wir $\omega = \omega_1$ und $c = a/(\omega_0^2 - \omega^2 + 2\delta\,\mathrm{i}\omega) = A\,\mathrm{e}^{-\mathrm{i}\varphi}$.
Das System reagiert mit derselben Frequenz wie die Anregung!
In Polardarstellung $c = A\,\mathrm{e}^{-\mathrm{i}\varphi}$ erhalten wir $z(t) = A\,\mathrm{e}^{\mathrm{i}(\omega_1 t - \varphi)}$ mit

$$A = \frac{a}{\sqrt{(\omega_0^2 - \omega_1^2)^2 + 4\delta^2\omega_1^2}}, \quad \varphi = \arctan\frac{2\delta\omega_1}{\omega_0^2 - \omega_1^2} + \begin{cases} 0 & \text{für } \omega_1 < \omega_0, \\ \pi & \text{für } \omega_1 > \omega_0. \end{cases}$$

☺ Damit haben wir die reelle Lösung $u(t) = A\cos(\omega t - \varphi)$ gefunden.

Erzwungene harmonische Schwingung



Frequenz ω_1 der äußeren Anregung $f(t) = a\cos(\omega_1 t)$

Die Amplitude ist maximal für $\omega_1^2 = \omega_0^2 - 2\delta^2$ bzw. $\omega_1 = 0$ falls $2\delta^2 > \omega_0^2$.
Die **Resonanz** ist dabei umso stärker, je kleiner die Dämpfung δ ist.
Für $\delta \approx 0$ und $\omega_1 \approx \omega_0$ kommt es zur **Resonanzkatastrophe**.

Erzwungene harmonische Schwingung

⚠ Im Sonderfall $\delta = 0$ und $\omega_1 = \omega_0$ schlägt unser Ansatz $c\,\mathrm{e}^{\mathrm{i}\omega t}$ fehl!

$$\ddot{z}(t) + \omega_0^2\,z(t) = \left[\omega_0^2 - \omega^2\right] c\,\mathrm{e}^{\mathrm{i}\omega t} \quad \neq \quad a\,\mathrm{e}^{\mathrm{i}\omega_0 t}$$

Zur Gleichheit muss $\omega = \omega_0$ gelten, aber dann verschwindet $[\omega_0^2 - \omega^2]$.
In obiger Formel für c ist das genau die Polstelle! Modifizierter Ansatz:

$$z(t) = c\,t\,\mathrm{e}^{\mathrm{i}\omega t}, \quad \dot{z}(t) = c\,\mathrm{e}^{\mathrm{i}\omega t} + c\,t\mathrm{i}\omega\,\mathrm{e}^{\mathrm{i}\omega t}, \quad \ddot{z}(t) = 2c\mathrm{i}\omega\,\mathrm{e}^{\mathrm{i}\omega t} - c\,t\,\omega^2\,\mathrm{e}^{\mathrm{i}\omega t}$$

$$\Longrightarrow \quad \ddot{z}(t) + \omega_0^2\,z(t) = \left[2\mathrm{i}\omega + t\,(\omega_0^2 - \omega^2)\right] c\,\mathrm{e}^{\mathrm{i}\omega t} \quad \stackrel{!}{=} \quad a\,\mathrm{e}^{\mathrm{i}\omega_0 t}$$

Durch Vergleich finden wir die Werte $\omega = \omega_0$ und $c = a/(2\mathrm{i}\omega_0)$. Also:

$$z(t) = \frac{at\,\mathrm{e}^{\mathrm{i}\omega_0 t}}{2\mathrm{i}\omega_0} = \frac{at\cos(\omega_0 t) + \mathrm{i}at\sin(\omega_0 t)}{2\mathrm{i}\omega_0} = \frac{at}{2\omega_0}\sin(\omega_0 t) - \mathrm{i}\frac{at}{2\omega_0}\cos(\omega_0 t)$$

Der Realteil $u(t) = (a/2\omega_0)\,t\sin(\omega_0 t)$ löst $\ddot{u}(t) + \omega_0^2\,u(t) = a\cos(\omega_0 t)$.

⚠ Das System reagiert mit derselben Frequenz ω wie die Anregung, aber die Amplitude wächst unbeschränkt: Man nennt dies **Resonanz**.

☺ Anschaulich: Jedes Kind lernt dieses Phänomen beim Schaukeln. Die Anregungsfrequenz trifft genau eine Eigenfrequenz des Systems!

Amplitude und Resonanz

Erzwungene Schwingungen sind ein weit verbreitetes Phänomen:

- Mechanik: Schaukel, Brücke bei gleichmäßigen Schritten / Wind, Vibrationen von Fahrzeugteilen bei bestimmten Drehzahlen,
- Akustik: Tonerzeugung in Musikinstrumenten, Resonanzkörper, Mitschwingen einer nicht gespielten Saite oder einer Stimmgabel,
- Elektrotechnik: elektrischer Schwingkreis, Radioempfang, WLAN,
- Hydromechanik: Tideresonanz der Ozeane und großen Meere.

Auch die (Hochschul-)Didaktik zeigt Resonanzphänomene: Jede Lernende folgt ihrem eigenen kognitiven Bewegungsgesetz (Rückstellkraft, Trägheit, Vergessen), wird von außen durch die Lehrende angeregt auf einer vorgegebenen Frequenz (als erzwungene Bewegung, extrinsich). Trifft die anregende Frequenz in etwa eine Eigenfrequenz (intrinsisches Interesse), so kommt es zur Resonanz: Das ist die ideale Lern- und Lehrsituation! Anregung mit zu niedriger oder zu hoher Frequenz hingegen zeigt kaum Wirkung. Auch das kennen Sie aus eigener Erfahrung.

Bei hunderten Teilnehmern sind die individuellen Eigenfrequenzen meist sehr breit gestreut. Egal auf welcher Frequenz ich sende, nur bei einen kleinen Teil bringt es eine Saite zum Klingen. Dieses Phänomen ist mir schmerzhaft bewusst, aber unter den gegebenen Bedingungen wohl unvermeidlich. Das erklärt auch die Bedeutung, sich aufeinander einzustellen. Ich versuche, auf verschiedenen Frequenzen zu senden, und lausche den Reaktionen. Das eigentlich Erstaunliche ist nicht, wie oft die Übertragung misslingt, sondern dass sie manchmal tatsächlich funktioniert.

Zusammenfassung: freie harmonische Schwingung

Gegeben seien reelle Konstanten $\delta, \omega_0 \in \mathbb{R}_{\geq 0}$ sowie $\omega_1, a \in \mathbb{R}_{>0}$.

Satz N2ı: freie harmonische Schwingung

(1) Die **homogene lineare Differentialgleichung**

$$\ddot{u}(t) + 2\delta\,\dot{u}(t) + \omega_0^2\,u(t) = 0$$

hat einen zweidimensionalen Lösungsraum; die allgemeine Lösung ist

$$u(t) = c_1 u_1(t) + c_2 u_2(t) \quad \text{mit freien Konstanten } c_1, c_2 \in \mathbb{K}$$

$$= \begin{cases} \mathrm{e}^{-\delta t}\left[c_1\cos(\omega t) + c_2\sin(\omega t)\right] & \text{für } \delta < \omega_0 \text{ und } \omega = \sqrt{\omega_0^2 - \delta^2}, \\ \mathrm{e}^{-\delta t}\left[c_1\,\mathrm{e}^{-\lambda t} + c_2\,\mathrm{e}^{\lambda t}\right] & \text{für } \delta > \omega_0 \text{ und } \lambda = \sqrt{\delta^2 - \omega_0^2}, \\ \mathrm{e}^{-\delta t}\left[c_1 + c_2 t\right] & \text{für } \delta = \omega_0 \text{ (kritische Dämpfung).} \end{cases}$$

Diese Lösungen sind reell, also eine Basis über $\mathbb{R}$, ebenso über $\mathbb{C}$.

Anfangswerte $u(t_0)$ und $\dot{u}(t_0)$ können beliebig vorgegeben werden: Sie legen die freien Konstanten c_1, c_2 eindeutig fest (und umgekehrt).

Zusammenfassung: erzwungene harmonische Schwingung

Satz N2ı: erzwungene harmonische Schwingung

(2) Die **inhomogene lineare Differentialgleichung**

$$\ddot{u}(t) + 2\delta\,\dot{u}(t) + \omega_0^2\,u(t) = a\cos(\omega_1 t)$$

hat einen zweidim. affinen Lösungsraum; die allgemeine Lösung ist

$$u(t) = u_0(t) + c_1 u_1(t) + c_2 u_2(t) \quad \text{mit freien Konstanten } c_1, c_2 \text{ und}$$

$$u_0(t) = \begin{cases} A\cos(\omega_1 t - \varphi) & \text{für } \delta > 0 \text{ oder } \omega_1 \neq \omega_0 \text{ (generisch N261),} \\ & \text{Amplitude } A = a/\sqrt{(\omega_0^2 - \omega_1^2)^2 + 4\delta^2\omega_1^2}, \\ & \text{Phase } \varphi = \arctan\left[2\delta\omega_1/(\omega_0^2 - \omega_1^2)\right] (+\pi), \\ \dfrac{at}{2\omega_1}\sin(\omega_1 t) & \text{für } \delta = 0 \text{ und } \omega_1 = \omega_0 \text{ (Resonanz N263).} \end{cases}$$

„Allgemeine Lösungen = partikuläre Lösung + homogene Lösungen“

Anfangswerte $u(t_0)$ und $\dot{u}(t_0)$ können beliebig vorgegeben werden: Sie legen die freien Konstanten c_1, c_2 eindeutig fest (und umgekehrt).

Freie und erzwungene harmonische Schwingung

Typische Beispiele: Bei **schwacher Dämpfung** $0 < \delta < \omega_0$ gilt

$$u(t) = \underbrace{A\cos(\omega_1 t - \varphi)}_{\text{periodische Lösung}} + \underbrace{\mathrm{e}^{-\delta t}\left[c_1\cos(\omega t) + c_2\sin(\omega t)\right]}_{\text{Einschwingvorgang} \to 0 \text{ für } t \to \infty}.$$

Nach Einschwingzeit sehen wir nur noch die periodische Lösung u_0: Das System reagiert mit derselben Frequenz ω_1 wie die Anregung, mit konstanter Amplitude A und Phasenverschiebung φ wie berechnet.

Für $\omega_1 \to 0$ gilt $A \to 1/\omega_0^2$: Niedrige Frequenzen werden gedämpft.
Für $\omega_1 \to \infty$ gilt $A \to 0$: Hohe Frequenzen werden verschluckt.

Der Sonderfall $\delta = 0$ und $\omega_1 = \omega_0$ führt zur **Resonanz(katastrophe)**:

$$u(t) = \underbrace{\frac{at}{2\omega_0}\sin(\omega_0 t)}_{\text{Amplitude wächst unbeschränkt}} + \underbrace{c_1\cos(\omega_0 t) + c_2\sin(\omega_0 t)}_{\text{periodisch, insbesondere beschränkt}}$$

Manchmal ist genau dies erwünscht, etwa beim Radioempfang.

🙂 Mit unseren Techniken lösen Sie alle Fälle vollständig und explizit.

Freie und erzwungene harmonische Schwingung

Die allgemeine Lösung / Schwingung $u : I \to \mathbb{R}$ ist die **Überlagerung** einer inhomogenen Lösung / **erzwungenen Schwingung** u_0 und einer homogenen Lösung / **freien Schwingung** $c_1 u_1 + c_2 u_2$.

Die Konstanten $c_1, c_2 \in \mathbb{R}$ ergeben sich aus Anfangsdaten $u(t_0), \dot{u}(t_0)$. Bei Dämpfung $\delta > 0$ klingen $u_1(t) \to 0$ und $u_2(t) \to 0$ exponentiell ab. Der Einfluss der Startwerte ist nach gewisser **Einschwingzeit** kaum noch spürbar, es bleibt schließlich nur die **periodische Lösung** u_0.

Im dämpfungsfreien Fall $\delta = 0$ klingen die freien Schwingungen $u_1(t) = \cos(\omega_0 t)$ und $u_2(t) = \sin(\omega_0 t)$ nicht ab. Zudem führt eine äußere Anregung mit Frequenz $\omega_1 = \omega_0$ zur **Resonanzkatastrophe**: Die Amplitude der Schwingung wächst (theoretisch) unbegrenzt.

Für **praktische Zwecke** gilt dies bereits für $\delta \approx 0$: Die Schwingungen u_1, u_2 klingen sehr langsam ab, bei realistischer Beobachtungsdauer sind Dämpfungsverluste kaum wahrnehmbar. Bei Anregung mit $\omega_1 \approx \omega_0$ kommt es zu sehr starker Resonanz, die Amplitude der erzwungenen Schwingung wächst schließlich über die Belastbarkeit des Materials.

Warum zelebriere ich dieses Beispiel so ausführlich?

N269
Erläuterung

Aus rein mathematischer Sicht ist die Gleichung des harmonischen Oszillators lediglich ein einfaches Beispiel unserer allgemeinen Theorie. Dennoch haben wir gute Gründe, dies hier gebührend zu feiern:

☺ Phänomene von Schwingungen und Resonanzen treten auch im Alltag sehr häufig auf: Achten Sie darauf und lernen Sie zu staunen!

☺ Die Frage und die Antwort sind anschaulich, motivierend und intuitiv: Anders als bei anderen Gleichungen können Sie die Lösungen spüren!

☺ In zahlreichen naturwissenschaftlich-technischen Anwendungen ist der harmonische Oszillator zentrales Modell und leuchtendes Vorbild.

☺ In embryonaler Form enthält das Beispiel alle Schwierigkeiten und Schönheiten der allgemeinen Theorie linearer Differentialgleichungen.

☺ Insbesondere zeigt es die Eleganz und geradezu die Notwendigkeit der komplexen Zahlen: Erst über $\mathbb{C}$ wird die Sachlage klar und einfach.

☺ Selbst einfache Beispiele entfalten eine beachtliche Komplexität. Erst mit der zugrundeliegenden Theorie verschaffen wir uns Überblick.

Warum sind Existenz und Eindeutigkeit so wichtig?

N270
Erläuterung

In der Geschichte der Mathematik wurde das Problem der *Existenz und Eindeutigkeit* von Lösungen erst erstaunlich spät entdeckt… und gelöst.

Im 17. Jahrhundert entwickeln Gottfried Wilhelm Leibniz (1646–1716) und Isaac Newton (1642–1726) und andere die Infinitesimalrechnung. Aus physikalisch–geometrischen Anwendungen treten dabei unmittelbar Differentialgleichungen in den Fokus des mathematischen Interesses. Existenz und Eindeutigkeit von Lösungen standen dabei nie in Zweifel. Umso schockierender waren daher die ersten Gegenbeispiele von Gleichungen mit mehrdeutigen Lösungen oder ganz ohne Lösung.

Augustin-Louis Cauchy (1789–1857) und seine Nachfolger begründeten die bis heute übliche mathematische Strenge. Existiert eine Lösung? Erst dann lohnt sich überhaupt danach zu suchen. Ist sie eindeutig? Haben wir eine, so brauchen wir nicht nach weiteren zu fahnden.

⚠ Erst nach Klärung dieser grundlegenden Fragen können wir uns weiteren Eigenschaften und numerischen Näherungen zuwenden.

Abstrakt bedeutet… vielseitig anwendbar!

N271
Erläuterung

Das einleitende Beispiel einer mechanischen Schwingung ist besonders anschaulich und sinnlich direkt zugänglich. Wir alle haben dies schon als Kinder spielerisch gelernt: beim Schaukeln, Seilspringen, usw.

Der elektrische Schwingkreis ist weniger sinnlich-anschaulich, doch er führt zu genau derselben Differentialgleichung! Dieselben Gleichungen und Lösungsmethoden lassen sich auf zahlreiche Probleme anwenden, die zunächst sehr verschieden anmuten, aber doch einen gemeinsamen Kern haben. Das ist das Gütesiegel für Effizienz und Denkökonomie!

Wir bestaunen und bewundern hier ein Paradebeispiel für die viel zitierte Abstraktion in der Mathematik: Sie ist kein Schimpfwort für „fern jeder Anwendung“, sondern eine Auszeichnung für „vielseitig anwendbar“. Zumindest sollte dies meiner Ansicht nach so sein. Achten Sie darauf, wenn jemand über „abstrakten Quatsch“ schimpft, vielleicht Sie selbst: Meist ist dies weniger eine objektive Aussage über den Gegenstand, sondern vielmehr das offene Bekenntnis der eigenen Ignoranz.

Grundlegende Theorie, große praktische Wirkung

N272
Erläuterung

So einfach der elektrische Schwingkreis auch erscheinen mag, er hat doch phantastische Anwendungen hervorgebracht wie den Funkverkehr, engl. *radio communication*, die unser heutiges Leben nachhaltig prägen.

Guglielmo Marconi (1874–1937) war ein italienischer Erfinder und Unternehmer. Als erstem gelangen ihm drahtlose Verbindungen über größere Entfernungen, 1903 die erste transatlantische Funkverbindung: Grußbotschaften zwischen König Edward VII. in England und Präsident Theodore Roosevelt in den USA. Marconi begründete unter anderem den Seefunkverkehr und bekam für seine Verdienste im April 1912 eine kostenlose Passage für die Jungfernfahrt der RMS Titanic angeboten; da er jedoch Schriftverkehr erledigen wollte, nahm er drei Tage früher die RMS Lusitania, da es an Bord dieses Schiffs eine Stenografin gab. Im Jahre 1930 gründete er gemeinsam mit Papst Pius XI. Radio Vatikan.

Für seine praktischen Arbeiten erhielt er 1909 den Nobelpreis für Physik, zusammen mit Ferdinand Braun, der die theoretischen Grundlagen dazu erarbeitete. (`de.wikipedia.org/wiki/Guglielmo_Marconi`)

Was sind Differentialgleichungssysteme?

N301

Wir arbeiten über dem Körper $\mathbb{K} = \mathbb{R}, \mathbb{C}$ der reellen / komplexen Zahlen.

In vielen Anwendungen geht es statt einer einzelnen Größe $x(t) \in \mathbb{K}$ um mehrere Größen $x_1(t), \dots, x_n(t) \in \mathbb{K}$, deren zeitliche Entwicklung durch **gekoppelte Differentialgleichungen** beschrieben wird:

$$\begin{cases} x_1'(t) = f_1\big(t, x_1(t), x_2(t), \dots, x_n(t)\big), \\ x_2'(t) = f_2\big(t, x_1(t), x_2(t), \dots, x_n(t)\big), \\ \quad\vdots \\ x_n'(t) = f_n\big(t, x_1(t), x_2(t), \dots, x_n(t)\big). \end{cases}$$

Mit $x = (x_1, x_2, \dots, x_n)$ und $f = (f_1, f_2, \dots, f_n)$ bündeln wir dies kurz und übersichtlich zu einer **vektorwertigen Differentialgleichung**:

$$\boxed{x'(t) = f(t, x(t))}$$

Bei einer **autonomen Differentialgleichung** hängt f nicht von t ab:

$$\boxed{x'(t) = f(x(t))}$$

Wir können autonomisieren durch Einführung von $x_0 = t$ und $f_0 = 1$.

Was sind Differentialgleichungssysteme?

N302
Erläuterung

Gegeben ist als rechte Seite die stetige Funktion $f : \mathbb{R} \times \mathbb{K}^n \supset G \to \mathbb{K}^n$ auf einem Gebiet $G \subset \mathbb{R} \times \mathbb{K}^n$, zumindest mit nicht-leerem Inneren.

Gesucht sind alle differenzierbaren Funktionen $x : I \to \mathbb{K}^n$ auf einem (maximalen) Intervall $I \subset \mathbb{R}$, die zunächst die Bedingung $(t, x(t)) \in G$ und dort die ersehnte Gleichung $x'(t) = f(t, x(t))$ für alle $t \in I$ erfüllen.

Zeitinvarianz: Bei einer autonomen Differentialgleichung $x' = f(x)$ ist mit jeder Lösung $x : I \to \mathbb{K}^n$ auch die um $\tau \in \mathbb{R}$ verschobene Funktion $\tilde{x} : \tilde{I} \to \mathbb{K}^n : \tilde{x}(t) = x(t - \tau)$ auf dem Intervall $\tilde{I} = I + \tau$ eine Lösung.

Dies führt uns zu den Grundfragen der Differentialgleichungen:

- Gibt es immer eine Lösung? mehrere?
- Wie finden wir eine Lösung? gar alle?

Wir benötigen wie immer zwei sich ergänzende Lösungsmethoden:

- Leistungsstarke Lösungstheorie als Grundlage
- Erprobte Rezepte für spezielle Gleichungen

Für manche f können wir die DG exakt lösen, sonst nur numerisch.

Was sind lineare Differentialgleichungssysteme?

N303

Jedes **lineare Differentialgleichungssystem** ist von folgender Form:

$$\begin{cases} x_1'(t) = a_{11}(t)\, x_1(t) + a_{12}(t)\, x_2(t) + \cdots + a_{1n}(t)\, x_n(t) + b_1(t) \\ x_2'(t) = a_{21}(t)\, x_1(t) + a_{22}(t)\, x_2(t) + \cdots + a_{2n}(t)\, x_n(t) + b_2(t) \\ \quad\vdots \\ x_n'(t) = a_{n1}(t)\, x_1(t) + a_{n2}(t)\, x_2(t) + \cdots + a_{nn}(t)\, x_n(t) + b_n(t) \end{cases}$$

Gegeben sind die **Koeffizienten** $a_{ij} : I \to \mathbb{K}$ und die **rechten Seiten** $b_i : I \to \mathbb{K}$ als stetige Funktionen auf einem Intervall $I \subset \mathbb{R}$, gebündelt:

$$\boxed{x'(t) = A(t)\, x(t) + b(t)}$$

Gesucht sind als **Lösungen** alle Funktionen $x : I \to \mathbb{K}^n$ in $\mathscr{C}^1(I, \mathbb{K}^n)$, die die Gleichung $x'(t) = A(t)\, x(t) + b(t)$ in jedem Punkt $t \in I$ erfüllen.

Die zugehörige **homogene Gleichung** erhalten wir für $b = 0$:

$$\boxed{x'(t) = A(t)\, x(t)}$$

Beim **Anfangswertproblem** ist zudem $x(t_0) = v \in \mathbb{K}^n$ vorgegeben.

Was sind lineare Differentialgleichungssysteme?

N304
Erläuterung

Wir nennen $A(t)$ die **Koeffizientenmatrix** oder die **Systemmatrix**. Die rechte Seite $b(t)$ heißt auch **Inhomogenität** oder **Störterm**.

Unser Ziel ist die Berechnung einer **Basis des Lösungsraumes**. Dazu können wir explizite Lösungsformeln angeben und für wichtige Beispiele ausrechnen. Hierzu benötigen wir geeignete Techniken aus der Analysis, insbesondere die allgegenwärtige Integration.

Lineare Differentialgleichungssysteme mit **konstanten Koeffizienten** sind der allereinfachste Fall: Die Lösung der Gleichung $x'(t) = A\, x(t)$ gelingt uns vollständig bereits mit den Techniken der Linearen Algebra: Wir finden eine Basis des Lösungsraums mit Hilfe der Hauptvektoren einer Jordan–Basis; die Integration tritt dabei in den Hintergrund.

Wir mobilisieren nahezu alle bisherigen Begriffe und Techniken: Vektorraum, Basis, Dimension, lineare Abbildung, Kern und Bild, Darstellung durch Matrizen, Determinante, charakteristisches Polynom, Eigenvektoren und Diagonalform, Hauptvektoren und Jordan–Form.

Reduktion eines DGSystems auf erste Ordnung

N305
Erläuterung

☺ Differentialgleichungen erster Ordnung sind universell: Wir können jede DG $n$ter Ordnung auf ein DGSystem erster Ordnung reduzieren!

Reduktion: Vorgelegt sei eine **Differentialgleichung $n$ter Ordnung**:

(1) $$x^{(n)}(t) = f\big(t, x(t), x'(t), \dots, x^{(n-1)}(t)\big)$$

Diese können wir umformulieren in ein **DGSystem erster Ordnung**:

(2) $$\begin{cases} x_0'(t) &= x_1(t) \\ x_1'(t) &= x_2(t) \\ &\vdots \\ x_{n-2}'(t) &= x_{n-1}(t) \\ x_{n-1}'(t) &= f(t, x_0(t), x_1(t), \dots, x_{n-1}(t)) \end{cases}$$

Übung: Rechnen Sie diesen genial-einfachen Trick sorgsam nach:
Löst $x : I \to \mathbb{K}$ die DG (1), so löst $(x, x', \dots, x^{(n-1)})$ das DGSystem (2).
Löst $(x_0, \dots, x_{n-1}) : I \to \mathbb{K}^n$ das DGSystem (2), so löst x_0 die DG (1).

Einfachste DGSysteme: entkoppelte Gleichungen

N306
Erläuterung

☺ Es genügt daher, **DGSysteme erster Ordnung** zu untersuchen!
Diese Formulierung ist einfacher und erlaubt starke Werkzeuge:
In jeder Dimension n gilt **Existenz & Eindeutigkeit & Stabilität** dank des Satzes von Picard–Lindelöf, den Sie in der Analysis kennenlernen.

☺ Der einfachste Fall sind **entkoppelte Gleichungen**:

$$\begin{aligned} x_1'(t) &= f_1(t, x_1(t)) \\ x_2'(t) &= f_2(t, x_2(t)) \\ &\vdots \\ x_n'(t) &= f_n(t, x_n(t)) \end{aligned}$$

Hierzu lösen wir n eindimensionale Differentialgleichungen.

⚠ Im Allgemeinen sind die gegebenen Gleichungen aber gekoppelt.
Für dieses Problem benötigen wir daher passende Rechenmethoden.
Hierzu nutzen wir die Werkzeuge der Analysis und der Linearen Algebra, insbesondere Eigen- und Hauptvektoren, wie wir gleich sehen werden.

Reduktion eines linearen DGSystems auf erste Ordnung

N307

Zu lösen sei eine lineare Differentialgleichung $n$ter Ordnung:

(1) $$x^{(n)}(t) + a_{n-1}(t)\, x^{(n-1)}(t) + \cdots + a_1(t)\, x'(t) + a_0(t)\, x(t) = b(t)$$

Diese ist äquivalent zu einem linearen DGSystem erster Ordnung:

(2) $$\begin{cases} x_0' &= & & x_1 & & & \\ &\vdots & & & & & \\ x_{n-2}' &= & & & & x_{n-1} & \\ x_{n-1}' &= & -a_0\, x_0 & -a_1\, x_1 & \dots & -a_{n-1}\, x_{n-1} & +b \end{cases}$$

Das entspricht $x'(t) = A(t)\, x(t) + B(t)$ mit zugehöriger Systemmatrix

$$A(t) = \begin{bmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ 0 & & 0 & 1 \\ -a_0(t) & -a_1(t) & \dots & -a_{n-1}(t) \end{bmatrix} \quad \text{und} \quad B(t) = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ b(t) \end{bmatrix}.$$

Beispiel: Wir nutzen dies für gekoppelte Oszillatoren, siehe N325.

Lineare DGSysteme: entkoppelte Gleichungen

N308
Erläuterung

☺ Besonders wichtig und gut zu lösen sind lineare DGSysteme $x'(t) = A\, x(t) + b(t)$ mit konstanter Koeffizientenmatrix $A \in \mathbb{K}^{n \times n}$.

☺ Der einfachste Fall sind auch hier **entkoppelte Gleichungen**:

$$\begin{aligned} x_1'(t) &= a_1\, x_1(t) \\ x_2'(t) &= a_2\, x_2(t) \\ &\vdots \\ x_n'(t) &= a_n\, x_n(t) \end{aligned}$$

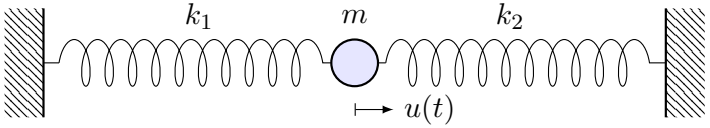
Die Lösungen $x_k(t) = c_k\, \mathrm{e}^{a_k t}$ können wir sofort ausschreiben!

☺ Oft lassen sich komplexe Lösungen $\mathrm{e}^{(\sigma \pm \mathrm{i}\omega)t}$ leichter berechnen und dann in reelle Lösungen $\mathrm{e}^{\sigma t}\cos(\omega t)$ und $\mathrm{e}^{\sigma t}\sin(\omega t)$ umrechnen.
Wir nutzen dies oben für den harmonischen Oszillator, siehe N253.

⚠ Im Allgemeinen sind die gegebenen Gleichungen aber gekoppelt.
Für dieses Problem benötigen wir daher passende Rechenmethoden.
Hierzu nutzen wir die Werkzeuge der Analysis und der linearen Algebra!

Der harmonische Oszillator als dynamisches System

N309
Beispiel



Aufgabe: Formulieren und lösen Sie den harmonischen Oszillator...
(1) als eine eindimensionale Differentialgleichung zweiter Ordnung,
(2) als ein zweidim. Differentialgleichungssystem erster Ordnung.

Lösung: (1) Zeit $t \in \mathbb{R}$, Position $u(t) \in \mathbb{R}$, Geschwindigkeit $\dot{u}(t) \in \mathbb{R}$, Beschleunigung $\ddot{u}(t) \in \mathbb{R}$, Kraft $-\omega_0^2\, u(t) - 2\delta\, \dot{u}(t)$, Bewegungsgesetz:

$$\ddot{u}(t) + 2\delta\, \dot{u}(t) + \omega_0^2\, u(t) = 0$$

Lösung $u(t) = \mathrm{e}^{-\delta t}[c_1 \cos(\omega t) + c_2 \sin(\omega t)]$ falls $\omega = \sqrt{\omega_0^2 - \delta^2} > 0$.
Die Anfangsdaten $(u(t_0), \dot{u}(t_0))$ bestimmen die Konstanten $c_1, c_2 \in \mathbb{R}$.

(2) Zustand $(x_1(t), x_2(t)) = (u(t), \dot{u}(t))$, Zustandsraum $\mathbb{R}^2$, DGSystem:

$$\left\{\begin{array}{rrr} \dot{x}_1 = & & x_2 \\ \dot{x}_2 = & -\omega_0^2 x_1 & -2\delta x_2 \end{array}\right\} \iff \begin{bmatrix}\dot{x}_1 \\ \dot{x}_2\end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -\omega_0^2 & -2\delta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Der harmonische Oszillator als dynamisches System

N310
Erläuterung

- Allgemeiner Trick: Reduktion von höherer auf erste Ordnung! N307
- DGSystem erster Ordnung = Vektorfeld auf dem Zustandsraum!

Der harmonische Oszillator dient uns weiterhin als zentrales Modell: Es ist besonders einfach und anschaulich, lässt sich leicht lösen, und zeigt im Prinzip bereits alle wesentlichen Phänomene! N253

Wir schreiben seine Differentialgleichung zweiter Ordnung hier neu als System erster Ordnung: Das ist ein Vektorfeld auf dem Zustandsraum!

Jedes solche Richtungsfeld ist geometrisch besonders anschaulich als ein „Fluss“, und dies nützt ebenso in der Analysis und der Numerik.

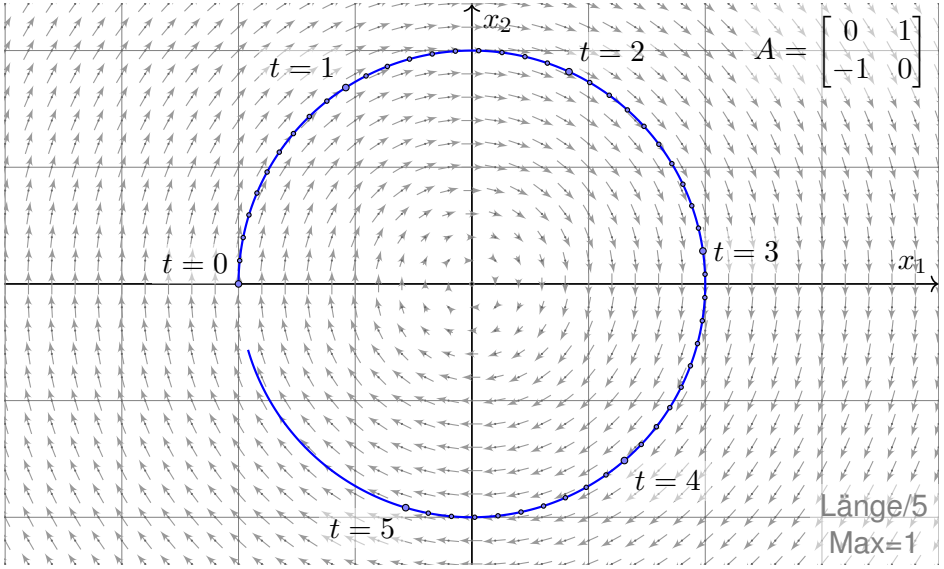
Lösungskurven des DGSystems sind die Trajektorien: Die nächsten beiden Graphiken zeigen den nicht bzw. schwach gedämpften Fall. Hierzu kennen wir bereits die exakten Lösungen. N265

Die dritte Graphik zeigt mehrere numerische Näherungen durch das Euler–Verfahren: Solche Näherungen sind nützlich, wenn wir keine exakte Lösung kennen oder mühsam beschaffen wollen, und nötig, wenn gar keine Lösungsformel in geschlossener Form existiert.

Der harmonische Oszillator im Zustandsraum $\mathbb{R}^2$

N311
Beispiel

Harmonischer Oszillator, keine Dämpfung $\delta = 0$, zum Beispiel $\omega_0 = 1$:

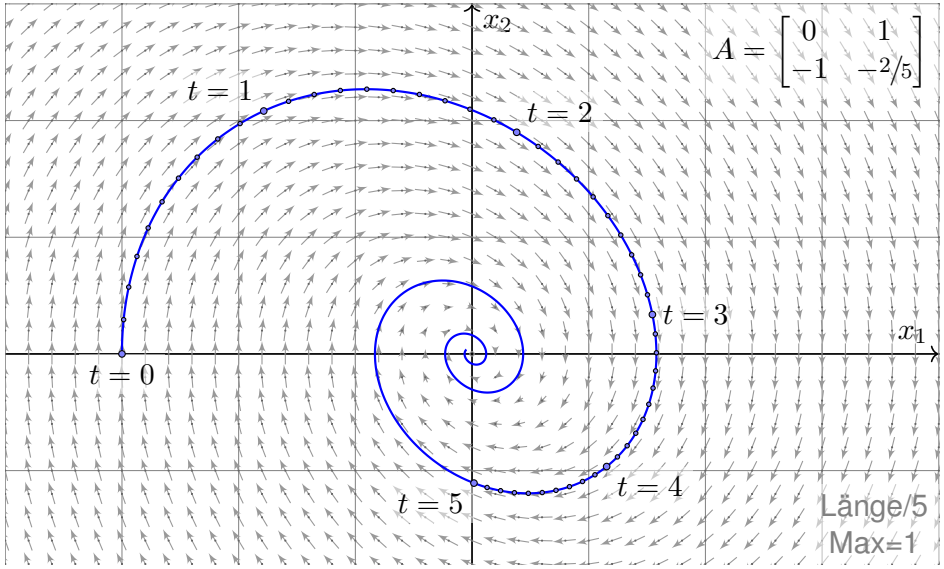


Kein Energieverlust, daher sogar Rückkehr in den Anfangszustand.

Der harmonische Oszillator im Zustandsraum $\mathbb{R}^2$

N312
Beispiel

Schwache Dämpfung $0 < \delta < \omega_0$, zum Beispiel $\delta = 1/5$ und $\omega_0 = 1$:

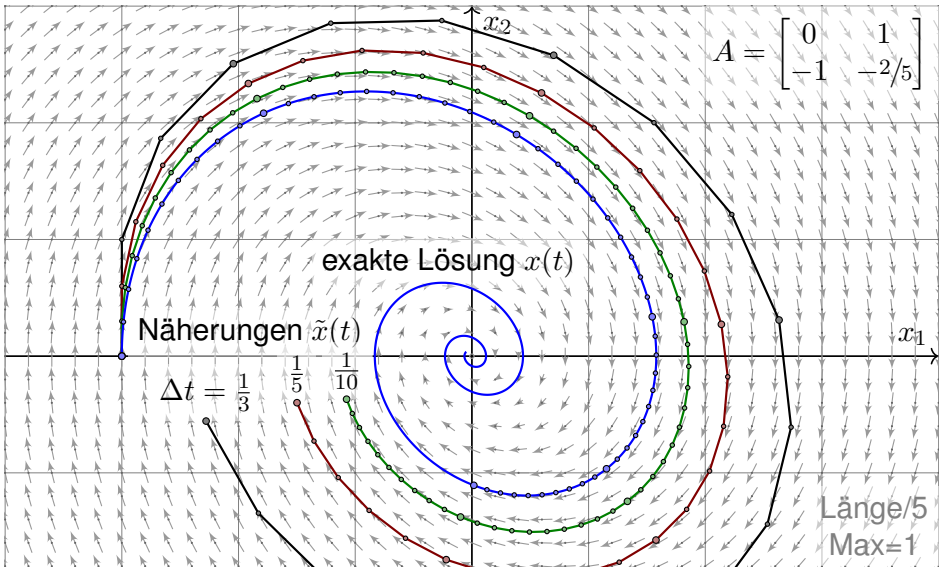


Echter Energieverlust, daher keine Rückkehr in den Anfangszustand.

Numerische Näherung durch das Euler–Verfahren

N313
Beispiel

Approximation durch das Euler–Verfahren mit Schrittweite $\Delta t = \frac{1}{3}, \frac{1}{5}, \frac{1}{10}$:



Wir erkennen graphisch den Rechenaufwand und Approximationsfehler.

Numerische Näherung durch das Euler–Verfahren

N314
Erläuterung

Zu lösen sei ein Differentialgleichungssystem erster Ordnung:

$$\dot{x}(t) = f(t, x(t)), \quad x(0) = x_0$$

☺ Dies ist im Wesentlichen ein Vektorfeld f auf dem Zustandsraum!
Gesucht ist eine Lösungskurve $x(t)$, die die obige Gleichung erfüllt.
Das **Euler–Verfahren** verschafft uns eine numerische Näherung $\tilde{x}$:

Wir wählen Zeitschritte $0 = t_0 < t_1 < t_2 < t_3 < \dots$ mit $\Delta t_i = t_{i+1} - t_i$.
Am einfachsten äquidistant $t_i = t_0 + i\Delta t$ mit fester Schrittweite $\Delta t > 0$.
Die Ableitung $\dot{x}$ approximieren wir durch den **Differenzenquotienten**:

$$\frac{x(t_{i+1}) - x(t_i)}{t_{i+1} - t_i} \quad \approx \quad \dot{x}(t_i) \quad \overset{!}{=} \quad f(t, x(t_i))$$

Damit berechnen wir Näherungswerte $\tilde{x}(t_1), \tilde{x}(t_2), \tilde{x}(t_3), \dots$ rekursiv:

$$\tilde{x}(t_{i+1}) = \tilde{x}(t_i) + f(t_i, \tilde{x}(t_i)) \cdot (t_{i+1} - t_i) \quad \text{für } i = 0, 1, 2, 3, \dots$$

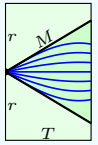
Unter geeigneten Bedingungen existiert genau eine Lösung $x(t)$ und die Euler–Approximation $\tilde{x}(t)$ kommt für kleine Schrittweiten beliebig nahe.

Numerische Näherung durch das Euler–Verfahren

N315
Erläuterung

Geometrische Voraussetzungen für das Euler–Verfahren:

Sei $I = [t_0, t_0 + T] \subset \mathbb{R}$ ein Zeitintervall der Länge $T > 0$.
Sei $K = \bar{B}(x_0, r) \subset \mathbb{K}^n$ der Ball um x_0 mit Radius $r > 0$.
Sei $f : I \times K \to \mathbb{K}^n$ stetig, somit beschränkt, also $|f| \le M$.
Hierbei gelte $T \cdot M \le r$, notfalls verkleinern wir T und I.
Dies garantiert, dass Lösungen nicht vorzeitig aus K rauslaufen.



Gesucht ist $x : I \to K$ diff'bar mit $x(t_0) = x_0$ und $\dot{x}(t) = f(t, x(t))$.
Das heißt: In jedem Punkt $(t, x(t))$ ist die Tangente $\dot{x}(t) = f(t, x(t))$.

Euler–Approximation: Wir wählen eine Partition des Zeitintervalls

$$P = \{t_0 < t_1 < \dots < t_N = t_0 + T\}.$$

Wie oben illustriert definieren wir hierzu den **Euler–Polygonzug**

$$\tilde{x} = \begin{bmatrix} t_0 & t_1 & t_2 & \dots & t_N \\ \tilde{x}_0 & \tilde{x}_1 & \tilde{x}_2 & \dots & \tilde{x}_N \end{bmatrix} \quad \text{mit} \quad \frac{\tilde{x}_{i+1} - \tilde{x}_i}{t_{i+1} - t_i} = f(t_i, \tilde{x}_i)$$

☺ Praktisch: Aus $\tilde{x}_0 = x_0$ berechnet man schrittweise $\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_N$:
Im Punkt $(t_i, \tilde{x}_i)$ wird die Kurve in Richtung $f(t_i, \tilde{x}_i)$ weitergeschickt.

Numerische Näherung durch das Euler–Verfahren

N316
Erläuterung

Satz N3A: Existenz von Lösungen, Peano 1890

Zu lösen sei die Differentialgleichung $\dot{x}(t) = f(t, x(t))$ mit $x(t_0) = x_0$.
Unter den oben erklärten geometrischen Voraussetzungen gilt:

Es existieren Partitionen $P_1, P_2, P_3, \dots \subset I$, deren Euler–Polygonzüge $\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \dots : I \to K$ gegen eine Lösung $x : I \to K$ konvergieren.

☺ Dies garantiert Existenz von Lösungen, ☹ keine Eindeutigkeit.
☺ Die Rechnung ist für $\Delta t = T/N$ sehr leicht zu implementieren.
☹ Präzision verlangt großes N, damit wächst der Rechenaufwand.
☹ Praktisches Problem: Der Satz ist nicht konstruktiv! Gegeben $\varepsilon > 0$, wie wählt man eine Partition P, um eine ε–Approximation zu erhalten?
☺ Die Numerik untersucht und optimiert solche Näherungsverfahren.
Ziel: gute Fehlerschranken und hohe Präzision bei geringem Aufwand.

Die **Numerik der gewöhnlichen Differentialgleichungen** ist ein hoch entwickeltes Gebiet und stellt umfangreiche Werkzeuge zur Verfügung.

Newtons Himmelsmechanik: die Bewegungsgleichung

N317

Aufgabe: Formulieren Sie die Bewegungsgleichungen von n Körpern mit Masse $m_k > 0$, Position $u_k(t) \in \mathbb{R}^3$ und Geschwindigkeit $v_k(t) \in \mathbb{R}^3$.

Lösung: Newtons Gravitationsgesetz ergibt die Differentialgleichungen

$$\dot{u}_k = v_k, \quad \dot{v}_k = f_k(u) := \sum\nolimits_{j \neq k} \gamma\, m_j \frac{u_j - u_k}{|u_j - u_k|^3}.$$

Vorgegeben sind die Anfangssdaten $u_k(0)$ und $v_k(0)$ zur Zeit $t = 0$.
Als Lösung gesucht ist die Bewegung $(u_1, v_1, \ldots, u_n, v_n) : [0, T[\to \mathbb{R}^{6n}$.
Erlaubt ein so komplexes System immer genau eine Lösung? Ja, das ist der zentrale ∃&E-Satz! Kollision oder Expulsion nach ∞ sind möglich: Eventuell existiert die Lösung nur für eine kurze Zeit $T > 0$. Für manche Startwerte sind Lösungen periodisch, oder beinahe: Zu unserem Glück!

- 🙂 Den Fall $n = 2$ lösen Kegelschnitte: Ellipsen, Parabeln, Hyperbeln.
- ☹ Für $n \geq 3$ lässt sich dieses DGSystem i.A. nicht geschlossen lösen!
- 🙂 Euler–Verfahren: diskrete Zeitschritte $0 = t_0 < t_1 < t_2 < t_3 < \ldots$,

$$u_k(t_{i+1}) \approx u_k(t_i) + v_k(t_i) \cdot (t_{i+1} - t_i),$$
$$v_k(t_{i+1}) \approx v_k(t_i) + f_k(u) \cdot (t_{i+1} - t_i).$$

Newtons Himmelsmechanik: der historische Triumph

N318
Erläuterung

Das Verständnis der **Himmelsmechanik** markiert den Übergang vom Mittelalter zur Neuzeit!

Die Beobachtung des Nachthimmels und seiner Sterne fasziniert uns Menschen seit Alters her. Neben den zahlreichen „Fixsternen“ (weit entfernte Sterne) erkennen wir einige „Wandelsterne“ (Planeten unseres Sonnensystems). Ihre Bewegung lässt Regeln erahnen, doch für Wandelsterne scheinen diese zunächst kompliziert und verwirrend. Sie quantitativ zu erfassen und gründlich zu verstehen, ist einer der großen Triumphe menschlicher Neugier und systematischer Forschung!

Von der Erde besehen scheinen sich alle Sterne um uns zu drehen, doch die exakte Bewegung der Planeten erweist sich als schrecklich kompliziert. Kopernikus' heliozentrisches Modell (1543) ist einfacher, daher nützlicher: Die Bahnen der Planeten um die Sonne erweisen sich recht genau als Ellipsen. Diese Koordinatentransformation hat enorme Wirkung und schreibt Weltgeschichte!

Aus Tycho Brahes präzisen **Beobachtungsdaten** leitete Johannes Kepler drei Gesetze ab, die die Ellipsenbewegung der Planeten um die Sonne gut *beschreiben*. Eine *Erklärung* der Bewegungen durch einheitliche physikalische Prinzipien gelang erst Isaac Newton 1686 mit seinen Principia!

Die moderne Naturwissenschaft beginnt mit Newtons Formulierung der drei Bewegungsgesetze, des universellen Gravitationsgesetzes und seiner Lösung des Zwei-Körper-Problems. Mit einer Handvoll physikalischer Prinzipien und den passenden mathematischen Werkzeugen konnte er die Keplerschen Regeln *erklären*, ja *herleiten*. Newtons revolutionäre Idee: Überall im Universum gelten dieselben Gesetze! Newtons Mechanik erklärt die Schwerkraft hier auf Erden ebenso wie außerirdische Phänomene: den Umlauf der Planeten um die Sonne und des Mondes um die Erde, sogar die Gezeiten unserer Meere, ebenso die Coriolis–Kraft und das Foucaultsche Pendel.

Newtons Himmelsmechanik: die Herausforderung

N319
Ausführung

Allein schon das obige Differentialgleichungssystem zu formulieren, ist eine Meisterleistung der Mathematik und Physik der Neuzeit. Wir nennen dies **Himmelsmechanik** und sind völlig zu Recht stolz auf sie: Mathematische Sprache und Werkzeuge erleuchten die gesamte Entwicklung und ebnen den Weg von Beobachtung über Erklärung und Berechnung bis zur Raumfahrt.

Auch nach über 300 Jahren sind Newtons Gleichungen immer noch nützlich wie am ersten Tag! Daten ändern sich, Methoden bleiben bestehen. Solide mathematische Arbeit hat eine extrem lange Wirksamkeit. Daher lohnt es sich auch für Sie heute, in mathematische Grundlagen zu investieren und diese wirksamen Werkzeuge zu erlernen, anzuwenden und fortzuführen.

Die drei Fälle $n = 1$ und $n = 2$ sowie $n \geq 3$ sind sehr verschieden! Für einen einzigen Körper ($n = 1$) enthalten Newtons Gleichungen $\dot{u}_1 = v_1$ und $\dot{v}_1 = 0$ keine gravitative Wechselwirkung. Ihre Lösung ist eine **geradlinige Bewegung**, nämlich $u_1(t) = u_1(0) + v_1 t$.

Ein Zwei-Körper-System ($n = 2$) wie Sonne-Erde oder Erde-Mond ist bereits ausgesprochen interessant. Newton konnte seine Gleichungen hier gut lösen, sie ergeben Ellipsenbahnen und erklären die Keplerschen Gesetze. Allgemeiner sind auch Parabeln und Hyperbeln als Lösungen möglich, je nach Anfangsdaten $u_1(0), v_1(0), u_2(0), v_2(0)$. In allen Fällen gelingt die Lösung hier noch in geschlossener Form. Man nennt ein solches System **vollständig integrabel**.

Newton betrachtete anschließend das Drei-Körper-System Sonne-Erde-Mond. Dies entzog sich jedoch hartnäckig einer Lösung und wurde zum berühmtesten offenen Problem der Mathematik. Das **Drei-Körper-Problem** gilt bis heute als eines der schwierigsten Probleme, die zahlreichen Anstrengungen zu seiner Lösung erfordern und erzeugen immer wieder wichtige neue Methoden.

Newtons Himmelsmechanik: mögliche Lösungsmethoden

N320
Ausführung

Für künstliche Satelliten wird das **zirkuläre restringierte Drei-Körper-Problem** (CR3BP) sehr ausgiebig untersucht: Zwei massereiche Körper umkreisen sich kreisförmig, während der dritte Körper nahezu masselos ist. Hier findet man die berühmten fünf Lagrange–Punkte.

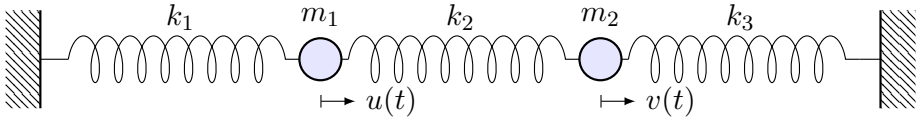
Nur wenige und sehr spezielle Sonderfälle des n–Körper-Problems sind geschlossen lösbar. Auch diese haben ihren eigenen Reiz: Seit 1994 wurden zahlreiche **Choreographien** entdeckt, in denen n Körper symmetrisch angeordnet werden und dann periodische Bahnen durchlaufen. Für generische Anfangsdaten hingegen ist die Bewegung **chaotisch** und kann nur numerisch annähernd berechnet werden. Siehe *Solving the Three Body Problem*, `youtu.be/et7XvBenEo8`.

Zum Kontrast untersuchen und vergleichen wir zwei klassische Anwendungen der Mechanik: Einerseits gekoppelte **lineare Systeme** wie harmonische Oszillatoren N309 N381, andererseits Planetenbewegung und ähnliche **nicht-lineare Systeme**. Nicht-lineare Systeme sind schwierig und verhalten sich oft chaotisch. Lineare Systeme sind besonders gutartig und einfach zu lösen. Daher sollten Sie Linearität wertschätzen, verstehen und nutzen lernen!

Auch nicht-lineare Systeme lassen sich mitunter gut lösen, wie einfache Beispiele zeigen. Dies sind aber Ausnahmen und seltene Glücksfälle. Typischerweise sind nicht-lineare Systeme nicht geschlossen lösbar. Es bleibt dann nur die **numerische Approximation** mit Hilfe geeigneter Näherungsverfahren, z.B. das Euler–Verfahren oder besser gleich das Runge–Kutta–Verfahren. Mehr hierzu erfahren Sie in der Numerik. Aufbauend auf den mathematischen Grundlagen können Sie die Numerik von Differentialgleichungen nutzen und wo nötig vertiefen.

Allgemeine Grundlagen und konkrete Anwendungen ergänzen sich wunderbar.

Gekoppelte Oszillatoren als dynamisches System



Zwei Massen $m_1, m_2 > 0$ sind durch Federn $k_1, k_2, k_3 > 0$ verbunden.

Aufgabe: Formulieren Sie das hier skizzierte dynamische System...
(0) als Bewegungsgleichung sowie (1) als DGSystem erster Ordnung.
(2) Welche Struktur hat die Lösungsmenge? (a) „Form“ und (b) „Größe“?

Lösung: (0) Auslenkungen $u(t), v(t)$ aus der Ruhelage. Kräftebilanz:

$$F_1(t) = -k_1\,u(t) - k_2\big[u(t) - v(t)\big]$$
$$F_2(t) = -k_3\,v(t) - k_2\big[v(t) - u(t)\big]$$

Bewegungsgesetz: $m_1\ddot{u}(t) = F_1(t)$ und $m_2\ddot{v}(t) = F_2(t)$. Hieraus folgt:

$$\ddot{u}(t) = -\tfrac{k_1+k_2}{m_1}\,u(t) + \tfrac{k_2}{m_1}\,v(t)$$
$$\ddot{v}(t) = +\tfrac{k_2}{m_2}\,u(t) - \tfrac{k_2+k_3}{m_2}\,v(t)$$

🙂 Zur Vereinfachung betrachten wir keine Reibung oder äußere Kräfte.

Gekoppelte Oszillatoren als dynamisches System

(1) Wir haben ein (lineares) DGSystem zweiter Ordnung:

$$\begin{cases} \ddot{u}(t) = a\,u(t) + b\,v(t) \\ \ddot{v}(t) = c\,u(t) + d\,v(t) \end{cases}$$

Neue Variablen $x_1 = u$, $x_2 = v$, $x_3 = \dot{u}$, $x_4 = \dot{v}$ reduzieren dies zu:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a & b & 0 & 0 \\ c & d & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}, \quad \text{kurz} \quad \dot{x} = A\,x$$

Das DGSystem (1) ist einfacher als (0), da erster Ordnung. Unser System $\dot{x} = Ax$ ist homogen linear mit Systemmatrix $A \in \mathbb{R}^{4\times4}$. Hier sind die Koeffizienten konstant, das heißt, sie hängen nicht von der Zeit t ab. Für solche homogen-linearen DGSysteme mit konstanten Koeffizienten entwickeln wir mit Hilfe der Linearen Algebra exakte und zudem effiziente Lösungsmethoden: Wie in der folgenden Aufgabe nutzen wir dazu Eigenvektoren und alle zugehörigen Techniken. Der grundlegende Existenz- und Eindeutigkeitssatz N3G erklärt ganz allgemein die Struktur:

(2) Die Lösungsmenge ist (a) ein $\mathbb{R}$–Vektorraum (b) der Dimension 4.

Gekoppelte Oszillatoren: Symmetrie und Ansatz

Aufgabe: (3) Lösen Sie den symmetrischen Fall $m_1 = m_2$, $k_1 = k_3$.
(4) Welche Bewegung folgt aus $u(0) = 2$, $v(0) = 0$, $\dot{u}(0) = \dot{v}(0) = 0$?

Lösung: Einstweilen nutzen wir unsere physikalische Anschauung!

(3a) Der Ansatz $u = v$ entkoppelt zu $\ddot{u} = -\frac{k_1}{m_1}u$, $\ddot{v} = -\frac{k_1}{m_1}v$.
Lösungen: $u_1(t) = \cos(\omega_1 t)$ und $u_2(t) = \sin(\omega_1 t)$ mit $\omega_1^2 = \frac{k_1}{m_1}$.

(3b) Der Ansatz $u = -v$ entkoppelt zu $\ddot{u} = -\frac{k_1+2k_2}{m_1}u$, $\ddot{v} = -\frac{k_1+2k_2}{m_1}v$.
Lösungen: $u_3(t) = \cos(\omega_2 t)$ und $u_4(t) = \sin(\omega_2 t)$ mit $\omega_2^2 = \frac{k_1+2k_2}{m_1}$.

Sind wir schon fertig? Ja! Jede Lösung ist eine Linearkombination

$$\begin{bmatrix} u(t) \\ v(t) \end{bmatrix} = \alpha_1 \begin{bmatrix} u_1(t) \\ v_1(t) \end{bmatrix} + \alpha_2 \begin{bmatrix} u_2(t) \\ v_2(t) \end{bmatrix} + \alpha_3 \begin{bmatrix} u_3(t) \\ v_3(t) \end{bmatrix} + \alpha_4 \begin{bmatrix} u_4(t) \\ v_4(t) \end{bmatrix}.$$

🙂 Als **Anfangswerte** zur Zeit t_0 können Position und Geschwindigkeit $u(t_0), v(t_0), \dot{u}(t_0), \dot{v}(t_0) \in \mathbb{R}$ beliebig vorgegeben werden: Sie legen die freien Konstanten $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}$ eindeutig fest (und umgekehrt).

Gekoppelte Oszillatoren: Symmetrie und Ansatz

🙂 Unser DGSystem ist sehr einfach: Die Gleichungen sind linear! Linearkombinationen von Lösungen sind daher wieder Lösungen. Mit anderen Worten: Der Lösungsraum ist ein **Vektorraum** über $\mathbb{R}$.

🙂 Unser **geschickter Ansatz** entkoppelt das Gleichungssystem: Eindimensionale Differentialgleichungen können wir bereits lösen!

Die einfache Rechnung bestätigt und präzisiert unsere physikalische Anschauung: Die Probe ist nun leicht: Einsetzen und Ausrechnen!

🙂 Wir haben vier Lösungen gefunden. Diese sind **linear unabhängig**. Der Lösungsraum hat also Dimension ≥ 4. Gibt es noch mehr?

⚠ Wir wünschen uns ein einfaches Kriterium für Dimension $= 4$. Dann wüssten wir sicher: Wir haben alle Lösungen gefunden!

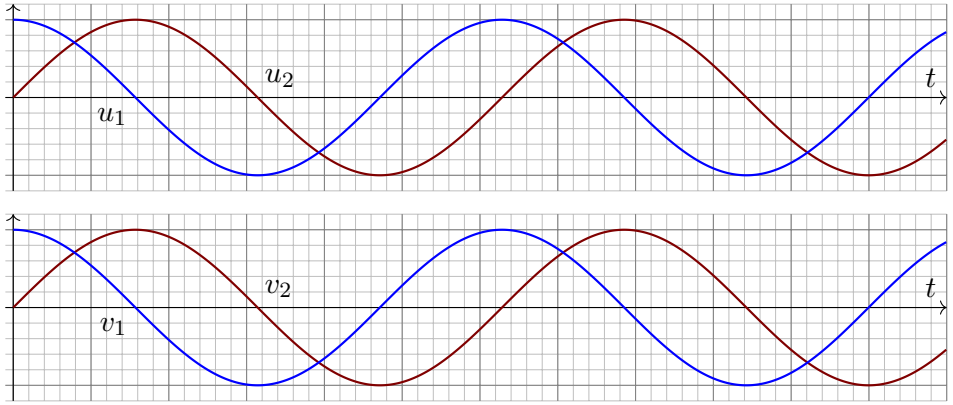
Physikalisch ist das plausibel: Jede Masse hat zur Zeit t_0 eine Position und eine Geschwindigkeit. Diese Daten sollten den weiteren Verlauf eindeutig festlegen. Wir hätten demnach genau 4 Freiheitsgrade.

🙂 Diese Heuristik lässt sich mathematisch formulieren und beweisen: Es gilt der grundlegende **Existenz- und Eindeutigkeitssatz N3G**!

Gekoppelte Oszillatoren: gleichsinnige Eigenschwingungen

N329

Illustration für den Fall $m_1 = m_2 = 1$ und $k_1 = k_2 = k_3 = 1$.
Gleichsinnige Eigenschwingungen zur Frequenz $\omega_1 = 1$:

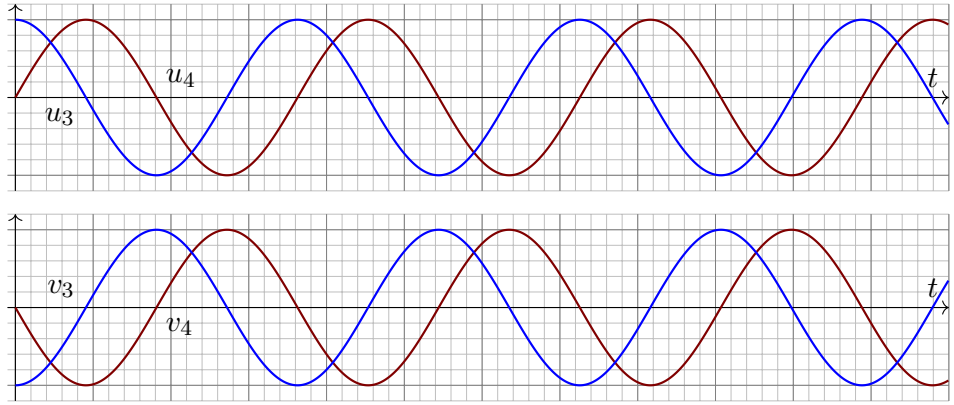


🙂 Die Eigenschwingungen unseres Systems sind besonders leicht zu berechnen. Zudem erweisen sie sich als einfach und übersichtlich: Harmonische Schwingung: Jede dieser vier Lösungen ist periodisch.

Gekoppelte Oszillatoren: gegensinnige Eigenschwingungen

N330

Illustration für den Fall $m_1 = m_2 = 1$ und $k_1 = k_2 = k_3 = 1$.
Gegensinnige Eigenschwingungen zur Frequenz $\omega_2 = \sqrt{3}$:



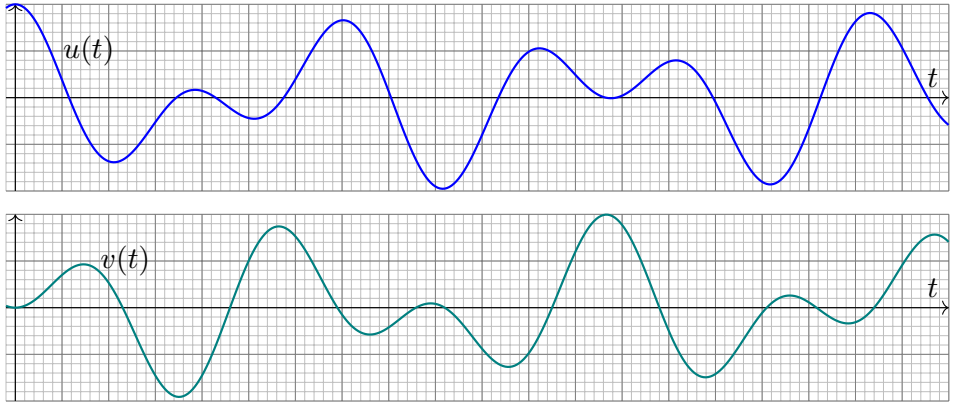
🙂 Die Frequenz der gegensinnigen Schwingung ist deutlich größer als die der gleichsinnigen Schwingung. Das ist anschaulich plausibel; probieren Sie es mal aus! Nun können wir es sogar präzise ausrechnen.

Überlagerung von Eigenschwingungen

N331

(4) Diese Linearkombination von Eigenschwingungen löst das AWP:

$$u(t) = \cos(t) + \cos(\sqrt{3}t), \quad u(0) = 2, \quad \dot{u}(0) = 0$$
$$v(t) = \cos(t) - \cos(\sqrt{3}t), \quad v(0) = 0, \quad \dot{v}(0) = 0$$



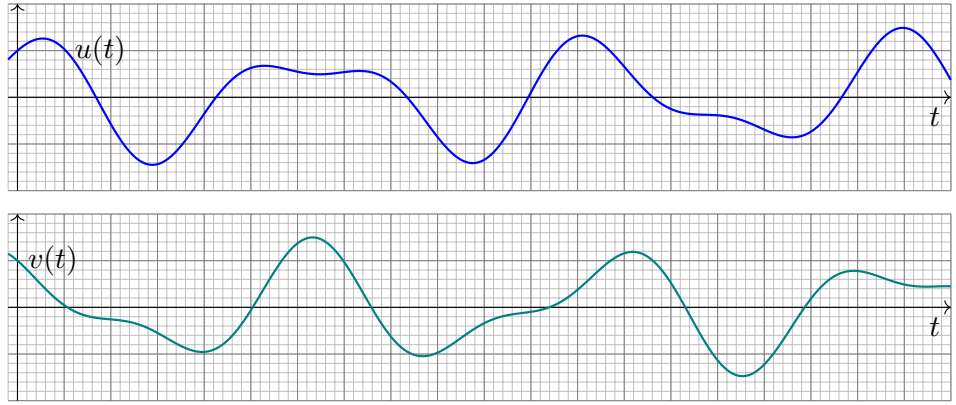
⚠ Diese Bewegung ist nicht periodisch! Sie scheint zuerst kompliziert, ist aber nur die Überlagerung von zwei harmonischen Schwingungen.

Überlagerung von Eigenschwingungen

N332
Erläuterung

Zur Illustration eine weitere Linearkombination von Eigenschwingungen:

$$u(t) = \cos(t) + \tfrac{1}{2}\sin(\sqrt{3}t)$$
$$v(t) = \cos(t) - \tfrac{1}{2}\sin(\sqrt{3}t)$$



🙂 Die Anfangswerte $u(0)$, $\dot{u}(0)$ sowie $v(0)$, $\dot{v}(0)$ können beliebig vorgegeben werden; sie legen den weiteren Verlauf eindeutig fest.

Schwache Kopplung führt zu Schwebungen.

N333
Erläuterung

Aufgabe: (5) Was geschieht bei schwacher Kopplung? Anschaulich? Nehmen Sie weiterhin $m_1 = m_2$ und $k_1 = k_3$ an, zudem $0 < k_2 \ll k_1$.

(6) Berechnen und diskutieren Sie ein konkretes Zahlenbeispiel mit den Massen $m_1 = m_2 = 1$ und den Federn $k_1 = k_3 = 400$ und $k_2 = 20.5$. Welche Bewegung folgt nun aus $u(0) = 2$, $v(0) = 0$, $\dot{u}(0) = \dot{v}(0) = 0$?

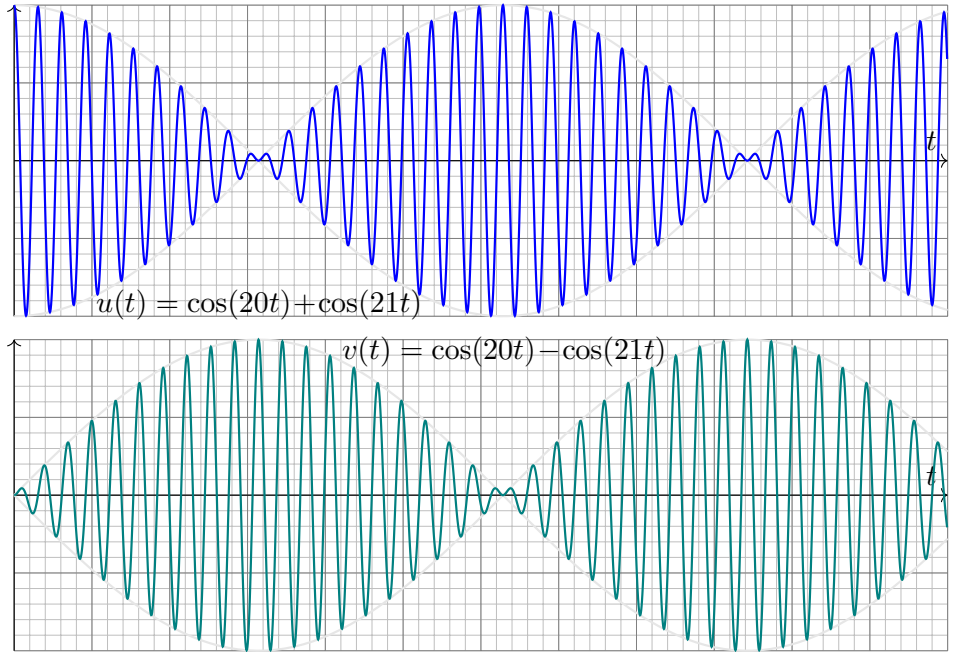
Lösung: (5) Zunächst die *qualitativ-anschauliche Erklärung:* Die beiden Eigenfrequenzen $\omega_1 = \sqrt{k_1/m_1}$ und $\omega_2 = \sqrt{(k_1 + 2k_2)/m_1}$ unseres Systems liegen nahe beieinander, da wir $0 < k_2 \ll k_1$ annehmen.

Wir erwarten eine *Schwebung*: in der Überlagerung $\cos(\omega_1 t) + \cos(\omega_2 t)$ nimmt die gesamte Amplitude der Summe periodisch zu und ab, additive Phasen und subtraktive Phasen wechseln sich ab.

(6) *Quantitativ-numerisches Beispiel:* Wir finden $\omega_1 = 20$ und $\omega_2 = 21$. Das Anfangswertproblem $u(0) = 2$, $v(0) = 0$ und $\dot{u}(0) = \dot{v}(0) = 0$ wird gelöst durch $u(t) = \cos(20t) + \cos(21t)$ und $v(t) = \cos(20t) - \cos(21t)$. Die folgenden Graphiken illustrieren den zeitlichen Verlauf für $t \in [0, 12]$.

Schwache Kopplung führt zu Schwebungen.

N334
Erläuterung



Schwache Kopplung führt zu Schwebungen.

N335
Erläuterung

Anschaulich geschieht hier folgendes: Wir können den linken Oszillator auslenken und dann loslassen. Er schwingt daraufhin nahezu frei, doch nach und nach überträgt sich (fast) seine gesamte Energie auf den rechten Oszillator, anschließend geschieht dasselbe umgekehrt.

Aufgabe: (7) Erklären Sie das oben skizzierte Phänomen der Schwebungen mit Hilfe der trigonometrischen **Additionstheoreme**.

Lösung: Aus der Euler–Gleichung $\mathrm{e}^{\mathrm{i}\alpha} = \cos\alpha + \mathrm{i}\sin\alpha$ und der Homomorphie $\mathrm{e}^{z+w} = \mathrm{e}^z\,\mathrm{e}^w$ erhalten wir (nach kurzer Rechnung):

$$\begin{aligned}
\cos\alpha + \cos\beta &= 2\cos\frac{\alpha-\beta}{2}\,\cos\frac{\alpha+\beta}{2}\\
\cos\alpha - \cos\beta &= -2\sin\frac{\alpha-\beta}{2}\,\sin\frac{\alpha+\beta}{2}\\
\sin\alpha + \sin\beta &= 2\cos\frac{\alpha-\beta}{2}\,\sin\frac{\alpha+\beta}{2}\\
\sin\alpha - \sin\beta &= 2\sin\frac{\alpha-\beta}{2}\,\cos\frac{\alpha+\beta}{2}
\end{aligned}$$

Schwache Kopplung führt zu Schwebungen.

N336
Erläuterung

In unserem Zahlenbeispiel erhalten wir:

$$\begin{aligned}
u(t) &= \cos(20t) + \cos(21t) = 2\cos(0.5t)\cdot\cos(20.5t)\\
v(t) &= \cos(20t) - \cos(21t) = -2\sin(0.5t)\cdot\sin(20.5t)
\end{aligned}$$

Wir interpretieren daher die Überlagerung $u(t) = A(t)\cos(20.5t)$ als eine Grundschwingung der mittleren Frequenz $\bar{\omega} = \frac{1}{2}(\omega_1 + \omega_2) = 20.5$ mit der variablen Amplitude $A(t) = 2\cos(0.5t)$; diese hat die deutlich niedrigere Frequenz $\delta = \frac{1}{2}|\omega_1 - \omega_2| = 0.5$, sodass $\omega_{1/2} = \bar{\omega} \mp \delta$ gilt.

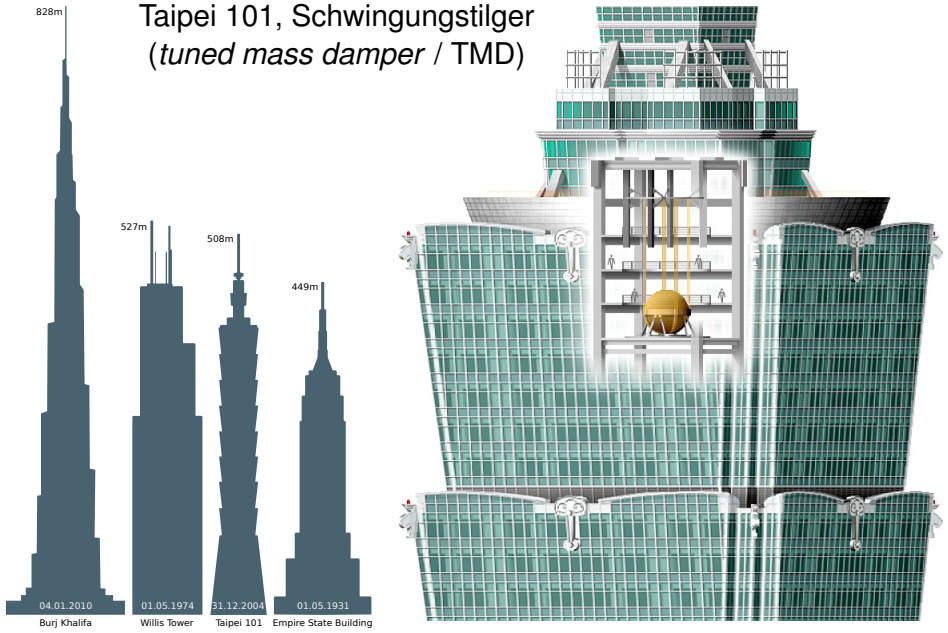
Diese Rechnung ist in der obigen Graphik schön anschaulich illustriert durch die Trägerschwingung $\cos(20.5t)$ und die Einhüllende $\pm 2\cos(0.5t)$.

Das Phänomen der Schwebung entsteht immer, wenn sich zwei ähnlich große Schwingungen mit nahezu gleichen Frequenzen überlagern.

In der Akustik sind solche Schwebungen deutlich zu hören: Der Ton ist moduliert, seine Lautstärke schwankt mit der Schwebungsfrequenz, was mitunter als recht unangenehm empfunden wird. Das ist keine akustische Täuschung, sondern ein reales physikalisches Phänomen.

Anwendung in Wolkenkratzern: Schwingungstilger

N337
Erläuterung



Anwendung in Wolkenkratzern: Schwingungstilger

N338
Erläuterung

Gebäude werden zu Schwingungen angeregt, extern durch Wind oder Erdbeben, intern durch Menschen oder Maschinen. Dagegen helfen **Schwingungstilger**, justiert auf die Eigenfrequenz des Gebäudes. Berlins Fernsehturm hat in seiner Spitze ein 1.5-Tonnen-Tilgerpendel. Londons Millennium Bridge, 2000 eröffnet und *wobbly bridge* genannt, wurde nachträglich mit 52 kleinen *tuned mass dampers* ausgestattet.

Das Taipei Financial Center in Taiwan hielt ab 2004 den Rekord des höchsten Gebäudes der Welt, bis es 2009 vom Burj Khalifa überholt wurde. Zwischen dem 88. und 92. Stockwerk befindet sich eine 660 Tonnen schwere Stahlkugel als Pendel mit ölhydraulischer Dämpfung. Es ist öffentlich zugänglich und eine beliebte Touristen-Attraktion.

Das Gebäude überträgt Schwingungsenergie auf diesen Oszillator, der sie absorbiert und dann durch Dämpfung in Wärme umwandelt. Die maximale Beschleunigung bei Stürmen wird so etwa halbiert! (Taiwan ist sowohl aktive Erdbebenregion als auch Taifungebiet.) Ein Video sagt mehr als tausend Worte: `youtu.be/f1U4SAgy60c`.

Anwendung im Schiffsbau: frahmscher Schlingertank

N339
Erläuterung

Wasserwellen regen ein Schiff zu Schwingungen an:

1. Das Schiff „rollt“ um seine Längsachse,
   kippt also nach links (Backbord) und rechts (Steuerbord).
2. Das Schiff „stampft“ um seine Querachse,
   neigt sich also nach vorne (zum Bug) und hinten (zum Heck).

Wenn die anregende Frequenz des Seegangs unglücklich nah an der Eigenfrequenz des Schiffes liegt, so kommt es zur Resonanz. Um eine Katastrophe zu verhindern, möchte man vorsorgen und die auftretenden Resonanzen so weit wie möglich abschwächen.

Für die Rollbewegung um die Längsachse gelingt dies recht effizient mit zwei raffiniert gekoppelten Schwingungen. Hierzu entwickelte der deutsche Schiffsbauer Hermann Frahm (1867–1939) um 1900 den sogenannten frahmschen **Schlingertank**. Dieser besteht aus zwei Wassertanks an den Längsseiten des Schiffes, die möglichst hoch liegen und über Rohre kommunizieren. Hierin füllt man Wasser, bis die Eigenfrequenz des Tanks der des Schiffes entspricht.

Anwendung im Schiffsbau: frahmscher Schlingertank

N340
Erläuterung

Seitlich auftreffende Wellen regen das Schiff zum Rollen an.
Im Resonanzfall erzwingt dies eine Schwingung des Schiffes mit der Phasenverschiebung um $\pi/2$ gegenüber der Anregung. Das rollende Schiff lässt nun seinerseits das Ballastwasser im Tank periodisch hin- und herströmen, ebenso mit einer Phasenverschiebung um $\pi/2$.

Die äußere Anregung und die innere Schwingung des Tanks sind daher gegenphasig. Die so wirkenden entgegengesetzten Drehmomente heben sich weitgehend auf, was die Rollbewegung deutlich verringert.

Die Grundidee ist genial-einfach und in unserem mathematischen Modell gut nachzuverfolgen. Die technische Ausführung erfordert die geeignete Kalibrierung der Parameter und ist eine eigene Kunst.

Das gesamte System ist in Wirklichkeit nicht-linear: Die Frequenz des Schiffes und des Ballastwasser hängen von der Amplitude ab, dadurch wird ihr Zusammenspiel recht kompliziert. Das Prinzip ist jedoch gleich.

Existenz und Eindeutigkeit dank Exponentialfunktion

N341

Zu lösen sei das folgende Differentialgleichungssystem mit konstanten Koeffizienten $A \in \mathbb{K}^{n\times n}$ und vorgegebenem Anfangswert $v \in \mathbb{K}^n$:

$$u'(t) = A\,u(t) \quad \text{mit} \quad u(0) = v$$

Aufgabe: (1) Existenz: Finden Sie eine Lösung $u : \mathbb{R} \to \mathbb{K}^n : t \mapsto u(t)$.
(2) Eindeutigkeit: Finden Sie alle Lösungen des Anfangswertproblems.

Idee: Für $n = 1$ haben wir die Exponentialfunktion $a \mapsto \mathrm{e}^a$ genutzt. N219
Nutzen Sie ebenso (noch naiv) die Matrix-Exponentialfunktion $A \mapsto \mathrm{e}^A$.

Lösung: (1) Die Funktion $u : \mathbb{R} \to \mathbb{K}^n : u(t) = \mathrm{e}^{tA}\,v$ ist eine Lösung.
Probe: Es gilt $u(0) = v$ und $u'(t) = A\,\mathrm{e}^{tA}\,v = A\,u(t)$ für alle $t \in \mathbb{R}$.

(2) Sei $\tilde{u} : \mathbb{R} \to \mathbb{K}^n$ eine weitere Lösung. Wir betrachten $w(t) = \mathrm{e}^{-tA}\,\tilde{u}(t)$.
Dank Produktregel erhalten wir $w'(t) = -A\,\mathrm{e}^{-tA} \cdot \tilde{u}(t) + \mathrm{e}^{-tA} \cdot A\tilde{u}(t) = 0$.
Dank Mittelwertsatz ist $w : \mathbb{R} \to \mathbb{K}^n$ konstant, also $\tilde{u}(t) = \mathrm{e}^{tA}\,v = u(t)$.

🙂 Es gibt genau eine Lösung $u : \mathbb{R} \to \mathbb{K}^n$, nämlich $u(t) = \mathrm{e}^{tA}\,v$.

Existenz und Eindeutigkeit dank Exponentialfunktion

N342
Erläuterung

⚠ Wir nutzen die Exponentialfunktion und ihre guten Eigenschaften!
Diese Rechnung ist nicht nur ein eitles Glasperlenspiel, sondern sie löst zwei fundamentale Probleme: Existenz und Eindeutigkeit einer Lösung.

🙂 Im vorigen Beispiel konnten wir vier unabhängige Lösungen raten, dank physikalischer Anschauung durch unseren geschickten Ansatz.
Diese Konstruktion beweist insbesondere die Existenz von Lösungen!

⚠ Dieser heuristische Lösungsansatz verrät uns jedoch noch nicht, ob es nicht vielleicht noch weitere Lösungen gibt, die verborgen auf uns lauern und uns womöglich böse Streiche und Kummer bereiten.

🙂 Unsere Rechnung mit der Matrix-Exponentialfunktion $A \mapsto \mathrm{e}^A$ garantiert, dass es zu jedem Startvektor v genau eine Lösung gibt.
Dieses Argument beweist insbesondere die Eindeutigkeit der Lösung!

🙂 Das ist schon raffiniert: Die *Existenz* der Matrix-Exponentialfunktion beweist die *Eindeutigkeit* der Lösung zu jedem Anfangswertproblems.

Die Exponentialfunktion für Skalare $a \in \mathbb{K}$

N343
Erläuterung

Erinnerung: Sei $a \in \mathbb{K}$. Wir suchen eine Lösung $u : \mathbb{R} \to \mathbb{K}$ der eindimensionalen Differentialgleichung $u'(t) = a\,u(t)$ mit $u(0) = 1$.

Hierzu gibt es genau eine Lösung, nämlich die Funktion $u(t) = \mathrm{e}^{at}$.
Wir nutzen dabei dankend die gute alte, vertraute Exponentialfunktion, am schönsten und bequemsten in ihrer Darstellung als Potenzreihe:

$$\exp : \mathbb{K} \to \mathbb{K} : x \mapsto \exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots$$

Diese Reihe konvergiert für jedes Element $x \in \mathbb{K}$ und definiert so die Exponentialfunktion $\exp : \mathbb{K} \to \mathbb{K}$. Diese Funktion erfreut sich vieler guter Eigenschaften, die Sie bereits kennen und lieben, und in zahlreichen Anwendungen auch liebend gerne nutzen.

🙂 Wir hätten so gerne diese Exponentialfunktion für Matrizen!
In der obigen Aufgabe haben wir ja schon ihren Nutzen erlebt.
Ebenso wird sie sich in weiteren Anwendungen bewähren.

Die Exponentialfunktion für Matrizen $A \in \mathbb{K}^{n\times n}$

N344
Erläuterung

Allgemeiner: Sei nun $A \in \mathbb{K}^{n\times n}$ eine Matrix (zuvor $n = 1$, jetzt $n \geq 2$).
Wir suchen $U : \mathbb{R} \to \mathbb{K}^{n\times n}$ mit $U'(t) = A\,U(t)$ und $U(0) = I$.

⚠ Wünschen ist erlaubt, doch nicht alles, was wir *definieren* können, existiert auch. Den Nachweis der Existenz erbringen wir idealerweise, indem wir das ersehnte Objekt *konstruieren*, so explizit wie möglich.

Als Lösung vermuten wir auch hier die Exponentialfunktion $U(t) = \mathrm{e}^{tA}$.
Am bequemsten wäre hierzu die Darstellung als Potenzreihe:

$$\exp : \mathbb{K}^{n\times n} \to \mathbb{K}^{n\times n} : X \mapsto \sum_{k=0}^{\infty} \frac{X^k}{k!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{3!} + \dots$$

🙂 Als schönes Video von 3Blue1Brown: `youtu.be/O85OWBJ2ayo`
Das sieht verwegen aus, aber es funktioniert ganz wunderbar:

Wir wagen diesen mutigen Schritt und setzen Matrizen nicht nur in Polynome $P \in \mathbb{K}[X]$ ein, sondern hier auch in eine Potenzreihe.

Der folgende Satz garantiert, dass diese Exponentialreihe tatsächlich für jede Matrix konvergiert und alle ersehnten Eigenschaften hat.

Die Exponentialfunktion für Matrizen

Satz N3B: die Exponentialfunktion für Matrizen

Wir arbeiten weiterhin über dem Körper $\mathbb{K} = \mathbb{R}, \mathbb{C}$.

0 Für jede Matrix $A \in \mathbb{K}^{n\times n}$ konvergiert die **Exponentialreihe**

$$\exp(A) := \sum_{k=0}^{\infty} \frac{A^k}{k!} = I + A + \frac{1}{2}A^2 + \frac{1}{3!}A^3 + \frac{1}{4!}A^4 + \dots.$$

1 Zudem gilt der Euler–Grenzwert $(1 + \frac{1}{n}A)^n \to \exp(A)$ für $n \to \infty$.

Die so definierte **Matrix-Exponentialfunktion** $\exp : \mathbb{K}^{n\times n} \to \mathbb{K}^{n\times n}$ erfüllt die von $\exp : \mathbb{R} \to \mathbb{R}$ und $\exp : \mathbb{C} \to \mathbb{C}$ vertrauten Eigenschaften:

2 Die Nullmatrix wird auf die Einheitsmatrix $\exp(0) = I$ abgebildet.

3 Aus $AB = BA$ folgt $\exp(A+B) = \exp(A)\exp(B) = \exp(B)\exp(A)$.

4 Insbesondere gilt $\exp(A)\exp(-A) = \exp(A - A) = \exp(0) = I$.
Somit ist die Matrix $\exp(A)$ invertierbar mit $\exp(A)^{-1} = \exp(-A)$.

5 Die Zuordnung $t \mapsto \exp(tA)$ definiert eine differenzierbare Kurve in $\mathrm{GL}_n \mathbb{K} \subset \mathbb{K}^{n\times n}$ mit $0 \mapsto I$ und $\frac{\mathrm{d}}{\mathrm{d}t}\exp(tA) = A\exp(tA)$.

Die Exponentialfunktion für Matrizen

Satz N3B: die Exponentialfunktion für Matrizen

Die Exponentialfunktion verträgt sich zudem mit Matrix-Operationen:

6 Transposition: $\exp(A^\intercal) = \exp(A)^\intercal$

7 komplexe Konjugation: $\exp(\overline{A}) = \overline{\exp(A)}$

8 Konjugation: $\exp(T^{-1}AT) = T^{-1}\exp(A)T$

9 Determinantenformel: $\det(\exp(A)) = \exp(\mathrm{tr}(A))$

Übung: Rechnen Sie alle Aussagen dieses Satzes sorgsam nach!

🙂 Dies gelingt wörtlich genauso wie für die reelle Exponentialfunktion!

Die Techniken der Analysis benötigen Sie vor allem für die Konvergenz (0,1). Alle weiteren Aussagen (2–9) erhalten Sie, indem Sie termweise rechnen – und dies dürfen Sie: Potenzreihen verhalten sich (innerhalb ihres Konvergenzbereichs) wie Polynome (von unendlichem Grad).

⚠ In $\mathbb{K} = \mathbb{R}, \mathbb{C}$ kommutieren je zwei Elemente, daher spüren Sie dort von der Kommutativität (3) nichts. Für Matrizen ist sie jedoch wesentlich.

Konvergenz der Exponentialfunktion für Matrizen

🙂 Wir wollen die Größe von Matrizen $A \in \mathbb{K}^{n\times n}$ messen und damit insbesondere Fragen der Konvergenz klären. Dazu benötigen wir eine **Matrixnorm**, also eine Abbildung $\|-\| : \mathbb{K}^{n\times n} \to \mathbb{R}$ mit den folgenden vier Eigenschaften für alle Matrizen $A, B \in \mathbb{K}^{n\times n}$ und Skalare $\lambda \in \mathbb{K}$:

N0:	$\|A\| \geq 0 = \|0\|$	(Positivität)
N1:	$\|A\| > 0$ für $A \neq 0$	(Definitheit)
N2:	$\|\lambda A\| = \|\lambda\| \cdot \|A\|$	(Homogenität)
N3:	$\|A + B\| \leq \|A\| + \|B\|$	(Dreiecksungleichung)
N4:	$\|A \cdot B\| \leq \|A\| \cdot \|B\|$	(Submultiplikativität)

Beispiel: Die **Frobenius–Norm** entspricht der euklidischen Norm:

$$|-| = \|-\|_F : \mathbb{K}^{m\times n} \to \mathbb{R} : A \mapsto \|A\|_F := \sqrt{\textstyle\sum_{i=1}^{m}\sum_{j=1}^{n}|a_{ij}|^2}$$

Auf $\mathbb{K}^{m\times n}$ ist dies eine Norm (N0–3) und zudem submultiplikativ (N4) für je zwei komponierbare Matrizen $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times r}$. (Übung!)
Wir untersuchen Normen und Skalarprodukte später noch genauer.

Konvergenz der Exponentialfunktion für Matrizen

Aufgabe: (0) Folgern Sie die Konvergenz der Matrix-Exponentialreihe.

Lösung: (a) Wir zeigen zuerst die absolute Konvergenz dieser Reihe:

$$\sum_{k=0}^{\infty}\left\|\frac{A^k}{k!}\right\| \overset{\text{N2}}{=} \sum_{k=0}^{\infty}\frac{\|A^k\|}{k!} \overset{\text{N4}}{\leq} \sum_{k=0}^{\infty}\frac{\|A\|^k}{k!} \overset{\text{Def}}{=} \exp(\|A\|) \overset{!}{<} \infty$$

(b) Der Raum $\mathbb{K}^{n\times n}$ ist Cauchy–vollständig bezüglich der Norm $\|-\|$.
(c) Dank (a) konvergiert die Exponentialreihe $\sum_{k=0}^{\infty} A^k/k!$ absolut, und dank (b) konvergiert sie auch in $\mathbb{K}^{n\times n}$. Zudem gilt die Abschätzung:

$$\|\exp(A)\| \overset{\text{Def}}{=} \left\|\sum_{k=0}^{\infty}\frac{A^k}{k!}\right\| \overset{\text{N3}}{\leq} \sum_{k=0}^{\infty}\left\|\frac{A^k}{k!}\right\| \overset{\text{(a)}}{\leq} \exp(\|A\|)$$

🙂 Für konvergente Potenzreihen gelten wunderschöne Rechenregeln: Sie verhalten sich (innerhalb ihres Konvergenzbereichs) wie Polynome!

Insbesondere dürfen wir solche Reihen umordnen, termweise addieren, multiplizieren und differenzieren – wie von Polynomen vertraut.

Genaueres hierzu lernen Sie im ersten Studienjahr der Analysis.
Wir wollen diese überaus nützlichen Rechenregeln dankend nutzen.

Beispiel: Diagonalmatrizen

N349

Aufgabe: Berechnen Sie die Exponentialfunktion $\exp(A)$ einer Diagonalmatrix $A = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ sowie $\exp(tA)$ für $t \in \mathbb{R}$.

Lösung: (0) Die Potenzen der Matrix A sind leicht zu berechnen:

$$A = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix} \quad \Longrightarrow \quad A^k = \begin{bmatrix} \lambda_1^k & & 0 \\ & \ddots & \\ 0 & & \lambda_n^k \end{bmatrix}$$

(1) Hieraus berechnen wir ebenso leicht die Exponentialreihe:

$$\exp(A) = \sum_{k=0}^{\infty} \frac{A^k}{k!} = \begin{bmatrix} \sum_{k=0}^{\infty} \frac{\lambda_1^k}{k!} & & 0 \\ & \ddots & \\ 0 & & \sum_{k=0}^{\infty} \frac{\lambda_n^k}{k!} \end{bmatrix} = \begin{bmatrix} \mathrm{e}^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \mathrm{e}^{\lambda_n} \end{bmatrix}$$

(2) Mit dem Zeitparameter $t \in \mathbb{R}$ im Exponenten erhalten wir:

$$\exp(tA) = \begin{bmatrix} \mathrm{e}^{t\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \mathrm{e}^{t\lambda_n} \end{bmatrix}$$

Beispiel: eine kleine Dreiecksmatrix

N350
Erläuterung

Aufgabe: Berechnen Sie $\exp(A)$ einer 2×2–Dreiecksmatrix.

Lösung: (0) Wir betrachten eine obere 2×2–Dreiecksmatrix:

$$A = \begin{bmatrix} a & c \\ 0 & b \end{bmatrix}, \; A^2 = \begin{bmatrix} a^2 & (a+b)c \\ 0 & b^2 \end{bmatrix}, \; A^3 = \begin{bmatrix} a^3 & (a^2+ab+b^2)c \\ 0 & b^3 \end{bmatrix}, \ldots$$

(1) Wir nehmen zunächst $a \neq b$ an. Per Induktion finden wir dann

$$A^k = \begin{bmatrix} a^k & \frac{a^k - b^k}{a-b} c \\ 0 & b^k \end{bmatrix} \quad \Longrightarrow \quad \exp \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} = \begin{bmatrix} \mathrm{e}^a & \frac{\mathrm{e}^a - \mathrm{e}^b}{a-b} c \\ 0 & \mathrm{e}^b \end{bmatrix}.$$

(2) Resonanz: Für $b \to a$ gilt $\frac{\mathrm{e}^a - \mathrm{e}^b}{a-b} \to \mathrm{e}^a$. Für $a = b$ finden wir tatsächlich:

$$A^k = \begin{bmatrix} a^k & k a^{k-1} c \\ 0 & a^k \end{bmatrix} \quad \Longrightarrow \quad \exp \begin{bmatrix} a & c \\ 0 & a \end{bmatrix} = \begin{bmatrix} \mathrm{e}^a & c\,\mathrm{e}^a \\ 0 & \mathrm{e}^a \end{bmatrix}.$$

Für große Matrizen ist diese Rechnung ebenso möglich, aber mühsam. Im Folgenden werden wir hierfür Eigen- und Hauptvektoren nutzen. Diese Werkzeuge erweisen sich auch hier als sehr effizient.

Beispiel: ein nilpotenter Jordan–Block

N351

Aufgabe: Berechnen Sie $\exp(tN)$ einer nilpotenten Jordan–Matrix

$$N = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \; N^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \; N^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \; \ldots$$

Lösung: (1) Es gilt $N^4 = 0$. Die Exponentialreihe bricht hier ab:

$$\exp \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \frac{N^0}{0!} + \frac{N^1}{1!} + \frac{N^2}{2!} + \frac{N^3}{3!} = \begin{bmatrix} 1 & 1 & \frac{1}{2!} & \frac{1}{3!} \\ 0 & 1 & 1 & \frac{1}{2!} \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

(2) Mit dem Zeitparameter $t \in \mathbb{R}$ im Exponenten erhalten wir:

$$\exp(tN) = \begin{bmatrix} 1 & t & \frac{t^2}{2!} & \frac{t^3}{3!} \\ 0 & 1 & t & \frac{t^2}{2!} \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Beispiel: ein allgemeiner Jordan–Block

N352

Aufgabe: Berechnen Sie $\exp(tB)$ einer beliebigen Jordan–Matrix

$$B = \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix} \in \mathbb{K}^{n \times n}.$$

Lösung: (1) Dank $B = \lambda I + N$ und $IN = NI$ erhalten wir

$$\exp(B) = \exp(\lambda I + N) = \exp(\lambda I) \exp(N) = \mathrm{e}^{\lambda} \begin{bmatrix} 1 & 1 & \frac{1}{2!} & \frac{1}{3!} \\ 0 & 1 & 1 & \frac{1}{2!} \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

(2) Mit dem Zeitparameter $t \in \mathbb{R}$ im Exponenten erhalten wir:

$$\exp(tB) = \mathrm{e}^{\lambda t} \begin{bmatrix} 1 & t & \frac{t^2}{2!} & \frac{t^3}{3!} \\ 0 & 1 & t & \frac{t^2}{2!} \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Beispiel: eine euklidische Drehmatrix

N353
Erläuterung

Aufgabe: Lösen Sie das DGSystem $x_1' = -x_2$ und $x_2' = x_1$.

Lösung: Wir lösen das Differentialgleichungssystem $x' = A\,x$ mit

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},\ A^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \dots$$

Hieraus berechnen wir mühelos die Matrix-Exponentialfunktion:

$$\exp(tA) = \begin{bmatrix} 1 - \frac{t^2}{2!} + \frac{t^4}{4!} - \dots & -t + \frac{t^3}{3!} - \frac{t^5}{5!} + \dots \\ t - \frac{t^3}{3!} + \frac{t^5}{5!} - \dots & 1 - \frac{t^2}{2!} + \frac{t^4}{4!} - \dots \end{bmatrix} = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}$$

Die Probe ist leicht: Für die Ableitung gilt wie gewünscht

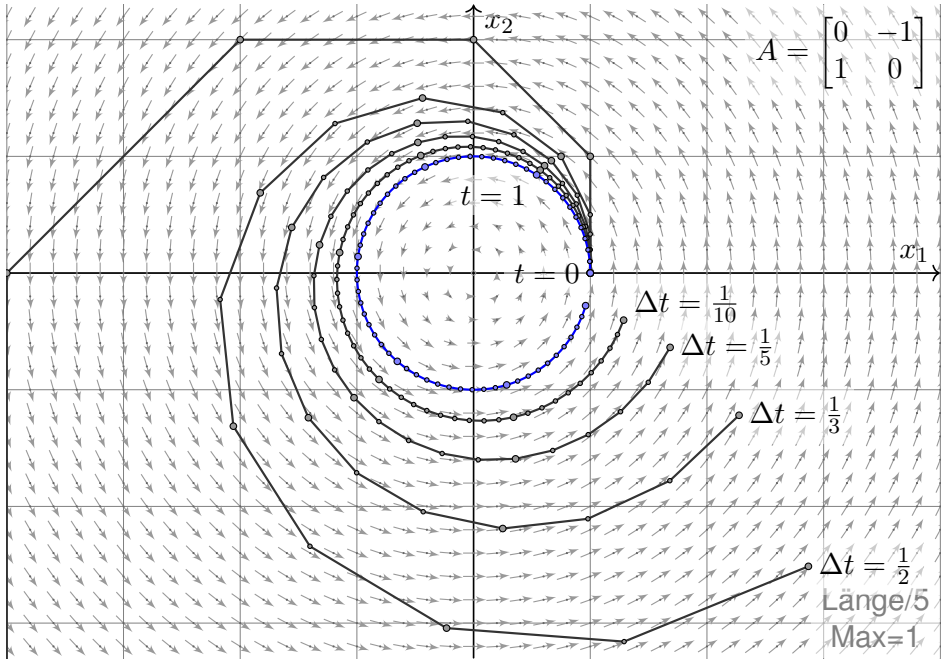
$$\frac{\mathrm{d}}{\mathrm{d}t} X(t) = \begin{bmatrix} -\sin t & -\cos t \\ \cos t & -\sin t \end{bmatrix} = A\,X(t).$$

☺ Das AWP $x' = A\,x$ mit $x(0) = v$ wird gelöst durch $x(t) = \exp(tA)\,v$.

☺ Das Euler–Verfahren zur numerischen Näherung entspricht hierbei dem Euler–Grenzwert $(1 + \frac{1}{n}A)^n \to \exp(A)$ wie in der Graphik illustriert.

Exponentialfunktion und Euler–Verfahren

N354
Erläuterung



Beispiel: eine hyperbolische Drehmatrix

N355
Erläuterung

Aufgabe: Lösen Sie das DGSystem $x_1' = x_2$ und $x_2' = x_1$.

Lösung: Wir lösen das Differentialgleichungssystem $x' = A\,x$ mit

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ A^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ A^3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \dots$$

Hieraus berechnen wir mühelos die Matrix-Exponentialfunktion:

$$\exp(tA) = \begin{bmatrix} 1 + \frac{t^2}{2!} + \frac{t^4}{4!} + \dots & t + \frac{t^3}{3!} + \frac{t^5}{5!} + \dots \\ t + \frac{t^3}{3!} + \frac{t^5}{5!} + \dots & 1 + \frac{t^2}{2!} + \frac{t^4}{4!} + \dots \end{bmatrix} = \begin{bmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{bmatrix}$$

Die Probe ist leicht: Für die Ableitung gilt wie gewünscht

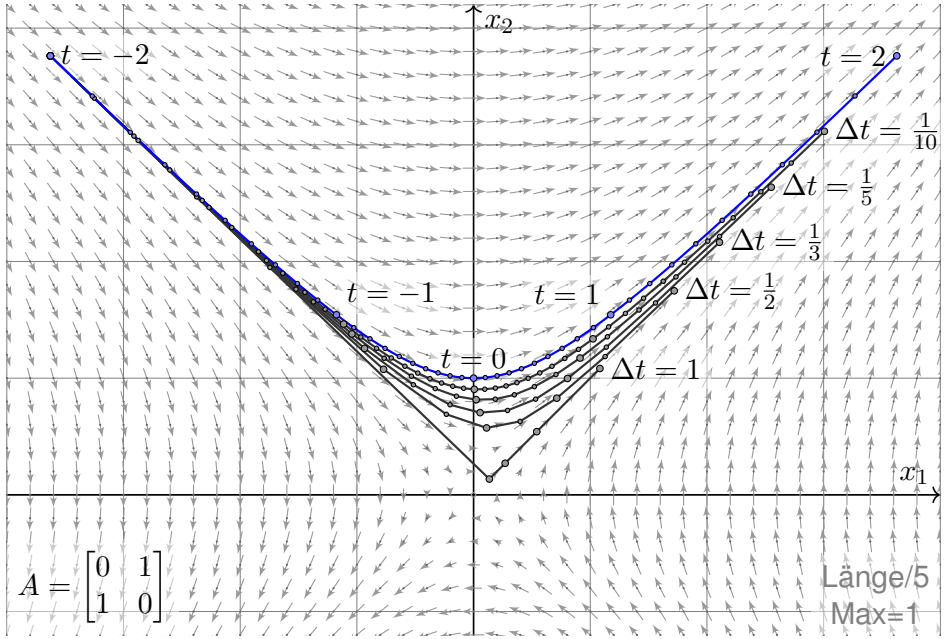
$$\frac{\mathrm{d}}{\mathrm{d}t} X(t) = \begin{bmatrix} \sinh t & \cosh t \\ \cosh t & \sinh t \end{bmatrix} = A\,X(t).$$

☺ Das AWP $x' = A\,x$ mit $x(0) = v$ wird gelöst durch $x(t) = \exp(tA)\,v$.

☺ Das Euler–Verfahren zur numerischen Näherung entspricht hierbei dem Euler–Grenzwert $(1 + \frac{1}{n}A)^n \to \exp(A)$ wie in der Graphik illustriert.

Exponentialfunktion und Euler–Verfahren

N356
Erläuterung



Die Matrix–Exponentialfunktion

N357
Erläuterung

☺ Diese schönen Beispiele illustrieren die Konstruktion von $\exp(A)$ und zeigen zugleich eindrücklich, wie wir die Matrix-Exponentialfunktion in vielen günstigen Fällen ganz explizit und effizient berechnen können.

So ermutigt beweisen wir nun die Aussagen (2–9) des Satzes N3B.
Die Aussagen (3) und (5) formuliere ich untenstehend als Aufgabe.

☺ Das ist eine gute Fingerübung, die jede/r Mathematiker/in im Schlaf beherrschen sollte: Die Rechnungen erweisen sich gleich als erfreulich einfache Umformungen. Das eigentlich Knifflige und das mathematisch Interessante sind die dahinterliegenden Rechenregeln für Potenzreihen!

☺ Wir danken der Analysis für die Bereitstellung guter Werkzeuge.
Wer sie noch nicht gehört hat, darf sich ab jetzt schon darauf freuen.

Bemerkung: Die Konvergenz bezüglich der Matrixnorm $\|-\|$ auf $\mathbb{K}^{n\times n}$ ist äquivalent zur Konvergenz jeder Koordinate im Grundkörper $\mathbb{K}$.

Für Konvergenzfragen sind daher alle Matrixnormen untereinander äquivalent, und wir dürfen uns die jeweils bequemste aussuchen.

Die Matrix–Exponentialfunktion

N358
Erinnerung

Den Euler–Grenzwert (1), also $(1+\frac{1}{n}A)^n \to \exp(A)$ für $n\to\infty$, werde ich hier nicht beweisen, sondern der Analysis überlassen — oder wenn Sie es selbst versuchen wollen: Ihrer mathematischen Abenteuerlust.

Die Aussage (2) des Satzes hingegen ist klar, denn wir haben:

$$\exp(0) \overset{\text{Def}}{=} \sum_{k=0}^{\infty} \frac{0^k}{k!} \overset{\text{Def}}{=} I + 0 + 0 + \ldots = I$$

Dank Funktionalgleichung (3) folgt daraus die Inversionsformel (4):

$$\exp(A)\exp(-A) \overset{(4)}{=} \exp(A-A) \overset{(2)}{=} I$$

Somit ist die Matrix $\exp(A)$ invertierbar mit $\exp(A)^{-1} = \exp(-A)$.

Wir kommen nun zu den interessanten Aussagen (3) und (5).
Diese haben wir in den obigen Beispielen bereits in Aktion gesehen.
Nun wollen wir diese nützlichen Rechenregeln allgemein beweisen.

Die Funktionalgleichung der Exponentialfunktion

N359

Aufgabe: (3) Für je zwei kommutierende Matrizen $A, B \in K^{n\times n}$ gilt:

$$\boxed{\exp(A+B) = \exp(A)\exp(B) \quad \text{falls} \quad AB = BA.}$$

Lösung: Dank (a) Umordnungssatz und (b) binomischem Lehrsatz gilt

$$\begin{aligned}
\exp(A)\exp(B) &\overset{\text{Def}}{=} \left[\sum_{k=0}^{\infty}\frac{A^k}{k!}\right]\left[\sum_{\ell=0}^{\infty}\frac{B^\ell}{\ell!}\right] \overset{\text{Lin}}{=} \sum_{k=0}^{\infty}\sum_{\ell=0}^{\infty}\frac{A^k}{k!}\frac{B^\ell}{\ell!} \\
&\overset{(a)}{=} \sum_{n=0}^{\infty}\sum_{k+\ell=n}\frac{A^k}{k!}\frac{B^\ell}{\ell!} \overset{\text{Def}}{=} \sum_{n=0}^{\infty}\frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}A^k B^{n-k} \\
&\overset{(b)}{=} \sum_{n=0}^{\infty}\frac{1}{n!}(A+B)^n \overset{\text{Def}}{=} \exp(A+B).
\end{aligned}$$

☺ Dies entspricht dem **Potenzgesetz**, daher die Kurzschreibweise

$$\mathrm{e}^A := \exp(A) \qquad \text{und} \qquad \mathrm{e}^{A+B} = \mathrm{e}^A\,\mathrm{e}^B.$$

☺ Das ist wörtlich die Rechnung für die reelle Exponentialfunktion!

Die Ableitung der Exponentialfunktion

N360

Aufgabe: (5) Aus der Exponentialreihe folgt die **Ableitungsregel**

$$\boxed{\frac{\mathrm{d}}{\mathrm{d}t}\exp(tA) = A\exp(tA).}$$

Lösung: Dank (a) Ableitungsregel für Potenzreihen gilt

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}t}\exp(tA) &\overset{\text{Def}}{=} \frac{\mathrm{d}}{\mathrm{d}t}\sum_{k=0}^{\infty}\frac{t^k}{k!}A^k \overset{(a)}{=} \sum_{k=0}^{\infty}\frac{\mathrm{d}}{\mathrm{d}t}\frac{t^k}{k!}A^k \\
&\overset{\text{Abl}}{=} \sum_{k=1}^{\infty}\frac{t^{k-1}}{(k-1)!}A^k \overset{\text{Ind}}{=} A\sum_{j=0}^{\infty}\frac{t^j}{j!}A^j \overset{\text{Def}}{=} A\exp(At).
\end{aligned}$$

Wir nutzen hier die Indexverschiebung $k = j+1$, umgekehrt $j = k-1$.

☺ In Kurzschreibweise erhalten wir die vertraute Formel

$$\frac{\mathrm{d}}{\mathrm{d}t}\,\mathrm{e}^{tA} = A\,\mathrm{e}^{tA}.$$

☺ Das ist eine definierende Eigenschaft der Exponentialfunktion.
Genau diese nutzen wir zur Lösung von Differentialgleichungen!

Aufgabe: Beweisen Sie sorgsam die Aussagen (6–9) des Satzes N3B.

Lösung: (6) Die Transposition $^\intercal : \mathbb{K}^{n\times n} \to \mathbb{K}^{n\times n}$ quadratischer Matrizen ist ein Ringantiautomorphismus, denn es gilt $(A+B)^\intercal = A^\intercal + B^\intercal$ und $(A\cdot B)^\intercal = B^\intercal \cdot A^\intercal$ sowie $(A^\intercal)^\intercal = A$ für alle $A, B \in \mathbb{K}^{n\times n}$. Daraus folgt:

$$\begin{aligned}\exp(A^\intercal) &\overset{\text{Def}}{=} \lim_{N\to\infty}\left[\sum_{k=0}^{N}\frac{(A^\intercal)^k}{k!}\right] \overset{\text{(a)}}{=} \lim_{N\to\infty}\left[\sum_{k=0}^{N}\frac{A^k}{k!}\right]^\intercal \\ &\overset{\text{(b)}}{=} \left[\lim_{N\to\infty}\sum_{k=0}^{N}\frac{A^k}{k!}\right]^\intercal \overset{\text{Def}}{=} \left[\sum_{k=0}^{\infty}\frac{A^k}{k!}\right]^\intercal \overset{\text{Def}}{=} \exp(A)^\intercal\end{aligned}$$

Für die Gleichung (b) nutzen wir die Stetigkeit der Abbildung $^\intercal$.
Wir gehen bei dieser einfachen Rechnung bewusst kleinschrittig vor, so sehen wir genau, welche Eigenschaften wirklich benötigt werden:
Für jeden stetigen Ring(anti)homomorphismus $\Phi : \mathbb{K}^{n\times n} \to \mathbb{K}^{n\times n}$ gilt

$$\boxed{\exp(\Phi(A)) = \Phi(\exp(A)).}$$

(7) Die komplexe Konjugation $^- : \mathbb{C} \to \mathbb{C} : z = x + \mathrm{i}y \mapsto z = x - \mathrm{i}y$ ist ein Körperautomorphismus, denn es gilt $\overline{z+w} = \overline{z} + \overline{w}$ und $\overline{z\cdot w} = \overline{z}\cdot\overline{w}$ sowie $\overline{\overline{z}} = z$ für alle $z, w \in \mathbb{C}$. Für Matrizen über $\mathbb{C}$ definieren wir die komplexe Konjugation koeffizientenweise durch

$$^- : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n} : A = (a_{ij}) \mapsto \overline{A} = (\overline{a_{ij}}).$$

Dies ist ein Ringautomorphismus von $(\mathbb{C}^{n\times n}, +, \cdot)$ und zudem stetig. (Warum? Nachrechnen!) Wie in (6) folgt daraus $\exp(\overline{A}) = \overline{\exp(A)}$.

(8) Für jede invertierbare Matrix $T \in \mathrm{GL}_n\,\mathbb{K}$ ist die Konjugation

$$\mathrm{conj}_T : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n} : A \mapsto T^{-1}AT$$

ein Ringautomorphismus von $(\mathbb{K}^{n\times n}, +, \cdot)$ und stetig. (Warum? Übung!) Wie in (6) folgt daraus $\exp(T^{-1}AT) = T^{-1}\exp(A)T$.

(9) Wir zeigen schließlich die bemerkenswerte Determinantengleichung

$$\boxed{\det(\exp(A)) = \exp(\mathrm{tr}(A)).}$$

(9a) Wir beweisen dies zunächst für Dreiecksmatrizen. Hier gilt:

$$A = \begin{bmatrix} a_{11} & * & * \\ 0 & \ddots & * \\ 0 & 0 & a_{nn} \end{bmatrix} \implies A^k = \begin{bmatrix} a_{11}^k & * & * \\ 0 & \ddots & * \\ 0 & 0 & a_{nn}^n \end{bmatrix}$$

Damit erhalten wir ohne weitere Mühe:

$$\begin{aligned}\det\exp\begin{bmatrix} a_{11} & * & * \\ 0 & \ddots & * \\ 0 & 0 & a_{nn} \end{bmatrix} &\overset{\text{Def}}{=} \det\begin{bmatrix} \exp(a_{11}) & * & * \\ 0 & \ddots & * \\ 0 & 0 & \exp(a_{nn}) \end{bmatrix} \\ &\overset{\text{L2v}}{=} \exp(a_{11})\cdots\exp(a_{nn}) \\ &\overset{\text{(3)}}{=} \exp(a_{11}+\cdots+a_{nn}) \\ &\overset{\text{Def}}{=} \exp(\mathrm{tr}(A))\end{aligned}$$

(9b) Für den allgemeinen Fall nutzen wir Satz M3B:
Über $\mathbb{K} = \mathbb{C}$ ist jede Matrix $A \in \mathbb{K}^{n\times n}$ trigonalisierbar,
es existiert also $T \in \mathrm{GL}_n\,\mathbb{C}$, so dass $T^{-1}AT$ trigonal ist.
Determinante und Spur bleiben dabei unverändert (M2F):

$$\begin{aligned}\det(\exp(A)) &\overset{\text{M2F}}{=} \det(T^{-1}\exp(A)T) \overset{\text{(8)}}{=} \det(\exp(T^{-1}AT)) \\ &\overset{\text{(9a)}}{=} \exp(\mathrm{tr}(T^{-1}AT)) \overset{\text{M2F}}{=} \exp(\mathrm{tr}(A))\end{aligned}$$

(9c) Jede Matrix $A \in \mathbb{R}^{n\times n}$ können wir in $\mathbb{C}^{n\times n}$ betrachten.
Determinante und Spur bleiben dabei unverändert.
Dank (9b) gilt somit $\det(\exp(A)) = \exp(\mathrm{tr}(A))$.

🙂 Wieder einmal fügen sich Theorie und Praxis wunderbar zusammen, solide Grundlagen führen zu hilfreichen Rechenregeln. Dazu betone ich: Im *Beweis* nutzen wir die Trigonalisierung, in *Rechnungen* jedoch nicht.

🙂 Für große Matrizen ist die Berechnung der Exponentialfunktion und der Determinante im Allgemeinen sehr aufwändig. Die Berechnung der Komposition $\det(\exp(A)) = \exp(\mathrm{tr}(A))$ hingegen ist erfreulich leicht!

Von Eigenvektoren zu Eigenfunktionen

Aufgabe: Gegeben seien die Matrix $A \in \mathbb{K}^{n\times n}$ und der Vektor $v \in \mathbb{K}^n$.
Zu lösen ist das Differentialgleichungssystem mit Anfangswert

$$u'(t) = A\,u(t), \quad u(0) = v.$$

Wie sieht die Lösung aus, wenn v ein Eigenvektor von A ist?

Lösung: Nach Voraussetzung gilt $Av = \lambda v$ mit dem Eigenwert $\lambda \in \mathbb{K}$.

(1) Wie betrachten die Funktion $u : \mathbb{R} \to \mathbb{K}^n : t \mapsto u(t) = \mathrm{e}^{\lambda t}\, v$.
Es gilt $u'(t) = \lambda u(t)$ und $Au(t) = \lambda u(t)$, also löst u die ersehnte Differentialgleichung $u'(t) = Au(t)$ mit dem Anfangswert $u(0) = v$.
Dank Eindeutigkeit ist dies *die* Lösung des Anfangswertproblems.

(2) Dieselbe Antwort erhalten wir, wenn wir die Exponentialfunktion e^{tA} auf den Eigenvektor v anwenden und $u(t) = \mathrm{e}^{tA}\, v$ vereinfachen:

$$\mathrm{e}^{tA}v = \left[\sum_{k=0}^{\infty} \frac{t^k}{k!} A^k\right] v = \sum_{k=0}^{\infty} \frac{t^k}{k!} (A^k v) = \sum_{k=0}^{\infty} \frac{t^k}{k!} (\lambda^k v) = \left[\sum_{k=0}^{\infty} \frac{t^k}{k!} \lambda^k\right] v = \mathrm{e}^{t\lambda}$$

Die Konvergenz klärt man wie oben, etwa mit der Frobenius–Norm.

Von Eigenvektoren zu Eigenfunktionen

Satz N3C: Lösung eines DGSystems durch Eigenfunktionen

Gegeben sei $A \in \mathbb{K}^{n\times n}$. Zu lösen sei das DGSystem $u'(t) = A\,u(t)$.

(1) Jeder Eigenvektor $v \in \mathbb{K}^n$ mit $Av = \lambda v$ definiert eine Eigenfunktion

$$u : \mathbb{R} \to \mathbb{K}^n : t \mapsto u(t) = \mathrm{e}^{\lambda t}\, v.$$

Diese löst das DGSystem $u'(t) = A\,u(t)$ mit dem Anfangswert $u(0) = v$.
Zeitlich verschoben zu $\tilde{u}(t) = u(t - t_0)$ gilt $\tilde{u}'(t) = A\,\tilde{u}(t)$ mit $\tilde{u}(t_0) = v$.

(2) Angenommen, die Matrix A ist über $\mathbb{K}$ diagonalisierbar, erlaubt also eine Basis $v_1, \dots, v_n \in \mathbb{K}^n$ aus Eigenvektoren. Dann lösen wir unser DGSystem durch eine Basis aus Eigenfunktionen $u_k(t) = \mathrm{e}^{\lambda_k t}\, v_k$:

Jede Lösung des DGSystems $u'(t) = A\,u(t)$ ist eine Linearkombination $u = c_1 u_1 + \cdots + c_n u_n$ mit eindeutigen Koeffizienten $c_1, \dots, c_n \in \mathbb{K}$.

🙂 Ist die Matrix A diagonalisierbar, so ist damit die Lösung leicht!

☹ Nicht jede Matrix ist diagonalisierbar. Was tun? Hauptvektoren!

Von Hauptvektoren zu Hauptfunktionen

🙂 Eine wichtige Anwendung von Eigen- und Hauptvektoren ist die exakte Lösung linearer Differentialgleichungssysteme $u'(t) = A\,u(t)$:

Satz N3D: Lösung eines DGSystems durch Hauptfunktionen

Gegeben sei $A \in \mathbb{K}^{n\times n}$. Zu lösen sei das DGSystem $u'(t) = A\,u(t)$.
Hierzu sei $0 \xleftarrow{A-\lambda} v_1 \xleftarrow{A-\lambda} v_2 \xleftarrow{A-\lambda} \dots \xleftarrow{A-\lambda} v_\ell$ eine **Hauptvektorkette**.
Diese löst das DGSystem durch die **Hauptfunktionen** $u_1, \dots, u_\ell$ mit

$$u_k(t) = \mathrm{e}^{\lambda t}\left[v_k + t\,v_{k-1} + \frac{t^2}{2} v_{k-2} + \cdots + \frac{t^{k-1}}{(k-1)!} v_1\right].$$

Wie die Hauptvektoren bilden auch die Hauptfunktionen eine Kette:

$$0 \xleftarrow{A-\lambda} u_1 \xleftarrow{A-\lambda} u_2 \xleftarrow{A-\lambda} \dots \xleftarrow{A-\lambda} u_\ell \quad \text{also} \quad Au_k = \lambda u_k + u_{k-1},$$
$$0 \xleftarrow{\partial-\lambda} u_1 \xleftarrow{\partial-\lambda} u_2 \xleftarrow{\partial-\lambda} \dots \xleftarrow{\partial-\lambda} u_\ell \quad \text{also} \quad u_k' = \lambda u_k + u_{k-1}.$$

Es gilt $u_k(0) = v_k$; verschoben zu $\tilde{u}_k(t) = u_k(t - t_0)$ gilt $\tilde{u}_k(t_0) = v_k$.

Von Hauptvektoren zu Hauptfunktionen

Die Hauptvektoren $v_1, \dots, v_\ell \in \mathbb{K}^n$ sind linear unabhängig, daher auch die zugehörigen Hauptfunktionen $u_1, \dots, u_\ell : \mathbb{R} \to \mathbb{K}^n$, denn $u_k(0) = v_k$.

Ist A diagonalisierbar, so existiert eine Basis aus Eigenfunktionen (N3C).
Ist A nicht diagonalisierbar, so doch immerhin noch jordanisierbar:
Über $\mathbb{K} = \mathbb{C}$ finden wir immer eine Basis aus Hauptvektorketten!
Über $\mathbb{K} = \mathbb{R}$ erhalten wir daraus reelle Lösungen, siehe unten.

🙂 Damit ist das zunächst recht schwierige analytische Problem, ein DGSystem $u'(t) = A\,u(t)$ zu lösen, zurückgeführt auf das einfachere algebraische Problem, Hauptvektoren der Matrix A zu berechnen.

🙂 Das ist mitunter mühsam aber letztlich Routinearbeit. Es kann insbesondere von Computer-Algebra-Systemen ausgeführt werden.
In günstigen Fällen gelingt uns die Lösung direkt per Handrechnung.

🙂 Wir erkennen hieran Stabilität und Langzeitverhalten der Lösungen:
Für $\mathrm{Re}(\lambda) < 0$ gilt exponentielles Abklingen, $|u_k(t)| \to 0$ für $t \to \infty$.
Für $\mathrm{Re}(\lambda) > 0$ gilt exponentielles Wachstum, $|u_k(t)| \to \infty$ für $t \to \infty$.
Für $\mathrm{Re}(\lambda) = 0$ ist u_1 beschränkt, aber $u_2, \dots, u_\ell$ wachsen polynomiell.

Anwendungsbeispiel zu Hauptfunktionen

Aufgabe: Finden Sie ein Fundamentalsystem aus Hauptfunktionen zu

(1) $u' = A\,u$ mit $A = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$ und (2) $u' = B\,u$ mit $B = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$.

Wie verhalten sich die Lösungen für $t \to \infty$ und $\lambda < 0$? $\lambda > 0$? $\lambda = 0$?

Lösung: (1) Die Matrix A hat den doppelten Eigenwert λ.
Eigenvektoren bestimmen wir durch $(A - \lambda)v = 0$:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} v = 0, \quad \text{mögliche Lösungen } v_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ v_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Wir erhalten das Fundamentalsystem bzw. die Fundamentalmatrix:

$$u_1(t) = \mathrm{e}^{\lambda t} \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad u_2(t) = \mathrm{e}^{\lambda t} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \Longrightarrow \quad U(t) = \begin{bmatrix} \mathrm{e}^{\lambda t} & 0 \\ 0 & \mathrm{e}^{\lambda t} \end{bmatrix}$$

🙂 Jede andere Basis $(v_1, v_2)^\intercal$ des $\mathbb{C}^2$ wäre hier ebenso möglich.
Sie führt zum Fundamentalsystem $u_1(t) = \mathrm{e}^{\lambda t} v_1$, $u_2(t) = \mathrm{e}^{\lambda t} v_2$.

⚠ Eigenvektoren von A entsprechen Eigenfunktionen von $u' = A\,u$,
aber es sind verschiedene Objekte: Bitte sauber unterscheiden!

Anwendungsbeispiel zu Hauptfunktionen

(2) Auch die Matrix B hat den doppelten Eigenwert λ. Eigenvektoren:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} v_1 = 0, \quad \text{eine Lösung } v_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Wir suchen daher noch einen Hauptvektor v_2 über v_1:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} v_2 = v_1, \quad \text{eine Lösung } v_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Wir erhalten das Fundamentalsystem bzw. die Fundamentalmatrix:

$$u_1(t) = \mathrm{e}^{\lambda t} \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad u_2(t) = \mathrm{e}^{\lambda t} \begin{bmatrix} t \\ 1 \end{bmatrix} \quad \Longrightarrow \quad U(t) = \begin{bmatrix} \mathrm{e}^{\lambda t} & t\,\mathrm{e}^{\lambda t} \\ 0 & \mathrm{e}^{\lambda t} \end{bmatrix}$$

🙂 Andere Wahlen sind möglich: Jeder Vektor $v_1 = (a, 0)^\intercal$ mit $a \neq 0$ ist Eigenvektor, und jeder Vektor $v_2 = (b, a)^\intercal$ liegt darüber als Hauptvektor.

$$u_1(t) = \mathrm{e}^{\lambda t} \begin{bmatrix} a \\ 0 \end{bmatrix},\ u_2(t) = \mathrm{e}^{\lambda t} \begin{bmatrix} at + b \\ a \end{bmatrix} \Longrightarrow U(t) = \begin{bmatrix} a\,\mathrm{e}^{\lambda t} & (at + b)\,\mathrm{e}^{\lambda t} \\ 0 & a\,\mathrm{e}^{\lambda t} \end{bmatrix}$$

⚠ Hauptvektoren von A entsprechen Hauptfunktionen von $u' = A\,u$,
aber es sind verschiedene Objekte: Bitte sauber unterscheiden!

Anwendungsbeispiel zu Hauptfunktionen

Anwendungsbeispiel zu Hauptfunktionen

Von komplexen zu reellen Lösungen

N373
Erläuterung

Zur Vereinfachung rechnen wir meist über den komplexen Zahlen $\mathbb{C}$.
Vorteil: Jede Matrix $A \in \mathbb{C}^{n\times n}$ hat n Eigenwerte $\lambda_1, \dots, \lambda_n \in \mathbb{C}$.

Für eine reelle Matrix $A \in \mathbb{R}^{n\times n}$ werden wir im Allgemeinen nicht n reelle Eigenwerte finden: Wir brauchen auch komplexe Eigenwerte!

Für reelle DGSysteme wollen wir aber meist nur reelle Lösungen!
Diesen Zusammenhang können wir nun klären, wie bereits gesehen:

Lemma N3E: Konjugation von Lösungen und Basiswechsel

(0) Sei $A \in \mathbb{C}^{n\times n}$. Zu lösen sei das DGSystem

$$\boxed{u'(t) = A\,u(t).}$$

Ist u Lösung von $u'(t) = A\,u(t)$, so ist $\overline{u}$ Lösung von $\overline{u}'(t) = \overline{A}\,\overline{u}(t)$.

(1) Genau dann ist die Matrix reell, also $A \in \mathbb{R}^{n\times n}$, wenn $\overline{A} = A$ gilt.
In diesem Fall ist zu u mit $u' = A\,u$ auch $\overline{u}$ mit $\overline{u}' = A\,\overline{u}$ eine Lösung.

Somit sind $\operatorname{Re} u = \frac{1}{2}(u + \overline{u})$ und $\operatorname{Im} u = \frac{1}{2\mathrm{i}}(u - \overline{u})$ reelle Lösungen.
Dies entspricht einem Basiswechsel von $(u, \overline{u})$ zu $(\operatorname{Re} u, \operatorname{Im} u)$.

Von komplexen zu reellen Lösungen

N374
Erläuterung

Satz N3F: reelle Lösungen

Gegeben sei $A \in \mathbb{R}^{n\times n}$. Zu lösen sei das DGSystem $u'(t) = A\,u(t)$.

Sei $0 \xleftarrow{A-\lambda} v_1 \xleftarrow{A-\lambda} \dots \xleftarrow{A-\lambda} v_\ell$ eine Hauptvektorkette zu $\lambda = \sigma + \mathrm{i}\omega$.

Dann ist $0 \xleftarrow{A-\overline{\lambda}} \overline{v_1} \dots \xleftarrow{A-\overline{\lambda}} \overline{v_\ell}$ eine Hauptvektorkette zu $\overline{\lambda} = \sigma - \mathrm{i}\omega$.

Somit hat das DGSystem die folgenden 2ℓ **reellen Lösungen**:

$$\boxed{\begin{aligned}
\operatorname{Re} u_k(t) &= \mathrm{e}^{\sigma t} \operatorname{Re}\left(\mathrm{e}^{\mathrm{i}\omega t} \left[v_k + t\,v_{k-1} + \frac{t^2}{2} v_{k-2} + \dots + \frac{t^{k-1}}{(k-1)!} v_1 \right] \right) \\
\operatorname{Im} u_k(t) &= \mathrm{e}^{\sigma t} \operatorname{Im}\left(\mathrm{e}^{\mathrm{i}\omega t} \left[v_k + t\,v_{k-1} + \frac{t^2}{2} v_{k-2} + \dots + \frac{t^{k-1}}{(k-1)!} v_1 \right] \right)
\end{aligned}}$$

Im Falle $\omega \neq 0$ sind diese 2ℓ Lösungen linear unabhängig. (Im Falle $\omega = 0$ erhalten wir nur eine Kette von ℓ linear unabhängigen Lösungen.)

☺ Wir erkennen hieran Stabilität und Langzeitverhalten der Lösungen, wie oben erklärt, je nach Vorzeichen $\sigma > 0$ oder $\sigma < 0$ oder $\sigma = 0$.

Anwendungsbeispiel: komplex und reell

N375
Erläuterung

Aufgabe: Zu lösen sei das Differentialgleichungssystem

$$\begin{cases} u_1' = -2u_1 + 1u_2, & u_1(0) = 1, \\ u_2' = -1u_1 - 2u_2, & u_2(0) = 2. \end{cases}$$

(1) Finden Sie ein komplexes Fundamentalsystem und (2) ein reelles.
(3) Stabilität: Wie verhalten sich die Lösungen für $t \to \infty$?
(4) Lösen Sie schließlich das AWP.

Lösung: In Matrix-Schreibweise gilt $u' = A\,u$ mit $A = \begin{bmatrix} -2 & 1 \\ -1 & -2 \end{bmatrix}$.
Das charakteristische Polynom der Matrix A ist:

$$\det(A - \lambda E) = \det \begin{bmatrix} -2-\lambda & 1 \\ -1 & -2-\lambda \end{bmatrix} = (-2-\lambda)^2 + 1 = \lambda^2 + 4\lambda + 5$$

Die Nullstellen sind $\lambda_{1/2} = -2 \pm \sqrt{4-5} = -2 \pm \mathrm{i}$. Eigenvektoren?

Zu $\lambda_1 = -2 + \mathrm{i}$: $\begin{bmatrix} -\mathrm{i} & 1 \\ -1 & -\mathrm{i} \end{bmatrix} v_1 = 0$, eine Lösung $v_1 = \begin{bmatrix} 1 \\ \mathrm{i} \end{bmatrix}$

Zu $\lambda_2 = -2 - \mathrm{i}$: $\begin{bmatrix} \mathrm{i} & 1 \\ -1 & \mathrm{i} \end{bmatrix} v_2 = 0$, eine Lösung $v_2 = \begin{bmatrix} 1 \\ -\mathrm{i} \end{bmatrix}$

Anwendungsbeispiel: komplex und reell

N376
Erläuterung

(1) Komplexes Fundamentalsystem des DGSystems:

$$u_1(t) = \mathrm{e}^{(-2+\mathrm{i})t} \begin{bmatrix} 1 \\ \mathrm{i} \end{bmatrix} = \mathrm{e}^{-2t} \begin{bmatrix} +\cos t + \mathrm{i}\sin t \\ -\sin t + \mathrm{i}\cos t \end{bmatrix}, \quad u_2(t) = \mathrm{e}^{(-2-\mathrm{i})t} \begin{bmatrix} 1 \\ -\mathrm{i} \end{bmatrix}$$

(2) Reelles Fundamentalsystem des DGSystems:

$$x_1(t) = \operatorname{Re} u_1(t) = \mathrm{e}^{-2t} \begin{bmatrix} \cos t \\ -\sin t \end{bmatrix}, \quad x_2(t) = \operatorname{Im} u_1(t) = \mathrm{e}^{-2t} \begin{bmatrix} \sin t \\ \cos t \end{bmatrix}$$

(3) Die allgemeine reelle Lösung klingt exponentiell ab:

$$x(t) = X(t)\,c = \mathrm{e}^{-2t} \begin{bmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \quad \text{mit} \quad \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \in \mathbb{R}^2$$

(4) Spezielle Lösung zu den gegebenen Anfangsdaten:

$$x(0) = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \overset{!}{=} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \quad \Longrightarrow \quad x(t) = \mathrm{e}^{-2t} \begin{bmatrix} \cos t + 2\sin t \\ 2\cos t - \sin t \end{bmatrix}.$$

☺ Dies löst das Anfangsgwertproblem. Machen Sie die Probe!

Lösungen eines homogenen Differentialgleichungssystems

Satz N3G: Lösungen eines homogenen DGSystems

Gegeben seien $A \in \mathbb{K}^{n\times n}$. Wir betrachten die Lösungsmenge

$$\boxed{L = \{\, u \in \mathscr{C}^1(I,\mathbb{K}^n) \mid u' = Au \,\}.}$$

(0) **Globale Existenz und Eindeutigkeit**: Zu jedem Anfangsdatum $(t_0, v) \in I \times \mathbb{K}^n$ existiert genau eine Lösung $u \in L$ mit $u(t_0) = v$:

$$\boxed{u(t) = \mathrm{e}^{(t-t_0)A}\, v}$$

Die Auswertung $\Psi_{t_0} : L \xrightarrow{\sim} \mathbb{K}^n : u \mapsto u(t_0)$ ist also eine Bijektion.

(1) $L = \{\, u \mid u' = Au \,\}$ ist ein **Vektorraum** der Dimension n über $\mathbb{K}$. Wir finden ein **Fundamentalsystem** $u_1, \ldots, u_n \in L$, also eine Basis:

$$\boxed{L = \{\, c_1u_1 + \cdots + c_nu_n \mid c_1, \ldots, c_n \in \mathbb{K} \,\} \;\cong\; \mathbb{K}^n}$$

(2) Über $\mathbb{C}$ finden wir explizit eine Basis aus Hauptfunktionen (N3D), über $\mathbb{R}$ entsprechend durch die zugehörigen reellen Lösungen (N3F).

Lösungen eines homogenen Differentialgleichungssystems

⚠ Die Menge $\mathscr{C}^n(I,\mathbb{K})$ aller n–mal stetig diff'baren Funktionen ist ein $\mathbb{K}$–Vektorraum. Allerdings ist er unendlich-dimensional; daher greifen die so erfolgreichen Methoden der Matrizenrechnung wie etwa der Gauß–Algorithmus hier nicht. Wir müssen genauer hinsehen!

🙂 Glücklicherweise ist unser Lösungsraum L endlich-dimensional, und wir können allgemein die Dimension $\dim_{\mathbb{K}}(L) = n$ bestimmen. Bei jeder konkreten Berechnung wissen wir daher genau, wie viele Lösungen wir suchen müssen und wann wir alle gefunden haben!

🙂 Die Dimension $\dim_{\mathbb{K}}(L) = n$ besagt $L \cong \mathbb{K}^n$, zunächst allgemein. Besonders nützlich sind die konkreten Isomorphismen $\Psi_{t_0} : L \xrightarrow{\sim} \mathbb{K}^n$. Wir haben Existenz und Eindeutigkeit oben explizit durchgerechnet.

🙂 Zu Verständnis und Lösung von Differentialgleichungen arbeiten Analysis und Lineare Algebra wunderbar zusammen. Hier wie überall lohnt sich Ihre Investition in solide mathematische Grundlagen.

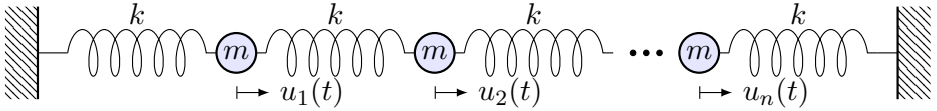
Lösungen eines homogenen Differentialgleichungssystems

Lösungen eines homogenen Differentialgleichungssystems

Gekoppelte Oszillatoren und stehende Wellen

N381

Wir untersuchen die Ausbreitung einer Welle, zum Beispiel einer Druck- oder Schallwelle, zunächst als diskretes, endlich-dimensionales Modell: mit Federn verbundene Massenpunkte. In diesem schönen Beispiel können wir alles explizit berechnen und anschaulich interpretieren. Zudem können wir unsere Methoden der linearen Algebra und Analysis erproben und schärfen.



Aufgabe: (1) Formulieren Sie das hier skizzierte dynamische System als ein lineares Differentialgleichungssystem erster Ordnung.

(2) Welche Struktur hat die Lösungsmenge? (a) „Form“ und (b) „Größe“?

(3) Finden Sie alle Lösungen zum Produktansatz $u_j(t) = \mathrm{e}^{\mathrm{i}\alpha j}\,\mathrm{e}^{\mathrm{i}\omega t}$.

(4) Gewinnen Sie hieraus eine reelle Basis des Lösungsraumes.

Gekoppelte Oszillatoren und stehende Wellen

N382
Übung

Lösung: (1a) Auslenkung $u_j(t) \in \mathbb{R}$ aus der Ruhelage,
lineare Rückstellkraft $F_j = k(u_{j+1} - u_j) + k(u_{j-1} - u_j)$,
Newtons Bewegungsgesetz $F_j = m\ddot{u}_j$. Mit $c^2 = k/m$ erhalten wir

$$\ddot{u}_j(t) = c^2\big[u_{j-1}(t) - 2u_j(t) + u_{j+1}(t)\big] \quad \text{mit} \quad u_0(t) = u_{n+1}(t) = 0.$$

Dies gilt für jeden der Massenpunkte $j = 1, \dots, n$ im Inneren der Kette.
Randbedingung: Die beiden Enden $u_0 = u_{n+1} = 0$ sind hierbei fixiert.

(1b) Diese Bewegungsgleichung ist zweiter Ordnung in n Unbekannten.
Wir reduzieren sie nun äquivalent zu erster Ordnung in $2n$ Unbekannten:

$$\frac{\mathrm{d}}{\mathrm{d}t}\begin{bmatrix} u(t) \\ \dot{u}(t) \end{bmatrix} = \begin{bmatrix} \dot{u}(t) \\ \ddot{u}(t) \end{bmatrix} = \begin{bmatrix} 0_n & I_n \\ c^2 B_n & 0_n \end{bmatrix} \begin{bmatrix} u(t) \\ \dot{u}(t) \end{bmatrix}$$

Für $x = (u, \dot{u})$ ist dies eine homogene lineare Differentialgleichung
$\dot{x}(t) = A\,x(t)$ mit der angegebenen Koeffizientenmatrix $A \in \mathbb{R}^{2n\times 2n}$.
Hier ist 0_n die $(n \times n)$–Nullmatrix und I_n die $(n \times n)$–Einheitsmatrix.

Gekoppelte Oszillatoren und stehende Wellen

N383
Übung

Die Bandmatrix B_n kodiert hierbei die geometrische Anordnung:

$$B_n := \begin{bmatrix} -2 & 1 & 0 & \cdots & \cdots & 0 \\ 1 & -2 & 1 & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 & 0 \\ \vdots & & \ddots & 1 & -2 & 1 \\ 0 & \cdots & \cdots & 0 & 1 & -2 \end{bmatrix} \in \mathbb{R}^{n\times n}$$

(2) Wir suchen $x : \mathbb{R} \to \mathbb{R}^{2n}$ mit $\dot{x}(t) = A\,x(t)$ und $A = \left(\begin{smallmatrix} 0 & I \\ c^2 B & 0 \end{smallmatrix}\right)$.
Die Menge aller Lösungen $x : \mathbb{R} \to \mathbb{R}^{2n}$ ist ein **$\mathbb{R}$–Vektorraum**.
Dank ∃&E-Satz N3G hat dieser Vektorraum die **Dimension** $2n$.
Genauer: Dank Existenz und Eindeutigkeit gehört zu jedem Startwert
$x(0) = (u(0), \dot{u}(0)) \in \mathbb{R}^{2n}$ genau eine Lösungsfunktion $x : \mathbb{R} \to \mathbb{R}^{2n}$.
🙂 Diese Information strukturiert und erleichtert unsere Rechnung:
Wir müssen jetzt nur noch $2n$ linear unabhängige Lösungen finden.
Das DGSystem scheint kompliziert, doch wir können es explizit lösen!

Gekoppelte Oszillatoren und stehende Wellen

N384
Übung

(3) Einsetzen des Produktansatzes $u_j(t) = \mathrm{e}^{\mathrm{i}\omega t}\,\mathrm{e}^{\mathrm{i}\alpha j}$ ergibt:

$$-\omega^2\,\mathrm{e}^{\mathrm{i}\omega t}\,\mathrm{e}^{\mathrm{i}\alpha j} = c^2\big[\mathrm{e}^{\mathrm{i}\omega t}\,\mathrm{e}^{\mathrm{i}\alpha(j-1)} - 2\,\mathrm{e}^{\mathrm{i}\omega t}\,\mathrm{e}^{\mathrm{i}\alpha j} + \mathrm{e}^{\mathrm{i}\omega t}\,\mathrm{e}^{\mathrm{i}\alpha(j+1)}\big] \quad \text{also}$$

$$\omega^2 = -c^2(\mathrm{e}^{-\mathrm{i}\alpha} - 2 + \mathrm{e}^{\mathrm{i}\alpha}) = -c^2(\mathrm{e}^{-\mathrm{i}\alpha/2} - \mathrm{e}^{\mathrm{i}\alpha/2})^2 = 4c^2\sin(\alpha/2)^2$$

Zu jedem α erhalten wir $\omega = \pm 2c\sin(\alpha/2)$. Reelle Lösungen sind:

$$u_j(t) = \begin{cases} \sin(\alpha j)\cos(\omega t), & \cos(\alpha j)\cos(\omega t), \\ \sin(\alpha j)\sin(\omega t), & \cos(\alpha j)\sin(\omega t), \end{cases}$$

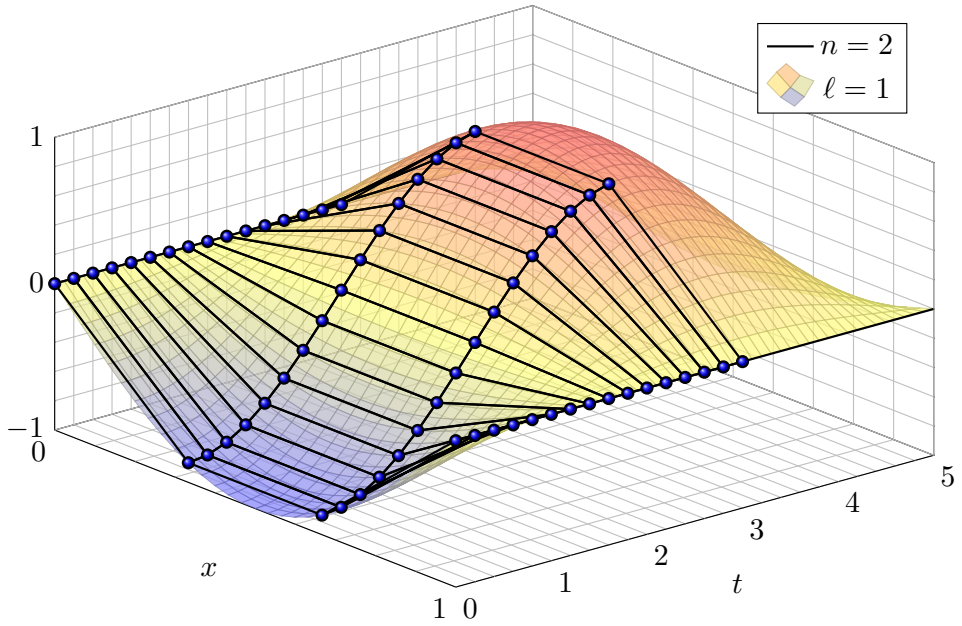
Randbedingungen: Die beiden linken Lösungen erfüllen $u_0(t) = 0$,
und $u_{n+1}(t) = 0$ für $\alpha = \ell\pi/(n+1)$ und $\ell = 1, \dots, n$. **Eigenfunktionen**:

$$\left.\begin{aligned} u_{\ell,j}(t) &= \sin(\alpha_\ell j)\cos(\omega_\ell t) \\ v_{\ell,j}(t) &= \sin(\alpha_\ell j)\sin(\omega_\ell t) \end{aligned}\right\} \quad \text{mit} \quad \begin{cases} \alpha_\ell = \ell\pi/(n+1), \\ \omega_\ell = 2c\sin(\alpha_\ell/2). \end{cases}$$

(4) Dies sind $2n$ linear unabhängige Lösungen, also eine **Basis**!
Je zwei unabhängige Eigenfunktionen, $\partial_t^2 u_\ell = -\omega_\ell^2 u_\ell$, $\partial_t^2 v_\ell = -\omega_\ell^2 v_\ell$.
Die doppelten Eigenwerte $\omega_1^2 < \omega_2^2 < \cdots < \omega_n^2$ sind verschieden.
Daher sind die zugehörigen Eigenfunktionen linear unabhängig.

Eigenfunktionen: Grundschwingung ($\ell = 1$)

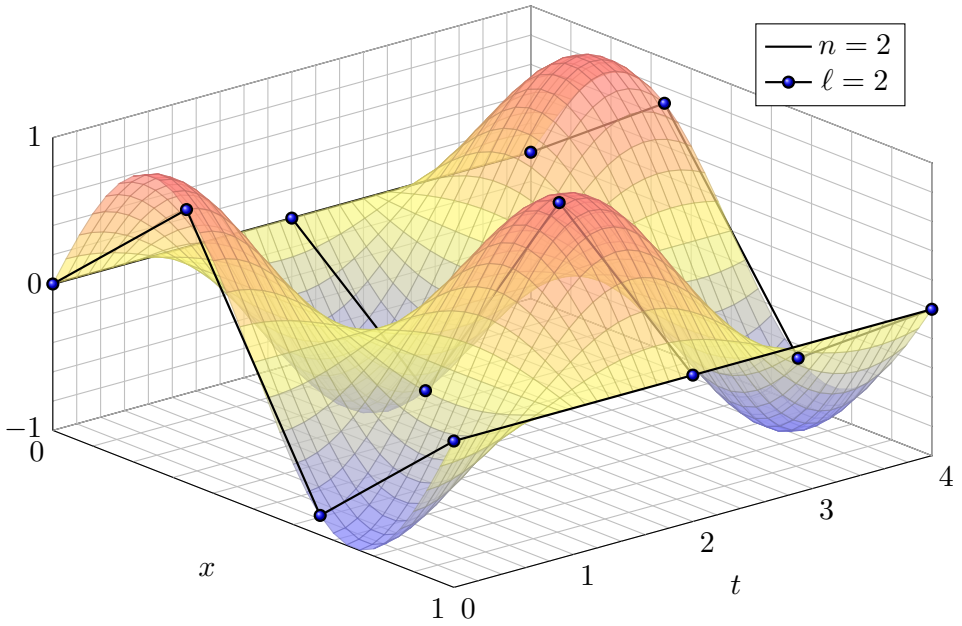
N385



Dies ist eine stehende Welle; Randbedingungen $u_0(t) = u_{n+1}(t) = 0$.

Eigenfunktionen: Oberschwingung ($\ell = 2$)

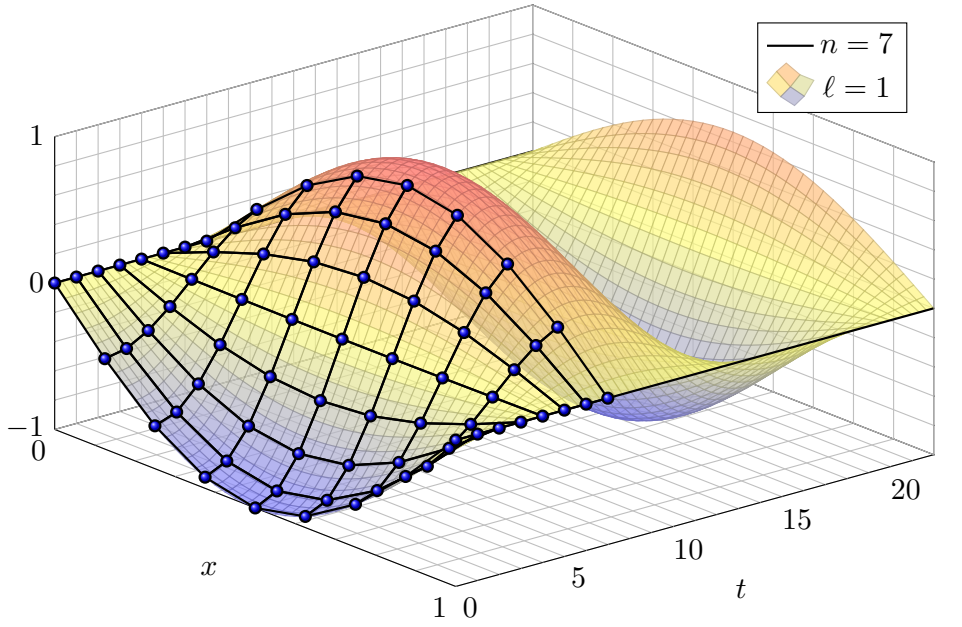
N386



Auch dies ist eine stehende Welle; die Frequenz $\omega_2 > \omega_1$ wird größer.

Eigenfunktionen: Grundschwingung ($\ell = 1$)

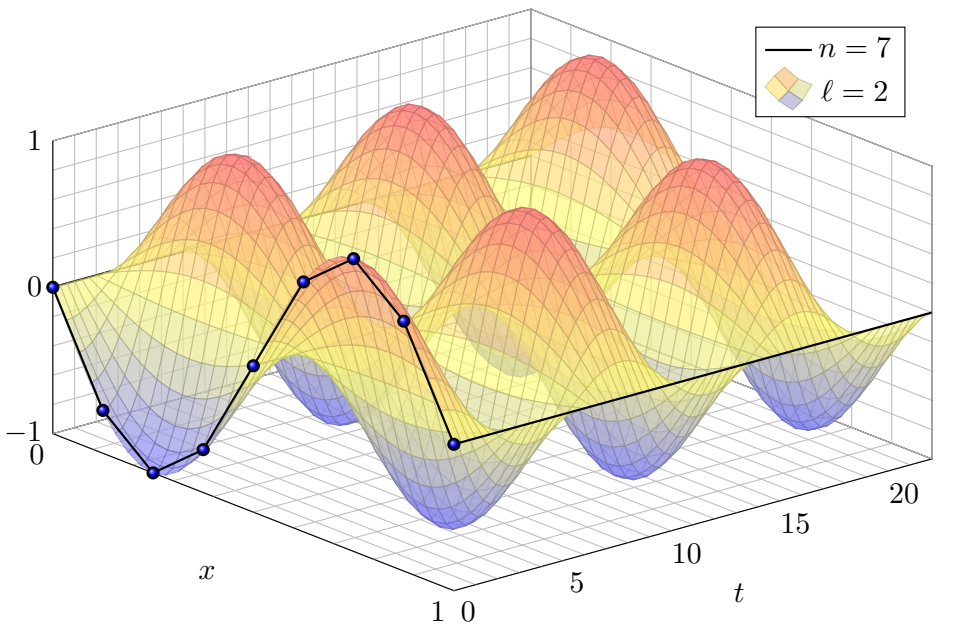
N387



Dieses Phänomen kennt jedes Kind vom Seilspringen. Probieren Sie es!

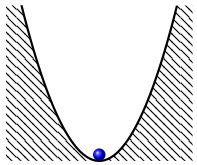
Eigenfunktionen: erste Oberschwingung ($\ell = 2$)

N388

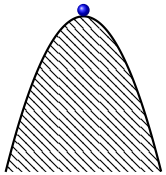


☺ Von der Intuition zur Präzision: Nun können wir alles ausrechnen!

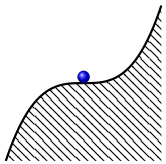
Gleichgewichtslagen und In/Stabilität von Fixpunkten



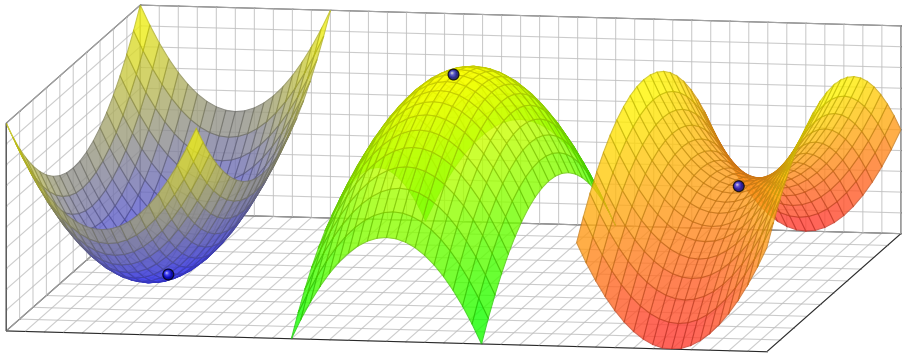
Der Fixpunkt ist stabil / attraktiv.



Der Fixpunkt ist instabil / repulsiv.



kritischer Fixpunkt (höhere Ordnung)



Gleichgewichtslagen und In/Stabilität von Fixpunkten

Anfangsdaten sind oft zufälligen kleinen Schwankungen unterworfen, etwa durch kleine äußere Störungen oder ungenaue Messdaten.

Wir wollen das Langzeitverhalten aller Trajektorien verstehen, die in einer Umgebung des Fixpunktes x_0 starten, also mit $|x(0) - x_0| < \delta$.

- Gilt Abklingen $|x(t) - x_0| \to 0$ für $t \to \infty$? sogar exponentiell?
- Gilt zumindest Beschränktheit $|x(t) - x_0| < \varepsilon$ für alle $t \in \mathbb{R}_{\geq 0}$?
- Oder entkommt $x(t)$ jeder kleinen ε–Umgebung von x_0?

⚠ Instabile Fixpunkte sind meist Opfer des **Schmetterlingseffekts**! Sie zeigen eine extrem sensible Abhängigkeit von den Anfangsdaten. Typischerweise können kleine Störungen exponentiell anwachsen. Beispiele wie $\dot{x}(t) = a\,x(t)$ zeigen, dass dies tatsächlich vorkommt.

⚠ Technische Anwendungen erfordern meist stabile Gleichgewichte! Die **Stabilitätstheorie** untersucht die Auswirkung kleiner Störungen, die als Abweichung von Gleichgewichtszuständen auftreten, etwa in der Technischen Mechanik oder in der Regelungstechnik.

Eindimensionale Dynamik um einen Fixpunkt

Aufgabe: (1) Wir untersuchen $\dot{x}(t) = a\,x(t)$ mit $x(0) = x_0$ und $a \in \mathbb{R}$. Welches asymptotische Verhalten haben die Lösungen für $t \to \infty$?

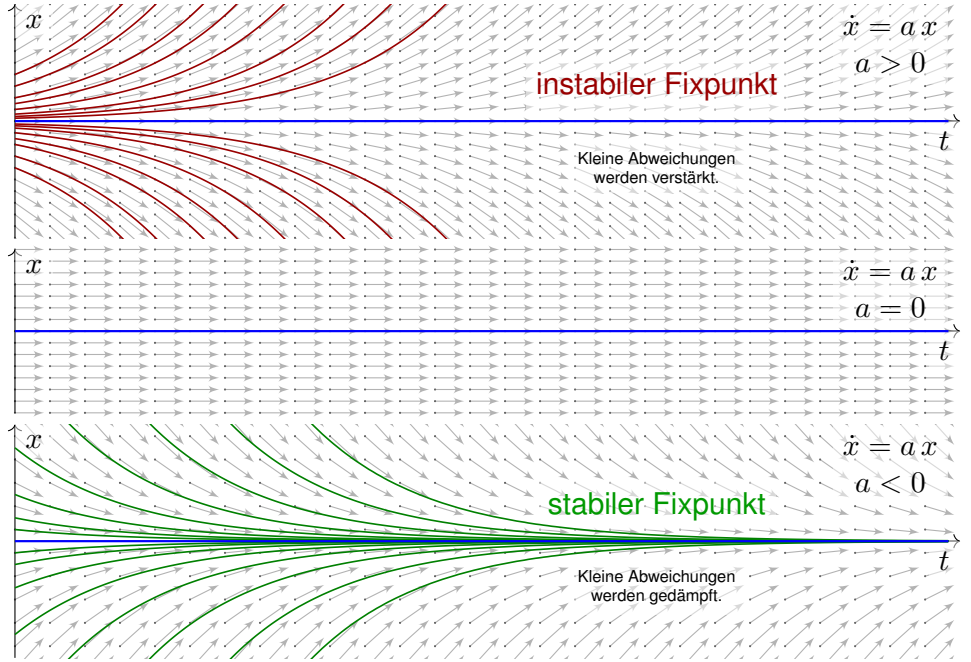
(2) Welches Verhalten erwarten Sie für eine nicht-lineare Gleichung $\dot{x}(t) = f(x(t))$ mit $x(0) = x_0$ und $f(x_0) = 0$? Ist x_0 ein Fixpunkt? Welche Rolle spielt die Ableitung $f'(x_0)$ für die Stabilität?

Lösung: (1) Dieses AWP hat als eindeutige Lösung $x(t) = x_0\,\mathrm{e}^{at}$. Die Dynamik eindimensionaler linearer Systeme ist sehr einfach:

- $a > 0$ streckt; Störungen werden exponentiell verstärkt. Der einzige Fixpunkt 0 ist **instabil**.
- $a < 0$ staucht: Störungen werden exponentiell gedämpft. Der einzige Fixpunkt 0 ist **stabil**.
- Im Falle $a = 0$ ist jeder Startpunkt x_0 ein Fixpunkt.

(2) Nicht-lineare Systeme sind wesentlich komplizierter! In der Nähe eines Fixpunktes können wir linearisieren und annähernd eine **lineare Dynamik** erwarten. Diese Technik wird im Folgenden ausgeführt.

Eindimensionale Dynamik um einen Fixpunkt



Linearisierung um Fixpunkte und In/Stabilität

Wir betrachten ein **autonomes Differentialgleichungssystem**:

$$\dot{x}(t) = f(x(t))$$

Hierbei sei $f : \mathbb{R}^n \supset G \to \mathbb{R}^n$ ein stetig differenzierbares Vektorfeld. Die rechte Seite $f(x)$ hängt nicht explizit von der Zeit t ab, daher **autonom**. Zu jedem Startpunkt $x_0 \in \mathring{G}$ existiert eine eindeutige Lösung $x : [0, T[\to \mathring{G}$ für $T > 0$ mit $x(0) = x_0$ und $\dot{x}(t) = f(x(t))$ für $t \in [0, T[$. Für das maximale T gilt entweder $T = \infty$ oder $f(t) \to \partial G \cup \{\infty\}$ für $t \nearrow T < \infty$.

Aufgabe: Was geschieht bei Start nahe einer Gleichgewichtslage?

Lösung: Jeder Startpunkt x_0 mit $f(x_0) = 0$ ist ein **Fixpunkt**.

Für kleine Auslenkungen $x(t) = x_0 + u(t)$ können wir **linearisieren**:

$$\dot{u}(t) = \dot{x}(t) = f(x(t)) = f(x_0 + u(t)) \approx f(x_0) + f'(x_0)\, u(t) = A\, u(t)$$

Sei $x : [0, T[\to \mathring{G}$ die Lösung zum Startpunkt $x(0) = x_0$ mit $\dot{x}(t) = f(x(t))$ für alle $t \in [0, T[$. **Ruhelage:** Genau dann herrscht Konstanz $x(t) = x_0$ für alle $t \in [0, T[$, wenn $f(x_0) = 0$ gilt. Die **Jacobi–Matrix** $A = f'(x_0) \in \mathbb{R}^{n \times n}$ von f beschreibt das Verhalten um den Fixpunkt x_0: Wir erhalten als Näherung die lineare Differentialgleichung $\dot{u}(t) = A\, u(t)$. Hierdurch erhalten lineare Differentialgleichungssysteme mit konstanten Koeffizienten ihre zentrale Bedeutung!

Linearisierung um Fixpunkte und In/Stabilität

🙂 Kleine Auslenkungen aus der Ruhelage x_0 folgen näherungsweise dem linearen DGSystem mit konstanter Systemmatrix $A = f'(x_0)$:

$$\text{nicht-linear } \dot{x}(t) = f(x(t)) \quad \rightsquigarrow \quad \text{linear } \dot{u}(t) = A\, u(t)$$

🙂 Linearisierung vereinfacht die ursprüngliche Gleichung enorm! Jede Lösung dieser Approximation ist von der Form $u(t) = \mathrm{e}^{tA}\, u_0$. Zu Eigenwerten $\lambda = \sigma \pm \mathrm{i}\omega$ gehören **Eigenfunktionen** der Form

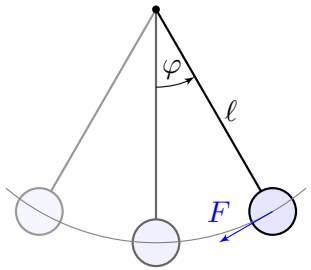
$$u(t) = \mathrm{e}^{\sigma t} \left[\cos(\omega t)\, v_1 + \sin(\omega t)\, v_2\right]$$

🙂 Der allgemeine Fall von **Hauptfunktionen** wurde oben ausgeführt. Damit erkennen wir die **Stabilität** des Fixpunktes:

- $\mathrm{Re}(\lambda) < 0$ staucht; kleine Störungen werden exponentiell gedämpft. Der Fixpunkt ist **stabil**, wenn $\mathrm{Re}(\lambda) < 0$ für alle Eigenwerte gilt.
- $\mathrm{Re}(\lambda) > 0$ streckt; kleine Störungen werden exponentiell verstärkt. Der Fixpunkt ist **instabil**, wenn $\mathrm{Re}(\lambda) > 0$ für einen Eigenwert gilt.

Der Grenzfall $\mathrm{Re}(\lambda_k) = 0$ bedarf genauerer Analyse (höhere Ordnung).

Linearisierung um Fixpunkte und In/Stabilität



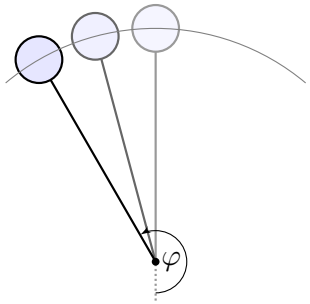
Dynamisches System:

$$\begin{bmatrix}\dot{\varphi}\\ \dot{\omega}\end{bmatrix} = \begin{bmatrix}\omega\\ -(g/\ell)\sin\varphi - 2\delta\omega\end{bmatrix}$$

Linearisierung um $(0, 0)$:

$$\begin{bmatrix}\dot{u}\\ \dot{v}\end{bmatrix} \approx \begin{bmatrix}0 & 1\\ -(g/\ell) & -2\delta\end{bmatrix}\begin{bmatrix}u\\ v\end{bmatrix}$$

Der Fixpunkt $(0, 0)$ ist stabil.



Dynamisches System:

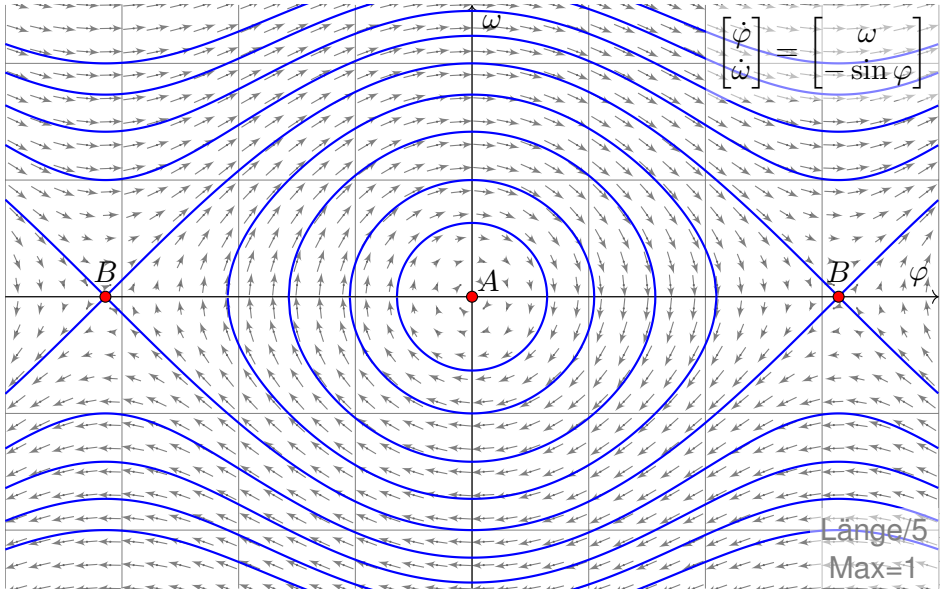
$$\begin{bmatrix}\dot{\varphi}\\ \dot{\omega}\end{bmatrix} = \begin{bmatrix}\omega\\ -(g/\ell)\sin\varphi - 2\delta\omega\end{bmatrix}$$

Linearisierung um $(\pi, 0)$:

$$\begin{bmatrix}\dot{u}\\ \dot{v}\end{bmatrix} \approx \begin{bmatrix}0 & 1\\ +(g/\ell) & -2\delta\end{bmatrix}\begin{bmatrix}u\\ v\end{bmatrix}$$

Der Fixpunkt $(\pi, 0)$ ist instabil.

Linearisierung um Fixpunkte und In/Stabilität



Wir erkennen harmonische Oszillation um das untere Gleichgewicht A. Der obere Scheitelpunkt B hingegen ist ein instabiles Gleichgewicht.

Zweidimensionale Dynamik um einen Fixpunkt

N397

Wir untersuchen das DGSystem $\dot{u}(t) = A\,u(t)$ zur Matrix $A \in \mathbb{R}^{2\times 2}$:
Polynom $\det(A - XI) = X^2 - 2aX + d$, Eigenwerte $\lambda_{1,2} = a \pm \sqrt{a^2 - d}$.
Spur $\operatorname{tr}(A) = 2a$, Determinante $\det(A) = d$, Diskriminante $\Delta = a^2 - d$.

Aufgabe: Skizzieren Sie die Dynamik je nach Lage der Eigenwerte (14 Fälle) und untersuchen Sie das Verhalten von $|u(t)|$ für $t \to \infty$.

- Gilt Abklingen $|u(t)| \to 0$ für $t \to \infty$? sogar exponentiell?
- Gilt Beschränktheit $0 < c_0 \le |u(t)| \le c_1 < \infty$ für alle $t \in \mathbb{R}_{\ge 0}$?
- Oder wächst $|u(t)|$ unbeschänkt? polynomiell? gar exponentiell?

Lösung: Wir unterscheiden zunächst reelle und komplexe Eigenwerte:

$a^2 < d$: komplex-konjugiert $\lambda_{1,2} = a \pm \mathrm{i}b$, $\quad A \sim \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

$a^2 > d$: zwei reelle Eigenwerte $\lambda_1 < \lambda_2$, $\quad A \sim \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$

$a^2 = d$: ein doppelter Eigenwert λ, $\quad A \sim \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$ oder $A \sim \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$

Zweidimensionale Dynamik um einen Fixpunkt

N398
Erläuterung

☺ Damit haben wir alle möglichen Fälle vollständig gelöst!
Dank Eigen- und Hauptfunktionen wird alles klar und einfach.

Ähnlichkeit $A \sim B$ bedeutet, dass A und B konjugiert sind (M2D) ,
also $B = T^{-1}AT$ für eine geeignete Basiswechselmatrix $T \in \mathrm{GL}_2\,\mathbb{R}$.

Dies beschreibt den Übergang zu unserer neuen Basis aus Eigen- bzw. Hauptvektoren, in der sich das Problem wesentlich einfacher darstellt.

☺ Wir finden drei Klassen, je nach Vorzeichen der Diskriminante

$$\Delta = \tfrac{1}{4}(\operatorname{tr} A)^2 - \det A.$$

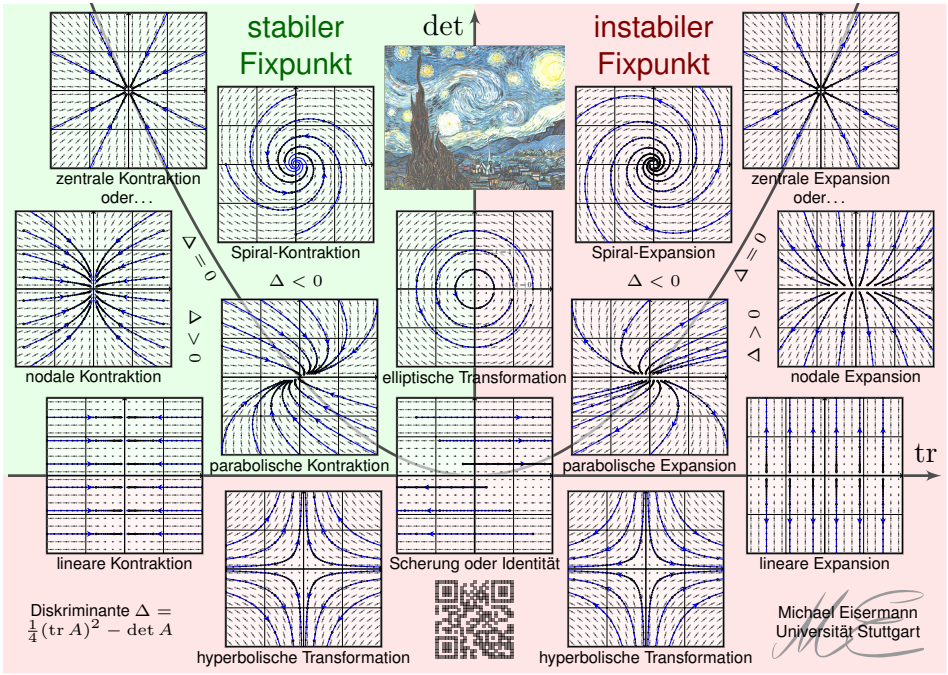
Das Vorzeichen der Diskriminante unterscheidet, wie oben gesehen, zwischen reellen Eigenwerten und (echt) komplexen Eigenwerten.

Der Fixpunkt ist stabil, wenn $\operatorname{Re}(\lambda) < 0$ für beide Eigenwerte gilt.
Das bedeutet: Kleine Störungen werden exponentiell gedämpft.

Das gilt hier genau dann, wenn $\operatorname{tr}(A) < 0$ und $\det(A) > 0$ gilt.
Die stabile Region ist grün gefärbt, die instabile Region rot.

Zweidimensionale Dynamik um einen Fixpunkt

N399



Zweidimensionale Dynamik um einen Fixpunkt

N3100
Erläuterung

Diese schöne Graphik gibt einen guten Überblick: Sie klassifiziert die (linearisierte) Dynamik um einen Fixpunkt in der Ebene $\mathbb{R}^2$.

Im obigen Beispiel des mathematischen Pendels haben wir bereits zwei Fälle gesehen, einen stabilen und einen instabilen Fixpunkt.

Die folgenden Folien diskutieren alle gezeigten Einzelfälle im Detail, wir zoomen also auf einzelne Punkte dieser Gesamtkunstwerks.

⚠ Wir betrachten hier als einfaches Modell die linearisierte Gleichung. Nicht-lineare dynamische Systeme sind meist wesentlich komplizierter!

Dennoch gibt uns das linearisierte Modell sehr nützliche Auskunft, denn im Kleinen verhält sich das nicht-lineare Modell ganz ähnlich:

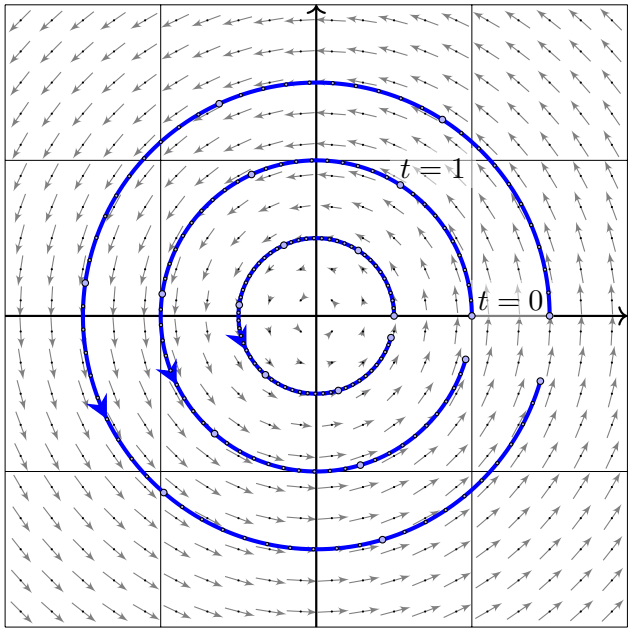
☺ Für die Stabilität des Fixpunktes x_0 genügt die Matrix $A = f'(x_0)$, falls alle Eigenwerte negativen Realteil haben (Satz von Lyapunov).

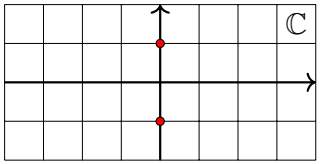
☺ In diesem Falle sieht die lokale Dynamik von $\dot{x} = f(x)$ topologisch aus wie im linearisierten Modell $\dot{u} = Au$ (Satz von Hartman–Grobman).

☺ Dieser Linearisierungssatz gilt ganz allgemein in jeder Dimension n um jeden *hyperbolischen* Fixpunkt (ohne Eigenwerte mit Realteil Null).

Wirbelpunkt: elliptische Transformation

N3101





Komplexe Eigenwerte

$\lambda_{1,2} = \pm \mathrm{i}b$

Allgemeiner Fall

$$A \sim \begin{bmatrix} 0 & -b \\ b & 0 \end{bmatrix}$$

Konkretes Beispiel

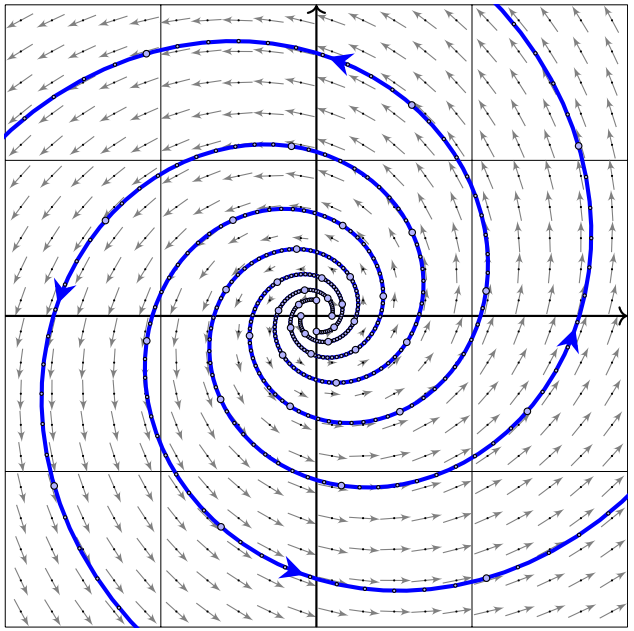
$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

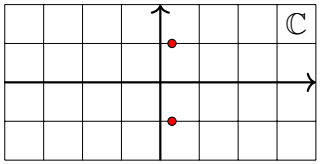
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}$$

Instabiler Strudel: Spiral-Expansion

N3102





Komplexe Eigenwerte

$\lambda_{1,2} = a \pm \mathrm{i}b, \quad a > 0$

Allgemeiner Fall

$$A \sim \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

Konkretes Beispiel

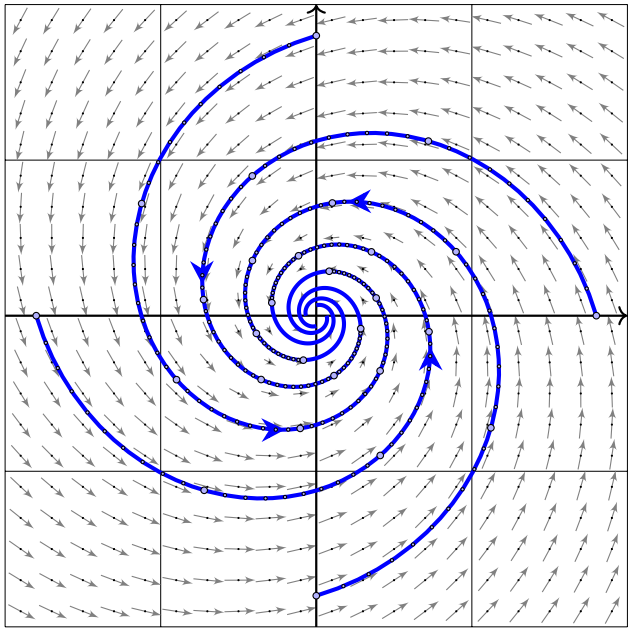
$$A = \begin{bmatrix} 0.3 & -1 \\ 1 & 0.3 \end{bmatrix}$$

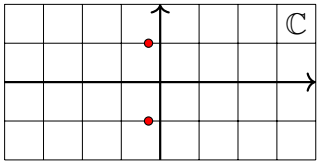
Fundamentalmatrix

$$\mathrm{e}^{0.3t} \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}$$

Stabiler Strudel: Spiral-Kontraktion

N3103





Komplexe Eigenwerte

$\lambda_{1,2} = a \pm \mathrm{i}b, \quad a < 0$

Allgemeiner Fall

$$A \sim \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

Konkretes Beispiel

$$A = \begin{bmatrix} -0.3 & -1 \\ 1 & -0.3 \end{bmatrix}$$

Fundamentalmatrix

$$\mathrm{e}^{-0.3t} \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}$$

Stabilität und Eigenwerte

N3104
Erläuterung

🙂 Die ersten drei Fälle komplex-konjugierter Eigenwerte zeigen bereits den Einfluss auf das Langzeitverhalten und die Stabilität der Lösungen:

- $\mathrm{Re}(\lambda) < 0$ staucht; kleine Störungen werden exponentiell gedämpft. Der Fixpunkt 0 ist **stabil**, wenn $\mathrm{Re}(\lambda) < 0$ für alle Eigenwerte gilt.
- $\mathrm{Re}(\lambda) > 0$ streckt; kleine Störungen werden exponentiell verstärkt. Der Fixpunkt 0 ist **instabil**, wenn $\mathrm{Re}(\lambda) > 0$ für einen Eigenwert gilt.

🙂 Wir diskutieren die verbleibenden Fälle reeller Eigenwerte $\lambda_1 \leq \lambda_2$:

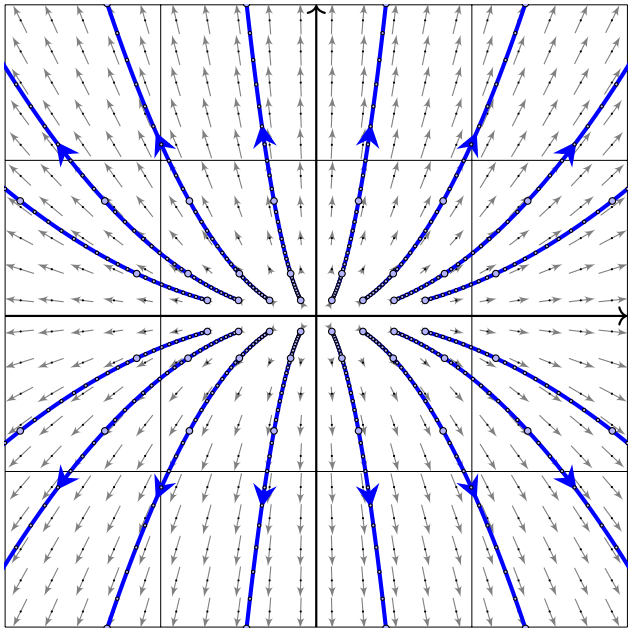
Im Falle $\lambda_1 < \lambda_2$ unterscheiden wir fünf Fälle je nach Lage zu 0:
Die Matrix A ist hierbei wegen $\lambda_1 \neq \lambda_2$ immer diagonalisierbar.

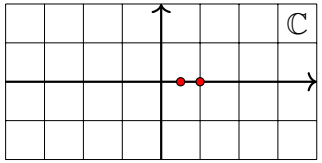
Im Falle $\lambda_1 = \lambda_2$ unterscheiden wir drei Fälle je nach Lage zu 0:
Im einfachsten Falle ist $A \sim \mathrm{diag}(\lambda, \lambda)$ diagonalisierbar (drei Fälle); andernfalls nutzen wir Hauptvektoren zur Jordan–Form (drei Fälle).

🙂 Dank unserer gründlichen Vorarbeit zu Eigen- und Hauptvektoren können wir alle 14 Fälle vollständig lösen und übersichtlich darstellen. Ebenso gelingt die Klassifikation linearer Dynamik in jeder Dimension!

Instabiler Knoten: nodale Expansion

N3105





Zwei reelle Eigenwerte

$0 < \lambda_1 < \lambda_2$

Allgemeiner Fall

$$A \sim \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$

Konkretes Beispiel

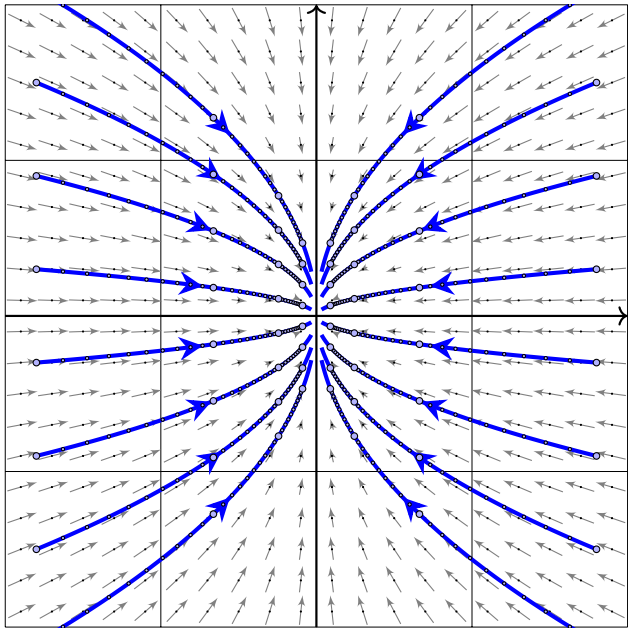
$$A = \begin{bmatrix} 0.5 & 0 \\ 0 & 1 \end{bmatrix}$$

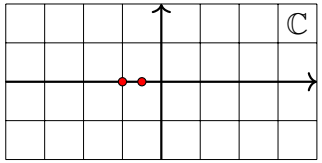
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \mathrm{e}^{t/2} & 0 \\ 0 & \mathrm{e}^{t} \end{bmatrix}$$

Stabiler Knoten: nodale Kontraktion

N3106





Zwei reelle Eigenwerte

$\lambda_1 < \lambda_2 < 0$

Allgemeiner Fall

$$A \sim \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$

Konkretes Beispiel

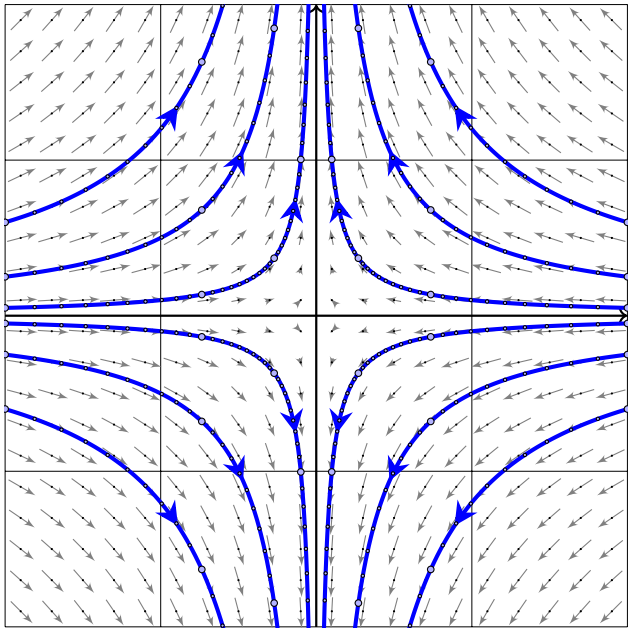
$$A = \begin{bmatrix} -1 & 0 \\ 0 & -0.5 \end{bmatrix}$$

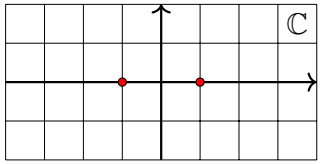
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \mathrm{e}^{-t} & 0 \\ 0 & \mathrm{e}^{-t/2} \end{bmatrix}$$

Sattelpunkt: hyperbolische Transformation

N3107





Zwei reelle Eigenwerte

$\lambda_1 < 0 < \lambda_2$

Allgemeiner Fall

$$A \sim \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$

Konkretes Beispiel

$$A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \mathrm{e}^{-t} & 0 \\ 0 & \mathrm{e}^{t} \end{bmatrix}$$

Eigenwerte und Eigenvektoren

N3108
Erläuterung

🙂 Die hier illustrierten Beispiele zeigen die typische ebene Dynamik um den Fixpunkt $(0,0)^\intercal$ im elliptischen und im hyperbolischen Fall:
Die Eigenwerte geben Auskunft über Dynamik und Stabilität!

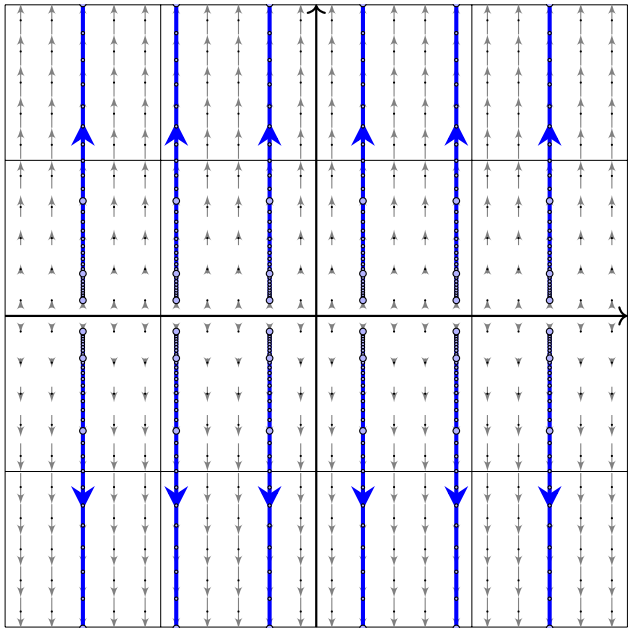
- Sind beide Eigenwerte positiv, so erhalten wir eine Expansion, typischerweise zwei Eigenräume / Achsen: langsam und schnell.
- Sind beide Eigenwerte negativ, so erhalten wir eine Kontraktion, typischerweise zwei Eigenräume / Achsen: langsam und schnell.
- Ist einer negativ und einer positiv, so erhalten wir eine stabile und eine instabile Richtung, wie im hyperbolischen Fall gezeigt.

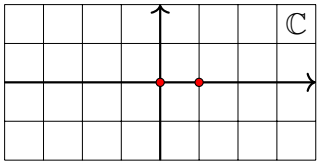
🙂 Die nächsten Folien zeigen schließlich alle Rand- und Sonderfälle.
Zur Vereinfachung transformieren wir die beiden Eigen/Hauptvektoren der Systemmatrix A auf $(1,0)^\intercal$ und $(0,1)^\intercal$; das ist übersichtlicher.

⚠ Im Allgemeinen liegen diese beiden Achsen beliebig in der Ebene; sie sind typischerweise verdreht und stehen nicht senkrecht zueinander.
Nach Koordinatenwechsel entsteht das hier gezeigte, einfache Bild.
Die Aufgabe auf Seite N3117 zeigt ein realistisches Beispiel.

Lineare Expansion

N3109
Erläuterung





Zwei reelle Eigenwerte

$0 = \lambda_1 < \lambda_2$

Allgemeiner Fall

$$A \sim \begin{bmatrix} 0 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$

Konkretes Beispiel

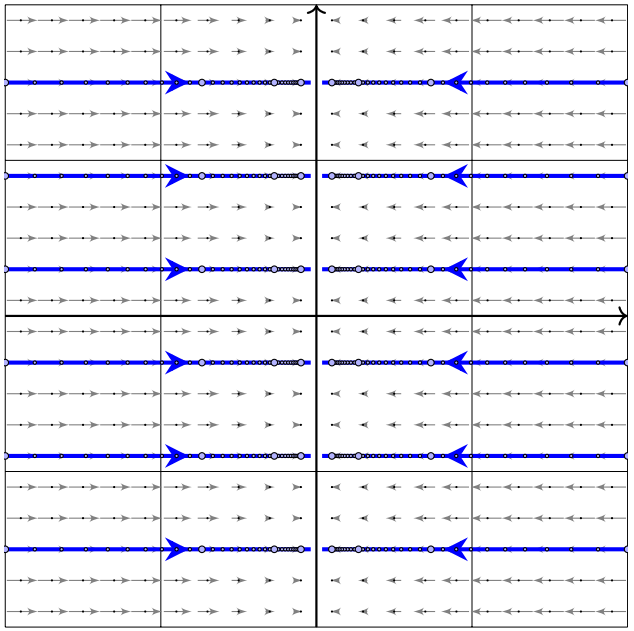
$$A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

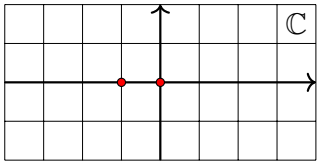
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{t} \end{bmatrix}$$

Lineare Kontraktion

N3110
Erläuterung





Zwei reelle Eigenwerte

$\lambda_1 < \lambda_2 = 0$

Allgemeiner Fall

$$A \sim \begin{bmatrix} \lambda_1 & 0 \\ 0 & 0 \end{bmatrix}$$

Konkretes Beispiel

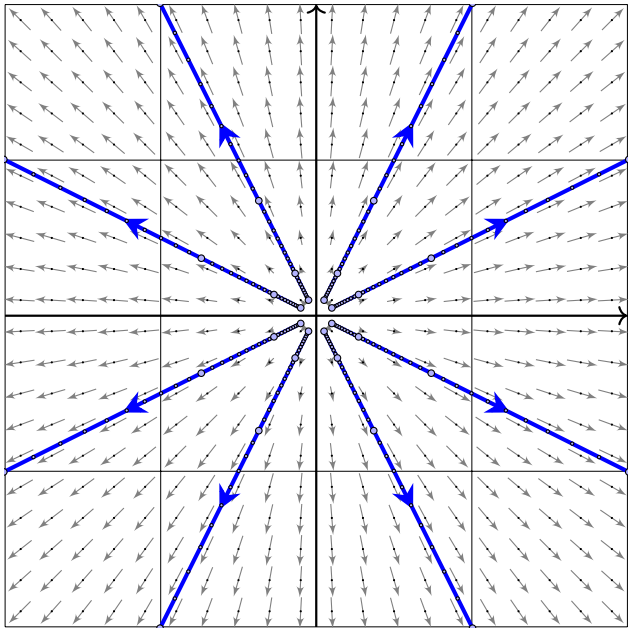
$$A = \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix}$$

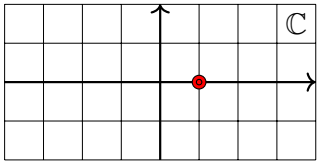
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \mathrm{e}^{-t} & 0 \\ 0 & 1 \end{bmatrix}$$

Zentrale Expansion

N3111
Erläuterung





Doppelter Eigenwert

$\lambda > 0$

Diagonalisierbarer Fall

$$A \sim \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$$

Konkretes Beispiel

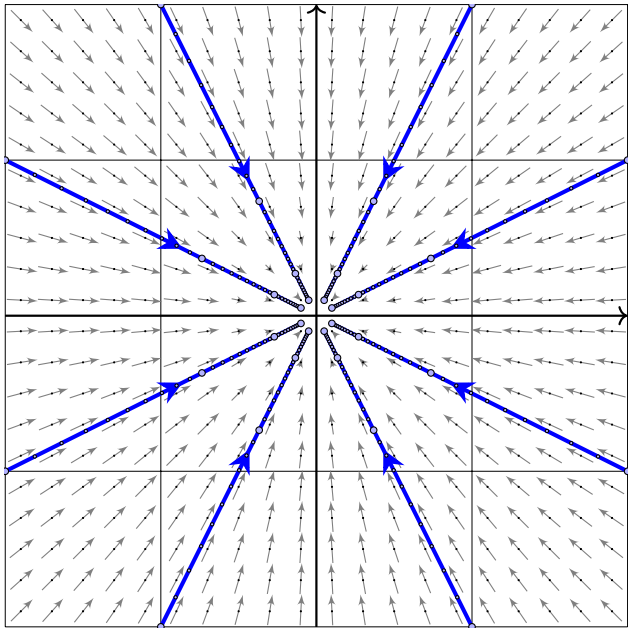
$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

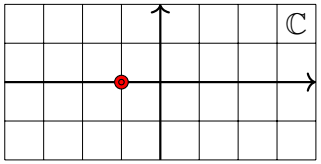
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \mathrm{e}^{t} & 0 \\ 0 & \mathrm{e}^{t} \end{bmatrix}$$

Zentrale Kontraktion

N3112
Erläuterung





Doppelter Eigenwert

$\lambda < 0$

Diagonalisierbarer Fall

$$A \sim \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$$

Konkretes Beispiel

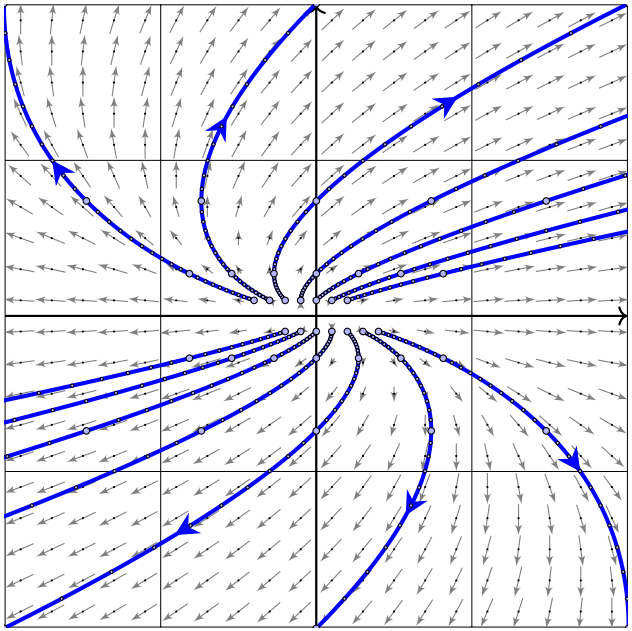
$$A = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

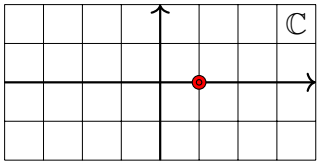
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \mathrm{e}^{-t} & 0 \\ 0 & \mathrm{e}^{-t} \end{bmatrix}$$

Instabiler Knoten: parabolische Expansion

N3113





Doppelter Eigenwert

$\lambda > 0$

Nicht-diagonalisierbar

$$A \sim \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$$

Konkretes Beispiel

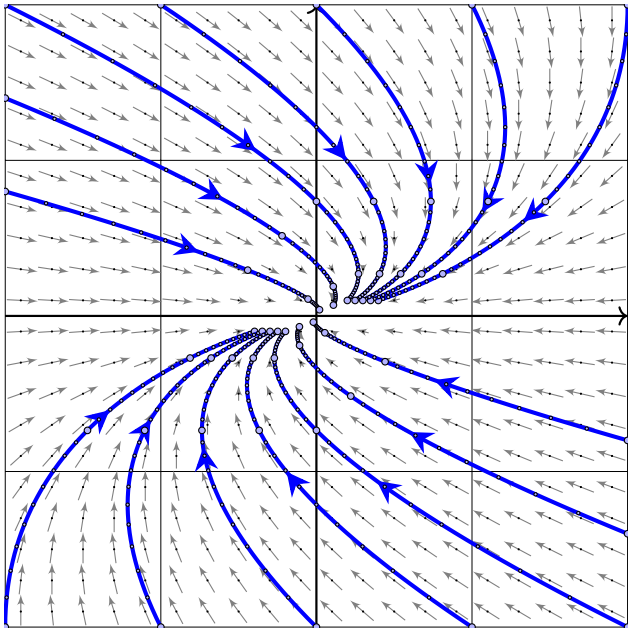
$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

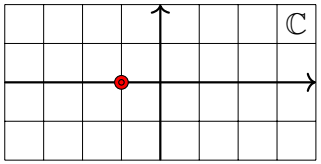
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \mathrm{e}^{t} & t\,\mathrm{e}^{t} \\ 0 & \mathrm{e}^{t} \end{bmatrix}$$

Stabiler Knoten: parabolische Kontraktion

N3114





Doppelter Eigenwert

$\lambda < 0$

Nicht-diagonalisierbar

$$A \sim \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$$

Konkretes Beispiel

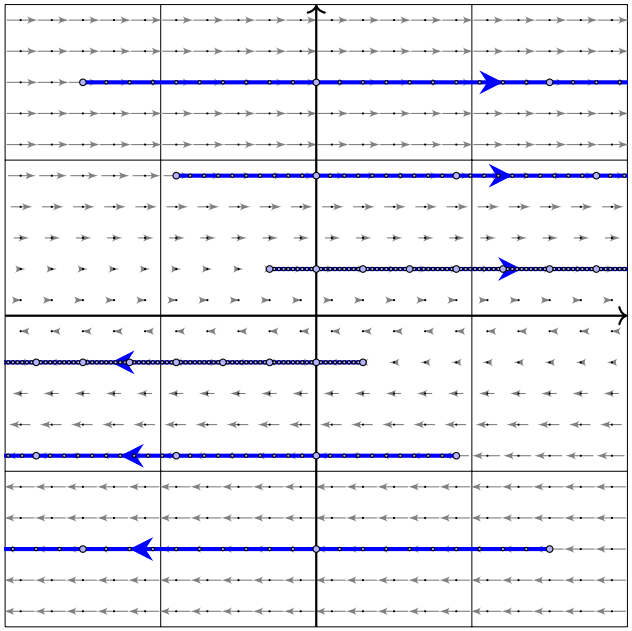
$$A = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$$

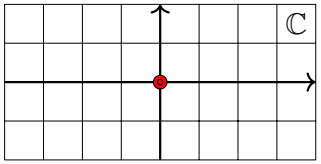
Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} \mathrm{e}^{-t} & t\,\mathrm{e}^{-t} \\ 0 & \mathrm{e}^{-t} \end{bmatrix}$$

Scherung

N3115
Erläuterung





Doppelter Eigenwert

$\lambda = 0$

Nicht-diagonalisierbar

$$A \sim \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

Konkretes Beispiel

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

Fundamentalmatrix

$$\mathrm{e}^{tA} = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$$

Diagonalisierbar oder nicht diagonalisierbar?

N3116
Erläuterung

Für jede Matrix $A \in \mathbb{R}^{2\times 2}$ mit doppeltem Eigenwert λ gilt $\lambda \in \mathbb{R}$ sowie

$$\text{entweder} \quad A \sim \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \quad \text{oder} \quad A \sim \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}.$$

Im ersten Fall existiert eine Basis des $\mathbb{R}^2$ aus Eigenvektoren von A. Die Matrix A wird hierdurch diagonalisiert. Es gilt dann:

$$\mathrm{e}^{tA} \;\sim\; \mathrm{e}^{\lambda t} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

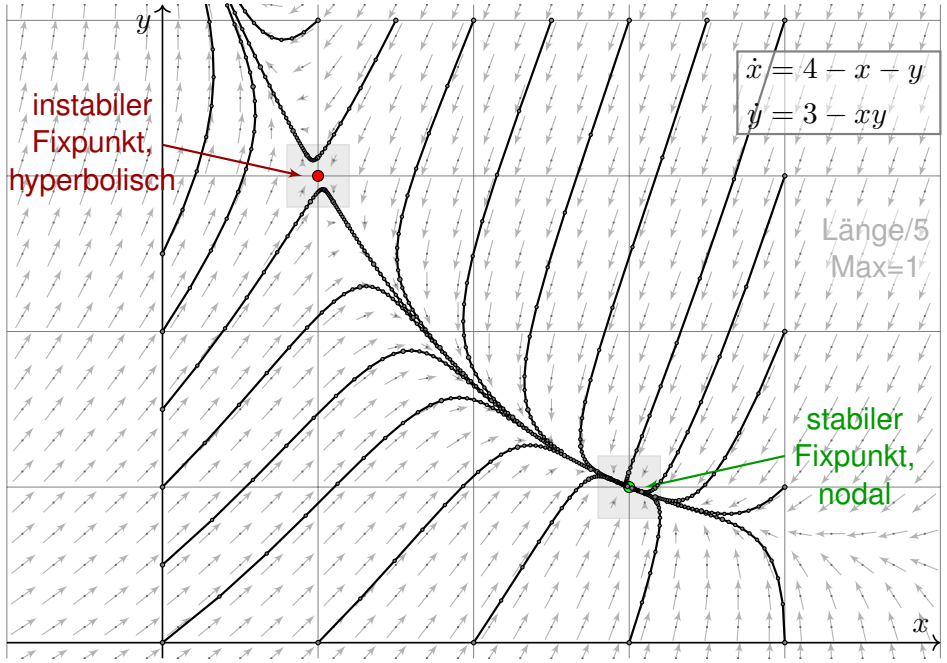
Andernfalls existiert eine Hauptvektorkette der Länge 2. Diese nutzen wir als Basis des $\mathbb{R}^2$ und erhalten obigen Jordan–Block. Es gilt dann:

$$\mathrm{e}^{tA} \;\sim\; \mathrm{e}^{\lambda t} \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$$

🙂 Nach demselben Schema können wir n–dimensionale autonome Systeme analysieren: Fixpunkte, Linearisierung, Eigenwerte, Stabilität. Unsere gründliche Vorarbeit zu Eigen- und Hauptvektoren zahlt sich aus!

Ein einfaches nicht-lineares DGSystem

N3117
Übung



Ein einfaches nicht-lineares DGSystem

N3118
Übung

Aufgabe: Wir untersuchen folgendes Differentialgleichungssystem:

$$\begin{cases} \dot{x} = 4 - x - y \\ \dot{y} = 3 - xy \end{cases}$$

(0) Skizzieren Sie das zugehörige Vektorfeld und einige Flusslinien.

(1a) Finden Sie alle Fixpunkte. Es gibt genau zwei: $(1, 3)$ und $(3, 1)$.
(1b) Linearisieren Sie um jeden Fixpunkt: Welche Dynamik gilt hier?
Leichtere Teilfrage: Ist der betrachtete Fixpunkt stabil oder instabil?
Was bedeuten die zugehörigen Eigenvektoren und die Eigenwerte?

(2) Erklären Sie (qualitativ anhand Ihrer Skizze) für jeden Startpunkt $(x(0), y(0)) \in \mathbb{R}^2$ das Verhalten der Lösung $(x(t), y(t))$ für $t \to \infty$.
(2a) Gibt es zu jedem Startwert eine Lösung? Ist sie eindeutig?
(2b) Für welche Startwerte konvergiert die Lösung gegen $(3, 1)$?
(2c) Für welche Startwerte konvergiert die Lösung gegen $(1, 3)$?
(2d) Für welche Startwerte divergiert die Lösung? gegen ∞?
Ist dieses Verhalten stabil? Wird das Ziel in endlicher Zeit erreicht?

Ein einfaches nicht-lineares DGSystem

N3119
Übung

Lösung: (1a) Fixpunkte sind die Nullstellen des Vektorfeldes:

$$\dot{x} = 4 - x - y \overset{!}{=} 0$$
$$\dot{y} = 3 - xy \quad \overset{!}{=} 0$$

Die erste Gleichung bedeutet $y = 4 - x$, einsetzen in die zweite ergibt:

$$3 - 4x + x^2 = 0 \quad \Longleftrightarrow \quad x \in \{1, 3\}$$

☺ Die beiden einzigen Fixpunkte sind daher $(1, 3)$ und $(3, 1)$. Probe!
(1b) Wir berechnen die Jacobi–Matrix in jedem der beiden Fixpunkte:

$$f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 4 - x - y \\ 3 - xy \end{bmatrix} \quad \Longrightarrow \quad f'\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} -1 & -1 \\ -y & -x \end{bmatrix}$$

$$f'\left(\begin{bmatrix} 1 \\ 3 \end{bmatrix}\right) = \begin{bmatrix} -1 & -1 \\ -3 & -1 \end{bmatrix} \quad \Longrightarrow \quad \begin{cases} \det = -2 < 0, \ \mathrm{tr} = -2 < 0 : \\ \text{instabil! genauer: hyperbolisch} \end{cases}$$

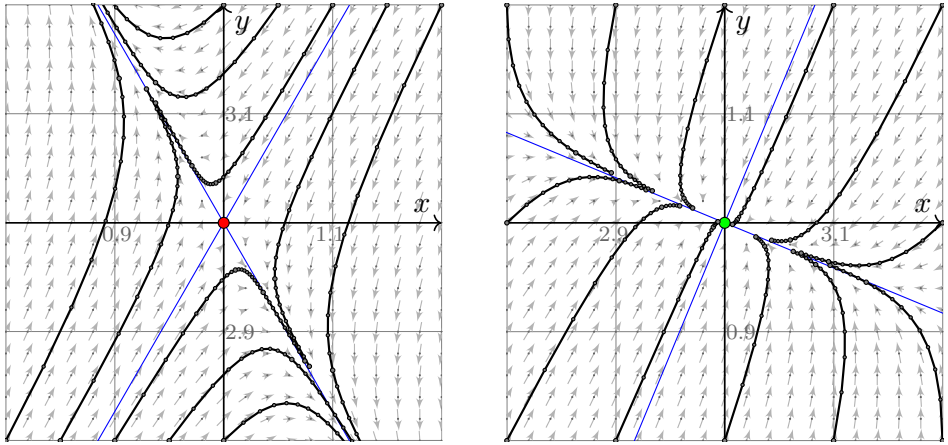
$$f'\left(\begin{bmatrix} 3 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} -1 & -1 \\ -1 & -3 \end{bmatrix} \quad \Longrightarrow \quad \begin{cases} \det = +2 > 0, \ \mathrm{tr} = -4 < 0 : \\ \text{stabil! genauer: nodale Kontraktion} \end{cases}$$

☺ Vergleich mit der obigen Skizze: Das entspricht der Anschauung!

Ein einfaches nicht-lineares DGSystem

N3120
Übung

Die Vergrößerung um die Fixpunkte zeigt annähernd lineares Verhalten:



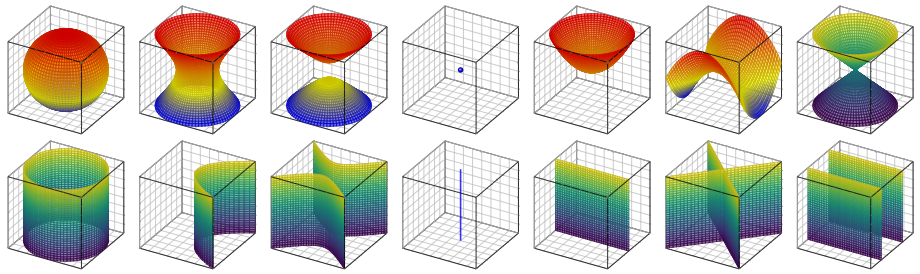
Die beiden Eigenvektoren entsprechen den Hauptachsen der Dynamik:

$$v = \begin{bmatrix} \pm 1/\sqrt{3} \\ 1 \end{bmatrix}, \ \lambda = \mp\sqrt{3} - 1 \qquad v = \begin{bmatrix} \pm\sqrt{2} - 1 \\ 1 \end{bmatrix}, \ \lambda = \mp\sqrt{2} - 2$$

☺ Rechts ist die Jacobi–Matrix symmetrisch, die EV daher orthogonal.

Kapitel O

Bilinearformen und Quadriken



Bildung ist nicht nur das Lernen von Fakten,
sondern die Schulung des Geistes zu denken.

Albert Einstein (1879–1955)

Inhalt dieses Kapitels O

Von linearen zu quadratischen Gleichungen

Bislang haben wir fast ausschließlich lineare Objekte untersucht: lineare Räume V, W und ihre linearen Abbildungen $f : V \to W$.

Die Lösungsmenge L jedes linearen Gleichungssystems $Ax = 0$ bzw. $Ax = b$ können wir effizient berechnen mit dem Gauß–Algorithmus.

Zudem kennen wir Form und Größe von L: Dies ist ein linearer bzw. affiner Teilraum, und wir können seine Dimension bestimmen.

Strukturell gilt dasselb für den Kern $\ker(f) = f^{-1}(\{0\})$ bzw. allgemein die Urbildmenge $f^{-1}(\{b\})$ jeder linearen Abbildung $f : V \to W$.

Statt linearer Gleichungen können wir allgemein Polynome von Grad $2, 3, 4, \ldots$ betrachten und deren Nullstellenmengen untersuchen.

Als wichtiges Beispiel kennen wir die Determinante $\det : K^{n\times n} \to K$. Die Determinante einer quadratischen Matrix A ist nicht linear in A, sondern multilinear in den Spalten bzw. Zeilen von A, und insgesamt ein homogenes Polynom von Grad n in den Koeffizienten von A.
Seine Nullstellenmenge sind die nicht-invertierbaren Matrizen.

Von linearen zu quadratischen Gleichungen

In diesem Kapitel geht es grundlegend um quadratische Polynome; deren Nullstellenmengen heißen Quadriken. Erfreulicherweise sind quadratische Polynome noch recht nah am linearen Fall, und wir können die bewährten Methoden der Linearen Algebra wunderbar anwenden.

Über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ gelingt uns so eine vollständige Klassifikation aller Quadriken im Raum $\mathbb{K}^n$ bis auf Affinität, also Koordinatenwechsel. Schon in der Ebene $\mathbb{R}^2$ und im Raum $\mathbb{R}^3$ begegnet uns dabei eine bewundernswerte Vielfalt. Die Klassifikation schafft Überblick und wohltuende Klarheit, dazu passt das Eingangszitat dieses Kapitels:

Bildung ist nicht nur das Lernen von Fakten,
sondern die Schulung des Geistes zu denken.

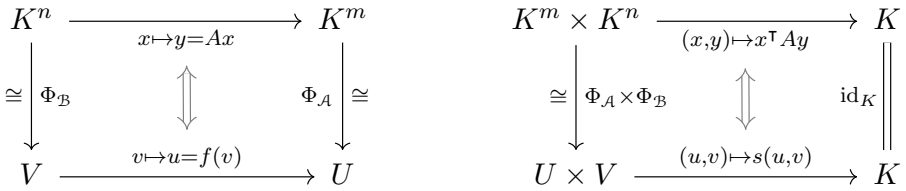
Albert Einstein (1879–1955)

Wir folgen dem Lernbuch von Fischer, 4. Auflage 2019 (mit Präzisierungen und Ergänzungen).

⚠ In der aktuellen Version bietet dieses Kapitel nur eine knappe Zusammenfassung zentraler Begriffe und Ergebnisse.

Zusammenfassung: Homomorphismen vs Bilinearformen

Sei K ein Körper sowie U, V Vektorräume über K mit Basen $\mathcal{A}, \mathcal{B}$.



(1) Wir können jede K–lineare Abbildung $f : V \to U$ darstellen durch eine Matrix $A = \mathrm{M}_{\mathcal{B}}^{\mathcal{A}}(f) \in K^{m \times n}$. Dies definiert den K–Isomorphismus

$$(\mathrm{M}_{\mathcal{B}}^{\mathcal{A}}, \mathrm{L}_{\mathcal{B}}^{\mathcal{A}}) \ : \ \mathrm{Hom}_K(V, U) \cong K^{m \times n}.$$

(2) Wir können jede K–Bilinearform $s : U \times V \to K$ darstellen durch eine Matrix $A = \mathrm{M}_{\mathcal{A},\mathcal{B}}(s) \in K^{m \times n}$. Wir erhalten so den K–Isomorphismus

$$(\mathrm{M}_{\mathcal{A},\mathcal{B}}, \mathrm{F}_{\mathcal{A},\mathcal{B}}) \ : \ \mathrm{Bil}_K(U, V; K) \cong K^{m \times n}.$$

⚠ Wir nutzen dieselben Matrizen für zwei ganz verschiedene Dinge!

Zusammenfassung: Homomorphismen vs Bilinearformen

In jedem dieser beiden Fällen formuliert das kommutative Diagramm die wesentliche Eigenschaft und legt damit auch die Definitionen fest.

(1) Gegeben ist im ersten Fall eine K–lineare Abbildung $f : V \to U$. Für die darstellende Matrix $A = \mathrm{M}_{\mathcal{B}}^{\mathcal{A}}(f) \in K^{m \times n}$ betrachten wir die Basis $\mathcal{B} = (b_1, \dots, b_n)$ des Startraums V und schreiben zu jedem Vektor b_j sein Bild $f(b_j) = \sum_{i=1}^{m} b'_i a_{i,j}$ im Zielraum U als Linearkombination der Basis $\mathcal{A} = (b'_1, \dots, b'_m)$. Dies definiert die Matrix $A = (a_{i,j})_{i,j}$.

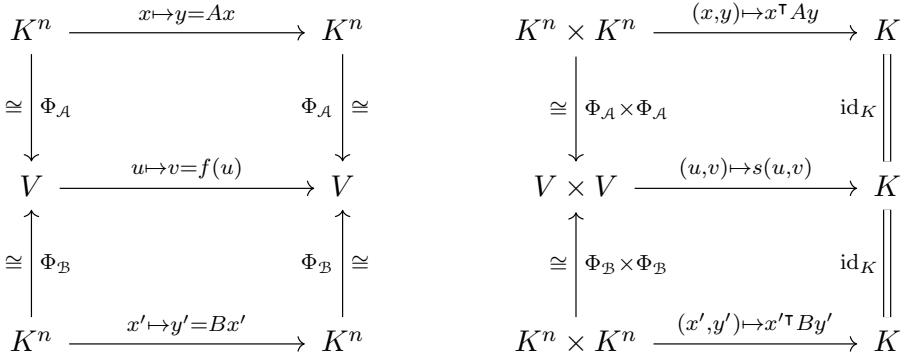
⚠ Per Konvention lassen wir Abbildungen und Matrizen hier von links auf Vektoren operieren, das impliziert dann alle weiteren Indexregeln. (Die Notation wäre noch etwas schöner bei Operation von rechts.)

(2) Gegeben ist im zweiten Falle eine K–Bilinearform $s : U \times V \to K$. Für die Matrix $A = \mathrm{M}_{\mathcal{A},\mathcal{B}}(s)$ betrachten wir die Basen $\mathcal{A} = (b'_1, \dots, b'_m)$ von U und $\mathcal{B} = (b_1, \dots, b_n)$ von V und setzen $a_{i,j} = s(b'_i, b_j)$ für alle i, j.

⚠ Auch dies definiert eine Matrix $A \in K^{m \times n}$, aber mit einer völlig anderen Herkunft und Bedeutung als im ersten Fall.

Zusammenfassung: Endomorphismen vs Bilinearformen

Wir betrachten speziell $U = V$ mit gemeinsamer Basis:



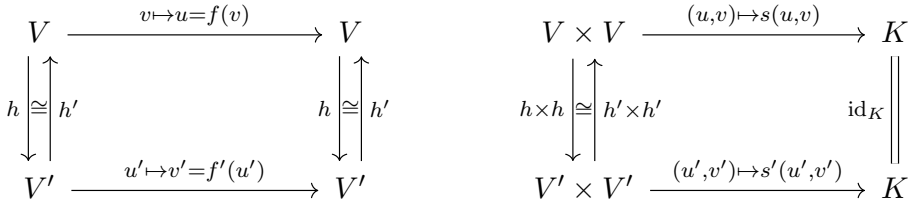
(1) Ähnlichkeit $A \sim B = S^{-1}AS$ (2) Kongruenz $A \sim B = S^\intercal AS$

Basiswechsel $S = \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} \in \mathrm{GL}_n(K)$ mit $x \mapsto x' = Sx = (\Phi_{\mathcal{B}}^{-1} \circ \Phi_{\mathcal{A}})(x)$.
Endomorphismus: $y' = Bx' \ \Leftrightarrow \ (Sy) = B(Sx) \ \Leftrightarrow \ y = (S^{-1}BS)x$
Bilinearform: $x'^\intercal By' = (Sx)^\intercal B(Sy) = x^\intercal (S^\intercal BS)y$

⚠ Verschiedene Bedeutung und anderes Transformationsverhalten!

Zusammenfassung: Endomorphismen vs Bilinearformen

Wir erklären Isomorphie für Endomorphismen und Bilinearformen:



Zwei Endomorphismen $f : V \to V$ und $f' : V' \to V'$ über K heißen **isomorph** oder **äquivalent**, falls ein Isomorphismus $(h, h') : V \cong V'$ mit $h \circ f = f' \circ h$ existiert, also $f' = h \circ f \circ h^{-1}$ bzw. $f = h^{-1} \circ f' \circ h$.

Zwei Bilinearformen $s : V \times V \to K$ und $s' : V' \times V' \to K$ über K heißen **isomorph** oder **isometrisch**, falls ein Isomorphismus $(h, h') : V \cong V'$ mit $s = s' \circ (h \times h)$ existiert, also $s(u, v) = s'(h(u), h(v))$ für alle $u, v \in V$.

Klassifikation: Wie erkennen wir Isomorphie möglichst effizient? Hier helfen uns **Normalformen** und **Invarianten**!

Diagonalisierung symmetrischer Bilinearformen

Satz O2A: Diagonalisierung symmetrischer Bilinearformen

Sei K ein Körper mit $\operatorname{char} K \neq 2$, hierüber sei V ein Vektorraum mit $n = \dim_K V < \infty$ und $s : V \times V \to K$ eine symmetrische Bilinearform.

(1) Dann existiert eine orthogonale Basis $\mathcal{B} = (v_1, \ldots, v_n)$ von V, mit

$$s(v_i, v_j) = 0 \quad \text{für alle } i \neq j.$$

Die darstellende Matrix von s bezüglich $\mathcal{B}$ ist demnach diagonal:

$$\mathrm{M}_{\mathcal{B},\mathcal{B}}(s) \overset{\text{Def}}{=} (s(v_i, v_j))_{i,j} \overset{(1)}{=} \begin{bmatrix} b_1 & 0 & \ldots & 0 \\ 0 & b_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & b_n \end{bmatrix}$$

(2) Jede symmetrische Matrix $A \in K^{n\times n}$ ist $\mathrm{GL}_n(K)$–kongruent zu einer Diagonalmatrix: Es existiert $S \in \mathrm{GL}_n(K)$, sodass

$$A \sim B = S^{\mathsf{T}} A S = \operatorname{diag}(b_1, b_2, \ldots, b_n).$$

Diagonalisierung symmetrischer Bilinearformen

🙂 Diesen Satz können wir auf zwei Arten beweisen (siehe Fischer):

(1) Einerseits per Induktion über die Dimension $n = \dim_K(V)$.

(2) Andererseits durch den symmetrisierten Gauß–Algorithmus.

Beide Beweise leisten im Wesentlichen dasselbe, betonen aber komplementäre Aspekte und ergänzen sich wunderbar.

🙂 Zum Kontrast blicken wir nochmal zurück auf die Diagonalisierung eines Endomorphismen $f : V \to V$. Diese ist wesentlich schwieriger und aufwändiger: charakteristisches Polynom, Zerfällung, Eigenräume, ...

☹ Die Diagonalisierung eines Endomorphismus gelingt nicht immer, daher haben wir ausführlich auch die Jordanisierung untersucht.

🙂 Die Diagonalisierung einer symmetrischen Bilinearform $s : V \times V \to K$ gelingt immer, einzige Voraussetzung ist $\operatorname{char} K \neq 2$.

Klassifikation symmetrischer Bilinearformen über $\mathbb{C}$

Satz O2B: Klassifikation symmetrischer Bilinearformen über $\mathbb{C}$

(1) Zu jeder symmetrischen Bilinearform $s : V \times V \to \mathbb{C}$ über $\mathbb{C}$ von Dimension n und Rang r existiert eine Basis $\mathcal{B} = (v_1, \ldots, v_n)$ von V mit

$$s(v_i, v_j) = 1 \quad \text{für } i = j \in \{1, \ldots, r\},$$
$$s(v_i, v_j) = 0 \quad \text{für alle anderen } (i, j).$$

Die darstellende Matrix von s bezüglich $\mathcal{B}$ ist demnach

$$\mathrm{M}_{\mathcal{B},\mathcal{B}}(s) \overset{\text{Def}}{=} (s(v_i, v_j))_{i,j} \overset{(1)}{=} \begin{bmatrix} 1_{r\times r} & 0_{r\times d} \\ 0_{d\times r} & 0_{d\times d} \end{bmatrix} \overset{\text{Def}}{=} D^r_{n\times n}.$$

(2) Jede symmetrische Matrix $A \in \mathbb{C}^{n\times n}$ ist $\mathrm{GL}_n(\mathbb{C})$–kongruent zu genau einer solchen Modellmatrix: Es existiert $S \in \mathrm{GL}_n(\mathbb{C})$, sodass

$$A \sim B = S^{\mathsf{T}} A S = \operatorname{diag}(1, \ldots, 1, 0, \ldots, 0).$$

(3) Genau dann sind zwei symmetrische Bilinearformen s, s' über $\mathbb{C}$ isometrisch, bzw. zwei symmetrische Matrizen A, A' über $\mathbb{C}$ kongruent, wenn Sie dieselbe Dimension und denselben Rang über $\mathbb{C}$ haben.

Klassifikation symmetrischer Bilinearformen über $\mathbb{C}$

🙂 Diese Klassifikation gilt wörtlich genau so über jedem Körper K, in dem jedes Element ein Quadrat ist. Dies gilt insbesondere über jedem algebraisch abgeschlossenen Körper, etwa den komplexen Zahlen $\mathbb{C}$.

Beweis: (1) Dank der oben erklärten Diagonalisierung (O2A) existiert zu s eine diagonalisierende Basis $(u_1, \ldots, u_n)$ von V mit $s(u_i, u_j) \in K^\times$ für $i = j \in \{1, \ldots, r\}$ und $s(u_i, u_j) = 0$ sonst.

Für $i = 1, \ldots, r$ wählen wir eine der beiden Quadratwurzeln $a_i \in K$ mit $a_i^2 = s(u_i, u_i)$ und setzen $v_i = u_i / a_i$. Damit gilt $s(v_i, v_i) = 1$.
Die Basisvektoren $v_i = u_i$ für $i = r + 1, \ldots, n$ ändern wir nicht.

(2) Dies ist die äquivalente Matrixformulierung der Aussage (1).

(3) „⇒“: Die Dimension und der Rang sind Invarianten unter Isometrie symmetrischer Bilinearformen bzw. Kongruenz symmetrischer Matrizen.

„⇐“: Haben s, s' dieselbe Dimension und denselben Rang, so finden wir diagonalisierende Basen $\mathcal{B}, \mathcal{B}'$ wie in (1), und diese liefern die ersehnte Isometrie $(h, h') : (V, s) \xrightarrow{\sim} (V', s') : v_i \leftrightarrows v_i'$. QED

Satz O2C: Klassifikation symmetrischer Bilinearformen über $\mathbb{R}$

(1) Zu jeder symmetrischen Bilinearform $s : V \times V \to \mathbb{R}$ über $\mathbb{R}$ von Dimension n und Rang r existiert eine Basis $\mathcal{B} = (v_1, \ldots, v_n)$ von V mit

$$\begin{aligned} s(v_i, v_j) &= +1 \quad \text{für } i = j \in \{1, \ldots, r_+\}, \\ s(v_i, v_j) &= -1 \quad \text{für } i = j \in \{r_+ + 1, \ldots, r_+ + r_-\}, \\ s(v_i, v_j) &= 0 \quad \text{für alle anderen Paare } (i, j). \end{aligned}$$

Die darstellende Matrix von s bezüglich $\mathcal{B}$ ist demnach

$$\mathrm{M}_{\mathcal{B},\mathcal{B}}(s) \overset{\text{Def}}{=} (s(v_i, v_j))_{i,j} \overset{(1)}{=} \begin{bmatrix} 1_{r_+ \times r_+} & 0_{r_+ \times r_-} & 0_{r_+ \times r_0} \\ 0_{r_- \times r_+} & -1_{r_- \times r_-} & 0_{r_- \times r_0} \\ 0_{r_0 \times r_+} & 0_{r_0 \times r_-} & 0_{r_0 \times r_0} \end{bmatrix}$$

(2) Jede symmetrische Matrix $A \in \mathbb{R}^{n \times n}$ ist $\mathrm{GL}_n(\mathbb{R})$–kongruent zu einer solchen Modellmatrix: Es existiert $S \in \mathrm{GL}_n(\mathbb{R})$, sodass

$$A \sim B = S^\mathsf{T} A S = \mathrm{diag}(+1, \ldots, +1, -1, \ldots, -1, 0, \ldots, 0).$$

Satz O2C: Klassifikation symmetrischer Bilinearformen über $\mathbb{R}$

(3) Sei $\mathcal{B}' = (v'_1, \ldots, v'_n)$ eine weitere Basis von V mit

$$\begin{aligned} s(v'_i, v'_j) &= +1 \quad \text{für } i = j \in \{1, \ldots, r'_+\}, \\ s(v'_i, v'_j) &= -1 \quad \text{für } i = j \in \{r'_+ + 1, \ldots, r'_+ + r'_-\}, \\ s(v'_i, v'_j) &= 0 \quad \text{für alle anderen Paare } (i, j). \end{aligned}$$

Dann gilt $(r_+, r_-, r_0) = (r'_+, r'_-, r'_0)$ dank Sylvesters Trägheitssatz.

Wir nennen diese Invariante (r_+, r_-, r_0) das **Signaturtripel** von s, mit dem **Positivitätsindex** r_+ und dem **Negativitätsindex** r_-. Ihre Differenz $\mathrm{sign}(s) := r_+ - r_-$ heißt auch die **Signatur** und $\mathrm{null}(s) := r_0$ die **Nullität** der reellen Bilinearform s.

(4) Genau dann sind zwei symmetrische Bilinearformen s, s' über $\mathbb{R}$ isometrisch, bzw. zwei symmetrische Matrizen A, A' über $\mathbb{R}$ kongruent, wenn Sie dieselben Signaturtripel haben, $(r_+, r_-, r_0) = (r'_+, r'_-, r'_0)$.

☺ Diese Klassifikation gilt wörtlich genau so über jedem geordneten Körper $(K, \leq)$, in dem jedes positive Element $a > 0$ ein Quadrat ist.

Beweis: (1) Dank O2A existiert eine Basis $(u_1, \ldots, u_n)$ von V mit $s(u_i, u_j) \in K^\times$ für $i = j \in \{1, \ldots, r\}$ und $s(u_i, u_j) = 0$ sonst. Für $i = 1, \ldots, r$ wählen wir eine der beiden Quadratwurzeln $a_i \in K$ mit $a_i^2 = |s(u_i, u_i)|$ und setzen $v_i = u_i / a_i$. Damit gilt $s(v_i, v_i) = \pm 1$. Die Basisvektoren $v_i = u_i$ für $i = r + 1, \ldots, n$ ändern wir nicht. Schließlich sortieren wir die Basis $(v_1, \ldots, v_n)$ wie angegeben.

(2) Dies ist die äquivalente Matrixformulierung der Aussage (1).

(3) Dies ist die Aussage des Trägheitssatzes von Sylvester.

(4) „⇒“: Über K ist das Signaturtripel eine Invariante unter Isometrie symmetrischer Bilinearformen bzw. Kongruenz symmetrischer Matrizen.

„⇐“: Haben s, s' dasselbe Signaturtripel, so finden wir hierzu diagonalisierende Basen $\mathcal{B}, \mathcal{B}'$ wie in (1), und diese liefern die ersehnte Isometrie $(h, h') : (V, s) \xrightarrow{\sim} (V', s') : v_i \leftrightarrows v'_i$. QED

Ausblick: Ganz analog können wir nach der Klassifikation quadratischer Formen über jedem kommutativen Ring K fragen. Von zentralem Interesse sind die klassischen Fälle $\mathbb{Z}, \mathbb{F}_q, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

☺ Die Fälle $\mathbb{R}$ und $\mathbb{C}$ haben wir oben vollständig klären können. Dies ist insbesondere für geometrische Anwendungen wichtig.

Über jedem endlichen Körper $\mathbb{F}_q$ sowie über den rationalen Zahlen $\mathbb{Q}$ ist die Klassifikation ebenfalls bekannt, doch wesentlich aufwändiger.

📖 L.J. Gerstein: *Basic Quadratic Forms.* Amer. Math. Soc. 2008
J. Milnor, D. Husemoller: *Symmetric Bilinear Forms.* Springer 1973
J.-P. Serre: *A Course in Arithmetic.* Springer 1973

Über den ganzen Zahlen $\mathbb{Z}$ ist die Untersuchung quadratischer Formen ein klassisches Problem, extrem facettenreich und faszinierend.

📖 J.H. Conway, N.J.A. Sloane: *Sphere Packings, Lattices and Groups.* Springer 1999, ch. 15: *On the Classification of Integral Quadratic Forms.*

Quadratische Polynome und zugehörige Quadriken

O301

☺ Eine Quadrik ist die Lösungsmenge einer quadratischen Gleichung.

Sei K ein Körper, geometrisch denken wir insbesondere an $K = \mathbb{R}, \mathbb{C}$.
Wir betrachten ein Polynom $P \in K[X_1, \dots, X_n]$ vom Grad ≤ 2:

$$P = \underbrace{a_{00}}_{\text{Konstante}} + \underbrace{2\textstyle\sum_{i=1}^{n} a_{i0} X_i}_{\text{lineare Terme}} + \underbrace{2\textstyle\sum_{1\leq i<j\leq n} a_{ij} X_i X_j}_{\text{gemischte Terme}} + \underbrace{\textstyle\sum_{i=1}^{n} a_{ii} X_i^2}_{\text{quadratische Terme}}$$

Die Koeffizienten fassen wir in zwei symmetrischen Matrix zusammen:

$$A = (a_{ij})_{i=1,\dots,n}^{j=1,\dots,n} \in K^{n\times n} \quad \text{und} \quad A' = (a_{ij})_{i=0,\dots,n}^{j=0,\dots,n} \in K^{n'\times n'}$$

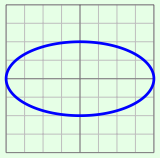
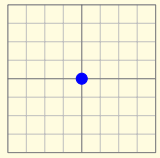
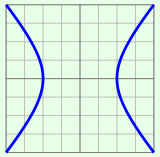
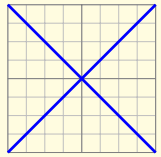
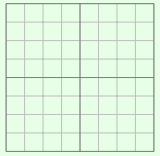
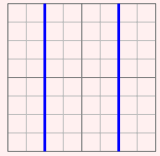
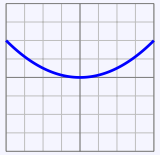
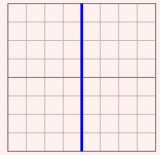
Hier ist $X^\intercal A X$ der homogene Teil in Grad 2: die quadratische Form.
Es gilt $P = X'^\intercal A' X'$ in homogenen Koordinaten $X'^\intercal = (1, X_1, \dots, X_n)$.
Im Falle $A = 0$ ist P nur ein Polynom vom Grad ≤ 1, also affin-linear.
Wir werden daher meist stillschweigend $A \neq 0$ annehmen.

Definition O3A: Quadrik

Sei $P \in K[X_1, \dots, X_n]$ ein quadratisches Polynom. Die zugehörige Nullstellenmenge $Q = \{\, x \in K^n \mid P(x) = 0 \,\}$ nennen wir eine **Quadrik**.

Beispiele: reelle Quadriken in der Ebene $\mathbb{R}^2$

O302

Kreis / Ellipse $x^2 + 4y^2 = 1$ 	Punkt $x^2 + y^2 = 0$ 
Hyperbel $4x^2 - 3y^2 = 1$ 	schneidendes Geradenpaar $x^2 - y^2 = 0$ 
leere Menge $x^2 + y^2 = -1$ 	paralleles Geradenpaar $4x^2 = 1$ 
Parabel $x^2 = 2y$ 	Gerade $x^2 = 0$ 

Affine Abbildungen

O303
Erläuterung

Sei K ein Körper sowie $A \in K^{m\times n}$ und $u \in K^m$. Wir nennen

$$f \,:\, K^n \to K^m \,:\, x \mapsto y = Ax + u$$

eine **affine Abbildung** oder auch **affin-lineare Abbildung**.

Das entspricht der Komposition der linearen Abbildung $x \mapsto \bar{x} = Ax$
mit der anschließenden Verschiebung $\bar{x} \mapsto y = \bar{x} + u$ um den Vektor u.
Der Spezialfall $u = 0$ entspricht einer linearen Abbildung $x \mapsto y = Ax$.

In der obigen Konvention identifizieren wir K^n mit $\{1\} \times K^n \subset K^{1+n}$
und erhalten so $f' : \{1\} \times K^n \to \{1\} \times K^m : x' \mapsto y' = A'x'$ mit
$x' = (1, x_1, \dots, x_n)^\intercal$ und $y' = (1, y_1, \dots, y_m)^\intercal$ und $A' = \left[\begin{smallmatrix} 1 & 0 \\ u & A \end{smallmatrix}\right]$.

Übung: (1) Die Identität $\mathrm{id}' : x' \mapsto x'$ ist eine affine Abbildung,
mit der Einheitsmatrix $I' = \left[\begin{smallmatrix} 1 & 0 \\ 0 & I \end{smallmatrix}\right]$ als darstellender Matrix.

(2) Die Komposition von zwei affinen Abbildungen $f' : x' \mapsto y' = A'x'$
und $g' : y' \mapsto z' = B'y'$ ist die affine Abbildung $g' \circ f' : x' \mapsto z' = B'A'x'$,
wobei $\left[\begin{smallmatrix} 1 & 0 \\ v & B \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ u & A \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ w & C \end{smallmatrix}\right]$ mit $C = BA$ und $w = v + Bu$ gilt.

Affinitäten aka affine Isomorphismen

O304
Erläuterung

Wir nennen f eine **Affinität**, wenn f zudem bijektiv ist. Dies ist genau dann der Fall, wenn $A \in \mathrm{GL}_n(K)$ gilt. In diesem Falle ist die Inverse $f^{-1} : K^n \to K^n : y \mapsto x = A^{-1}(y - u) = A^{-1}y - A^{-1}u$ selbst affin.
Somit gilt $f'^{-1} : \{1\} \times K^n \to \{1\} \times K^n : y' \mapsto x' = A'^{-1}y'$.

Übung: Die Affinitäten von K^n bilden eine Gruppe, kurz $(\mathrm{GA}(K^n), \circ)$,
genauer: eine Untergruppe in der symmetrischen Gruppe $(\mathrm{Sym}(K^n), \circ)$.
Für $n = 1$ gilt $\mathrm{GA}(K) = \{\, f : K \xrightarrow{\sim} K : x \mapsto ax + u \mid a \in K^\times,\, u \in K \,\}$.

In obiger Matrixdarstellung definieren wir hierzu die Matrixgruppe

$$\mathrm{GA}_n(K) := \left\{\, T' = \left[\begin{smallmatrix} 1 & 0 \\ u & T \end{smallmatrix}\right] \;\middle|\; T \in \mathrm{GL}_n(K),\, u \in K^n \,\right\} \leq \mathrm{GL}_{n+1}(K).$$

Wir erhalten so eine kurze exakte Sequenz von Gruppen:

$$1 \longrightarrow K^n \xhookrightarrow{\;i\;} \mathrm{GA}_n(K) \underset{j}{\overset{p}{\rightleftarrows}} \mathrm{GL}_n(K) \longrightarrow 1$$

mit $i(u) = \left[\begin{smallmatrix} 1 & 0 \\ u & I \end{smallmatrix}\right]$ und $p(\left[\begin{smallmatrix} 1 & 0 \\ u & T \end{smallmatrix}\right]) = T$ sowie $j(T) = \left[\begin{smallmatrix} 1 & 0 \\ 0 & T \end{smallmatrix}\right]$.
Speziell für $n = 1$ gilt $\mathrm{GA}_1(K) = \{\, \left[\begin{smallmatrix} 1 & 0 \\ u & a \end{smallmatrix}\right] \mid u \in K,\, a \in K^\times \,\}$.

Transformation unter Affinitäten

🙂 Unsere obige Definition einer Quadrik $Q \subseteq K^n$ ist unabhängig von den willkürlich gewählten affinen Koordinaten: Jedes Bild der Quadrik Q unter einer Affinität $f : K^n \to K^n$ ist wieder eine Quadrik. Genauer gilt:

Satz O3B: Transformationsformel für Quadriken

(1) Sei $Q = \{ x \in K^n \mid x'^\intercal A' x' = 0 \}$ die Quadrik zu $A' \in K^{n' \times n'}$.

Sei $f : K^n \to K^n$ eine Affinität gegeben durch $S' \in \mathrm{GA}_n(K)$ mit der Inversen $T' = S'^{-1}$. Dann ist auch die Bildmenge $f(Q) \subseteq K^n$ eine Quadrik, nämlich $f(Q) = \{ x \in K^n \mid x'^\intercal B' x' = 0 \}$ mit $B' = T'^\intercal A' T'$.

(2) Dies definiert eine Äquivalenzrelation $\sim$ auf $K^{n' \times n'}$.

Wir betrachten $A', B' \in K^{n' \times n'}$ als affin-äquivalent, kurz $A' \sim B'$, wenn es eine Matrix $T' \in \mathrm{GA}_n(K)$ gibt, sodass $B' = T'^\intercal A' T'$ gilt.

Wir nutzen durchgehend erweiterte Matrizen $A' = \left[\begin{smallmatrix} c & b^\intercal \\ b & A \end{smallmatrix}\right] \in K^{n' \times n'}$ und die erweiterte Dimension $n' = n + 1$ als bequeme Abkürzungen.

Transformation unter Affinitäten

Aufgabe: Diese Rechnung ist Routine. Führen Sie sie aus!

Lösung: (1) Für $y' = f'(x')$ gilt $y' = S'x'$ und umgekehrt $x' = T'y'$.

$$\begin{aligned} y \in f(Q) &\iff x = f^{-1}(y) \in Q &&\iff x'^\intercal A' x' = 0 \\ &\iff (T'y')^\intercal A' (T'y') = 0 &&\iff y'^\intercal (T'^\intercal A' T') y' = 0 \end{aligned}$$

Also gilt $f(Q) = \{ y \in K^n \mid y'^\intercal B' y' \}$, wie behauptet.

(2) Die Äquivalenzeigenschaften folgen aus den Gruppeneigenschaften:

Reflexivität: Es gilt $A' = I'^\intercal A' I'$ dank der Identität $I' = \left[\begin{smallmatrix} 1 & 0 \\ 0 & I \end{smallmatrix}\right]$.

Symmetrie: Aus $B' = T'^\intercal A' T'$ folgt $A' = S'^\intercal A' S'$ dank $S' = T'^{-1}$.

Transitivität: Aus $B' = T'^\intercal A' T'$ und $C' = U'^\intercal B' U'$ folgt $C' = V'^\intercal A' V$ dank $V' = T'U'$, denn $U'^\intercal T'^\intercal A' T' U' = U'^\intercal B' U' = C'$. QED

Affinitäten und Skalierungen

Die Nullstellenmenge $Q = \{ x \in K^n \mid P(x) = 0 \}$ ändert sich nicht, wenn wir das Polynom P mit einem Skalar $\lambda \in K^\times$ multiplizieren.

Neben Koordinatenwechsel durch Affinitäten erlauben wir daher im Folgenden auch Skalierungen $P \mapsto \lambda P$ bzw. $A' \mapsto \lambda A'$ mit $\lambda \in K^\times$.

Definition O3C: Äquivalenz unter Affinitäten und Skalierungen

(1) Wir betrachten $A', B' \in K^{n' \times n'}$ als **affin–skalierungs–äquivalent**, geschrieben $A' \equiv B'$, wenn es einen Skalar $\lambda \in K^\times$ und eine Matrix $T' \in \mathrm{GA}_n(K)$ gibt, sodass $B' = \lambda T'^\intercal A' T'$ gilt.

(2) Dies ist eine Äquivalenzrelation auf der Menge $K^{n' \times n'}$ der Matrizen. Wir bezeichnen mit $[A']$ die Äquivalenzklasse von A' bezüglich $\equiv$.

Affinitäten und Skalierungen

Wir suchen im Folgenden eine Klassifikation aller Quadriken $Q \subseteq K^n$, genauer gesagt: der sie definierenden quadratischen Polynome $P \in K[X_1, \ldots, X_n]$, modulo Affinitäten und Skalierungen.

Anders gesagt, wir wollen die Quotientenmenge aller Matrizen $K^{n' \times n'}$ modulo $\equiv$ verstehen, also modulo Affinitäten und Skalierungen.

🙂 Die folgende Klassifikation verschafft uns eine einfache Übersicht, zunächst allgemein über jedem Körper der Charakteristik $\mathrm{char}\, K \neq 2$.

🙂 Anschließend wollen wir dies speziell für $K = \mathbb{C}, \mathbb{R}$ präzisieren, indem wir die Formel weiter vereinfachen und so eindeutig machen.

Affine Klassifikation der Quadriken

Satz O3D: affine Klassifikation der Quadriken

Sei K ein Körper der Charakteristik $\operatorname{char} K \neq 2$.
Gegeben sei eine Quadrik $Q = \{\, x \in K^n \mid x'^{\mathsf{T}} A' x' = 0 \,\}$.

(0) Für $r := \operatorname{rang} A$ und $r' := \operatorname{rang} A'$ gilt $\delta := r' - r \in \{0, 1, 2\}$.

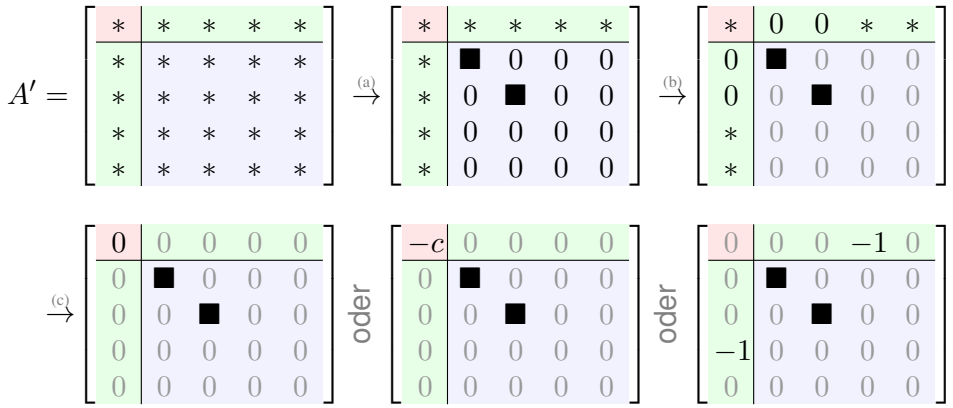
(1) Es existiert eine Affinität $f : K^n \xrightarrow{\sim} K^n$, sodass $f(Q) \subseteq K^n$ gegeben ist durch eine Gleichung in Standardform

$$\underbrace{a_1 y_1^2 + \cdots + a_r y_r^2}_{=:\, q(y_1, \ldots, y_r)} = \begin{cases} 0 & \text{falls } \delta = 0 \quad \text{(kegeliger Typ)}, \\ 1 & \text{falls } \delta = 1 \quad \text{(zentraler Typ)}, \\ 2y_{r+1} & \text{falls } \delta = 2 \quad \text{(parabolischer Typ)}. \end{cases}$$

Hier ist q eine diagonale quadratische Form vom Rang r; es genügt ein Repräsentant modulo Kongruenz und (für $\delta \neq 1$ auch) Skalierung.

Wir interessieren uns hier zunächst nur für die Nullstellenmenge Q, und eine Skalierung $A' \mapsto \lambda A'$ mit $\lambda \in K^\times$ ändert diese nicht.

Affine Klassifikation der Quadriken



Beweis: (1) Wir bringen $P = X'^{\mathsf{T}} A' X'$ in die gewünschte Standardform:
(a) Dank Satz O2A diagonalisieren wir zunächst die quadratische Form.
(b) Damit löschen wir soweit möglich den linearen Teil (links und oben).
(c) Wir unterscheiden $\delta \in \{0, 1, 2\}$ und verschieben wie angegeben.
(d) Im Falle $\delta = 1$ nutzen wir zudem eine Skalierung zum Wert $c = 1$.

Affine Klassifikation quadratischer Polynome

Satz O3D: affine Klassifikation quadratischer Polynome

(2) Die symmetrische Matrix $A \in K^{n \times n}$ ist $\mathrm{GL}_n(K)$–kongruent zu einer Diagonalmatrix (O2A): Es existiert $S \in \mathrm{GL}_n(K)$, sodass

$$A \sim B = S^{\mathsf{T}} A S = \operatorname{diag}(b_1, \ldots, b_r, 0, \ldots, 0) \quad \text{mit} \quad b_1, \ldots, b_r \neq 0.$$

(3) Es existiert eine Affinität $f : K^n \to K^n : x' \mapsto y' = T'^{-1} x'$ mit $T' = \left[\begin{smallmatrix} 1 & 0 \\ v & T \end{smallmatrix}\right] \in \mathrm{GA}_n(K)$, sodass $B' = T'^{\mathsf{T}} A' T'$ gegeben ist durch

$$y'^{\mathsf{T}} B' y' = b_1 y_1^2 + \cdots + b_r y_r^2 - \{\, 0,\, c,\, 2y_{r+1} \,\}.$$

(4) Nach Skalierung erhalten wir $C' = \lambda U'^{\mathsf{T}} A' U'$ mit $U' \in \mathrm{GA}_n(K)$ und

$$z'^{\mathsf{T}} C' z' = c_1 z_1^2 + \cdots + c_r z_r^2 - \{\, 0,\, 1,\, 2z_{r+1} \,\}.$$

Im Falle $\delta = 1$ nutzen wir $\lambda = c^{-1}$ und $U' = T'$. Im Falle $\delta \neq 1$ können wir $\lambda \in K^\times$ beliebig wählen; für $\delta = 2$ kompensieren wir durch $z_{r+1} = \lambda y_{r+1}$.

Genauer als nur die Nullstellenmengen in (1) untersuchen wir in (2,3,4) quadratische Polynome modulo Kongruenz, Affinität und Skalierung.

Affine Klassifikation quadratischer Polynome

☺ Für die Quadrik sind Skalierungen des Polynoms unerheblich.
Für die Polynome selbst macht es jedoch einen Unterschied.

⚠ Vorsicht, hier irrt das Lernbuch von Fischer (in der aktuellen 4. Auflage von 2019), da es die Aussagen (1) und (2,3,4) vermischt.

Allein durch Affinität ist die Standardform (4) *für das Polynom* nicht zu erreichen. Dennoch resümiert Fischer auf Seite 430 etwas kryptisch:

Affine Normalform der Gleichung eines Kegelschnitts *Ist $Q \subset \mathbb{R}^2$ ein Kegelschnitt, so kann man seine Gleichung durch eine affine Transformation auf genau eine der oben angegebenen Normalformen bringen.*

Gemeint ist eine affine Bijektion, also eine Affinität.

Wann sind zwei Gleichungen gleich? Ist hier das Polynom gemeint? Dann wäre es falsch.

☺ Wir klassifizieren anschließend alle Quadriken über $\mathbb{C}$ und über $\mathbb{R}$.
Die positiven Konstanten $\alpha, \beta, \gamma > 0$ können wir dabei frei wählen.
Zur affinen Normalform setzen wir überall $\alpha = \beta = \gamma = 1$.

⚠ Vorsicht, auch auf Seite 436 irrt das Lernbuch von Fischer:
Das Signaturtripel ist nur im Falle $\delta = 1$ eindeutig festgelegt. Im Falle $\delta \neq 1$ können wir durch Skalierung mit -1 alle Vorzeichen umklappen.

Affine Klassifikation quadratischer Polynome über $\mathbb{C}$

Satz O3E: affine Klassifikation quadratischer Polynome über $\mathbb{C}$

Gegeben sei die symmetrische Matrix $A' \in \mathbb{C}^{n' \times n'}$ und damit das quadratische Polynom $P = X'^{\intercal} A' X' \in \mathbb{C}[X_1, \ldots, X_n]$.

(0) Für $r := \operatorname{rang} A$ und $r' := \operatorname{rang} A'$ gilt $\delta := r' - r \in \{0, 1, 2\}$.

(1) Durch Affinität und Skalierung können wir das Polynom P in genau eine der folgenden Normalformen überführen:

$$y_1^2 + \cdots + y_r^2 - \begin{cases} 0 & \text{falls } \delta = 0 \quad \text{(kegeliger Typ)}, \\ 1 & \text{falls } \delta = 1 \quad \text{(zentraler Typ)}, \\ 2y_{r+1} & \text{falls } \delta = 2 \quad \text{(parabolischer Typ)}. \end{cases}$$

(2) Die beiden Zahlen (r, r') bilden somit ein vollständiges System von Invarianten für diese algebraische Klassifikation über $\mathbb{C}$.

🙂 Im Vergleich zu Satz O3D erhalten wir über $\mathbb{C}$ zwei Verbesserungen: Erstens, die Gleichungen für Quadriken werden noch weiter vereinfacht. Zweitens, die oben angegebene Normalform ist nun sogar eindeutig!

Affine Klassifikation quadratischer Polynome über $\mathbb{R}$

Satz O3F: affine Klassifikation quadratischer Polynome über $\mathbb{R}$

Gegeben sei die symmetrische Matrix $A' \in \mathbb{R}^{n' \times n'}$ und damit das quadratische Polynom $P = X'^{\intercal} A' X' \in \mathbb{R}[X_1, \ldots, X_n]$.

(0) Für $r := \operatorname{rang} A$ und $r' := \operatorname{rang} A'$ gilt $\delta := r' - r \in \{0, 1, 2\}$.

(1) Durch Affinität und Skalierung können wir das Polynom P in genau eine der folgenden Normalformen überführen:

$$y_1^2 + \cdots + y_p^2 - y_{p+1}^2 - \cdots - y_r^2 - \begin{cases} 0 & \text{falls } \delta = 0, \\ 1 & \text{falls } \delta = 1, \\ 2y_{r+1} & \text{falls } \delta = 2. \end{cases}$$

Dabei gilt $0 \le p \le r$ falls $\delta = 1$ und $r/2 \le p \le r$ falls $\delta \neq 1$.

(2) Die drei Zahlen (r, r', p) bilden somit ein vollständiges System von Invarianten für diese algebraische Klassifikation über $\mathbb{R}$.

🙂 Im Vergleich zu Satz O3E erhalten wir über $\mathbb{R}$ als weitere Invariante $|\operatorname{sign}(A)|$, den Betrag der Signatur der symmetrischen Matrix $A \in \mathbb{R}^{n \times n}$.

Klassifikation der reellen Quadriken in der Ebene $\mathbb{R}^2$

Ellipse $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1$	Punkt $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 0$
Hyperbel $\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 1$	schneidendes Geradenpaar $\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 0$
leere Menge $-\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 1$	paralleles Geradenpaar $\frac{x^2}{\alpha^2} = 1$
Parabel $\frac{x^2}{\alpha^2} = 2y$	Gerade $\frac{x^2}{\alpha^2} = 0$

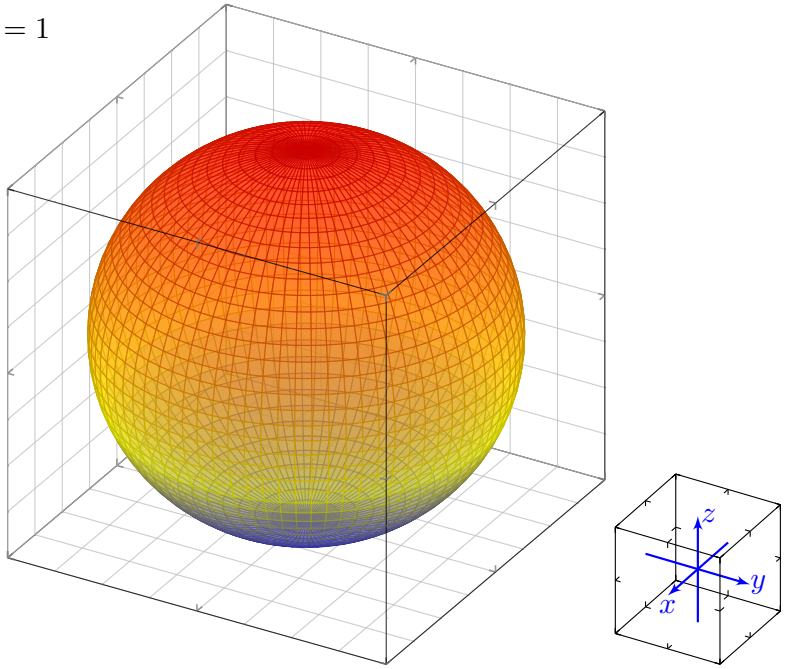
Klassifikation der reellen Quadriken im Raum $\mathbb{R}^3$

Ellipsoid $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} = 1$	elliptischer Doppelkegel $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} - \frac{z^2}{\gamma^2} = 0$	Punkt $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} = 0$
einschaliges Hyperboloid $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} - \frac{z^2}{\gamma^2} = 1$	elliptischer Zylinder $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1$	Gerade $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 0$
zweischaliges Hyperboloid $-\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} = 1$	parabolischer Zylinder $\frac{x^2}{\alpha^2} = 2y$	Ebene $\frac{x^2}{\alpha^2} = 0$
leere Menge $-\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} - \frac{z^2}{\gamma^2} = 1$	hyperbolischer Zylinder $\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 1$	schneidendes Ebenenpaar $\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 0$
elliptisches Paraboloid $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 2z$	hyperbolisches Paraboloid $\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 2z$	paralleles Ebenenpaar $\frac{x^2}{\alpha^2} = 1$

Reelle Quadriken im $\mathbb{R}^3$: Ellipsoid

O317

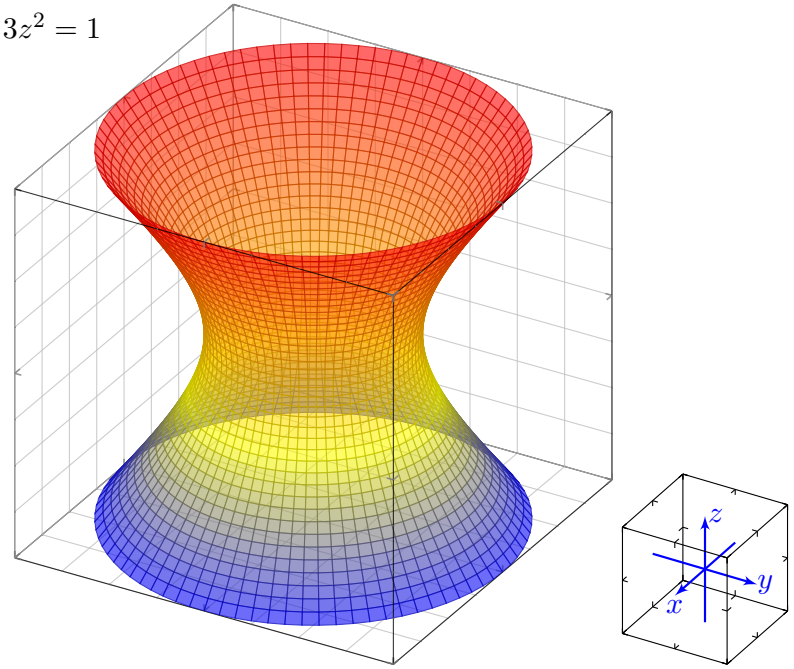
$x^2 + y^2 + z^2 = 1$



Reelle Quadriken im $\mathbb{R}^3$: einschaliges Hyperboloid

O318

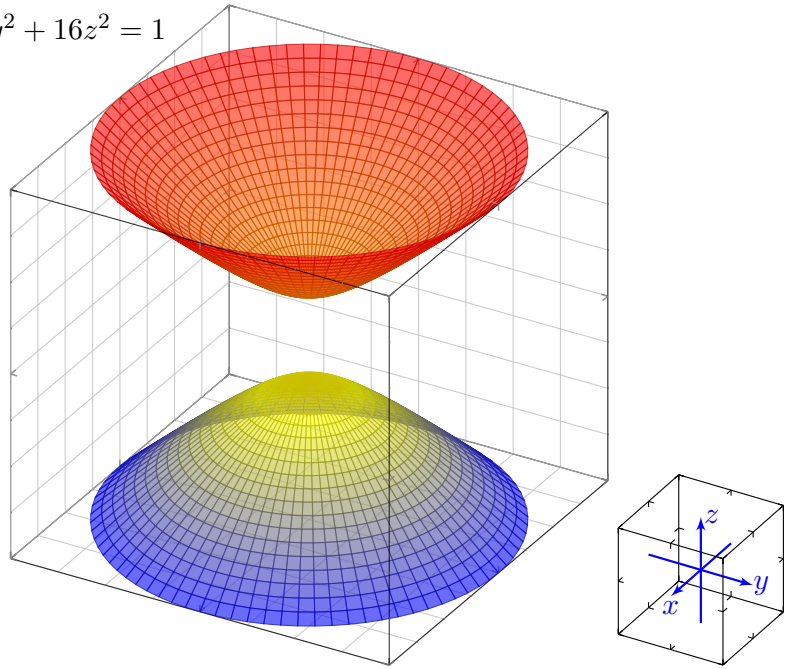
$4x^2 + 4y^2 - 3z^2 = 1$



Reelle Quadriken im $\mathbb{R}^3$: zweischaliges Hyperboloid

O319

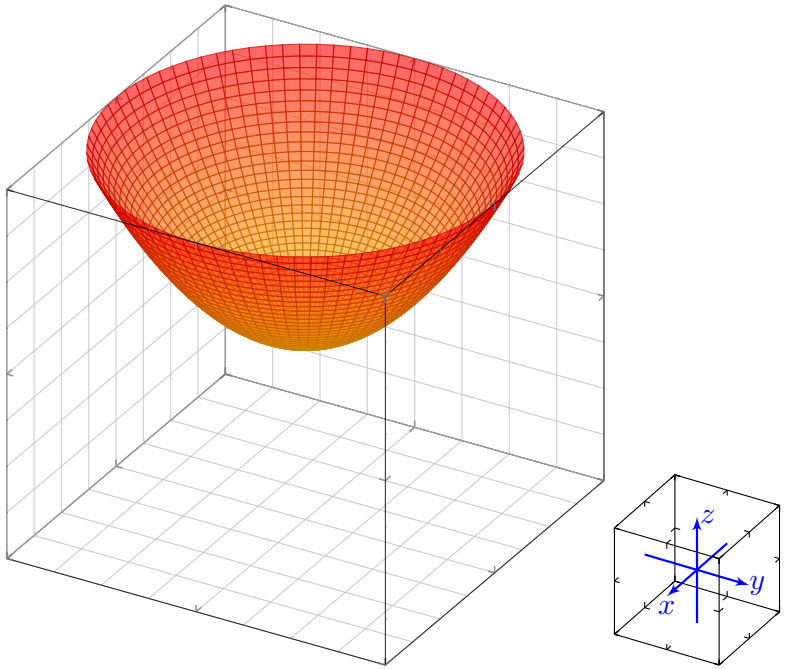
$-15x^2 - 15y^2 + 16z^2 = 1$



Reelle Quadriken im $\mathbb{R}^3$: elliptisches Paraboloid

O320

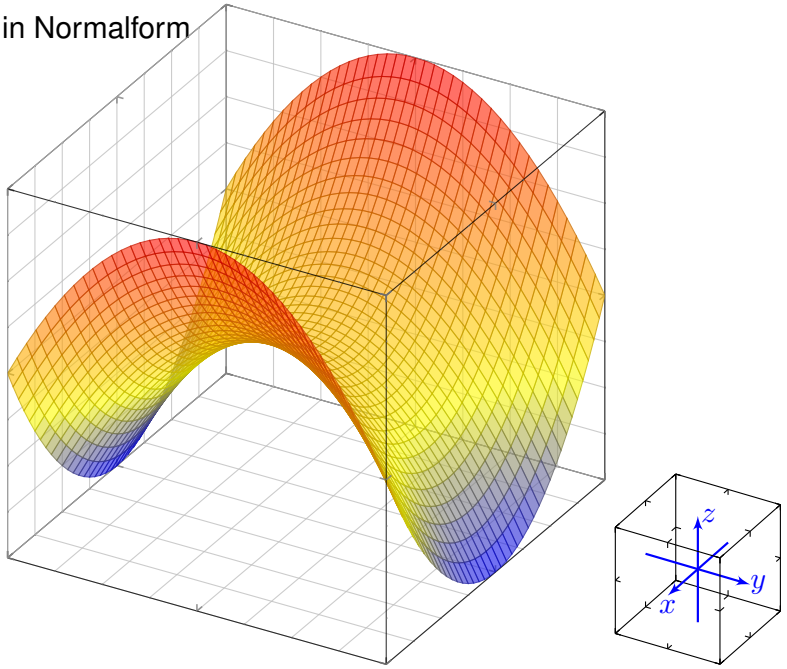
$z = x^2 + y^2$



Reelle Quadriken im $\mathbb{R}^3$: hyperbolisches Paraboloid

O321

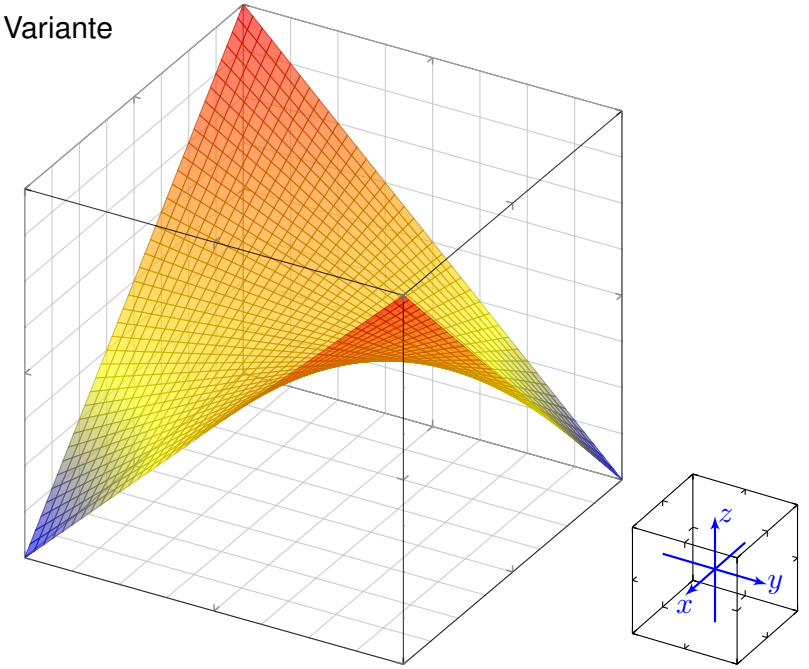
$z = x^2 - y^2$, in Normalform



Reelle Quadriken im $\mathbb{R}^3$: hyperbolisches Paraboloid

O322

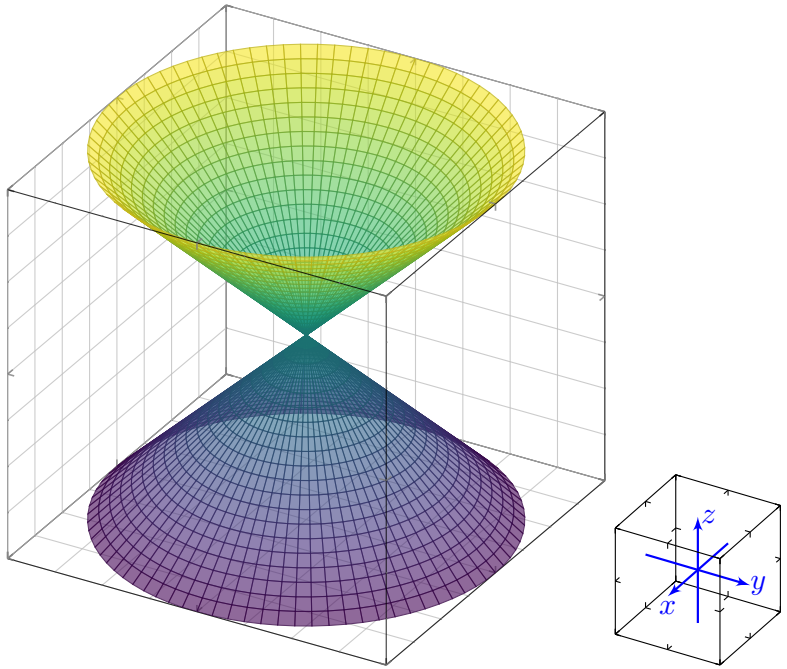
$z = xy$, als Variante



Reelle Quadriken im $\mathbb{R}^3$: elliptischer Doppelkegel

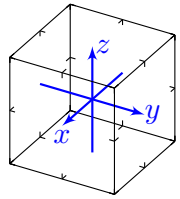
O323

$z^2 = x^2 + y^2$



Reelle Quadriken im $\mathbb{R}^3$

O324
Erläuterung



Alle Graphiken zeigen den Standardwürfel $[-1,1]^3$.
Der Ästhetik halber spare ich alle Beschriftungen,
da sie sich ohne jede Mühe rekonstruieren lassen.
Die Skalierungskonstanten $\alpha, \beta, \gamma \in \mathbb{R}_{>0}$ wähle ich
jeweils so, dass ein harmonisches Bild entsteht.

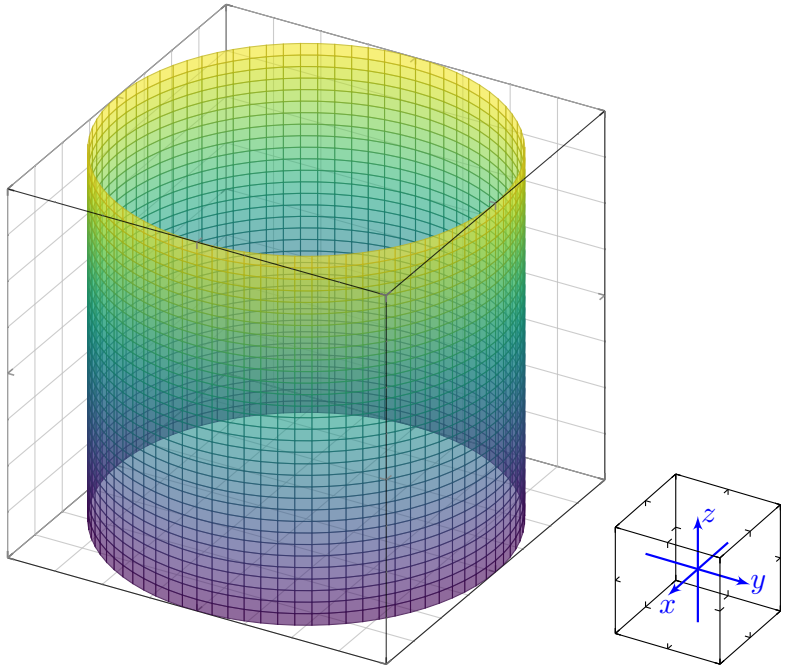
Unter einer typischen Quadrik im $\mathbb{R}^3$ stellen wir uns eine Fläche vor.
Die leere Menge, Punkt und Gerade sehen jedoch recht mager aus.
Es gibt in diesen Fällen allerdings noch viele Punkte im Komplexen,
also Lösungen in $\mathbb{C}^3$, die wir im Schnitt mit $\mathbb{R}^3 \subset \mathbb{C}^3$ nicht sehen.

Die folgenden Polynome enthalten nicht alle drei Variablen x, y, z,
sondern nur zwei Variablen x, y oder gar nur noch eine Variable x.
(Ganz ohne Variablen könnten wir auch noch 0 und 1 hinzufügen.)
Die zugehörige Quadrik ist daher ein Zylinder über einer Quadrik
in kleinerer Dimension. Wir erkennen hier die zuvor diskutierte
Klassifikation der reellen Quadriken in der Ebene $\mathbb{R}^2$.

Reelle Quadriken im $\mathbb{R}^3$: elliptischer Zylinder

O325

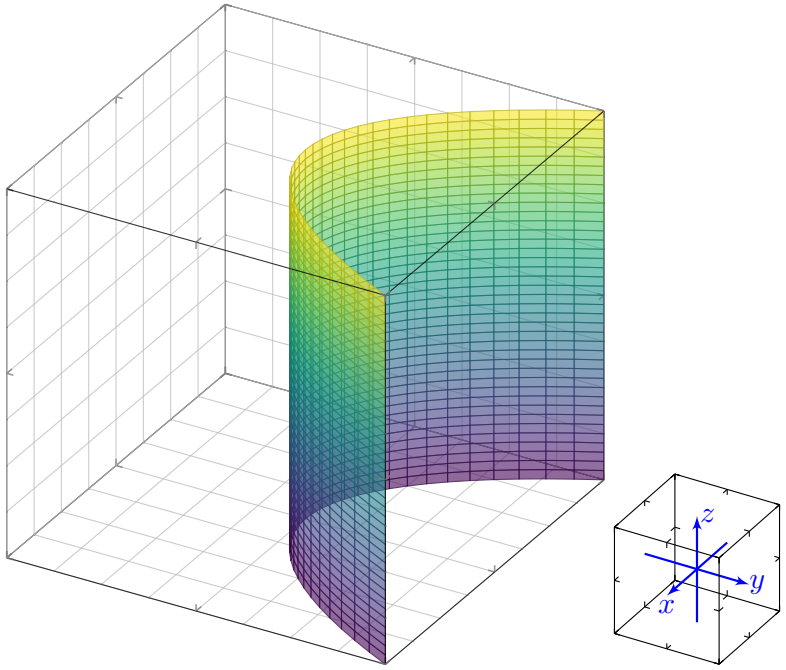
$x^2 + y^2 = 1$



Reelle Quadriken im $\mathbb{R}^3$: parabolischer Zylinder

O326

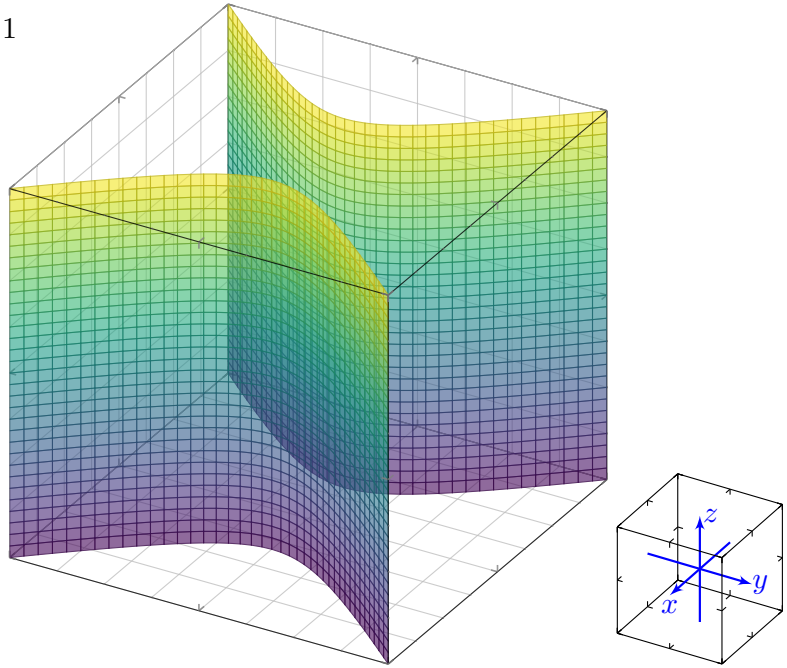
$y = x^2$



Reelle Quadriken im $\mathbb{R}^3$: hyperbolischer Zylinder

O327

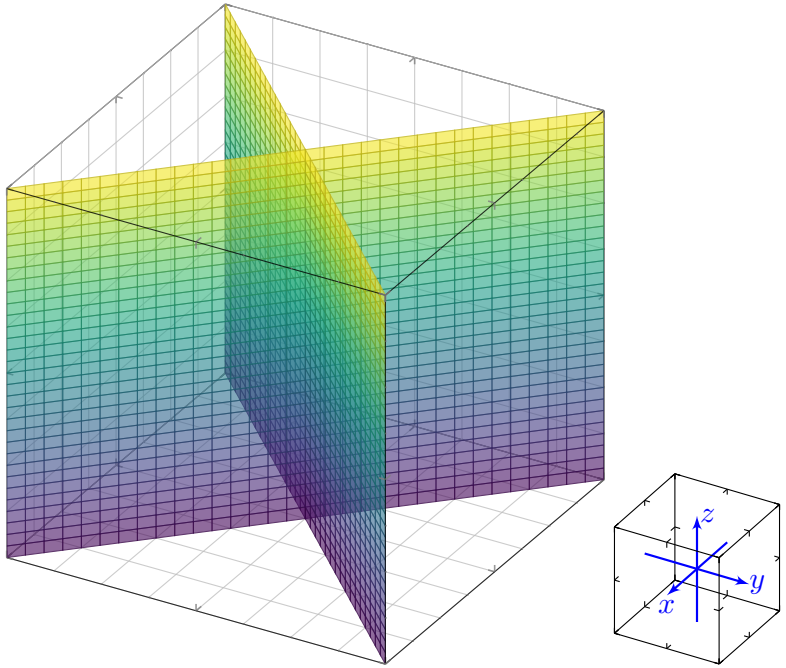
$9x^2 - 8y^2 = 1$



Reelle Quadriken im $\mathbb{R}^3$: schneidendes Ebenenpaar

O328

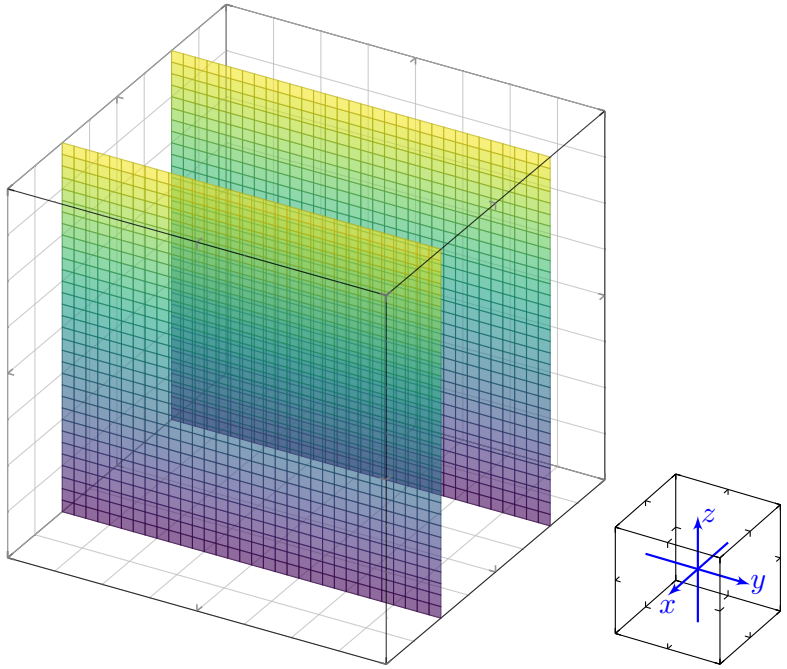
$x^2 - y^2 = 0$



Reelle Quadriken im $\mathbb{R}^3$: paralleles Ebenenpaar

O329

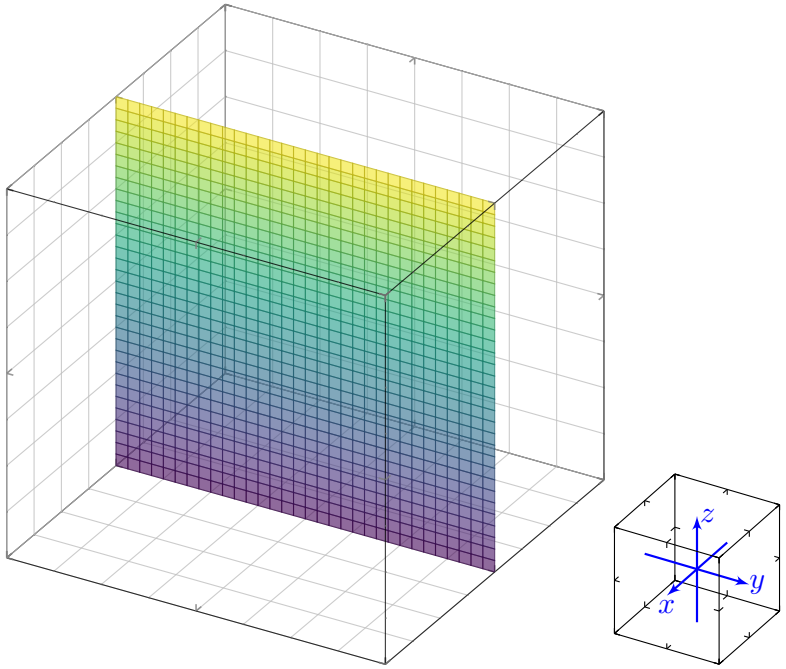
$4x^2 = 1$



Reelle Quadriken im $\mathbb{R}^3$: Ebene

O330

$x^2 = 0$



Die affine Klassifikation der reellen Quadriken

O331
Übung

Übung: Machen Sie sich mit der Klassifikation O316 vertraut: Nehmen Sie sich die Liste aller Normalformen und fertigen Sie jeweils selbst eine Skizze an. Umgekehrt: Übersetzen Sie die Abbildungen in Gleichungen.

Anleitung zum Zeichnen von solchen Nullstellen- / Lösungsmengen: Lege eine Koordinate fest, etwa $z = \text{const}$, und zeichne den Schnitt; wiederhole so oft wie nötig oder gewünscht, bis ein Bild entsteht.

Übung: Sind wirklich alle Fälle aus der Klassifikation O3F abgebildet? Welche Quadriken fehlen? Welche Quadriken treten mehrfach auf? Beschreiben $z = x^2 - y^2$ und $z = xy$ affin-äquivalente Quadriken?

Übung: Bei Quadriken $x'^{\mathsf{T}} A' x' = 0$ verlangen wir normalerweise $A \neq 0$. Welche Quadriken kommen noch hinzu, falls wir $A = 0$ erlauben? Klassifizieren Sie alle Quadriken $Q \subset \mathbb{R}^1$ in Dimension 1.

Übung: Welche Quadriken $Q \subset \mathbb{R}^3$ sind Vereinigung von Geraden? Bei den meisten ist dies offensichtlich, doch bei zweien überraschend! Hinweis: Es gibt eine mit $(r, r') = (3, 4)$ und eine mit $(r, r') = (2, 4)$.

Die affine Klassifikation der reellen Quadriken

O332
Übung

Für $n = 1, 2, 3$ betrachten wie die Klassifikation von $A' \in \mathbb{R}^{n' \times n'}$ modulo der Äquivalenz $\equiv$ unter Affinitäten und Skalierungen, wie in O3C erklärt.

Übung: Bestimmen Sie jeweils $r = \operatorname{rang} A$ und $r' = \operatorname{rang} A'$ sowie $s = |\operatorname{sign} A|$ und $s' = |\operatorname{sign} A'|$. Sind dies Invarianten unter Äquivalenz? Können Sie damit bereits alle Äquivalenzklassen $[A']$ unterscheiden?

Übung: Wenn Sie die Koeffizienten der Matrix A' zufällig wählen (unabhängig, stetig verteilt), welchen Typ $\delta \in \{0, 1, 2\}$ erwarten Sie?

Übung: Welche Äq'klassen $[A']$ sind stabil bei kleinen Störungen? Das heißt: Liegt B' genügend nahe bei A', so ist B' äquivalent zu A'.

Übung: Wir sagen $[A']$ liegt im Rand von $[C']$ wenn gilt: Es gibt beliebig kleine Änderungen von A' zu einem B', sodass B' äquivalent zu C' ist.

Anschaulich sagen wir auch: Die Klasse $[C']$ degeneriert zu $[A']$.
Beispiel: Beide Hyperboloide degenerieren zum Doppelkegel.

(1) Diese Relation ist reflexiv und transitiv, also eine Präordnung (F1A).
(2) Bestimmen Sie diese Präordnung für die obigen $3, 8, 15$ Klassen.

Kapitel P

Vektorräume mit Skalarprodukt

Unsere Allergrößten, wie Archimedes, Newton, Gauß,
haben stets Theorie und Anwendungen gleichmäßig umfasst.
Felix Klein (1849–1925)

Inhalt dieses Kapitels P

Motivation und Überblick

Wir untersuchen in diesem Kapitel reelle und komplexe Vektorräume mit einem Skalarprodukt. Damit messen wir Winkel, Längen und Abstände, wir betreiben also **Geometrie** im traditionellen, wörtlichen Sinne.

Diese fundamentale Idee kennen Sie bereits aus der Schulgeometrie, im Folgenden ist sie ebenso grundlegend für die **Lineare Algebra und Analytische Geometrie**. Darüber hinaus spielt sie (verallgemeinert) die zentrale Rolle in der Untersuchung von gekrümmten Flächen und allgemein in der Riemannschen Geometrie auf Mannigfaltigkeiten, bis hin zur speziellen und allgemeinen Relativitätstheorie.

Skalarprodukte begegnen Ihnen ebenso in der **Analysis**, zunächst als euklidisches Skalarprodukt bei der Untersuchung der metrischen und topologischen Eigenschaften des euklidischen Raumes $\mathbb{R}^n$, später dann ebenso in der Fourier–Theorie bei der Zerlegung periodischer Funktionen in harmonische Grundschwingungen, sowie in zahlreichen weiteren Anwendungen.

Motivation und Überblick

Ebenso wie die Analysis nutzt auch die **Numerik** Skalarprodukte, Normen und Metriken zur Messung von Abständen und von Fehlern, zur Kontrolle von Näherungen und zur Definition der Konvergenz.

Auch die **Methode der kleinsten Quadrate** beruht auf der Technik von Skalarprodukten und wird überall eingesetzt, wo fehlerbehaftete Daten verarbeitet werden, insbesondere linearisiert oder ähnlich geglättet.

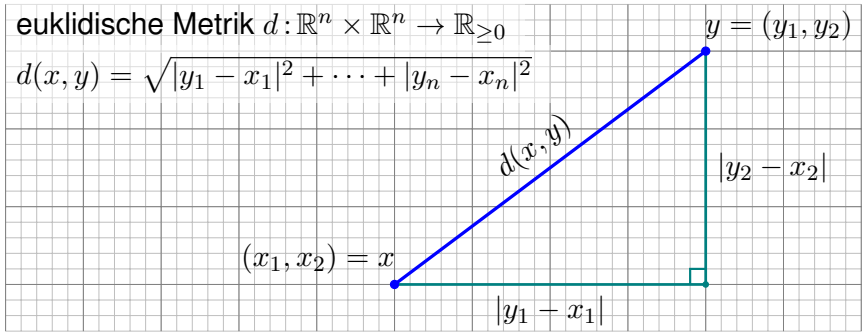
In der **Stochastik** verhält sich die Co/Varianz reeller Zufallsvariablen wie ein Skalarprodukt, und die lineare Regression nutzt die Methode der kleinsten Quadrate zur Untersuchung linearer Zusammenhänge.

In der **Physik** schließlich beruht die Quantenmechanik auf dem Modell, dass die Zustände eines Systems beschrieben werden durch Vektoren in einem Hilbert–Raum, also einem $\mathbb{C}$–Vektorraum mit Skalarprodukt.

Heisenbergs Unschärferelation entspricht (in geeigneter Übersetzung) der Cauchy–Schwarz–Ungleichung für Skalarprodukte von Vektoren.

Die euklidische Metrik: Satz des Pythagoras im $\mathbb{R}^n$

Wir betrachten den affinen Raum $\mathbb{R}^n$ über den reellen Zahlen $\mathbb{R}$.



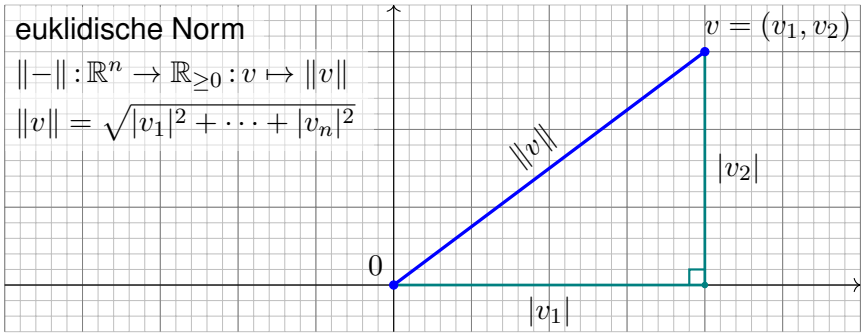
Die **euklidische Metrik** $d(x,y)$ misst den Abstand vom Punkt x zum Punkt y, also die Länge des Vektors $y - x$. Dank Pythagoras gilt:

$$d(x,y) = \sqrt{|y_1 - x_1|^2 + \cdots + |y_n - x_n|^2}$$

Die obige Skizze zeigt dies für $n = 2$. Übung: Skizzieren und begründen Sie dies für $n = 3$. Der allgemeine Fall $n \in \mathbb{N}$ gelingt dann per Induktion.

Die euklidische Norm: Satz des Pythagoras im $\mathbb{R}^n$

Wir betrachten den Vektorraum $\mathbb{R}^n$ über den reellen Zahlen $\mathbb{R}$.



Die **euklidische Norm** $\|v\|$ misst die Länge des Vektors $v \in \mathbb{R}^n$ als den Abstand vom Ursprung 0 zum Punkt v. Dank Pythagoras gilt:

$$\|v\| = \sqrt{|v_1|^2 + \cdots + |v_n|^2}$$

Das Normquadrat $\|v\|^2 = v_1^2 + \cdots + v_n^2$ ist eine quadratische Form. Die zugehörige Bilinearform ist das **euklidische Skalarprodukt**.

Das euklidische Skalarprodukt auf dem Raum $\mathbb{R}^n$

Beispiel P1A: das euklidische Skalarprodukt auf dem Raum $\mathbb{R}^n$

Auf $V = \mathbb{R}^n$ über $\mathbb{R}$ definieren wir das **euklidische Skalarprodukt**

$$\langle - \mid - \rangle : V \times V \to \mathbb{R} : (u,v) \mapsto \langle u \mid v \rangle := u_1 v_1 + \cdots + u_n v_n.$$

Für alle Vektoren $u, v, w \in V$ und Skalare $\lambda, \mu \in \mathbb{R}$ gilt:

S0: Positivität, $\langle u \mid u \rangle \geq 0 = \langle 0 \mid 0 \rangle$

S1: positive Definitheit, $\langle u \mid u \rangle > 0$ für $u \neq 0$

S2: Symmetrie, $\langle v \mid u \rangle = \langle u \mid v \rangle$

S3: Linearität rechts, $\langle u \mid \lambda v + \mu w \rangle = \lambda \langle u \mid v \rangle + \mu \langle u \mid w \rangle$

Aus (S2) und (S3) folgt Linearität auch in der ersten Variablen:

S4: Linearität links, $\langle \lambda u + \mu v \mid w \rangle = \lambda \langle u \mid w \rangle + \mu \langle v \mid w \rangle$

Aus dem euklidischen Skalarprodukt erhalten wir die **euklidische Norm** $\|-\| : V \to \mathbb{R}_{\geq 0} : v \mapsto \|v\| = \sqrt{\langle v \mid v \rangle}$, und aus dieser Norm wiederum die **euklidische Metrik** $d : V \times V \to \mathbb{R}_{\geq 0} : (x,y) \mapsto d(x,y) = \|y - x\|$.

Das euklidische Skalarprodukt auf dem Raum $\mathbb{R}^n$

Somit ist das euklidische Skalarprodukt $\langle - \mid - \rangle$ auf $V = \mathbb{R}^n$ über $\mathbb{R}$ eine **symmetrische Bilinearform** (S2,3) und **positiv definit** (S0,1). Dies sind die wesentlichen Eigenschaften des Skalarprodukts!

Aufgabe: Rechnen Sie die hier gemachten Aussagen nach.

Lösung: Symmetrie (S2) und Bilinearität (S3,4) sind klar.

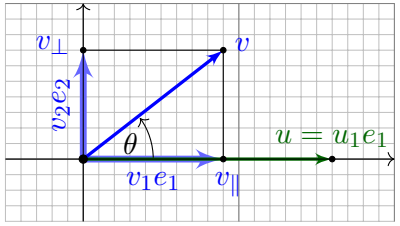
(S0) Für jeden Vektor $u \in \mathbb{R}^n$ gilt $\langle u \mid u \rangle = u_1^2 + \cdots + u_n^2 \geq 0$.

(S1) Im Falle $u \neq 0$ gilt $u_i \neq 0$ für mindestens ein $i \in \{1, \ldots, n\}$. Daraus folgt sofort die strikte Ungleichung $\langle u \mid u \rangle \geq u_i^2 > 0$.

Bemerkung: Aus (S1) folgt (S0), denn $\langle 0 \mid 0 \rangle = 0$ dank Linearität (S3). Die Formulierung der Eigenschaften (S0–3) ist daher etwas redundant; ich möchte damit die positive Definitheit (S1) besonders hervorheben.

Gilt in späteren Anwendungen statt positiver Definitheit (S1) nur die schwächere Eigenschaft (S0), so heißt $\langle - \mid - \rangle$ **positiv semidefinit**. Daher ist es sinnvoll, die Eigenschaft (S1) separat zu formulieren.

Geometrische Interpretation des euklidischen Skalarprodukts



Aus der Schule kennen Sie die geometrische Interpretation:
$\langle u \mid v \rangle = \|u\| \cdot \|v\| \cdot \cos \angle(u, v)$

Diese Formel gilt offensichtlich für $u = u_1e_1$ und $v = v_1e_1 + v_2e_2$ dank $v_1 = \|v\| \cos\theta$, $v_2 = \|v\| \sin\theta$.

🙂 Insbesondere folgt daraus die Ungleichung $|\langle u \mid v \rangle| \leq \|u\| \cdot \|v\|$.

Wir nutzen hierzu unsere geometrische Anschauung der Ebene. Das ist hilfreich zur Vorstellung und willkommen als Motivation.

⚠ Die Anschauung ist in der Mathematik meist eine gute Stütze, doch sie allein ist erfahrungsgemäß kein tragfähiges Fundament.

Wir werden für diese geometrischen Begriffe im Folgenden eine solide und allgemeine Grundlage erarbeiten, die sich nicht auf Anschauung oder Vorwissen beruft. Im Gegenteil werden wir so die geometrische Anschauung und die Anfänge der Trigonometrie begründen.

Geometrische Interpretation des euklidischen Skalarprodukts

Zu der obigen Interpretation $\langle u \mid v \rangle = \|u\| \cdot \|v\| \cdot \cos \angle(u, v)$ können Sie zu Recht einwenden, dass dies nur in dieser sehr speziellen Lage gilt.

🙂 Die gute Nachricht ist jedoch: Wir können zu u und v unsere Basis $e_1, e_2, \ldots$ immer so wählen, dass genau diese spezielle Lage entsteht, also $u = u_1e_1$ und $v = v_1e_1 + v_2e_2$ gilt. Das vereinfacht, wie gesehen!

Die geometrische Idee lässt sich auch ohne Koordinaten beschreiben: Bezüglich u zerlegen wir den Vektor $v = v_\parallel + v_\perp$ in seinen tangentialen Anteil $v_\parallel$ parallel zu u und seinen normalen Anteil $v_\perp$ senkrecht zu u.

🙂 Mit dem Skalarprodukt gelingt dies bequem und explizit wie folgt:

$$v_\parallel = u \frac{\langle u \mid v \rangle}{\langle u \mid u \rangle} \quad \text{und} \quad v_\perp = v - v_\parallel, \quad \text{somit} \quad \langle u \mid v_\perp \rangle = 0.$$

Das ist die Grundidee des Gram–Schmidt–Verfahrens (Satz P2A), das aus jeder Basis $b_1, \ldots, b_n$ eine Orthonormalbasis konstruiert.

🙂 Der obige Spezialfall erweist sich damit als allgemein: Wir wählen eine Orthonormalbasis $e_1, e_2, \ldots$ mit $u = u_1e_1$ und $v = v_1e_1 + v_2e_2$.

Geometrische Interpretation des euklidischen Skalarprodukts

Als leuchtendes Beispiel haben wir eingangs den Vektorraum $V = \mathbb{R}^n$ über $\mathbb{R}$ betrachtet. Hierauf haben wir das **euklidische Skalarprodukt**. Es heißt auch das **Standardskalarprodukt** auf dem Raum $V = \mathbb{R}^n$ oder das **kanonische Skalarprodukt**, weil es das Modellbeispiel eines Skalarprodukts ist. (Es gibt darüber hinaus viele weitere.)

Das so gebildete Paar $(\mathbb{R}^n, \langle - \mid - \rangle)$ nennen wir den **n–dimensionalen euklidischen Vektorraum** oder auch kurz den **euklidischen Raum**: Mit diesen Daten können wir Winkel, Längen und Abstände messen. Er ist das grundlegende Modell für die **euklidische Geometrie** (altgr. γεωμετρία , ‘Erdmessung’, ‘Landmessung’).

Speziell in niedriger Dimension $n = 2$ und $n = 3$ haben wir hierzu eine geometrische Anschauung und (mit etwas Glück schon in der Schule) eine mathematisch-physikalische Vorerfahrung. Dies wollen wir nutzen und zu einer tragfähigen Theorie und Rechenmethoden ausbauen.

Geometrische Interpretation des euklidischen Skalarprodukts

Daneben gibt es weitere nützliche Skalarprodukte auf dem Raum $\mathbb{R}^n$ sowie auf anderen $\mathbb{R}$–Vektorräumen V, auch unendlich-dimensional.

Damit können wir auch in diesen allgemeineren Räumen Winkel, Längen und Abstände messen, also Geometrie betreiben wie im $\mathbb{R}^n$.

Die Erfahrung zeigt, dass die oben gesammelten Eigenschaften (S1–3) die wesentliche Grundlage für all unsere weiteren Rechnungen sind.

Diese Eigenschaften erheben wir daher nun zur Definition P1B und erklären so, was wir allgemein unter einem Skalarprodukt verstehen.

Das ist ein kühner Schritt der Verallgemeinerung, doch erweist sich als effizient und klärend: Sie schärft den Blick für das Wesentliche.

Abstraktion strukturiert und vereinfacht: Eine allgemeine Tatsache ist oft leichter zu verstehen und zu erklären als ihre zahlreichen Spezialfälle.

Skalarprodukt: allgemeine Definition

Definition P1B: Skalarprodukt über $\mathbb{R}$

Ein **Skalarprodukt** auf einem $\mathbb{R}$–Vektorraum V ist eine positiv definite, symmetrische Bilinearform $\langle - \mid - \rangle : V \times V \to \mathbb{R}$, erfüllt also (S1–3).

Die zugehörige **Norm** ist dann $\|-\| : V \to \mathbb{R}_{\geq 0} : v \mapsto \|v\| = \sqrt{\langle v \mid v \rangle}$.

♦ Beispiel P1A: die Produktsumme auf $\mathbb{R}^n$

Auf dem $\mathbb{R}$–Vektorraum $\mathbb{R}^n$ haben wir das euklidische Skalarprodukt

$$\langle u \mid v \rangle = \sum_{k=1}^{n} u_k v_k.$$

♦ Beispiel P1Q: das Produktintegral auf $\mathscr{C}([a,b],\mathbb{R})$

Sei $a < b$ in $\mathbb{R}$ und $\mathscr{C}([a,b],\mathbb{R})$ der $\mathbb{R}$–Vektorraum aller stetigen Funktionen $f, g : [a,b] \to \mathbb{R}$. Hierauf haben wir das Skalarprodukt

$$\langle f \mid g \rangle = \int_{t=a}^{b} f(t)g(t)\,\mathrm{d}t.$$

Die Cauchy–Schwarz–Ungleichung

Wir legen hier nur die drei Eigenschaften (S1–3) zugrunde. In vorigen Beispiel P1A des euklidischen Skalarprodukts waren dies *Folgerungen* aus der explizit gegebenen Formel. In Definition P1B erheben wir diese nun zu den grundlegenden *Forderungen*. Damit können wir arbeiten:

Satz P1C: Cauchy–Schwarz–Ungleichung (CSU)

Aus (S1–3) folgt für alle $u, v \in V$ die **Cauchy–Schwarz–Ungleichung**:

$$|\langle u \mid v \rangle|^2 \leq \langle u \mid u \rangle \langle v \mid v \rangle \quad \text{kurz} \quad |\langle u \mid v \rangle| \leq \|u\| \cdot \|v\|$$

Gleichheit gilt genau dann, wenn u, v über $\mathbb{R}$ linear abhängig sind.

Kurzbeweis: Dies ist klar für $v = 0$. Sei also $v \neq 0$. Für alle $t \in \mathbb{R}$ gilt:

$$0 \overset{(S1)}{\leq} \langle u + tv \mid u + tv \rangle \overset{(S2,3)}{=} \underbrace{\langle u \mid u \rangle}_{c \in \mathbb{R}_{\geq 0}} + 2 \underbrace{\langle u \mid v \rangle}_{b \in \mathbb{R}} t + \underbrace{\langle v \mid v \rangle}_{a \in \mathbb{R}_{>0}} t^2$$

Demnach ist die Diskriminante nicht positiv: $b^2 - ac \leq 0$. QED

Die Cauchy–Schwarz–Ungleichung

Ausführlicher Beweis: Für $v = 0$ ist alles klar. Sei also $v \neq 0$.

(1) Wir setzen $z := au - bv$ mit $a = \langle v \mid v \rangle$ und $b = \langle v \mid u \rangle$ und rechnen:

$$\begin{aligned} 0 &\overset{(S0)}{\leq} \langle z \mid z \rangle \overset{\text{Def}}{=} \langle au - bv \mid au - bv \rangle \\ &\overset{(S3,4)}{=} a^2 \langle u \mid u \rangle - ab\langle u \mid v \rangle - ab\langle v \mid u \rangle + b^2 \langle v \mid v \rangle \\ &\overset{(S2)}{=} \langle v \mid v \rangle \left[\langle u \mid u \rangle \langle v \mid v \rangle - |\langle u \mid v \rangle|^2 \right] \end{aligned}$$

Dank (S1) gilt $\langle v \mid v \rangle > 0$. Wir erhalten so die ersehnte Ungleichung:

$$\langle u \mid u \rangle \langle v \mid v \rangle - |\langle u \mid v \rangle|^2 \geq 0$$

(2) Gleichheit impliziert $0 = \langle z \mid z \rangle$, also $0 = z$ und somit $u = (b/a)v$.
Umgekehrt folgt aus linearer Abhängigkeit $u = \lambda v$ direkt die Gleichheit

$$\begin{aligned} |\langle u \mid v \rangle|^2 &\overset{\text{Def}}{=} |\langle \lambda v \mid v \rangle|^2 \overset{(S2)}{=} \langle \lambda v \mid v \rangle \langle v \mid \lambda v \rangle \\ &\overset{(S3)}{=} \langle \lambda v \mid \lambda v \rangle \langle v \mid v \rangle \overset{\text{Def}}{=} \langle u \mid u \rangle \langle v \mid v \rangle. \end{aligned}$$

Damit ist die Cauchy–Schwarz–Ungleichung bewiesen. QED

Die Cauchy–Schwarz–Ungleichung

Beide Beweise sind elegant, genial-einfach und einfach-genial!
Beide Argumente zaubern trickreich ein Kaninchen aus dem Hut:
Wir betrachten hier eine Linearkombination $z = au - bv$ mit $a, b \in \mathbb{R}$.
Als profitabel erweisen sich die Wahlen $a = \langle v \mid v \rangle$ und $b = \langle v \mid u \rangle$.

☺ Der Rest ist Ausrechnen und Ablesen der ersehnten Ungleichung.

Wie kommt man auf diese Koeffizienten? Wie merkt man sie sich?
Anders gefragt: Wie führt man den Beweis, wenn man sich zwar an den Ansatz $z = au - bv$ erinnert, aber nicht an a und b?

Die Rechnung bis zur zweiten Zeile ist noch ganz allgemein.
Wenn wir die letzten beiden Summanden auslöschen möchten, dann gelingt dies mit der Wahl $a = \langle v \mid v \rangle$ und $b = \langle v \mid u \rangle$. Voilà!

☺ So lassen sich Ansatz und Strategie leicht verstehen und merken.

Der folgende, dritte Beweis gibt hierzu eine geometrische Motivation, und erklärt insbesondere, wie man auf den Ansatz $z = au - bv$ kommt.

Dritter Beweis: Für $v = 0$ ist alles klar. Sei also $v \neq 0$.
Wir zerlegen $u = u_{\parallel} + u_{\perp}$ mit $u_{\parallel} = \lambda v$ und $u_{\perp} = u - u_{\parallel}$.
Um Orthogonalität $v \perp u_{\perp}$ zu erreichen, betrachten wir
$\langle v \mid u_{\perp} \rangle = \langle v \mid u \rangle - \lambda \langle v \mid v \rangle$ und setzen $\lambda = \langle v \mid u \rangle / \langle v \mid v \rangle$.
Hier nutzen wir (S1), dies garantiert $\langle v \mid v \rangle > 0$. Damit gilt:

$$\begin{aligned} 0 &\overset{(S0)}{\leq} \langle u_{\perp} \mid u_{\perp} \rangle \overset{\text{Def}}{=} \langle u - \lambda v \mid u - \lambda v \rangle \\ &\overset{(S3,4)}{=} \langle u \mid u \rangle - \lambda \langle u \mid v \rangle - \lambda \langle v \mid u \rangle + \lambda^2 \langle v \mid v \rangle \\ &\overset{(S2)}{=} \langle u \mid u \rangle - |\langle u \mid v \rangle|^2 \langle v \mid v \rangle^{-1} \end{aligned}$$

Hieraus lesen wir sofort die Cauchy–Schwarz–Ungleichung ab.
Gleichheit gilt genau dann, wenn $u_{\perp} = 0$, also $u = u_{\parallel} = \lambda v$. QED

Übung: Vergleichen Sie den zweiten und den dritten Beweis.
Beide beruhen im Wesentlichen auf derselben Rechnung!
Der dritte ist geometrisch motiviert und dadurch instruktiv.
Der zweite ist algebraisch optimiert und etwas eleganter.

In unserem ursprünglichen Beispiel des euklidischen Skalarprodukts bedeutet die Cauchy–Schwarz–Ungleichung ganz konkret und explizit:

$$(u_1^2 + \cdots + u_n^2)(v_1^2 + \cdots + v_n^2) \geq (u_1 v_1 + \cdots + u_n v_n)^2$$

für alle reellen Zahlen $u_1, \ldots, u_n, v_1, \ldots, v_n \in \mathbb{R}$.

Übung: Bitte versuchen Sie, diese Ungleichung möglichst „direkt“ zu zeigen, ohne „Umweg“ über die allgemeine Theorie der Skalarprodukte.

Vermutlich werden Sie spüren, dass diese ganz konkret und harmlos erscheinende Ungleichung alles andere als leicht zu beweisen ist.

Nach eigenen Versuchen werden Sie feststellen, dass der oben erklärte allgemeine Begriff des Skalarprodukts und der so entwickelte Beweis gar kein Umweg ist, sondern eine Abkürzung! Ich betone daher erneut:

Abstraktion strukturiert und vereinfacht: Eine allgemeine Tatsache ist oft leichter zu verstehen und zu erklären als ihre zahlreichen Spezialfälle.

Die Cauchy–Schwarz–Ungleichung ist eine der zentralen und universell nützlichen Ungleichungen in der Mathematik und ebenso für die Physik. Sie findet Anwendungen in der Geometrie, der Analysis, der Stochastik und der Quantenmechanik (etwa als Heisenbergs Unschärferelation).

Augustin-Louis Cauchy (1789–1857) veröffentlichte seine berühmte Ungleichung 1821 und in seinem Lehrbuch *Cours d'Analyse Algébrique*, dem wohl ersten, aus heutiger Sicht strengen Aufbau der Analysis.

Victor Yacovlevich Bunyakovsky (1804–1889) studierte in Paris bei Cauchy und übertrug dessen Ungleichung von Summen auf Integrale, veröffentlicht 1859 in St. Petersburg, allerdings noch ohne Beweis.

Hermann Amandus Schwarz (1843–1921) arbeitete 1885 in Göttingen an Flächen minimaler Krümmung und benötigte dazu auch Chauchys Ungleichung für Integrale. Ihm gelang die allgemeine Formulierung, und der obige Beweis geht im Wesentlichen auf Schwarz zurück.

🙂 Eine genial-einfache Idee liefert alle nötigen Informationen.

Im deutsch-sprachigen Raum ist die Bezeichnung *Cauchy–Schwarz–Ungleichung* üblich. In englisch-sprachigen Texten findet man häufig nur *Schwarz's inequality*, in französisch-sprachigen entsprechend *l'inegalité de Schwarz*, die russische Tradition hingegen bevorzugt *Cauchy–Bunyakovsky–Schwarz Ungleichung*. Alle drei Sichtweisen haben ihre Gründe; historische Gerechtigkeit ist meist schwierig.

Die gesamte Analysis beruht zu weiten Teilen auf Ungleichungen, und die Cauchy–Schwarz–Ungleichung ist hier ein erstes wichtiges Ergebnis sowie Vorbild für zahlreiche nachfolgende Ungleichungen.

📖 J.M. Steele: *The Cauchy–Schwarz master class. An Introduction to the Art of Mathematical Inequalities.* Cambridge University Press 2004.

Übung: Sei V ein Vektorraum mit Skalarprodukt und $u, v \in V$.
(1) Orthogonalität $u \perp v$ ist äquivalent zu $\|u + tv\| \geq \|u\|$ für alle $t \in \mathbb{R}$.
(2) Machen Sie eine Skizze und interpretieren Sie dies geometrisch.

Winkel dank Cauchy–Schwarz–Ungleichung

Sei V ein $\mathbb{R}$–Vektorraum mit einem Skalarprodukt $\langle - \mid - \rangle : V \times V \to \mathbb{R}$.
Folgerung aus der CSU: Für je zwei Vektoren $u, v \in V \smallsetminus \{0\}$ gilt

$$\frac{\langle u \mid v \rangle}{\|u\| \cdot \|v\|} \in [-1, 1].$$

Daher existiert genau eine reelle Zahl $\theta \in [0, \pi]$ mit

$$\cos\theta = \frac{\langle u \mid v \rangle}{\|u\| \cdot \|v\|}.$$

Wir definieren den **Winkel** zwischen den Vektoren u und v durch

$$\boxed{\angle(u,v) := \theta = \arccos\left(\frac{\langle u \mid v \rangle}{\|u\| \cdot \|v\|}\right).}$$

So überführen wir unsere geometrische Intuition in eine solide Definition und bequeme Rechnung: Damit können wir Winkel effizient berechnen. Die obige Formel ist vollkommen explizit und bereit zum Einsatz.

Winkel dank Cauchy–Schwarz–Ungleichung

🙂 Das ist eine genial-einfache Idee und elegante Definition. Wie sonst sollten wir den Winkel zwischen zwei Vektoren u und v ermitteln?

In der euklidischen Ebene $\mathbb{C} = \mathbb{R}^2$ gelingt dies mit dem Bogenmaß und den trigonometrischen Funktionen $\sin$ und $\cos$, wie oben erklärt (P105).

Noch informativer ist der **orientierte Winkel** $\alpha \in \,]-\pi, \pi]$, definiert durch

$$\frac{v}{\|v\|} = e^{i\alpha}\frac{u}{\|u\|} \quad \text{also} \quad \frac{1}{\|v\|}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \frac{1}{\|u\|}\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}.$$

🙂 Die oben erklärte Gleichung $\langle u \mid v \rangle = \|u\| \cdot \|v\| \cdot \cos\theta$ genügt, um den **absoluten Winkel** $\theta = |\alpha| \in [0, \pi]$ zu bestimmen. Das **Vorzeichen** entspricht der Orientierung des Winkels und gelingt nur in der Ebene, wo wir Links- und Rechtsdrehung unterscheiden vermöge $\det(u, v) \geq 0$ oder $\det(u, v) < 0$. Schon im Raum $\mathbb{R}^3$ ist dies nicht mehr möglich.

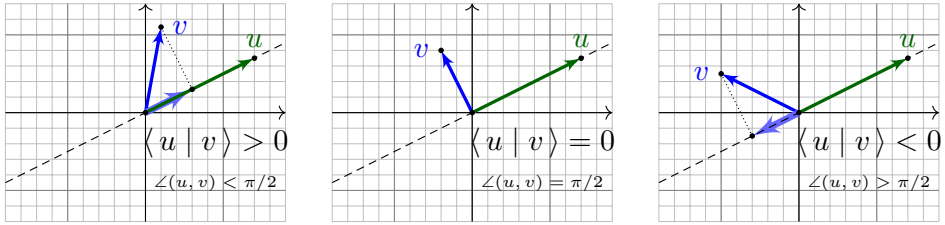
In höherdimensionalen Räumen verlässt uns die Anschauung vollends. Wie wollen Sie den Winkel zwischen zwei Vektoren im $\mathbb{R}^{100}$ messen? So gesehen ist die obige Definition wirklich einfach und elegant.

Winkel dank Cauchy–Schwarz–Ungleichung

Damit gilt weiterhin die gewohnte Gleichung

$$\boxed{\langle u \mid v \rangle \;=\; \|u\| \cdot \|v\| \cdot \cos\angle(u,v).}$$

Wie zuvor ist $\|v\| \cos\angle(u,v)$ die Länge der Projektion von v parallel zu u.



Im wichtigen Spezialfall $\langle u \mid v \rangle = 0$ sagen wir, die Vektoren u und v sind **orthogonal** oder **stehen senkrecht** zueinander, geschrieben

$$\boxed{u \perp v \;\;:\Longleftrightarrow\;\; \langle u \mid v \rangle = 0.}$$

Winkel dank Cauchy–Schwarz–Ungleichung

⚠ Den Winkel $\angle(u, v)$ können wir nur für Vektoren $u, v \in V$ definieren, die ungleich Null sind, da wir durch die Normen $\|u\|$ und $\|v\|$ dividieren.

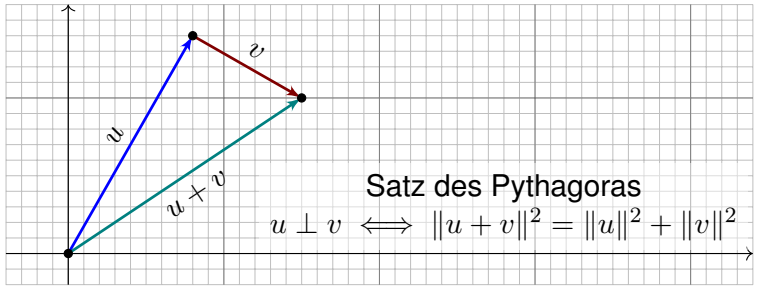
🙂 Orthogonalität hingegen können wir für je zwei beliebige Vektoren $u, v \in V$ definieren durch die einfache Bedingung $\langle u \mid v \rangle = 0$.

Orthogonalität wird im Folgenden eine große Rolle spielen, sowohl für die Entwicklung der Theorie als auch in der Anwendung der Methoden.

Als zwei einfacher doch eindrückliche Beispiele diskutieren wir den Satz des Pythagoras und die Parallelogrammgleichung.

Eingangs haben wir das euklidische Skalarprodukt durch Pythagoras motiviert und hergeleitet. Schön zu sehen und beruhigend zu wissen, dass dieser wichtige Satz bei unserer Abstraktion nicht verloren geht. Im Gegenteil, er erhält nun seine gebührend allgemeine Formulierung.

Satz des Pythagoras



☺ In Worten: In jedem rechtwinkligen Dreieck ist das Normquadrat der Hypotenuse gleich der Summe der Normquadrate der Katheten.

Satz des Pythagoras

Satz P1D: Pythagoras

Sei V ein $\mathbb{R}$–Vektorraum mit einem Skalarprodukt

$$\langle - \mid - \rangle : V \times V \to \mathbb{R} : (u, v) \mapsto \langle u \mid v \rangle.$$

(1) Für je zwei Vektoren $u, v \in V$ gilt dann die Gleichung

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2 + 2\,\langle u \mid v \rangle.$$

Mit dem oben eingeführten Winkel $\angle(u, v)$ schreibt sich dies wie folgt:

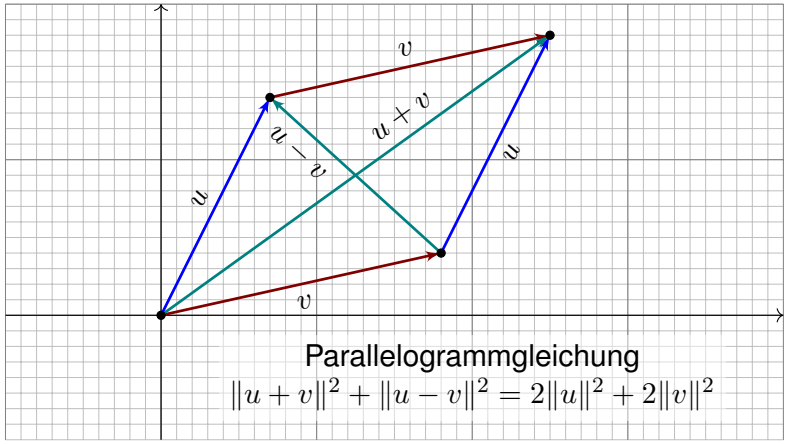
$$\|u + v\|^2 = \|u\|^2 + \|v\|^2 + 2\,\|u\| \cdot \|v\| \cdot \cos \angle(u, v)$$

(2) Stehen u und v senkrecht zueinander, so entfällt der letzte Term:

$$u \perp v \quad \Longleftrightarrow \quad \|u + v\|^2 = \|u\|^2 + \|v\|^2$$

Übung: Alles steht explizit da. Rechnen Sie es sorgsam nach!

Die Parallelogrammgleichung



☺ In Worten: In jedem Parallelogramm ist die Summe der Quadrate der vier Seiten gleich der Summe der Quadrate der beiden Diagonalen.

Die Parallelogrammgleichung

Satz P1E: Parallelogrammgleichung

Sei V ein $\mathbb{R}$–Vektorraum mit einem Skalarprodukt

$$\langle - \mid - \rangle : V \times V \to \mathbb{R} : (u, v) \mapsto \langle u \mid v \rangle.$$

(1) Für je zwei Vektoren $u, v \in V$ gilt dann die Gleichung

$$\|u + v\|^2 + \|u - v\|^2 = 2\|u\|^2 + 2\|v\|^2.$$

(2) Allein aus der Norm $\|-\|$ lässt sich das Skalarprodukt $\langle - \mid - \rangle$ rekonstruieren dank der folgenden Polarisationsformel:

$$\langle u \mid v \rangle = \frac{1}{4}\Big[\|u + v\|^2 - \|u - v\|^2\Big]$$

☺ Insbesondere folgt damit $u \perp v \;\Leftrightarrow\; \|u + v\| = \|u - v\|$.
Jeder gute Handwerker kennt diesen Test zur Rechtwinkligkeit.

Norm und Dreiecksungleichung

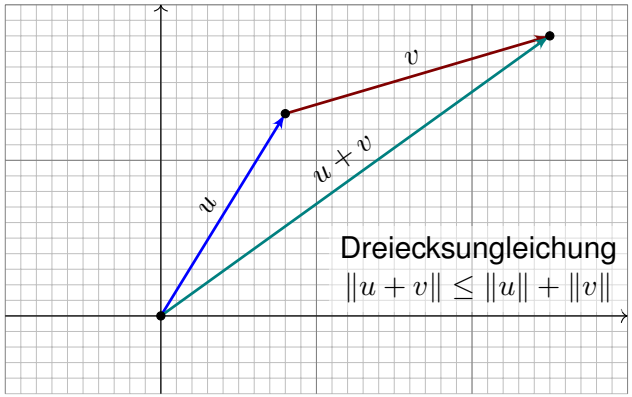
Sei V ein $\mathbb{R}$–Vektorraum mit einem Skalarprodukt

$$\langle - \mid - \rangle : V \times V \to \mathbb{R} : (u, v) \mapsto \langle u \mid v \rangle.$$

Die zugehörige **Norm** misst die Länge von Vektoren:

$$\|-\| : V \to \mathbb{R}_{\geq 0} : v \mapsto \|v\| = \sqrt{\langle v \mid v \rangle}$$

Was sind ihre wesentlichen Eigenschaften?



Eigenschaften der Norm

Satz P1F: Eigenschaften der Norm

Für alle Vektoren $u, v \in V$ und Skalare $\lambda \in \mathbb{R}$ gilt:

N0:	Positivität,	$\|u\| \geq 0 = \|0\|$
N1:	positive Definitheit,	$\|u\| > 0$ für $u \neq 0$
N2:	absolute Homogenität,	$\|\lambda u\| = \|\lambda\| \cdot \|u\|$
N3:	Dreiecksungleichung,	$\|u + v\| \leq \|u\| + \|v\|$

Wir benötigen: Die Wurzelfunktion $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto \sqrt{x}$ erfüllt $\sqrt{0} = 0$, ist streng monoton, $x < y \Rightarrow \sqrt{x} < \sqrt{y}$, und multiplikativ, $\sqrt{xy} \leq \sqrt{x}\sqrt{y}$.

Beweis: Aus (S0,1,2) folgt (N0,1,2), und (N3) folgt dank CSU:

$$\|u+v\|^2 \overset{\text{Def}}{=} \langle u+v \mid u+v \rangle \overset{\text{Bil}}{=} \langle u \mid u \rangle + \langle u \mid v \rangle + \langle v \mid u \rangle + \langle v \mid v \rangle$$
$$\overset{\text{CSU}}{\leq} \|u\|^2 + 2\,\|u\|\,\|v\| + \|v\|^2 \overset{\text{Bin}}{=} (\|u\| + \|v\|)^2$$

Daraus folgt $\|u + v\| \leq \|u\| + \|v\|$, wie behauptet. QED

Weitere Beispiele: Taxinorm und Maximumsnorm

Eine Abbildung $\|-\| : V \to \mathbb{R}_{\geq 0}$ mit den obigen Eigenschaften (N1–3) nennen wir eine **Norm** auf dem Vektorraum V, siehe Definition P1L.

Beispiel: Auf dem Vektorraum $\mathbb{R}^n$ nutzen wir je nach Bedarf vor allem

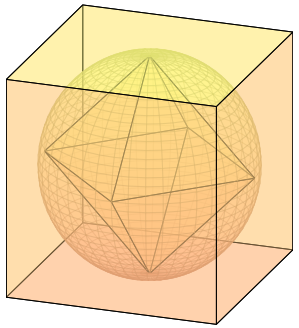
die Taxinorm	$\|x\|_1 := \|x_1\| + \|x_2\| + \cdots + \|x_n\|,$
die Maximumsnorm	$\|x\|_\infty := \max\{\, \|x_1\|, \|x_2\|, \ldots, \|x_n\| \,\},$
die euklidische Norm	$\|x\|_2 := \sqrt{\|x_1\|^2 + \|x_2\|^2 + \cdots + \|x_n\|^2}\,.$

Übung: (1) Weisen Sie nach, dass dies tatsächlich Normen sind.
(2) Taxinorm und Maximumsnorm kommen jedoch nicht von einem Skalarprodukt, denn sie erfüllen nicht die Parallelogrammgleichung P1E.

Statt der Schreibweise $\|u\|$ für Normen ist abkürzend auch $|u|$ üblich. Erstere dient zur Betonung und zur Unterscheidung vom Betrag.

Ein Vektor $u \in V$ heißt **normiert**, falls $\|u\| = 1$ gilt. Wir können jeden Vektor $v \in V \smallsetminus \{0\}$ normieren zu $u = \|v\|^{-1} v$ mit $\|u\| = \|v\|^{-1}\|v\| = 1$.

Weitere Beispiele: Taxinorm und Maximumsnorm



Die euklidische Norm $\|-\|_2 : \mathbb{R}^n \to \mathbb{R}_{\geq 0} : v \mapsto \sqrt{\langle v \mid v \rangle}$ definiert den **abgeschlossenen / offenen Einheitsball** und die **Einheitssphäre**:

$$\mathbb{D}^n := \{\, x \in \mathbb{R}^n \mid \|x\|_2 \leq 1 \,\} = \{\, x \in \mathbb{R}^n \mid x_1^2 + \cdots + x_n^2 \leq 1 \,\},$$
$$\mathbb{B}^n := \{\, x \in \mathbb{R}^n \mid \|x\|_2 < 1 \,\} = \{\, x \in \mathbb{R}^n \mid x_1^2 + \cdots + x_n^2 < 1 \,\},$$
$$\mathbb{S}^{n-1} := \{\, x \in \mathbb{R}^n \mid \|x\|_2 = 1 \,\} = \{\, x \in \mathbb{R}^n \mid x_1^2 + \cdots + x_n^2 = 1 \,\}.$$

Für die Maximumsnorm erhalten wir hier stattdessen den **Würfel**.
Für die Taxinorm erhalten wir dual hierzu das **Kreuzpolytop**.

Metrik und Dreiecksungleichung

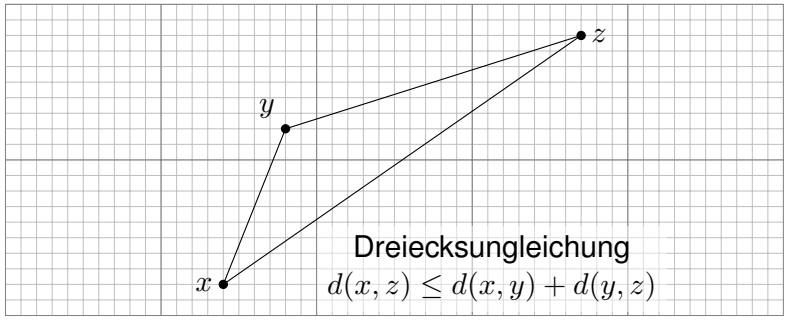
Sei V ein $\mathbb{R}$–Vektorraum mit einer Norm

$$\|-\| : V \to \mathbb{R}_{\geq 0} : v \mapsto \|v\| = \sqrt{\langle v \mid v \rangle}$$

Die zugehörige **Metrik** misst den Abstand von Punkten:

$$d : V \times V \to \mathbb{R}_{\geq 0} : (x, y) \mapsto d(x, y) = \|y - x\|$$

Was sind ihre wesentlichen Eigenschaften?



Die Dreiecksungleichung besagt anschaulich: Der Weg von x nach z wird nicht kürzer, wenn wir einen Umweg über y machen.

Eigenschaften der Metrik

Satz P1G: Eigenschaften der Metrik

Die zur Norm $\|-\| : V \to \mathbb{R}_{\geq 0}$ gehörige Metrik

$$d : V \times V \to \mathbb{R}_{\geq 0} : (x, y) \mapsto d(x, y) := \|y - x\|$$

erfreut sich folgender Eigenschaften für alle $x, y, z \in V$:

M0: Positivität,	$d(x,y) \geq 0 = d(x,x)$
M1: positive Definitheit,	$d(x,y) > 0$ für $x \neq y$
M2: Symmetrie,	$d(x,y) = d(y,x)$
M3: Dreiecksungleichung,	$d(x,z) \leq d(x,y) + d(y,z)$

Aufgabe: Rechnen Sie dies zur Übung nach!

Lösung: Aus (N0,1,2,3) folgt (M0,1,2,3), hier für (M3) ausführlich:

$$\begin{aligned} d(x,z) &\overset{\text{Def}}{=} \|z - x\| \overset{\text{Vek}}{=} \|z - y + y - x\| \\ &\overset{(N3)}{\leq} \|z - y\| + \|y - x\| \overset{\text{Def}}{=} d(x,y) + d(y,z) \end{aligned}$$

Weitere Beispiele für Metriken

Ein **metrischer Raum** (X, d) ist eine Menge X mit einer Metrik d, also einer Abbildung $d : X \times X \to \mathbb{R}_{\geq 0}$, die (M0–3) erfüllt.

Mit einer Metrik können wir immerhin noch Abstände messen. Sie ist auf jeder beliebigen Menge definierbar und hat im Allgemeinen keinen Bezug mehr zu Vektorräumen oder Längen und Winkeln von Vektoren.

Beispiel: Auf jeder beliebigen Menge X lässt sich eine besonders einfache Metrik definieren, die nur die Werte 0 und 1 annimmt: Diese **diskrete Metrik** auf X ist gegeben durch

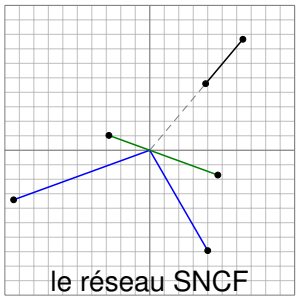
$$d : X \times X \to \{0, 1\} : (x, y) \mapsto \begin{cases} 0 & \text{falls } x = y, \\ 1 & \text{falls } x \neq y. \end{cases}$$

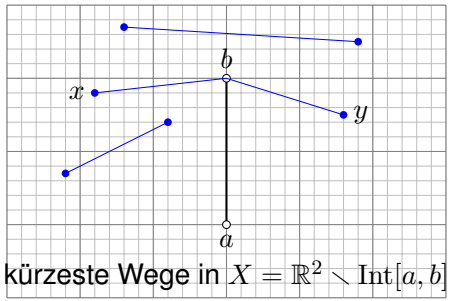
Übung: (1) Weisen Sie nach, dass dies tatsächlich eine Metrik ist.
(2) Die diskrete Metrik auf dem $\mathbb{R}^n$ kommt nicht von einer Norm.
(3) Dasselbe gilt für folgende Metrik: Die kürzeste Verbindung zwischen zwei französischen Städten x und y führt über Paris, es sei denn beide Städte liegen auf einer gemeinsamen Eisenbahnstrecke nach Paris.

Weitere Beispiele für Metriken

Beispiel: Die **französische Eisenbahnmetrik** auf der Menge $\mathbb{R}^n$ ist

$$d = d_{\text{SNCF}} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_{\geq 0} : (x, y) \mapsto \begin{cases} |x - y| & \text{falls } \mathbb{R}x = \mathbb{R}y, \\ |x| + |y| & \text{falls } \mathbb{R}x \neq \mathbb{R}y. \end{cases}$$


le réseau SNCF



kürzeste Wege in $X = \mathbb{R}^2 \setminus \operatorname{Int}[a, b]$

Beispiel: Sei $X \subseteq \mathbb{R}^n$ eine Teilmenge des euklidischen Raum oder allgemein ein beliebiger metrischer Raum (X, d). Wir definieren die **Wegmetrik** $\check{d} : X \times X \to [0, \infty]$ für je zwei Punkte $x, y \in X$ als die infimale Länge aller Wege von x nach y. **Übung:** Führen Sie dies aus.

Abstand Punkt-Menge und Menge-Menge

Sei (X, d) ein metrischer Raum. Der Abstand eines Punktes $a \in X$ zu einer Teilmenge $B \subseteq X$ bzw. zwischen zwei Teilmengen $A, B \subseteq X$ ist definiert als das Infimum der punktweisen Abstände:

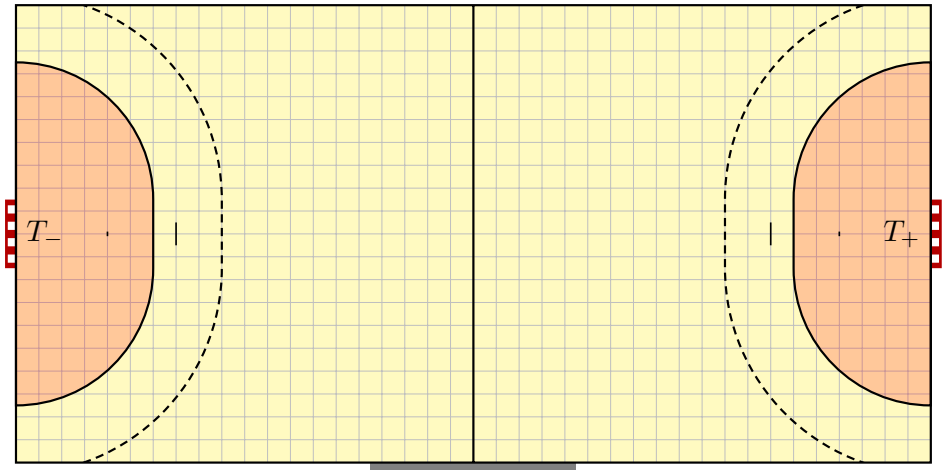
$$d(a, B) := \inf\{\, d(a, b) \mid b \in B \,\}$$
$$d(A, B) := \inf\{\, d(a, b) \mid a \in A,\ b \in B \,\}$$

Aufgabe: Zeichnen Sie ein Handballfeld nach folgenden Maßgaben, siehe Regeln 1:1 bis 1:9 der *International Handball Federation*:

$X = [-20, 20] \times [-10, 10] \subset \mathbb{R}^2$	die Spielfläche
$M = \{0\} \times [-10, 10]$	die Mittellinie
$T = \{-20, 20\} \times [-1.5, 1.5]$	die beiden Torlinien
$S = \{\, x \in X \mid d(x, T) = 6 \,\}$	Sechs-Meter-Linie („Kreis“)
$N = \{\, x \in X \mid d(x, T) = 9 \,\}$	Neun-Meter-Linie („Freiwurflinie“)

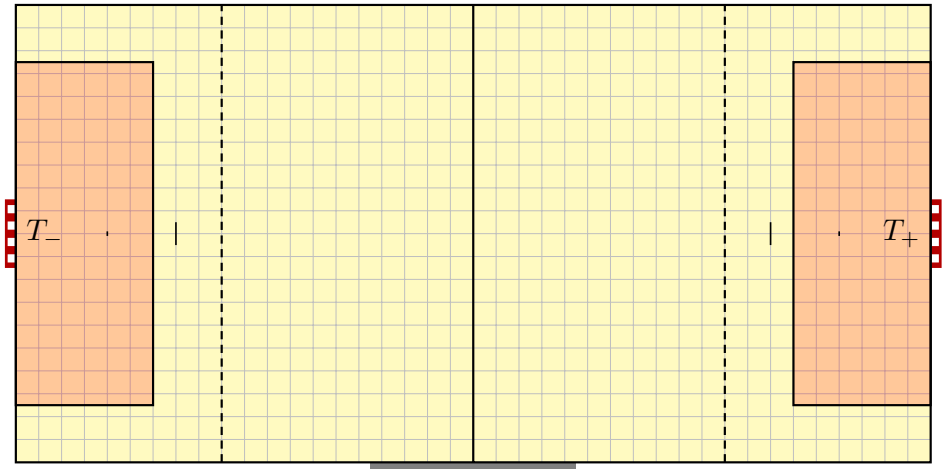
Wie sieht das Feld bezüglich der üblichen, euklidischen Metrik aus? zum Vergleich mit der Maximumsmetrik? und mit der Taximetrik?

Handballfeld in der euklidischen Metrik



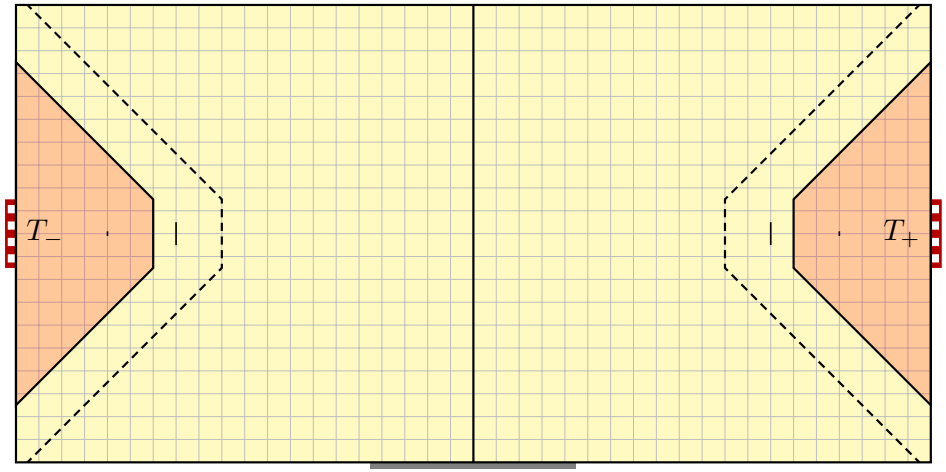
☺ Die Sechs-Meter-Linie, der sogenannte „Kreis“, ist gar keiner! Sie besteht aus zwei Viertelkreisen und einem Geradenstück.

Handballfeld in der Maximumsmetrik



☺ In der Maximumsmetrik ist die Sechs-Meter-Linie ein Rechteck.
Fun fact: Im Fußball folgen Tor- und Strafraum dieser Konvention.

Handballfeld in der Taximetrik



☺ In der Taximetrik ist die Sechs-Meter-Linie ein Trapez.
Das sieht ulkig aus und illustriert eindrücklich die Taximetrik .

Anwendungen von Skalarprodukt, Norm und Metrik

Das euklidische Skalarprodukt auf dem $\mathbb{R}^n$ sowie die zugehörige euklidische Norm und die euklidische Metrik sind grundlegend: Sie spielen in vielen Anwendungen eine tragende Rolle.

Daneben gibt es andere Normen und andere Metriken, die je nach Anwendung natürlich auftreten, aber gänzlich andere geometrische Eigenschaften haben. Mein Anliegen in den obigen Ergänzungen ist, durch illustrative Beispiele den nötigen Kontrast zu schaffen. Nur so sehen Sie, wie schön und einfach das euklidische Skalarprodukt ist.

Dies ist das zentrale Beispiel und ein leuchtendes Vorbild für die gesamte Lineare Algebra und viele Anwendungen in der Analysis, der Numerik, der Stochastik, der Physik und vielen weiteren Gebieten.

Anwendungen von Skalarprodukt, Norm und Metrik

Normen und Metriken begegnen Ihnen vor allem in der Analysis und der Numerik, aber ebenso auch in der Geometrie und der Topologie. Sie dienen zur Messung von Abständen, zur Abschätzung von Fehlern, zur Kontrolle von Näherungen und zur Definition der Konvergenz.

Beide Handlungsstränge, Vektorräume und Normen, führen schließlich in der Funktionalanalysis wieder zusammen. Für die Untersuchung von unendlich-dimensionalen Vektorräumen sind Skalarprodukte, Normen, Metriken und Topologien unentbehrliche Hilfsmittel.

Zunächst sind Normen und Metriken hier nur ein amüsanter Ausblick, doch sie sind zugleich wichtig genug, jetzt schon erwähnt zu werden. Wir konzentrieren uns im Folgenden wieder auf das Skalarprodukt.

Anwendungen von Skalarprodukt, Norm und Metrik

🙂 Mit dem Skalarprodukt auf V messen wir Winkel und Längen. Damit gewinnen wir für V wichtige geometrische Werkzeuge:

- **Orthogonalität:** $u, v \in V$ stehen senkrecht, wenn $\langle u \mid v \rangle = 0$.
- **Norm:** Die Länge eines Vektors $v \in V$ ist $\|v\| = \sqrt{\langle v \mid v \rangle}$.
- **Cauchy–Schwarz–Ungleichung:** Es gilt $|\langle u \mid v \rangle| \leq \|u\| \cdot \|v\|$.
- **Winkel:** $\langle u \mid v \rangle = \|u\| \cdot \|v\| \cdot \cos(\theta)$ mit $\theta = \angle(u, v) \in [0, \pi]$.
- **Dreiecksungleichung:** Es gilt $\|u + v\| \leq \|u\| + \|v\|$.
- **Metrik:** Der Abstand zweier Vektoren u, v ist $\|v - u\|$.
- **Konvergenz** $v_n \to v$ ist definiert durch $\|v_n - v\| \to 0$.
- **Vollständigkeit:** Jede Cauchy–Folge in V konvergiert in V.
- **Stetigkeit** von Funktionen $f : V \to W$, linear oder nicht.
- **Differenzierbarkeit**, lineare und höhere Approximation.

Skalarprodukt und Norm auf einem reellen Vektorraum

Zusammenfassend vereinbaren wir den folgenden Sprachgebrauch für Skalarprodukte auf Vektorräumen über $\mathbb{R}$ (und anschließend über $\mathbb{C}$):

♦ Definition P1L: Skalarprodukt und Norm

Sei V ein Vektorraum über dem Körper $\mathbb{R}$. Ein **Skalarprodukt** auf V ist eine Abbildung $\langle - \mid - \rangle : V \times V \to \mathbb{R}$, die (S1–3) erfüllt.

Das Paar $(V, \langle - \mid - \rangle)$ heißt dann **$\mathbb{R}$–Vektorraum mit Skalarprodukt** oder **euklidischer Vektorraum** oder ein reeller **Prä–Hilbert–Raum** und bei metrischer Vollständigkeit auch ein reeller **Hilbert–Raum**.

Eine **Norm** auf V ist eine Abbildung $\|-\| : V \to \mathbb{R}_{\geq 0}$, die (N1–3) erfüllt.

Das Paar $(V, \|-\|)$ heißt dann **normierter $\mathbb{R}$–Vektorraum** oder auch **Prä–Banach–Raum** und bei Vollständigkeit reeller **Banach–Raum**.

Für ein **semidefinites Skalarprodukt** fordern wir nur (S0,2,3), für eine **Seminorm** oder **Halbnorm** entsprechend nur (N0,2,3). Beide Abschwächungen kommen in Anwendungen natürlich vor.

Der Betrag komplexer Zahlen

Erinnerung: Zu jeder komplexen Zahl $z = x + \mathrm{i}y$ mit $x, y \in \mathbb{R}$ haben wir die konjugierte Zahl $\overline{z} = x - \mathrm{i}y$. Ihr Produkt ist somit $z\overline{z} = x^2 + y^2 \geq 0$.

Den Betrag $|-| : \mathbb{C} \to \mathbb{R}_{\geq 0}$ komplexer Zahlen definieren wir durch

$$|z| := \sqrt{z\overline{z}}, \quad \text{also} \quad |x + \mathrm{i}y| := \sqrt{x^2 + y^2} \quad \text{für alle } x, y \in \mathbb{R}.$$

Für alle komplexen Zahlen $u, v \in \mathbb{C}$ gilt dann:

N0: Null und Eins, $|0| = 0$ und $|1| = 1$

N1: positive Definitheit, $|u| > 0$ für $u \neq 0$

N2: Multiplikativität, $|u \cdot v| = |u| \cdot |v|$

N3: Dreiecksungleichung, $|u + v| \leq |u| + |v|$

Aufgabe: (1) Wiederholen bzw. beweisen Sie diese Aussagen.

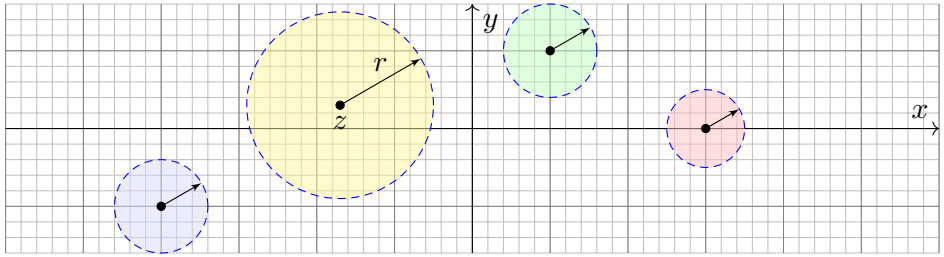
(2) Zeichnen Sie für verschiedene Werte von $z \in \mathbb{C}$ und $r \in \mathbb{R}_{>0}$ die Menge $B(z, r) := \{\, u \in \mathbb{C} \mid |u - z| < r \,\}$ in der komplexen Ebene $\mathbb{C}$.

Der Betrag komplexer Zahlen

Lösung: (1) Wir haben $\mathbb{C} = \mathbb{R}^2$ und hierauf ist $|-|$ die euklidische Norm. Daraus folgt (N0,1,3) dank P1F. Dank A3B ist die komplexe Konjugation $^- : \mathbb{C} \to \mathbb{C} : (x, y) \mapsto (x, -y)$ ein Körperautomorphismus, also gilt:

$$|uv| = \sqrt{uv \cdot \overline{uv}} = \sqrt{u\overline{u} \cdot v\overline{v}} = \sqrt{u\overline{u}} \cdot \sqrt{v\overline{v}} = |u| \cdot |v|$$

(2) Die Menge $B(z, r) := \{\, u \in \mathbb{C} \mid |u - z| < r \,\}$ ist eine offene Kreisscheibe um den Mittelpunkt $z \in \mathbb{C}$ mit Radius $r \in \mathbb{R}_{>0}$.



Das euklidische Skalarprodukt auf dem Raum $\mathbb{C}^n$

Beispiel P1H: das euklidische Skalarprodukt auf dem Raum $\mathbb{C}^n$

Auf $V = \mathbb{C}^n$ über $\mathbb{C}$ definieren wir das **euklidische Skalarprodukt**

$$\langle - \mid - \rangle : V \times V \to \mathbb{C} : (u, v) \mapsto \langle u \mid v \rangle := \overline{u_1} v_1 + \cdots + \overline{u_n} v_n.$$

Für alle Vektoren $u, v, w \in V$ und Skalare $\lambda, \mu \in \mathbb{C}$ gilt:

S0: Positivität, $\langle u \mid u \rangle \geq 0 = \langle 0 \mid 0 \rangle$

S1: positive Definitheit, $\langle u \mid u \rangle > 0$ für $u \neq 0$

S2: konjugierte Symmetrie, $\langle v \mid u \rangle = \overline{\langle u \mid v \rangle}$

S3: Linearität rechts, $\langle u \mid \lambda v + \mu w \rangle = \lambda \langle u \mid v \rangle + \mu \langle u \mid w \rangle$

Aus (S2) und (S3) folgt konjugierte Linearität in der ersten Variablen:

S4: konjugierte Linearität links, $\langle \lambda u + \mu v \mid w \rangle = \overline{\lambda} \langle u \mid w \rangle + \overline{\mu} \langle v \mid w \rangle$

Zu (S4) sagt man auch **semilinear**, zu (S3,4) daher kurz **sesquilinear** (lat. *sesqui*, ‘anderthalb’). Zu (S2) sagt man **hermitesch**, zu Ehren des französischen Mathematikers Charles Hermite (1822–1901).

Das euklidische Skalarprodukt auf dem Raum $\mathbb{C}^n$

Somit ist das euklidische Skalarprodukt $\langle - \mid - \rangle$ auf $V = \mathbb{C}^n$ über $\mathbb{C}$ eine **hermitesche Sesquilinearform** (S2,3) und **positiv definit** (S0,1).

Eigenschaft (S2) impliziert $\overline{\langle u \mid u \rangle} = \langle u \mid u \rangle$, also ist dieser Wert reell und die Frage nach $\langle u \mid u \rangle \geq 0$ oder $\langle u \mid u \rangle > 0$ ist überhaupt sinnvoll.

Aufgabe: Rechnen Sie die hier gemachten Aussagen nach.

Lösung: Hermitizität (S2) und Sesquilinearität (S3,4) sind klar.

(S0) Für jeden Vektor $u \in \mathbb{C}^n$ gilt $\langle u \mid u \rangle = |u_1|^2 + \cdots + |u_n|^2 \geq 0$.

(S1) Im Falle $u \neq 0$ gilt $u_i \neq 0$ für mindestens ein $i \in \{1, \ldots, n\}$. Daraus folgt sofort die strikte Ungleichung $\langle u \mid u \rangle \geq |u_i|^2 > 0$.

Bemerkung: Auf dem Vektorraum $\mathbb{R}^n$ ist die Bilinearform $(u, v) \mapsto u_1 v_1 + \cdots + u_n v_n$ positiv definit, auf $\mathbb{C}^n$ jedoch nicht.

Zur Korrektur müssen wir eine der beiden Variablen konjugieren. Ich plädiere für die erste, dadurch werden einige Formeln schöner.

⚠ Manche Autoren wählen die zweite; das ist eine Geschmacksfrage. Beide Konventionen sind durch Konjugation ineinander umzurechnen.

Definition P1I: Skalarprodukt über $\mathbb{C}$

Ein **Skalarprodukt** auf einem $\mathbb{C}$–Vektorraum V ist eine positiv definite, hermitesche Sesquilinearform $\langle - \mid - \rangle : V \times V \to \mathbb{C}$, erfüllt also (S1–3).
Die zugehörige **Norm** ist dann $\|-\| : V \to \mathbb{R}_{\geq 0} : v \mapsto \|v\| = \sqrt{\langle v \mid v \rangle}$.

Bemerkung: Die reelle und die komplexe Definition stimmen überein, wenn wir die beiden Grundkörper $\mathbb{R}$ und $\mathbb{C}$ ausstatten mit der Identität $^- : \mathbb{R} \to \mathbb{R} : x \mapsto x$ bzw. der Konjugation $^- : \mathbb{C} \to \mathbb{C} : (x, y) \mapsto (x, -y)$.

Satz P1J: Cauchy–Schwarz–Ungleichung (CSU)

Aus (S1–3) folgt für alle $u, v \in V$ die **Cauchy–Schwarz–Ungleichung**:

$$|\langle u \mid v \rangle|^2 \leq \langle u \mid u \rangle \langle v \mid v \rangle \quad \text{kurz} \quad |\langle u \mid v \rangle| \leq \|u\| \cdot \|v\|$$

Gleichheit gilt genau dann, wenn u, v über $\mathbb{C}$ linear abhängig sind.

Aufgabe: Beweisen Sie dies, indem Sie den reellen Beweis anpassen.

Lösung: Die Aussage ist klar für $v = 0$. Im Folgenden sei also $v \neq 0$.
Wir setzen $z := au - bv$ mit $a = \langle v \mid v \rangle$ und $b = \langle v \mid u \rangle$ und rechnen:

$$\begin{aligned} 0 &\overset{(S0)}{\leq} \langle z \mid z \rangle \overset{\text{Def}}{=} \langle au - bv \mid au - bv \rangle \\ &\overset{(S3,4)}{=} |a|^2 \langle u \mid u \rangle - \overline{a}b \langle u \mid v \rangle - a\overline{b} \langle v \mid u \rangle + |b|^2 \langle v \mid v \rangle \\ &\overset{(S2)}{=} \langle v \mid v \rangle \left[\langle u \mid u \rangle \langle v \mid v \rangle - |\langle u \mid v \rangle|^2 \right] \end{aligned}$$

Dank (S1) gilt $\langle v \mid v \rangle > 0$. Wir erhalten so die ersehnte Ungleichung:

$$\langle u \mid u \rangle \langle v \mid v \rangle - |\langle u \mid v \rangle|^2 \geq 0$$

Gleichheit impliziert $0 = \langle z \mid z \rangle$, also $0 = z$ und somit $u = (b/a)v$.
Umgekehrt folgt aus linearer Abhängigkeit $u = \lambda v$ direkt die Gleichheit

$$\begin{aligned} |\langle u \mid v \rangle|^2 \overset{\text{Def}}{=} |\langle \lambda v \mid v \rangle|^2 &\overset{(S2)}{=} \langle \lambda v \mid v \rangle \langle v \mid \lambda v \rangle \\ &\overset{(S3)}{=} \langle \lambda v \mid \lambda v \rangle \langle v \mid v \rangle \overset{\text{Def}}{=} \langle u \mid u \rangle \langle v \mid v \rangle. \end{aligned}$$

Damit ist die Cauchy–Schwarz–Ungleichung bewiesen. QED

Aufgabe: Übertragen Sie soweit möglich die Eigenschaften des reellen auf das komplexe Skalarprodukt: Norm? Metrik? Winkel? Orthogonalität? Pythagoras? Parallelogrammgleichung? Polarisationsformel?

Lösung: (1) Die Eigenschaften der zugehörigen Norm (P1F) und der daraus abgeleiteten Metrik (P1G) gelten wörtlich genauso über $\mathbb{C}$.

(2) Im Reellen ist der Winkel $\theta = \angle(u, v)$ zwischen u und v definiert durch $\langle u \mid v \rangle = \|u\| \cdot \|v\| \cdot \cos\theta$. Im Komplexen ist $\langle u \mid v \rangle$ i.A. nicht reell. Notgedrungen definieren wir θ daher durch $\operatorname{Re}\langle u \mid v \rangle = \|u\| \cdot \|v\| \cdot \cos\theta$.

(3) Orthogonalität vermöge $u \perp v :\Leftrightarrow \langle u \mid v \rangle = 0$ ist weiterhin sinnvoll. Vorsicht: Hierzu ist $\angle(u, v) = \pi/2$ notwendig, aber nicht hinreichend.

(4) Der Satz des Pythagoras (P1D) gilt weiterhin, nun in der Form $\|u + v\|^2 = \|u\|^2 + \|v\|^2 + 2\operatorname{Re}\langle u \mid v \rangle = \|u\|^2 + \|v\|^2 + 2\|u\| \cdot \|v\| \cdot \cos\theta$. Aus $u \perp v$ folgt $\|u + v\|^2 = \|u\|^2 + \|v\|^2$, die Umkehrung gilt nicht mehr.

(5) Die Parallelogrammgleichung (P1E) gilt wörtlich genauso wie zuvor. Die Polarisationsformel muss um den Imaginärteil ergänzt werden. Der folgende Satz führt beide Fälle noch einmal explizit aus.

Satz P1K: Polarisationsformel, reell und komplex

(1) Über $\mathbb{R}$ lässt sich aus der Norm $\|-\|$ das Skalarprodukt $\langle - \mid - \rangle$ rekonstruieren dank der folgenden, reellen Polarisationsformel:

$$\langle u \mid v \rangle = \frac{\|u + v\|^2 - \|u - v\|^2}{4}$$

(2) Über $\mathbb{C}$ lässt sich aus der Norm $\|-\|$ das Skalarprodukt $\langle - \mid - \rangle$ rekonstruieren dank der folgenden, komplexen Polarisationsformel:

$$\langle u \mid v \rangle = \frac{\|u + v\|^2 - \|u - v\|^2}{4} + \mathrm{i}\,\frac{\|u - \mathrm{i}v\|^2 - \|u + \mathrm{i}v\|^2}{4}.$$

Übung: Alles steht explizit da. Rechnen Sie es sorgsam nach!

Insbesondere gilt $\angle(u, v) = \pi/2 \Leftrightarrow \|u + v\| = \|u - v\|$ und vollständig $u \perp v \Leftrightarrow \|u + v\| = \|u - v\| \wedge \|u - \mathrm{i}v\| = \|u + \mathrm{i}v\|$.

☺ Komplexe Handwerker benötigen zwei Tests zur Rechtwinkligkeit.

Skalarprodukt und Norm über $\mathbb{K} = \mathbb{R}, \mathbb{C}$

Zusammenfassend vereinbaren wir den folgenden Sprachgebrauch:

Definition P1L: Skalarprodukt und Norm über $\mathbb{K} = \mathbb{R}, \mathbb{C}$

Sei V ein Vektorraum über dem Körper $\mathbb{K} = \mathbb{R}, \mathbb{C}$. Ein **Skalarprodukt** auf V ist eine Abbildung $\langle - \mid - \rangle : V \times V \to \mathbb{K}$, die (S1–3) erfüllt.

Das Paar $(V, \langle - \mid - \rangle)$ heißt dann **$\mathbb{K}$–Vektorraum mit Skalarprodukt** oder **euklidischer $\mathbb{R}$–Vektorraum** bzw. **unitärer $\mathbb{C}$–Vektorraum**,

In der Analysis heißt $(V, \langle - \mid - \rangle)$ auch **Prä–Hilbert–Raum** über $\mathbb{K}$ und bei metrischer Vollständigkeit schließlich **Hilbert–Raum** über $\mathbb{K}$.

Eine **Norm** auf V ist eine Abbildung $\|-\| : V \to \mathbb{R}_{\geq 0}$, die (N1–3) erfüllt.

Das Paar $(V, \|-\|)$ heißt dann **normierter $\mathbb{K}$–Vektorraum** oder auch **Prä–Banach–Raum** und bei Vollständigkeit **Banach–Raum** über $\mathbb{K}$.

Für ein **semidefinites Skalarprodukt** fordern wir nur (S0,2,3).
Für eine **Seminorm** oder **Halbnorm** fordern wir nur (N0,2,3).
Beide Abschwächungen kommen in Anwendungen natürlich vor.

Orthogonale und orthonormale Familien

Definition P1M: Orthonormalbasis

Sei V ein $\mathbb{K}$–Vektorraum mit Skalarprodukt $\langle - \mid - \rangle$ und Norm $\|-\|$.

Eine Familie $(u_i)_{i \in I}$ in V heißt **orthogonal**, falls $\langle u_i \mid u_j \rangle = 0$ für alle $i \neq j$ in I gilt, und **orthonormal**, falls zudem $\|u_i\| = 1$ für alle $i \in I$ gilt:

$$\langle u_i \mid u_j \rangle = \begin{cases} 0 & \text{falls } i \neq j, \\ 1 & \text{falls } i = j. \end{cases}$$

Ist $(u_i)_{i \in I}$ zudem eine Basis von V, so nennen wir dies eine **Orthogonalbasis** bzw. eine **Orthonormalbasis** (kurz ONB).

Daraus können wir das Skalarprodukt rekonstruieren gemäß

$$\Big\langle \sum_{i \in I} a_i u_i \;\Big|\; \sum_{j \in I} b_j u_j \Big\rangle \overset{\text{ONB}}{=} \sum_{k \in I} \overline{a_k} b_k.$$

🙂 Jede orthogonale Familie in $V \smallsetminus \{0\}$ ist linear unabhängig (P1O).
Zur Basis fehlt dann nur noch, dass $(u_i)_{i \in I}$ den Vektorraum V erzeugt.

Satz des Pythagoras

Satz P1N: Pythagoras

Sei V ein Vektorraum über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ mit Skalarprodukt $\langle - \mid - \rangle$.

(1) Sind $u_1, \ldots, u_n \in V$ orthogonal, also $\langle u_k \mid u_\ell \rangle = 0$ für $k \neq \ell$, so gilt

$$\|u_1 + \cdots + u_n\|^2 = \|u_1\|^2 + \cdots + \|u_n\|^2.$$

(2) Sind $e_1, \ldots, e_n \in V$ orthonormal und $c_1, \ldots, c_n \in \mathbb{K}$, so gilt demnach

$$\|c_1 e_1 + \cdots + c_n e_n\|^2 = |c_1|^2 + \cdots + |c_n|^2.$$

Beweis: (1) Das Normquadrat erhalten wir aus dem Skalarprodukt:

$$\Big\|\sum_k u_k\Big\|^2 = \Big\langle \sum_k u_k \;\Big|\; \sum_\ell u_\ell \Big\rangle = \sum_k \sum_\ell \langle u_k \mid u_\ell \rangle = \sum_k \|u_k\|^2$$

(2) Für $u_k = c_k e_k$ mit $\|e_k\| = 1$ gilt $\|u_k\|^2 = |c_k|^2 \, \|e_k\|^2 = |c_k|^2$. QED

🙂 Der klassische Satz des Pythagoras ist der erste interessante Fall, nämlich die Ebene $V = \mathbb{R}^2$ über $\mathbb{K} = \mathbb{R}$ mit euklidischem Skalarprodukt.

Fourier–Koeffizienten

Satz P1O: Fourier–Koeffizienten

Sei V ein Vektorraum über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ mit Skalarprodukt $\langle - \mid - \rangle$.

Sei $(u_k)_{k \in I}$ eine orthogonale Familie von Vektoren $u_k \in V \smallsetminus \{0\}$.

(1) Für jede Linearkombination $v = \sum_\ell c_\ell u_\ell$ über $\mathbb{K}$ gilt dann

$$c_k = \frac{\langle u_k \mid v \rangle}{\langle u_k \mid u_k \rangle}.$$

(2) Insbesondere ist die Familie $(u_k)_{k \in I}$ linear unabhängig.

Beweis: (1) Die Koeffizientenformel folgt direkt aus der Orthogonalität:

$$\langle u_k \mid v \rangle = \Big\langle u_k \;\Big|\; \sum_\ell c_\ell u_\ell \Big\rangle = \sum_\ell c_\ell \langle u_k \mid u_\ell \rangle = c_k \langle u_k \mid u_k \rangle.$$

(2) Gilt $v = 0$, so folgt $c_k = 0$ für alle $k \in I$. QED

🙂 Das Skalarprodukt filtert den gewünschten Koeffizienten heraus!
In allen Rechnungen ist das überaus praktisch und hilfreich.

Kanonisches Beispiel: das euklidische Skalarprodukt

Wir betrachten weiterhin die beiden Grundkörper $\mathbb{K} = \mathbb{R}, \mathbb{C}$ gemeinsam.
Dazu statten wir den Körper $\mathbb{R}$ aus mit der Identität $^- : \mathbb{R} \to \mathbb{R} : x \mapsto x$
und den Körper $\mathbb{C}$ mit der Konjugation $^- : \mathbb{C} \to \mathbb{C} : (x, y) \mapsto (x, -y)$.

Beispiel P1P: die Produktsumme auf $\mathbb{K}^n$

(1) Auf dem $\mathbb{K}$–Vektorraum $\mathbb{K}^n$ haben wir das euklidische Skalarprodukt

$$\boxed{\langle u \mid v \rangle = \sum_{k=1}^{n} \overline{u_k} v_k.}$$

Somit gilt $\langle u \mid v \rangle = u^\intercal v$ über $\mathbb{R}$ und entsprechend $\langle u \mid v \rangle = \overline{u}^\intercal v$ über $\mathbb{C}$.
Die Standardbasis $(e_1, \ldots, e_n)$ wird hierdurch zur Orthonormalbasis.

Zu jeder Matrix $A = (a_{ij})_{ij}$ in $\mathbb{C}^{m\times n}$ ist $A^\dagger = A^H = \overline{A}^\intercal = (\overline{a_{ij}})_{ji}$ in $\mathbb{C}^{n\times m}$ die **transponiert-konjugierte Matrix** (G2K). Wir erhalten die Abbildung

$$^\dagger : \mathbb{C}^{m\times n} \to \mathbb{C}^{n\times m} : A \mapsto A^\dagger.$$

Dies nennt man auch die **hermitesch transponierte Matrix** oder auch die **adjungierte Matrix** (nicht zu verwechseln mit der Adjunkten L2S).

Kanonisches Beispiel: das euklidische Skalarprodukt

Beispiel P1P: die Produktsumme auf $\mathbb{K}^{(I)}$

(2) Sei I eine beliebige Menge, egal ob endlich oder unendlich.
Auf dem $\mathbb{K}$–Vektorraum $\mathbb{K}^{(I)}$ haben wir das euklidische Skalarprodukt

$$\boxed{\langle u \mid v \rangle_{\ell^2} := \sum_{k\in I} \overline{u_k} v_k.}$$

Die Standardbasis $(e_i)_{i\in I}$ wird hierdurch zur Orthonormalbasis.
Die Vervollständigung $\ell^2(I, \mathbb{K})$ untersuchen Sie in der Analysis.

(3) Jeder $\mathbb{K}$–Vektorraum V besitzt eine Basis $(b_i)_{i\in I}$ für eine geeignete Indexmenge I (dank Satz J2B) und erlaubt somit das Skalarprodukt

$$\boxed{\left\langle \sum_{i\in I} u_i b_i \;\middle|\; \sum_{j\in I} v_j b_j \right\rangle := \sum_{k\in I} \overline{u_k} v_k.}$$

Die gewählte Basis $(b_i)_{i\in I}$ wird hierdurch zur Orthonormalbasis.

Bemerkung: Die Summe ist jeweils endlich, denn nach Voraussetzung sind die beiden Träger $\operatorname{supp}(u)$ und $\operatorname{supp}(v)$ in I endlich, also hat auch $w : k \mapsto \overline{u_k} v_k$ endlichen Träger, genauer $\operatorname{supp}(w) = \operatorname{supp}(u) \cap \operatorname{supp}(v)$.

Kanonisches Beispiel: das euklidische Skalarprodukt

Aufgabe: Rechnen Sie die hier gemachten Aussagen sorgsam nach.

Lösung: Hermitizität (S2) ist klar, denn die Konjugation $^- : \mathbb{K} \to \mathbb{K}$ ist ein Körperautomorphismus, also insbesondere verträglich mit der Addition:

$$\overline{\langle u \mid v \rangle} = \overline{\sum_{k\in I} \overline{u_k} v_k} = \sum_{k\in I} \overline{\overline{u_k} v_k} = \sum_{k\in I} \overline{v_k} u_k = \langle v \mid u \rangle$$

Linearität (S3) ist ebenfalls klar, denn die Summe ist linear in v:

$$\begin{aligned} \langle u \mid \lambda v + \mu w \rangle &= \sum_{k\in I} \overline{u_k} (\lambda v_k + \mu w_k) \\ &= \sum_{k\in I} \lambda (\overline{u_k} v_k) + \mu (\overline{u_k} w_k) \\ &= \lambda \sum_{k\in I} (\overline{u_k} v_k) + \mu \sum_{k\in I} (\overline{u_k} w_k) \\ &= \lambda \langle u \mid v \rangle + \mu \langle u \mid w \rangle \end{aligned}$$

(S0) Für jeden Vektor $u \in \mathbb{K}^{(I)}$ gilt $\langle u \mid u \rangle = \sum_{i\in i} |u_i|^2 \geq 0$.
(S1) Im Falle $u \neq 0$ gilt $u_i \neq 0$ für mindestens ein $i \in I$.
Daraus folgt sofort die strikte Ungleichung $\langle u \mid u \rangle \geq |u_i|^2 > 0$.

Analytisches Beispiel: das Produktintegral

Beispiel P1Q: das Produktintegral auf $\mathscr{C}([a, b], \mathbb{K})$

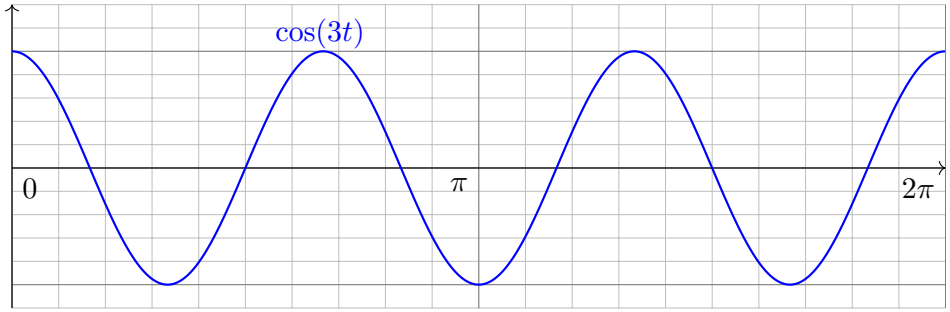
Sei $a < b$ in $\mathbb{R}$ und $V = \mathscr{C}([a, b], \mathbb{K})$ der $\mathbb{K}$–Vektorraum aller stetigen Funktionen $f, g : [a, b] \to \mathbb{K}$. Hierauf haben wir das Skalarprodukt

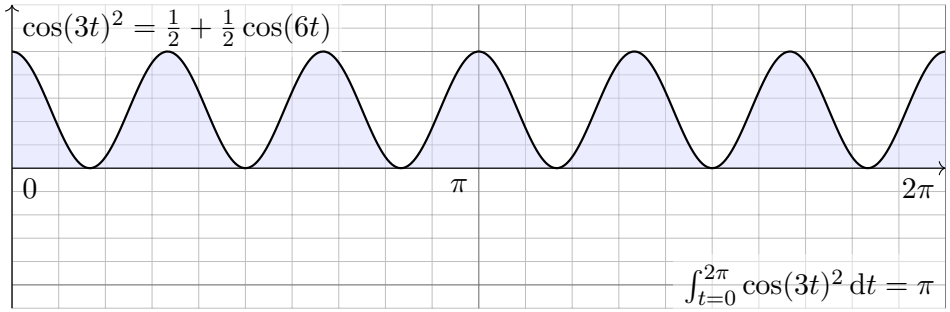
$$\boxed{\langle f \mid g \rangle_{L^2} = \int_{t=a}^{b} \overline{f(t)} g(t) \, \mathrm{d}t.}$$

Beweis: Die Eigenschaften (S2,3) sind klar, denn das Integral ist linear.
Auch Positivität (S0) ist klar, denn es gilt $\langle f \mid f \rangle = \int_{t=a}^{b} |f(t)|^2 \, \mathrm{d}t \geq 0$.
Für positive Definitheit (S1) müssen wir jedoch genauer hinschauen!
Sei $f \neq 0$, also $f(t_0) \neq 0$ für ein $t_0 \in [a, b]$, und somit $\delta := |f(t_0)|^2 > 0$.
Wir können $t_0 \in]a, b[$ annehmen, die Randfälle $t_0 \in \{a, b\}$ sind analog.
Dank der Stetigkeit von f existiert ein hinreichend kleines $\varepsilon \in \mathbb{R}_{>0}$, sodass $|f(t)|^2 \geq \delta/2$ für alle $t \in [t_0 - \varepsilon, t_0 + \varepsilon] \subseteq [a, b]$ gilt.
Daraus folgt $\langle f \mid f \rangle = \int_{t=a}^{b} |f(t)|^2 \, \mathrm{d}t \geq \varepsilon\delta > 0$. QED

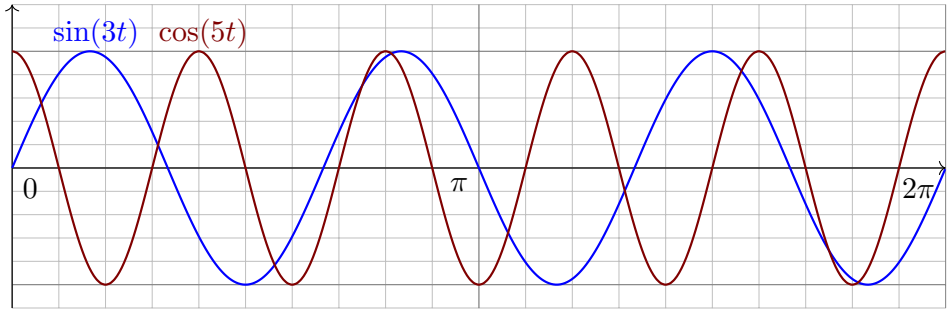
🙂 Die Vervollständigung $L^2([a, b], \mathbb{K})$ dieses Raumes untersuchen Sie in der Analysis und nutzen dies insbesondere für die Fourier–Theorie.

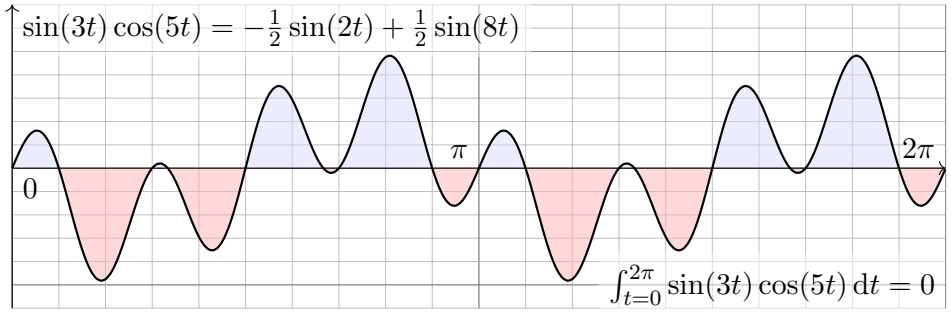
Beispiel: Orthogonalität trigonometrischer Funktionen





Beispiel: Orthogonalität trigonometrischer Funktionen





Beispiel: Orthogonalität trigonometrischer Funktionen

Aufgabe: Zur Periode $T > 0$ ist die Grundfrequenz $\omega = 2\pi/T$.
(1) Integrieren Sie für $k, \ell \in \mathbb{N}$ folgende Funktionen über $[0, T]$:

$$\cos(k\omega t)\cos(\ell\omega t), \quad \sin(k\omega t)\sin(\ell\omega t), \quad \sin(k\omega t)\cos(\ell\omega t).$$

Wir erinnern hierzu an die stets nützlichen Additionstheoreme

$$\begin{aligned}
\cos(\alpha)\cos(\beta) &= \tfrac{1}{2}\big[\cos(\alpha-\beta)+\cos(\alpha+\beta)\big],\\
\sin(\alpha)\sin(\beta) &= \tfrac{1}{2}\big[\cos(\alpha-\beta)-\cos(\alpha+\beta)\big],\\
\sin(\alpha)\cos(\beta) &= \tfrac{1}{2}\big[\sin(\alpha-\beta)+\sin(\alpha+\beta)\big].
\end{aligned}$$

(0) Leiten Sie diese Additionstheoreme her aus der Euler–Formel $\mathrm{e}^{\mathrm{i}\alpha} = \cos\alpha + \mathrm{i}\sin\alpha$ und dem Exponentialgesetz $\mathrm{e}^{\mathrm{i}\alpha+\mathrm{i}\beta} = \mathrm{e}^{\mathrm{i}\alpha}\,\mathrm{e}^{\mathrm{i}\beta}$.

Lösung: (1) Zur Berechnung nutzen wir die Grundintegrale

$$\int_{t=0}^{T} \sin(n\omega t)\,\mathrm{d}t = 0 \quad \text{für alle } n \in \mathbb{Z},$$

$$\int_{t=0}^{T} \cos(n\omega t)\,\mathrm{d}t = \begin{cases} 0 & \text{für } n \neq 0,\\ T & \text{für } n = 0. \end{cases}$$

Beispiel: Orthogonalität trigonometrischer Funktionen

Die Familie $1, \cos(\omega t), \sin(\omega t), \cos(2\omega t), \sin(2\omega t), \cos(3\omega t), \sin(3\omega t), \ldots$ ist orthogonal bezüglich des Skalarprodukts $\langle f \mid g \rangle = \int_{t=0}^{T} f(t)g(t)\,\mathrm{d}t$:

$$\int_{t=0}^{T} \cos(k\omega t)\cos(\ell\omega t)\,\mathrm{d}t = \frac{1}{2}\int_{t=0}^{T} \cos((k-\ell)\omega t) + \cos((k+\ell)\omega t)\,\mathrm{d}t$$
$$= \begin{cases} 0 & \text{falls } k \neq \ell,\\ T/2 & \text{falls } k = \ell \geq 1,\\ T & \text{falls } k = \ell = 0. \end{cases}$$

$$\int_{t=0}^{T} \sin(k\omega t)\sin(\ell\omega t)\,\mathrm{d}t = \frac{1}{2}\int_{t=0}^{T} \cos((k-\ell)\omega t) - \cos((k+\ell)\omega t)\,\mathrm{d}t$$
$$= \begin{cases} 0 & \text{falls } k \neq \ell,\\ T/2 & \text{falls } k = \ell \geq 1,\\ 0 & \text{falls } k = \ell = 0. \end{cases}$$

$$\int_{t=0}^{T} \sin(k\omega t)\cos(\ell\omega t)\,\mathrm{d}t = \frac{1}{2}\int_{t=0}^{T} \sin((k-\ell)\omega t) + \sin((k+\ell)\omega t)\,\mathrm{d}t = 0$$

☺ Das ist schön. Alles wird noch schöner und übersichtlicher für die komplexe Funktion $\mathrm{e}^{\mathrm{i}k\omega t} = \cos(k\omega t) + \mathrm{i}\sin(k\omega t)$, siehe nächste Aufgabe.

Beispiel: die trigonometrische Orthonormalbasis

Für Funktionen $f, g : \mathbb{R} \to \mathbb{C}$ mit Periode T nutzen wir das Skalarprodukt

$$\langle f \mid g \rangle := \frac{1}{T} \int_{t=0}^{T} \overline{f(t)}\, g(t)\, \mathrm{d}t.$$

Sei $\omega = 2\pi/T$. Als **Basisfunktion** $e_k : \mathbb{R} \to \mathbb{C}$ mit $k \in \mathbb{Z}$ definieren wir

$$e_k(t) := \mathrm{e}^{\mathrm{i}k\omega t} = \cos(k\omega t) + \mathrm{i}\sin(k\omega t).$$

Ihre Linearkombinationen nennen wir **Fourier–Polynome**:

$$f(t) = \sum_{k=-n}^{n} \widehat{f}(k)\, \mathrm{e}^{\mathrm{i}k\omega t}, \quad g(t) = \sum_{\ell=-n}^{n} \widehat{g}(\ell)\, \mathrm{e}^{\mathrm{i}\ell\omega t} \quad \text{mit} \quad \widehat{f}(k), \widehat{g}(\ell) \in \mathbb{C}.$$

Aufgabe: Wie bestimmt die Funktion $f : \mathbb{R} \to \mathbb{C}$ ihr Spektrum $\widehat{f} : \mathbb{Z} \to \mathbb{C}$?
Wir nutzen Orthonormalität: Berechnen Sie hierzu die Skalarprodukte

(0) $\langle 1 \mid e_n \rangle$, (1) $\langle e_k \mid e_\ell \rangle$, (2) $\langle e_k \mid g \rangle$, (3) $\langle f \mid g \rangle$, (4) $\langle f \mid f \rangle$.

(5) Entwickeln Sie $f(t) = \sin^2 t$ und $g(t) = \cos^3 t$ in Fourier–Polynome.

(6) Berechnen Sie daraus $\frac{1}{2\pi} \int_{t=0}^{2\pi} \cos^4 t\, \mathrm{d}t$ und $\frac{1}{2\pi} \int_{t=0}^{2\pi} \cos^6 t\, \mathrm{d}t$.

Beispiel: die trigonometrische Orthonormalbasis

Lösung: (0) Wir berechnen $\langle 1 \mid e_n \rangle$. Für $n = 0$ ist es besonders leicht:

$$\langle 1 \mid e_0 \rangle \overset{\text{Def}}{=} \frac{1}{T} \int_{t=0}^{T} 1 \cdot \mathrm{e}^{\mathrm{i}0\omega t}\, \mathrm{d}t = \frac{1}{T} \int_{t=0}^{T} 1\, \mathrm{d}t = 1.$$

Für $n \in \mathbb{Z} \smallsetminus \{0\}$ nutzen wir die vorige Aufgabe oder den HDI:

$$\langle 1 \mid e_n \rangle \overset{\text{Def}}{=} \frac{1}{T} \int_{t=0}^{T} 1 \cdot \mathrm{e}^{\mathrm{i}n\omega t}\, \mathrm{d}t \overset{\text{HDI}}{=} \frac{1}{T} \Big[\frac{1}{\mathrm{i}n\omega}\, \mathrm{e}^{\mathrm{i}n\omega t} \Big]_{t=0}^{T} = 0.$$

(1) **Orthonormalität** — Wir berechnen die gesuchten Skalarprodukte:

$$\langle e_k \mid e_\ell \rangle \overset{\text{Def}}{=} \frac{1}{T} \int_{t=0}^{T} \overline{e_k(t)}\, e_\ell(t)\, \mathrm{d}t \overset{\text{Def}}{=} \frac{1}{T} \int_{t=0}^{T} \mathrm{e}^{-\mathrm{i}k\omega t}\, \mathrm{e}^{\mathrm{i}\ell\omega t}\, \mathrm{d}t$$
$$\overset{\text{Exp}}{=} \frac{1}{T} \int_{t=0}^{T} \mathrm{e}^{\mathrm{i}(\ell-k)\omega t}\, \mathrm{d}t \overset{(0)}{=} \begin{cases} 1 & \text{für } k = \ell, \\ 0 & \text{für } k \neq \ell. \end{cases}$$

☺ Die Basis $(e_k)_{k \in \mathbb{Z}}$ ist orthonormal bezüglich des Skalarprodukts!
Das ist analog zur Geometrie des euklidischen Raumes $\mathbb{R}^n$ bzw. $\mathbb{C}^n$.

☺ Im Komplexen ist alles halb so schwer und doppelt so schön!

Beispiel: die trigonometrische Orthonormalbasis

(2) **Fourier** — Dank Linearität und Orthonormalität erhalten wir:

$$\langle e_k \mid g \rangle \overset{\text{Def}}{=} \Big\langle e_k \,\Big|\, \sum_{\ell=-n}^{n} \widehat{g}(\ell)\, e_\ell \Big\rangle \overset{\text{Lin}}{=} \sum_{\ell=-n}^{n} \widehat{g}(\ell) \langle e_k \mid e_\ell \rangle \overset{(1)}{=} \widehat{g}(k)$$

☺ Das Skalarprodukt filtert den gewünschten Koeffizienten heraus!

(3) **Parseval** — Dank Bilinearität und Orthonormalität erhalten wir:

$$\langle f \mid g \rangle \overset{\text{Def}}{=} \Big\langle \sum_{k=-n}^{n} \widehat{f}(k)\, e_k \,\Big|\, \sum_{\ell=-n}^{n} \widehat{g}(\ell)\, e_\ell \Big\rangle \overset{\text{Lin}}{=} \sum_{k=-n}^{n} \overline{\widehat{f}(k)} \Big\langle e_k \,\Big|\, \sum_{\ell=-n}^{n} \widehat{g}(\ell)\, e_\ell \Big\rangle$$
$$\overset{\text{Lin}}{=} \sum_{k=-n}^{n} \sum_{\ell=-n}^{n} \overline{\widehat{f}(k)}\, \widehat{g}(\ell) \langle e_k \mid e_\ell \rangle \overset{(1)}{=} \sum_{k=-n}^{n} \overline{\widehat{f}(k)}\, \widehat{g}(k).$$

☺ Diese Rechnung gilt allgemein für Orthonormalbasen.

(4) **Energiegleichung** — Für das Normquadrat gilt Pythagoras (P1N):

$$\langle f \mid f \rangle \overset{(3)}{=} \sum_{k=-n}^{n} |\widehat{f}(k)|^2$$

☺ Das Normquadrat ist die Summe der Koeffizientenquadrate.

Beispiel: die trigonometrische Orthonormalbasis

(5) Wir entwickeln f und g dank der Euler–Formel $\mathrm{e}^{\mathrm{i}t} = \cos t + \mathrm{i}\sin t$:

$$f(t) = \sin(t)^2 = \left(\frac{\mathrm{e}^{\mathrm{i}t} - \mathrm{e}^{-\mathrm{i}t}}{2\mathrm{i}} \right)^2 = -\frac{1}{4}\mathrm{e}^{2\mathrm{i}t} + \frac{1}{2} - \frac{1}{4}\mathrm{e}^{-2\mathrm{i}t} = \frac{1}{2} - \frac{1}{2}\cos(2t)$$

$$g(t) = \cos(t)^3 = \left(\frac{\mathrm{e}^{\mathrm{i}t} + \mathrm{e}^{-\mathrm{i}t}}{2} \right)^3 = \frac{1}{8}\mathrm{e}^{3\mathrm{i}t} + \frac{3}{8}\mathrm{e}^{\mathrm{i}t} + \frac{3}{8}\mathrm{e}^{-\mathrm{i}t} + \frac{1}{8}\mathrm{e}^{-3\mathrm{i}t}$$
$$= \frac{3}{4}\cos(t) + \frac{1}{4}\cos(3t)$$

☺ Dank Orthonormalität lesen wir die Fourier–Koeffizienten ab (2).

(6) Wir nutzen die Energiegleichung (4) und Fourier–Koeffizienten (5):

$$\frac{1}{2\pi} \int_{t=0}^{2\pi} \sin^4 t\, \mathrm{d}t \overset{\text{Def}}{=} \langle f \mid f \rangle \overset{(4)}{=} \sum_{k=-n}^{n} |\widehat{f}(k)|^2 \overset{(5)}{=} \frac{3}{8}$$

$$\frac{1}{2\pi} \int_{t=0}^{2\pi} \cos^6 t\, \mathrm{d}t \overset{\text{Def}}{=} \langle g \mid g \rangle \overset{(4)}{=} \sum_{k=-n}^{n} |\widehat{g}(k)|^2 \overset{(5)}{=} \frac{5}{16}$$

☺ Die Energiegleichung gilt allgemein für Fourier–Reihen!

Satz P1R: trigonometrische Orthonormalbasis

Die Menge aller Funktionen $f : \mathbb{R} \to \mathbb{C}$ ist ein $\mathbb{C}$–Vektorraum. Hierin ist die Teilmenge aller T–periodischen Funktionen ein Untervektorraum. Als Basisfunktion $e_k : \mathbb{R} \to \mathbb{C}$ mit $k \in \mathbb{Z}$ und $\omega = 2\pi/T$ definieren wir

$$e_k(t) := \mathrm{e}^{\mathrm{i}k\omega t} = \cos(k\omega t) + \mathrm{i}\sin(k\omega t).$$

Diese erzeugen den Unterraum $V = \{ \sum_{k=-n}^{n} c_k \, \mathrm{e}^{\mathrm{i}k\omega t} \mid n \in \mathbb{N},\ c_k \in \mathbb{C} \}$ der Fourier–Polynome. Hierauf haben wir das Skalarprodukt

$$V \times V \to \mathbb{C} : (f, g) \mapsto \langle f \mid g \rangle := \frac{1}{T} \int_{t=0}^{T} \overline{f(t)}\, g(t)\, \mathrm{d}t.$$

Damit gelten die Orthonormalitätsrelationen

$$\langle e_k \mid e_\ell \rangle = \begin{cases} 0 & \text{für } k \neq \ell: \quad \text{paarweise Orthogonalität,} \\ 1 & \text{für } k = \ell: \quad \text{Normierung auf Länge } 1. \end{cases}$$

Korollar P1S: Fourier–Koeffizienten durch Skalarprodukt

(1) Wir betrachten ein trigonometrisches Polynom:

$$f(t) \;=\; \sum_{\ell=-n}^{n} c_\ell \, \mathrm{e}^{\mathrm{i}\ell\omega t} \;=\; \frac{a_0}{2} + \sum_{\ell=1}^{n} a_\ell \cos(\ell\omega t) + b_\ell \sin(\ell\omega t)$$

Die Funktion f bestimmt die Koeffizienten durch Fourier–Integrale:

$$c_k = \langle e_k \mid f \rangle \qquad = \frac{1}{T} \int_{t=0}^{T} \mathrm{e}^{-\mathrm{i}k\omega t} f(t)\, \mathrm{d}t,$$

bzw.

$$a_k = \langle 2\cos(k\omega t) \mid f \rangle = \frac{2}{T} \int_{t=0}^{T} \cos(k\omega t)\, f(t)\, \mathrm{d}t,$$

$$b_k = \langle 2\sin(k\omega t) \mid f \rangle = \frac{2}{T} \int_{t=0}^{T} \sin(k\omega t)\, f(t)\, \mathrm{d}t.$$

☺ Die Formeln für die Koeffizienten c_k sind besonders schön, da die Funktionen $\mathrm{e}_k(t) = \mathrm{e}^{\mathrm{i}k\omega t}$ orthonormal sind. Hingegen sind $\cos(k\omega t)$ und $\sin(k\omega t)$ zwar orthogonal, aber mit L^2–Norm $\sqrt{2}/2$ statt Normierung 1.

☺ Das Skalarprodukt beschert uns Struktur, Klarheit und Übersicht. Die Orthonormalität der Basis $(e_k)_{k\in\mathbb{Z}}$ vereinfacht die Rechnung.

☺ Das Fourier–Integral filtert den gewünschten Koeffizienten heraus! Diese Gleichungen nutzen wir ebenso für Fourier–Reihen $(n = \infty)$.

Korollar P1S: Jede Funktion bestimmt ihre Koeffizienten.

(2) Die Funktionen $f, g : \mathbb{R} \to \mathbb{C}$ seien gegeben als Fourier–Polynome

$$f(t) = \sum_{k=-n}^{n} \widehat{f}(k)\, \mathrm{e}^{\mathrm{i}k\omega t} \quad \text{und} \quad g(t) = \sum_{k=-n}^{n} \widehat{g}(k)\, \mathrm{e}^{\mathrm{i}k\omega t}.$$

Aus $\widehat{f}(k) = \widehat{g}(k)$ für alle $k = -n, \ldots, n$ folgt offensichtlich $f = g$.
Umgekehrt folgt aus $f = g$ auch $\widehat{f} = \widehat{g}$, dank der Fourier–Integrale:

$$\widehat{f}(k) = \frac{1}{T} \int_{t=0}^{T} \mathrm{e}^{-\mathrm{i}k\omega t} f(t)\, \mathrm{d}t \quad = \quad \frac{1}{T} \int_{t=0}^{T} \mathrm{e}^{-\mathrm{i}k\omega t} g(t)\, \mathrm{d}t = \widehat{g}(k)$$

☺ Für Letzteres genügt bereits Gleichheit $f = g$ fast überall.

Korollar P1S: Norm und Skalarprodukt

(3) Koeffizienten $\widehat{f}(k), \widehat{g}(k) \in \mathbb{C}$ definieren Fourier–Polynome

$$f(t) = \sum_{k=-n}^{n} \widehat{f}(k)\, \mathrm{e}^{\mathrm{i}k\omega t} \quad \text{und} \quad g(t) = \sum_{k=-n}^{n} \widehat{g}(k)\, \mathrm{e}^{\mathrm{i}k\omega t}.$$

Für ihre Norm und ihr Skalarprodukt gilt nach Pythagoras (P1N)

$$\frac{1}{T} \int_{t=0}^{T} \big|f(t)\big|^2 \, \mathrm{d}t = \sum_{k=-n}^{n} \big|\widehat{f}(k)\big|^2, \qquad \text{kurz} \quad \|f\|_{L^2} = \|\widehat{f}\|_{\ell^2},$$

$$\frac{1}{T} \int_{t=0}^{T} \overline{f(t)}\, g(t)\, \mathrm{d}t = \sum_{k=-n}^{n} \overline{\widehat{f}(k)}\, \widehat{g}(k), \quad \text{kurz} \quad \langle f \mid g \rangle_{L^2} = \langle \widehat{f} \mid \widehat{g} \rangle_{\ell^2}.$$

☺ Diese Isometrie ist eine zentrale Eigenschaft der Fourier–Theorie. Für Fourier–Polynome folgt dies direkt aus der Orthonormalität der Basis $(e_k)_{k\in\mathbb{Z}}$. Erfreulicherweise gilt dies nach Vervollständigung sogar allgemein für alle quadrat-integrierbaren Funktionen!

Orthonormalisierung nach Gram–Schmidt

Wie können wir aus einer Basis eine Orthonormalbasis konstruieren?

Satz P2A: Laplace 1816, Gram 1883, Schmidt 1907

Sei V ein Vektorraum über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ mit Skalarprodukt $\langle - \mid - \rangle$.
Sei $b_1, \dots, b_n \in V$ eine Basis des Unterraums $U_n = \langle\, b_1, \dots, b_n \,\rangle_{\mathbb{K}}^{!}$.
(1) Daraus erhalten wir rekursiv die Orthogonalbasis $u_1, \dots, u_n$ durch

$$u_n := b_n - \sum_{k=1}^{n-1} u_k \lambda_k \quad \text{mit} \quad \lambda_k = \frac{\langle\, u_k \mid b_n \,\rangle}{\langle\, u_k \mid u_k \,\rangle}.$$

(2) Optional können wir u_n ersetzen durch $u'_n = u_n \mu_n$ mit $\mu_n \in \mathbb{K}^\times$.
(3) Normiert zu $e_k := u_k / \|u_k\|$ erhalten wir eine Orthonormalbasis:

$$\langle\, u_k \mid u_\ell \,\rangle = \begin{cases} 0 & \text{für } k \neq \ell, \\ \|u_k\|^2 > 0 & \text{für } k = \ell, \end{cases} \quad \text{und} \quad \langle\, e_k \mid e_\ell \,\rangle = \begin{cases} 0 & \text{für } k \neq \ell, \\ 1 & \text{für } k = \ell. \end{cases}$$

Dasselbe Verfahren gelingt für jede abzählbare Basis $(b_k)_{k\in\mathbb{N}}$ von V.

Orthonormalisierung nach Gram–Schmidt

Aufgabe: Alles steht explizit da. Rechnen Sie es sorgsam nach!

Lösung: (1) Wir führen Induktion über n. Für $n = 1$ ist die Aussage klar.
Sei nun $n \geq 2$. Im Unterraum $U_{n-1} \leq V$ haben wir die gegebene Basis $(b_1, \dots, b_{n-1})$ bereits zur Orthogonalbasis $(u_1, \dots, u_{n-1})$ transformiert.
Im Unterraum U_n erhalten wir aus der Basis $(b_1, \dots, b_{n-1}, b_n)$ zunächst $(u_1, \dots, u_{n-1}, b_n)$ und dann $(u_1, \dots, u_{n-1}, u_n)$ mit $u_n := b_n - \sum_{k=1}^{n-1} u_k \lambda_k$.
Für alle $j = 1, \dots, n-1$ gilt $\langle\, u_j \mid u_n \,\rangle = \langle\, u_j \mid b_n \,\rangle - \langle\, u_j \mid u_j \,\rangle \lambda_j \overset{!}{=} 0$.
Dies verschwindet genau für $\lambda_j = \langle\, u_j \mid b_n \,\rangle / \langle\, u_j \mid u_j \,\rangle$. Voilà!

(2) Basiseigenschaft und Orthogonalität bleiben nach Skalierung von u_n zu $u'_n = u_n \mu_n$ mit $\mu_n \in \mathbb{K}^\times$. Das verschafft uns zusätzlichen Spielraum.

(3) Da $(u_1, \dots, u_n)$ eine Basis von U_n ist, gilt insbesondere $u_n \neq 0$.
Normierung zu $e_n := u_n / \|u_n\|$ liefert also eine Orthonormalbasis.

Dasselbe Verfahren gelingt für jede abzählbare Basis $(b_k)_{k\in\mathbb{N}}$:
Aus $b_0, b_1, b_2, \dots$ konstruieren wir $u_0, u_1, u_2, \dots$ und $e_0, e_1, e_2, \dots$. QED

Orthonormalisierung nach Gram–Schmidt

Aufgabe: Vergleichen Sie das Gram–Schmidt–Verfahren P2A mit dem Diagonalisierungsverfahren O2A für symmetrische Bilinearformen.
Was ist dabei gleich? Wo liegt der entscheidende Unterschied?

Lösung: Das Gram–Schmidt–Verfahren P2A verläuft wörtlich genau so wie das allgemeine Verfahren O2A für jede symmetrische Bilinearform!

☺ Dies wird stark vereinfacht durch die Garantie $\langle\, u_n \mid u_n \,\rangle > 0$, daher ist nun keine Fallunterscheidung zu $\langle\, u_n \mid u_n \,\rangle = 0$ mehr nötig.

☺ Zudem können wir in $\mathbb{R}$ die Quadratwurzel aus $\langle\, u_n \mid u_n \,\rangle$ ziehen, sodass wir im letzten Schritt zu $e_n = u_n / \|u_n\|$ normieren können.

Aufgabe: Formulieren Sie eine Verallgemeinerung dieses Verfahrens, die als Eingabe ein beliebiges Erzeugendensystem $b_1, \dots, b_m$ von U erlaubt und daraus wie zuvor eine Orthonormalbasis konstruiert.

Lösung: Wir wenden das Gram–Schmidt–Verfahren P2A an;
im Falle $u_n = 0$ löschen wir b_n aus dem Erzeugendensystem.

☺ Der folgende Algorithmus präzisiert die Buchführung der Indizes.

Orthonormalisierung nach Gram–Schmidt

☺ Aus jedem Erzeugendensystem können wir eine ONB konstruieren:

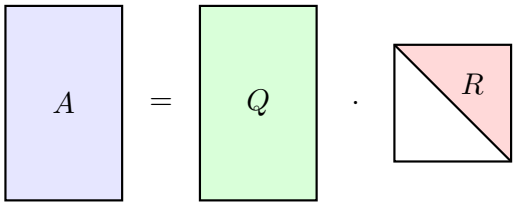
Algo P2A: Orthonormalisierung nach Gram–Schmidt

Eingabe: ein Erzeugendensystem $\mathcal{B} = (b_1, \dots, b_m)$ des Unterraums U
Ausgabe: eine Orthonormalbasis $\mathcal{E} = (e_1, \dots, e_n)$ des Unterraums U

1: $n \leftarrow 0$
2: for ℓ from 1 to m do
3: $\quad n \leftarrow n+1$; $b'_n \leftarrow b_\ell$; $u_n \leftarrow b'_n - \sum_{k=1}^{n-1} u_k \langle\, u_k \mid b'_n \,\rangle / \langle\, u_k \mid u_k \,\rangle$
4: $\quad$ if $u_n = 0$ then $n \leftarrow n-1$ else $e_n \leftarrow u_n / \|u_n\|$
5: return $(e_1, \dots, e_n)$

Dieser Algorithmus berechnet aus $\mathcal{B}$ drei interessante Basen von U:
(1) die Teilfamilie $\mathcal{B}' = (b'_1, \dots, b'_n)$ wie im Basisauswahlsatz J2B,
(2) hieraus abgeleitet die Orthogonalbasis $\mathcal{U} = (u_1, \dots, u_n)$
(3) und daraus die Orthonormalbasis $\mathcal{E} = (e_1, \dots, e_n)$.

Übung: Sei $V = \mathbb{K}^d$ mit dem Standardskalarprodukt. Zählen Sie die Operationen in $\mathbb{K}$. Vergleichen Sie (1) mit dem Gauß–Algorithmus B2C.



Satz P2B: Existenz und Eindeutigkeit der QR–Zerlegung

Gegeben sei eine Matrix $A \in \mathbb{K}^{m\times n}$ mit linear unabhängigen Spalten, also $\operatorname{rang} A = n \leq m$. Dann existiert genau eine Zerlegung der Form

$$A = QR$$

wobei $Q \in \mathbb{K}^{m\times n}$ orthonormale Spalten hat, also $Q^\dagger Q = I_n$ erfüllt, und $R \in \mathbb{K}^{n\times n}$ eine obere Dreiecksmatrix ist, also $r_{i,j} = 0$ für $i > j$, und zudem positive Diagonaleinträge hat, also $r_{i,i} > 0$ für alle i.

Insbesondere gilt $\det R > 0$ und $R \in \mathrm{GL}_n \mathbb{K}$.

Aufgabe: Folgern Sie dies aus dem Gram–Schmidt–Verfahren P2A.

Lösung: Wir beweisen die **Existenz** von (Q, R) durch Konstruktion.

Dank Gram–Schmidt konstruieren wir aus den Spalten $a_1, \ldots, a_n \in \mathbb{K}^m$ der Matrix A eine orthonormale Familie $q_1, \ldots, q_n \in \mathbb{K}^m$ wie folgt:

$$\begin{aligned} b_1 &:= a_1, & q_1 &:= b_1/\|b_1\|, \\ b_2 &:= a_2 - q_1\langle\, q_1 \mid a_2 \,\rangle, & q_2 &:= b_2/\|b_2\|, \\ &\vdots & &\vdots \\ b_n &:= a_n - \textstyle\sum_{k=1}^{n-1} q_k\langle\, q_k \mid a_n \,\rangle, & q_n &:= b_n/\|b_n\|. \end{aligned}$$

Umgekehrt gelesen erhalten wir daraus $A = QR$, denn

$$\begin{aligned} a_1 &= q_1\|b_1\|, \\ a_2 &= q_2\|b_2\| + q_1\langle\, q_1 \mid a_2 \,\rangle, \\ &\vdots \\ a_n &= q_n\|b_n\| + \textstyle\sum_{k=1}^{n-1} q_k\langle\, q_k \mid a_n \,\rangle. \end{aligned}$$

Dabei ist $Q = (q_1, \ldots, q_n) \in \mathbb{K}^{m\times n}$ orthonormal und $R \in \mathrm{GL}_n \mathbb{K}$ mit $r_{i,i} = \|b_i\| > 0$ sowie $r_{i,j} = 0$ für $i > j$ und $r_{i,j} = \langle\, q_i \mid a_j \,\rangle$ für $i < j$.

Die **Eindeutigkeit** von (Q, R) folgt ebenso per Induktion über n.

Angenommen, es gilt $A = QR$, in den Spalten von A und Q also

$$\begin{aligned} a_1 &= q_1 r_{1,1} \\ a_2 &= q_1 r_{1,2} + q_2 r_{2,2} \\ &\vdots \\ a_n &= q_1 r_{1,n} + \cdots + q_{n-1} r_{n-1,n} + q_n r_{n,n} \end{aligned}$$

Hierbei seien $q_1, q_2, \ldots, q_n \in \mathbb{K}^m$ orthonormal und $r_{i,i} > 0$ für alle i.
Dann sind (Q, R) die Daten aus dem Gram–Schmidt–Verfahren:

Für $k < n$ folgt $\langle\, q_k \mid a_n \,\rangle = \langle\, q_k \mid q_n \,\rangle r_{n,n} + \sum_{\ell=1}^{n-1} \langle\, q_k \mid q_\ell \,\rangle r_{\ell,n} = r_{k,n}$.
Wir setzen $b_n := a_n - \sum_{k=1}^{n-1} q_k\langle\, q_k \mid a_n \,\rangle$ und erhalten $b_n = q_n r_{n,n}$.
Wegen $\|q_n\| = 1$ und $r_{n,n} > 0$ gilt $r_{n,n} = \|b_n\|$ und $q_1 = b_1/\|b_1\|$. QED

🙂 Alternativ kann man auch die Eindeutigkeit zuerst beweisen...
und entdeckt auf diesem Wege erneut das Gram–Schmidt–Verfahren!

Die QR–Zerlegung ist in der Numerik ein wichtiges Werkzeug,
etwa zur Berechnung einer Orthonormalbasis (wie oben)
oder zur Behandlung von linearen Ausgleichsproblemen.

Die Zerlegung $A = QR$ ist eindeutig, also eine Abbildung $A \mapsto (Q, R)$.
Sie kann jedoch mit verschiedenen Algorithmen berechnet werden!

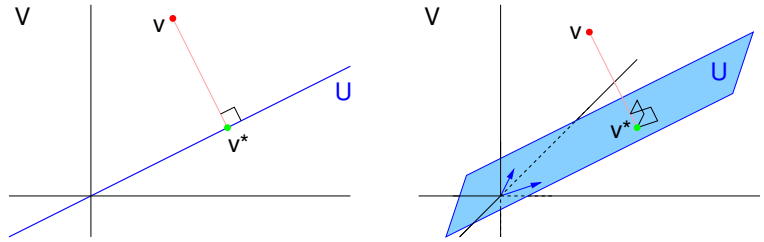
Die bekanntesten sind neben dem obigen Gram–Schmidt–Verfahren
vor allem Givens–Rotationen und Householder–Spiegelungen.

Ersteres wird üblicherweise in der Linearen Algebra benutzt,
da es geometrisch anschaulich ist und leicht zu erklären.

In der oben angegebenen Standardform ist es leider numerisch instabil:
Es kann Eingabefehler und Rundungsfehler ungünstig verstärken.

In der Numerik werden Sie daher weitere Verfahren zur QR–Zerlegung
kennenlernen und ihre Eigenschaften noch genauer analysieren.

🙂 Die Grundlage hierzu ist der Existenz- und Eindeutigkeitssatz P2B;
er erklärt, was wir erreichen wollen, und dass es eindeutig möglich ist.



Sei V ein $\mathbb{K}$–Vektorraum mit Skalarprodukt $\langle - \mid - \rangle$ und Norm $\|-\|$.
Hierin sei $U \leq V$ ein endlich-dim. Untervektorraum, $\dim U = n < \infty$.

Approximationsproblem: Zu einem gegebenen Vektor $v \in V$ suchen wir den / einen Vektor $v^* \in U$, der v am nächsten liegt.

Lösung: Wir projizieren v orthogonal auf U, siehe Skizze und Satz P2C.

☺ Schon der Fall $V = \mathbb{R}^2$ und $n = 1$ (und ebenso $V = \mathbb{R}^3$ und $n = 1, 2$) ist interessant und Ihnen vielleicht noch gut aus der Schule vertraut.

Die folgenden Argumente gelten jedoch ganz allgemein: Der Raum V darf beliebig groß sein, zum Beispiel ein Funktionenraum. Lediglich der Unterraum U muss zunächst noch endlich-dimensional bleiben.

Satz P2C: Gauß 1795, Bessel 1818

Sei V ein $\mathbb{K}$–Vektorraum mit Skalarprodukt $\langle - \mid - \rangle$ und Norm $\|-\|$.
Hierin sei $U \leq V$ ein Unterraum mit Orthonormalbasis $e_1, \ldots, e_n$.

(0) Zu jedem Vektor $v \in V$ existiert genau eine **Bestapproximation** in U, also ein Vektor $v^* \in U$ mit $\|v - v^*\| < \|v - u\|$ für alle $u \in U \smallsetminus \{v^*\}$.

(1) Diese ist gegeben durch die **Orthogonalprojektion** von v auf U:

$$v^* = \textstyle\sum_{k=1}^n v_k e_k \quad \text{mit Fourier–Koeffizienten} \quad v_k = \langle e_k \mid v \rangle.$$

(2) Zudem ist v^* der einzige Vektor in U, für den $(v - v^*) \perp U$ gilt.

(3) Dank Pythagoras P1N gilt daher die **Bessel–Gleichung**:

$$\underbrace{|v_1|^2 + \cdots + |v_n|^2}_{\text{Längenquadrat von } v^*} + \underbrace{\|v - v^*\|^2}_{\text{Approximationsfehler}} = \underbrace{\|v\|^2}_{\text{Längenquadrat von } v}$$

(4) Hieraus folgt vergröbernd die **Bessel–Ungleichung**:

$$|v_1|^2 + \cdots + |v_n|^2 = \|v^*\|^2 \quad \leq \quad \|v\|^2$$

Zusatz: Für die Aussagen (1,2,3) genügt es zu fordern, dass $\langle - \mid - \rangle$ auf V eine hermitesche Sesquilinearform ist. Dank der vorausgesetzten Orthonormalbasis ist sie dann positiv definit auf dem Unterraum $U \leq V$. Für (4) benötigen wir zudem, dass $\langle - \mid - \rangle$ auf V positiv semidefinit ist.

Beweis: (1) Wir betrachten den genannten Vektor

$$v^* := \textstyle\sum_{k=1}^n v_k e_k \quad \text{mit den Koeffizienten} \quad v_k = \langle e_k \mid v \rangle.$$

Für jeden Vektor $u \in U$ gilt $u = \sum_{k=1}^n u_k e_k$ mit Koeffizienten $u_k \in \mathbb{K}$.
Den Abstand zwischen v und u berechnen wir dank Skalarprodukt:

$$\begin{aligned}
\|v-u\|^2 &= \langle v-u \mid v-u \rangle = \langle v \mid v \rangle - \langle v \mid u \rangle - \langle u \mid v \rangle + \langle u \mid u \rangle \\
&= \langle v \mid v \rangle - \langle v \mid \textstyle\sum_k u_k e_k \rangle - \langle \sum_k u_k e_k \mid v \rangle + \langle \sum_k u_k e_k \mid \sum_\ell u_\ell e_\ell \rangle \\
&= \langle v \mid v \rangle - \textstyle\sum_k u_k \langle v \mid e_k \rangle - \sum_k \overline{u_k} \langle e_k \mid v \rangle + \sum_k \sum_\ell \overline{u_k} u_\ell \langle e_k \mid e_\ell \rangle \\
&= \langle v \mid v \rangle - \textstyle\sum_k u_k \overline{v_k} - \sum_k \overline{u_k} v_k + \sum_k |u_k|^2 \\
&= \|v\|^2 - 2\,\mathrm{Re}\langle u \mid v^* \rangle + \|u\|^2
\end{aligned}$$

Speziell für $u = v^*$ folgt $\|v - v^*\|^2 = \|v\|^2 - \|v^*\|^2$. Im Vergleich gilt:

$$\begin{aligned}
\|v-u\|^2 - \|v-v^*\|^2 &= \textstyle\sum_k |u_k|^2 - \sum_k u_k \overline{v_k} - \sum_k \overline{u_k} v_k + \sum_k |v_k|^2 \\
&= \textstyle\sum_k (\overline{u_k} - \overline{v_k})(u_k - v_k) = \sum_k |u_k - v_k|^2 \geq 0
\end{aligned}$$

Gleichheit gilt hierbei nur für $u = v^*$, andernfalls $\|v - u\| > \|v - v^*\|$.

(2) Die behauptete Orthogonalität rechnen wir ebenso direkt nach.
Für alle $u, u^* \in U$, also $u = \sum_k u_k e_k$ und $u^* = \sum_\ell u^*_\ell e_\ell$, gilt:

$$\langle u \mid v - u^* \rangle = \langle \textstyle\sum_k u_k e_k \mid v - \sum_\ell u^*_\ell e_\ell \rangle = \sum_k \overline{u_k} \big[\langle e_k \mid v \rangle - u^*_k \big] \stackrel{!}{=} 0$$

Demnach gilt $u \perp (v - u^*)$ für alle $u \in U$ genau dann, wenn die Koeffizienten $u^*_k = \langle e_k \mid v \rangle$ gewählt werden, also $u^* = v^*$ gilt.

Aus der expliziten Formel (1) und der Orthogonalität (2) folgt sofort die Bessel–Gleichung (3). Dank positiver Semidefinitheit von $\langle - \mid - \rangle$ auf V gilt $\|v - v^*\| \geq 0$ und somit die Bessel–Ungleichung (4). QED

Problemstellung: Zu lösen sei das lineare Gleichungssystem

$$Ax = b$$

mit $A \in \mathbb{K}^{m\times n}$ von Rang $\operatorname{rang} A = n \leq m$ und rechter Seite $b \in \mathbb{K}^m$.

Seien $a_1, \ldots, a_n \in \mathbb{K}^m$ die Spalten von A und $U = \langle\, a_1, \ldots, a_n \,\rangle \leq \mathbb{K}^m$ der Spaltenraum von A. Genau dann ist $Ax = b$ lösbar, wenn $b \in U$ gilt.

Allgemein suchen wir eine Näherungslösung $x^* \in \mathbb{K}^n$. Der Fehlervektor

$$v = Ax^* - b$$

soll dabei möglich klein sein, wir wollen also die Norm $\|v\|$ minimieren. Nach Satz P2C ist dies äquivalent zu $v \perp U$, und somit zu $v \perp a_i$ für alle $i = 1, \ldots, n$, kurz $A^\dagger v = 0$. Ausgeschrieben bedeutet das:

$$A^\dagger A x^* = A^\dagger b$$

☺ Statt unserer ursprünglichen, eventuell überbestimmten Gleichung $Ax = b$ lösen wir diese Umformung; letztere ist eindeutig lösbar.

Lemma P2D

Für jede Matrix $A \in \mathbb{K}^{m\times n}$ ist $A^\dagger A \in \mathbb{K}^{n\times n}$ symmetrisch (über $\mathbb{R}$) bzw. hermitesch (über $\mathbb{C}$), erfüllt $\ker(A^\dagger A) = \ker A$ und $\operatorname{rang}(A^\dagger A) = \operatorname{rang} A$.

Beweis: Zunächst gilt $(A^\dagger A)^\dagger = A^\dagger (A^\dagger)^\dagger = A^\dagger A$.

Wir zeigen $\ker(A^\dagger A) = \ker A$. Die Inklusion „$\supseteq$“ ist klar. Wir zeigen „$\subseteq$“: Sei $v \in \ker(A^\dagger A)$, also $A^\dagger A v = 0$. Dann gilt $0 = v^\dagger (A^\dagger A v) = (Av)^\dagger (Av)$, also $Av = 0$ und somit $v \in \ker A$.

Daraus folgt $\operatorname{rang}(A^\dagger A) = \operatorname{rang} A$ dank Dimensionsformel. QED

Bemerkung: Wir nutzen hier wesentlich $\mathbb{K} = \mathbb{R}, \mathbb{C}$ und die positive Definitheit des euklidischen Skalarprodukts $\langle\, u \mid v \,\rangle = u^\dagger v$.

Für beliebige Körper gilt diese Aussage nicht! Als einfaches Gegenbeispiel betrachte man die Matrix $A = \left[\begin{smallmatrix}1\\1\end{smallmatrix}\right] \in \mathbb{F}_2^2$ mit $A^\intercal A = 0$.

Satz P2E: Näherungslösung einer überbestimmten Gleichung

Zu lösen ist das lineare Gleichungssystem

$$Ax = b$$

mit $A \in \mathbb{K}^{m\times n}$ von Rang $\operatorname{rang} A = n \leq m$ und rechter Seite $b \in \mathbb{K}^m$.

(0) Dann P2C existiert genau eine Bestapproximation $x^* \in \mathbb{K}^n$ mit minimaler Fehlernorm $\|Ax^* - b\|$, gegeben durch $A^\dagger A x^* = A^\dagger b$.

(1) Dank des vorigen Lemmas ist $A^\dagger A \in \mathbb{K}^{n\times n}$ invertierbar, also gilt:

$$x^* = (A^\dagger A)^{-1} A^\dagger b$$

(2) Ist $A = QR$ die QR–Zerlegung von A gemäß Satz P2B, so folgt:

$$Rx^* = Q^\dagger b$$

Diese Gleichung kann durch Rückwärtseinsetzen leicht gelöst werden.

Beweis: Die Aussagen (0) und (1) haben wir zuvor schon hergeleitet.
(2) Aus $A^\dagger A x^* = A^\dagger b$ und $A = QR$ folgt $R^\dagger Q^\dagger Q R x^* = R^\dagger Q^\dagger b$, dank $Q^\dagger Q = E_n$ also $Rx^* = Q^\dagger x$. QED

☺ Wir nennen $A^+ = (A^\dagger A)^{-1} A^\dagger$ daher die **Pseudoinverse** zu A.
Zur Gleichung $Ax = b$ berechnet sie die Näherungslösung $x = A^+ b$.

Ist die Matrix A invertierbar, so auch $A^\dagger$, und dann gilt $A^+ = A^{-1}$.
In diesem Falle ist unsere Näherungslösung die exakte Lösung.

Aus der QR–Zerlegung $A = QR$ folgt $A^+ = R^{-1} Q^\dagger$.
Das ist besonders elegant und einfach zu rechnen.

☺ Die QR–Zerlegung ist ein Standardverfahren der (numerischen) Linearen Algebra und in jeder guten Softwarebibliothek professionell implementiert. Darauf können und sollten wir zurückgreifen.

Daher ist es sinnvoll, ein gegebenes Problem, wie oben $Ax = b$, auf ein solches, bewährtes Standardverfahren zurückzuführen.
Sobald dies gelingt, ist unser Problem gelöst.

Die Methode der kleinsten Quadrate

Die hier gezeigte Technik heißt **Methode der kleinsten Quadrate**. Wir minimieren dabei die Summe der Fehlerquadrate.

Sie ist ein wunderbar-geniales Universalwerkzeug, beginnend mit der Bestapproximation P2C nach Gauß–Bessel, über die Näherungslösung P2E einer überbestimmten Gleichung, hin zu zahlreichen Varianten und Anwendungen der Ausgleichsrechnung etwa in der Numerik, der Statistik oder dem maschinellen Lernen.

Überbestimmte Gleichungssysteme $Ax = b$ treten typischerweise wie folgt auf: Wir interessieren uns für eine (kleine) Anzahl von Kenngrößen $x_1, \ldots, x_n$. Zu ihrer Bestimmung haben wir eine (große) Anzahl von Messungen $b_1, \ldots, b_m$. Bei jedem Messvorgang treten unvermeidliche Messfehler auf, daher ist es im Prinzip vorteilhaft, möglichst viele Messungen zu machen. Andererseits können wir dann nicht mehr erwarten, hierzu eine exakte Lösung x zu finden.

Die Methode der kleinsten Quadrate

Die Methode der kleinsten Quadrate wurde unabhängig von Gauß und Legendre entwickelt (Legendre veröffentlichte sie 1805, Gauß 1809). Beide nutzten dieses Verfahren, um astronomische Umlaufbahnen anhand von Beobachtungsdaten möglichst genau zu bestimmen.

Am Neujahrstag 1801 entdeckte der Astronom Giuseppe Piazzi den Zwergplaneten Ceres. Vierzig Tage lang konnte er seine Bahn verfolgen, doch dann verschwand Ceres hinter der Sonne. Viele Astronomen versuchten erfolglos, anhand von Piazzis Beobachtungensdaten die Bahn zu berechnen und zu verfolgen, doch Ceres bleib verschwunden.

Dem 24-jährigen Gauß gelang der Durchbruch, die Bahn wesentlich genauer zu berechnen, indem er zur Ausgleichsrechnung die Methode der kleinsten Quadrate nutzte. Ausgehend von Gauß' Vorhersage konnte der Astronom Franz Xaver von Zach nach einem Jahr, am 7. und 31. Dezember 1801 Ceres tatsächlich wiederfinden.

Die Methode der kleinsten Quadrate

Ceres befand sich etwa $7°$ von der zuvor vermuteten Stelle, also mehr als 13 Vollmondbreiten. Das illustriert die schwierige Datenlage und die durchschlagende Verbesserung durch Mathematik und neue Verfahren. Dieser sensationelle Erfolg machten Gauß und seine Methode berühmt.

Übrigens nutzte Gauß im Zuge seiner astronomischen Berechnungen ganz systematisch noch ein weiteres wichtiges Werkzeug: die Lösung linearer Gleichungssysteme durch sukzessive Elimination der Variablen. Diese Rechenmethode war zuvor schon benutzt worden, doch Gauß führte sie virtuos zu höchster Blüte. Seine erste Veröffentlichung zu diesem Thema stammt aus dem Jahr 1810. Die Mathematik allgemein, und speziell die Lineare Algebra, entspringt und nützt direkt praktischen Anwendungen. Sie als abstrakt zu beschimpfen zeugt von Ignoranz.

Sowohl das Ausgleichs- als auch das Eliminationsverfahren wurden in der Folgezeit in der Geodäsie zur Landvermessung eingesetzt. Daher ist der zweite Namensgeber des Gauß–Jordan–Verfahrens nicht etwa der Mathematiker Camille Jordan, sondern der Geodät Wilhelm Jordan.

Die Methode der kleinsten Quadrate

Dieser historische Rückblick ist in sich schon eine faszinierende Geschichte. Zudem sehen wir daran erneut sehr eindrücklich, dass die scheinbar so abstrakten Methoden der Linearen Algebra auf ganz konkrete Fragestellungen und Bedürfnisse antworten.

Daher das eingangs zitierte Motto dieses Kapitels:

Unsere Allergrößten, wie Archimedes, Newton, Gauß,
haben stets Theorie und Anwendungen gleichmäßig umfasst.

Felix Klein (1849–1925)

Mathematik ist immer beides: sowohl abstrakte Theorie als auch konkrete Anwendung; sie sind keine Gegensätze, sie ergänzen sich, die eine kann nur mit der anderen dauerhaft erfolgreich sein.

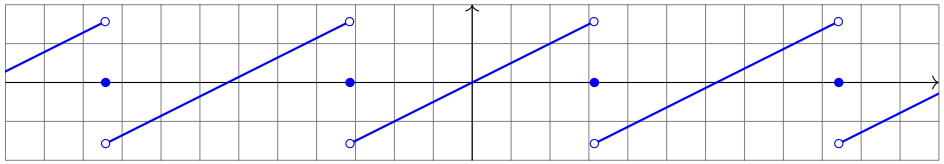
Am besten, Sie beherrschen beides!

Anwendung: Fourier–Entwicklung der Sägezahnfunktion

Sei V der $\mathbb{C}$–Vektorraum aller 2π–periodischen, stückweise stetigen Funktionen $f, g : \mathbb{R} \to \mathbb{C}$ mit dem (semidefiniten) Skalarprodukt

$$\langle f \mid g \rangle = \frac{1}{2\pi} \int_{-\pi}^{\pi} \overline{f(x)} g(t)\, \mathrm{d}x.$$

Sei $f : \mathbb{R} \to \mathbb{R}$ ungerade und 2π–periodisch mit $f(x) = x/2$ für $|x| < \pi$. Der erste Teil der Übung ist wie immer, die Funktion zu skizzieren:



Aufgabe: Berechnen Sie die Bestapproximation $f_n \in U_n$ im Unterraum $U_n = \langle e_k \mid -n \le k \le n \rangle \le V$ der Fourier–Polynome vom Grad $\le n$.

🙂 Das scheint zunächst ein verblüffend schwieriges Problem zu sein, doch dank Satz P2C wird alles leicht! Integration aus der Schule genügt.

Anwendung: Fourier–Entwicklung der Sägezahnfunktion

Lösung: Der Fourier–Koeffizient c_0 ist der Mittelwert über eine Periode:

$$c_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{x}{2}\, \mathrm{d}x = 0 \qquad \text{(ungerader Integrand)}$$

Für $k \neq 0$ nutzen wir partielle Integration:

$$c_k \overset{\text{Def}}{=} \frac{1}{4\pi} \int_{-\pi}^{\pi} \mathrm{e}^{-\mathrm{i}kx} x\, \mathrm{d}x \overset{\text{part}}{=} \frac{1}{4\pi} \left(\left[\frac{\mathrm{i}}{k} \mathrm{e}^{-\mathrm{i}kx} x \right]_{-\pi}^{\pi} - \int_{-\pi}^{\pi} \frac{\mathrm{i}}{k} \mathrm{e}^{-\mathrm{i}kx}\, \mathrm{d}x \right)$$
$$= \frac{\mathrm{i}}{4\pi k} \left[\mathrm{e}^{-\mathrm{i}\pi k} \pi - \mathrm{e}^{\mathrm{i}\pi k} \pi \right] = (-1)^k \frac{\mathrm{i}}{2k}$$

Damit haben wir zu $f \in V$ die Bestapproximation $f_n \in U_n$ gefunden:

$$f_n(x) = \sum_{k=1}^{n} (-1)^k \mathrm{i}\, \frac{\mathrm{e}^{\mathrm{i}kx} - \mathrm{e}^{-\mathrm{i}kx}}{2k} = \sum_{k=1}^{n} (-1)^{k+1} \frac{\sin(kx)}{k}$$
$$= \sin x - \frac{\sin 2x}{2} + \frac{\sin 3x}{3} - \frac{\sin 4x}{4} + \cdots + (-1)^{n+1} \frac{\sin nx}{n}$$

Anwendung: Fourier–Entwicklung der Sägezahnfunktion

Umrechnung der Koeffizienten für die Sinus-Cosinus-Reihe:

$$a_k = c_k + c_{-k} = 0, \qquad b_k = \mathrm{i}(c_k - c_{-k}) = (-1)^{k+1} \frac{1}{k}.$$

Zum Vergleich nochmal direkt die Integrale für a_k, b_k mit $k \ge 1$:

$$a_k = \frac{1}{\pi} \int_{-\pi}^{\pi} \frac{x}{2} \cos(kx)\, \mathrm{d}x \qquad \text{(ungerader Integrand)}$$
$$= \frac{1}{2\pi} \left(\left[x \frac{\sin(kx)}{k} \right]_{-\pi}^{\pi} - \int_{-\pi}^{\pi} \frac{\sin(kx)}{k}\, \mathrm{d}x \right) = 0$$

$$b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} \frac{x}{2} \sin(kx)\, \mathrm{d}x$$
$$= \frac{1}{2\pi} \left(\left[x \frac{-\cos(kx)}{k} \right]_{-\pi}^{\pi} + \int_{-\pi}^{\pi} \frac{\cos(kx)}{k}\, \mathrm{d}x \right) = (-1)^{k+1} \frac{1}{k}$$

Zur Berechnung von a_k, b_k sind zwei reelle Integrale nötig, für c_k nur ein komplexes; die Wahl des Rechenwegs ist meist Geschmackssache. Die Umrechnung zwischen a_k, b_k und c_k gelingt jedenfalls leicht.

Anwendung: Fourier–Entwicklung der Sägezahnfunktion

🙂 Die Fourier–Koeffizienten a_k, b_k, c_k sind hier leicht zu berechnen. Da f reell ist, gilt $a_k, b_k \in \mathbb{R}$ und $c_{-k} = \overline{c_k}$. Da f ungerade, gilt $a_k = 0$.

🙂 Die folgenden Graphiken zeigen hierzu die **Fourier–Polynome** f_n. Wir wollen verstehen, ob und in welchem Sinne f_n gegen f konvergiert.

🙂 Für jeden Punkt $x \in \mathbb{R}$ gilt augenscheinlich $f_n(x) \to f(x)$ für $n \to \infty$: In den Punkten $x = 0$ und $x = \pi$ ist dies klar, ansonsten keineswegs!

☹ Die Koeffizienten klingen nur langsam ab ($\sim 1/k$), das heißt auch hohe Frequenzen tragen noch deutlich bei: Die Fourier–Reihe ist „rau“.

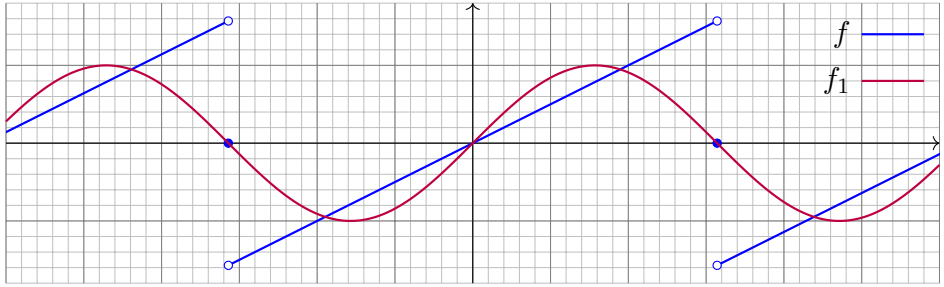
⚠ Wir sehen recht eindringlich das sogenannte **Gibbs–Phänomen**: Die Funktionen f_n überschwingen in Sprungstellen um ca. 9%.

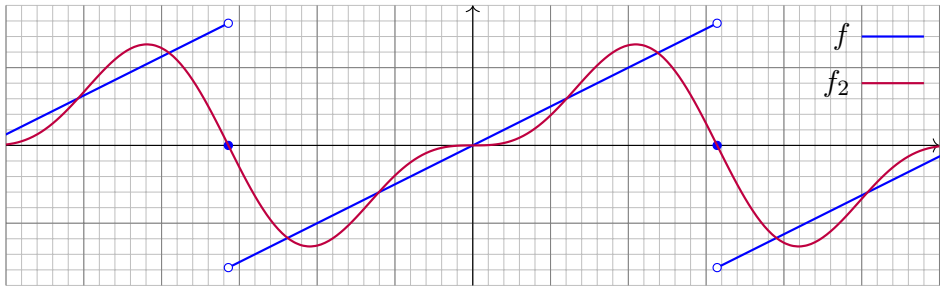
☹ Es gilt daher **keine gleichmäßige Konvergenz** $f_n \to f$ auf $\mathbb{R}$: Ein kleiner ε–Schlauch um f enthält nicht alle f_n für $n \ge n_0$.

🙂 Auf jedem Intervall $I = [-\pi + \delta, \pi - \delta]$ **abseits der Sprungstellen** konvergiert f_n gleichmäßig gegen f: Zu jedem $\varepsilon > 0$ liegen schließlich alle f_n im ε–Schlauch um f auf I. Auch das ist bemerkenswert!

Anwendung: Fourier–Entwicklung der Sägezahnfunktion

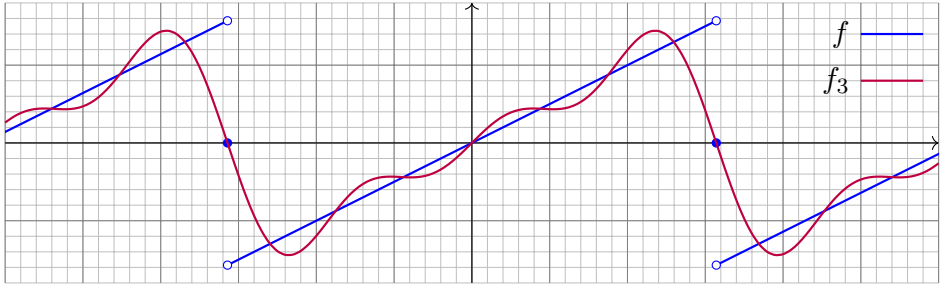
Die ersten Fourier–Polynome f_1, f_2 ähneln f zunächst nur grob:

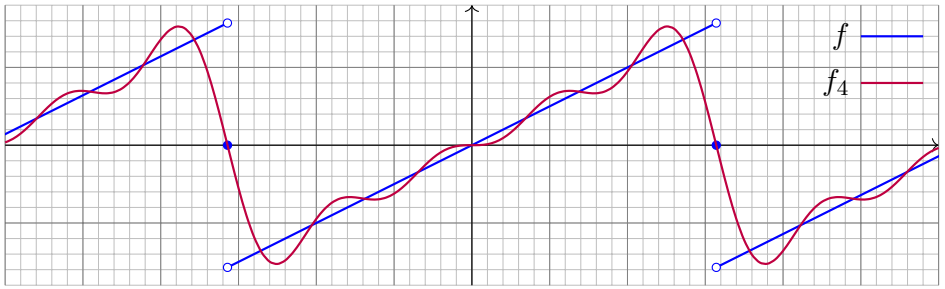




Anwendung: Fourier–Entwicklung der Sägezahnfunktion

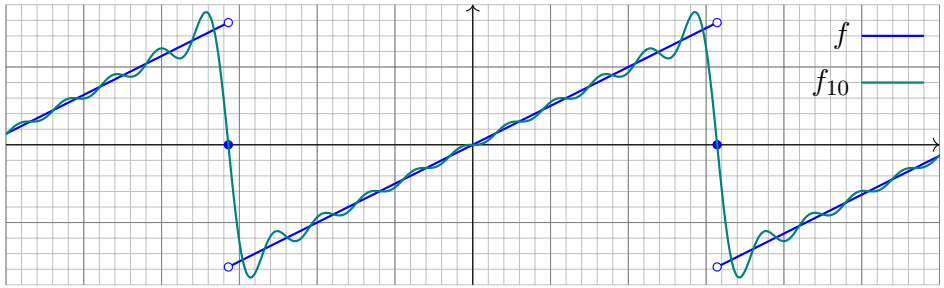
Die nächsten Fourier–Polynome f_3, f_4 ähneln f schon etwas mehr:

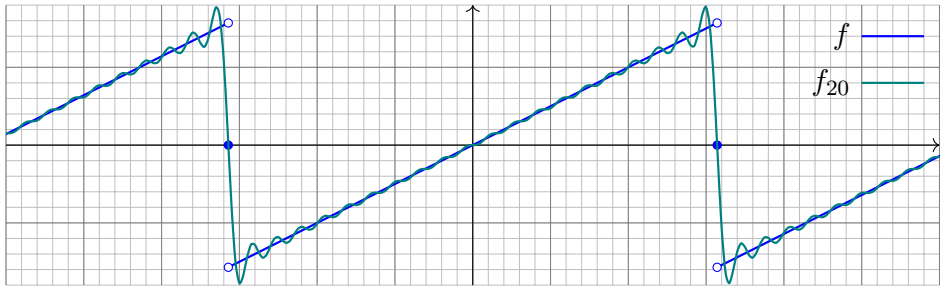




Anwendung: Fourier–Entwicklung der Sägezahnfunktion

Die Fourier–Polynome überschwingen bis zu 9% der Sprunghöhe:





Was bedeutet Konvergenz der Fourier–Reihe?

Wir haben die Sägezahnfunktion $f : \mathbb{R} \to \mathbb{R}$ durch Fourier–Polynome $f_1, f_2, f_3, \ldots : \mathbb{R} \to \mathbb{R}$ angenähert: Dies ist die L^2–Bestapproximation! Die gezeigten Graphiken suggerieren, dass dies erstaunlich gut gelingt. Obwohl f unstetig ist, nähern sich die Funktionen f_n doch recht gut an.

Ich habe dieses Beispiel so weit getrieben, wie es mit den Werkzeugen der Linearen Algebra (und etwas Integration aus der Schule) möglich ist. Die genauere Untersuchung lernen Sie in der Analysis. Als Ausblick will ich die Antworten auf die Konvergenzfrage wenigstens kurz skizzieren.

Es gilt Konvergenz im quadratischen Mittel: Für jede 2π–periodische Funktion $f : \mathbb{R} \to \mathbb{C}$ mit $\|f\| < \infty$ gilt $\|f - f_n\| \searrow 0$, somit $\|f_n\| \nearrow \|f\|$. Bezüglich der L^2–Norm gilt also: Jede quadrat-integrierbare Funktion f lässt sich beliebig gut durch ihre Fourier–Polynome f_n approximieren.

Die Frage der punktweisen Konvergenz $|f(x) - f_n(x)| \to 0$ oder der gleichmäßigen Konvergenz $\sup_{x\in\mathbb{R}} |f(x) - f_n(x)| \to 0$ ist kniffliger. Hierzu nenne ist das folgende berühmte Kriterium von Dirichlet, das für viele praktischen Anwendungen genügt.

Konvergenz im quadratischen Mittel

Satz P2F: Konvergenz bezüglich der L^2–Norm

Sei $f : \mathbb{R} \to \mathbb{C}$ absolut integrierbar auf $[0, T]$ und T–periodisch.

Die **Fourier–Analyse** zerlegt das Signal f in sein Spektrum $\widehat{f} : \mathbb{Z} \to \mathbb{C}$ gegeben durch die Koeffizienten $\widehat{f}(k) := \langle\, e_k \mid f \,\rangle = \frac{1}{T} \int_{t=0}^{T} \mathrm{e}^{-\mathrm{i}k\omega t} f(t)\, \mathrm{d}t$.

Dabei gilt die **Parseval–Gleichung**, auch **Energiegleichung** genannt:

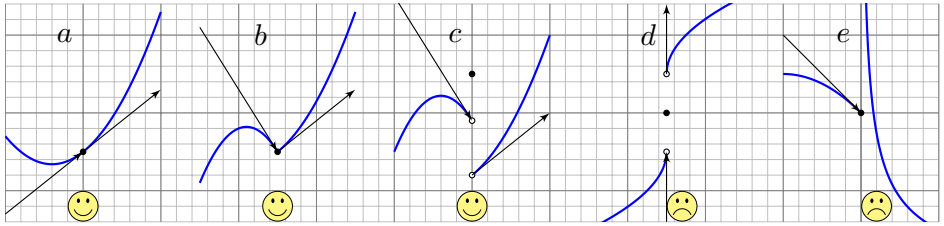
$$\|f\|_{L^2} = \|\widehat{f}\|_{\ell^2} \quad \text{also} \quad \frac{1}{T} \int_{t=0}^{T} |f(t)|^2 \, \mathrm{d}t = \sum_{k=-\infty}^{\infty} |\widehat{f}(k)|^2$$

Ist f quadrat-integrierbar, also $\|f\| < \infty$, so konvergieren die Fourier–Polynome f_n bezüglich der L^2–Norm, also $\|f - f_n\| \searrow 0$ für $n \to \infty$.

Beispiel: Die Sägezahnfunktion liefert die bemerkenswerte Gleichung

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}.$$

Punktweise Konvergenz von Fourier–Reihen



Links-/rechtsseitiger Grenzwert und Ableitungen von f im Punkt x:

$$f(x-) := \lim_{\xi \nearrow x} f(\xi), \qquad f(x+) := \lim_{\xi \searrow x} f(\xi),$$

$$f'(x-) := \lim_{\xi \nearrow x} \frac{f(\xi) - f(x-)}{\xi - x}, \qquad f'(x+) := \lim_{\xi \searrow x} \frac{f(\xi) - f(x+)}{\xi - x}.$$

Die **Dirichlet–Bedingung** fordert, dass alle vier Grenzwerte existieren.
Wir nennen f **sprungnormiert**, falls $f(x) = \frac{1}{2}\big[f(x+) + f(x-)\big]$ gilt.

Stetigkeit im Punkt $x \in \mathbb{R}$ ist äquivalent zu $f(x+) = f(x-) = f(x)$.
Im Falle $f(x+) \neq f(x-)$ hat f in x eine **Sprungstelle** (siehe Skizze).

Differenzierbarkeit im Punkt x impliziert Stetigkeit und ist äquivalent zu Dirichlet mit $f(x+) = f(x-) = f(x)$ und $f'(x+) = f'(x-) = f'(x)$.

Punktweise Konvergenz von Fourier–Reihen

Satz P2G: Dirichlet–Kriterium für Fourier–Reihen

Sei $f : \mathbb{R} \to \mathbb{C}$ absolut integrierbar auf $[0, 2\pi]$ und 2π–periodisch.

(1) Angenommen, $f : \mathbb{R} \to \mathbb{C}$ erfüllt die Dirichlet–Bedingung im Punkt x, d.h. beide Grenzwerte $f(x\pm)$ und beide Ableitungen $f'(x\pm)$ existieren. Dann konvergiert in diesem Punkt x die Fourier–Reihe $f_n(x)$ gemäß

$$f_n(x) = \textstyle\sum_{k=-n}^{n} c_k \, \mathrm{e}^{\mathrm{i}kx} \quad \to \quad \frac{1}{2}\big[f(x+) + f(x-)\big] \quad \text{für} \quad n \to \infty.$$

Spezialfälle: (1a) Es gilt $f_n(x) \to f(x)$ falls f in x sprungnormiert ist, also $f(x) = \frac{1}{2}[f(x+) + f(x-)]$, oder sogar stetig, also $f(x\pm) = f(x)$.

(1b) Ist $f : \mathbb{R} \to \mathbb{C}$ stückweise stetig differenzierbar und überall stetig bzw. sprungnormiert, dann konvergiert $f_n(x) \to f(x)$ in jeden Punkt $x \in \mathbb{R}$.

(2) Ist $f : \mathbb{R} \to \mathbb{C}$ stetig und stückweise stetig differenzierbar mit $|f'| \leq L$, so konvergiert die Fourier–Reihe $f_n \to f$ sogar gleichmäßig auf ganz $\mathbb{R}$:

$$\big|f_n(x) - f(x)\big| \quad \leq \quad 2L \cdot \ln(n)/n \quad \to 0 \quad \text{für} \quad n \to \infty$$

Punktweise Konvergenz von Fourier–Reihen

Beispiel: Unsere Sägezahnfunktion erfüllt die Dirichlet–Bedingung in jedem Punkt $x \in \mathbb{R}$ (Übung!) und ist zudem sprungnormiert. Daher gilt in jedem Punkt $x \in \mathbb{R}$ die Konvergenz $f_n(x) \to f(x)$ für $n \to \infty$.

🙂 Damit haben wir die Funktion f in ihre Fourier–Reihe entwickelt!
Das ist kein Fourier–Polynom mehr, sondern eine unendliche Reihe:

$$\begin{aligned} f(x) &= \sum_{k=1}^{\infty} (-1)^k \, \mathrm{i} \, \frac{\mathrm{e}^{\mathrm{i}kx} - \mathrm{e}^{-\mathrm{i}kx}}{2k} = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{\sin(kx)}{k} \\ &= \sin x - \frac{\sin 2x}{2} + \frac{\sin 3x}{3} - \frac{\sin 4x}{4} + \frac{\sin 5x}{5} \mp \dots \end{aligned}$$

🙂 Daraus können wir für erstaunliche Reihen den Grenzwert ablesen.
Die Auswertung im Punkt $x = \pi/2$ bzw. $x = \pi/3$ zum Beispiel ergibt:

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15} + \dots = \frac{\pi}{4} = 0.7853981633\dots$$

$$1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \frac{1}{10} - \frac{1}{11} + \dots = \frac{\pi}{3\sqrt{3}} = 0.6045997880\dots$$

Kapitel Q

Spektralsatz und Anwendungen

Zitat

Inhalt dieses Kapitels Q

Dieses Kapitel ist noch in Arbeit und wird später eingefügt.

Kapitel R

Linearformen und Dualität

Inhalt dieses Kapitels R

Dualräume: grundlegend & allgemein = schwierig?

In diesem Kapitel behandeln wir die sagenhaften Dualräume. Dies ist ein grundlegendes und letztlich einfaches Konzept. Wir nutzen es schon lange, ohne es bisher benannt zu haben. Das wollen wir nun nachholen, und mit unseren festen Werkzeugen wird uns dies bestens gelingen.

Wir werden dabei viele gute, alte Bekannte wiedertreffen und erfolgreich mit ihnen arbeiten: lineare Räume, lineare Abbildungen und Matrizen, Basen und lineare Fortsetzungen, in/sur/bijektive Abbildungen, uvm. Dualräume sind ein ideales Testfeld für all unsere Techniken!

In studentischer Folklore gelten Dualräume traditionell als schwierig. Beim ersten Kontakt kann ich das gut verstehen, denn die Begriffe sind neu und allgemein. Nach einem ersten Durchgang sollte dies einem erleichterten „Achso!“ weichen, denn es ist wirklich nicht schwer.

Neben präzisen Vokabeln und sorgsamen Rechnungen gibt es hier keine wirklichen mathematischen Schwierigkeiten. Wohl gibt es die üblichen lernpsychologischen Hürden, wie so oft bei neuen Begriffen. Wie immer helfen Ihnen Stift und Papier und selbständiges Rechnen.

Dualräume: grundlegend & allgemein = schwierig?

In diesem Kapitel arbeiten wir durchweg über einem beliebigen Ring R. Um Trivialitäten zu vermeiden, fordern wir lediglich $1 \neq 0$, also $R \neq \{0\}$. Unser Ring R muss dabei kein Körper sein, ja nicht einmal kommutativ; mögliche Beispiele sind $\mathbb{Z}/n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, K^{r\times r}, \ldots$ und viele mehr.

Ich habe mich hier ganz bewusst zu dieser Allgemeinheit entschlossen, teils aus mathematischen Motiven, vor allem als psychologische Hilfe:

1. Oft kostet Allgemeinheit mehr Mühe, hier jedoch ist es umgekehrt: Alle Beweise sind im allgemeinen Fall keinen Deut schwieriger, sondern im Gegenteil wesentlich klarer und dadurch leichter.
2. Der nicht-kommutative Fall zwingt uns zu Links-Rechts-Disziplin. Dadurch gibt es keine Wahlmöglichkeiten und keine Abzweigungen. Es gibt nur genau eine Formulierung, und diese ist dann die richtige!
3. Wir erhalten gratis ein riesiges Repertoire an Gegen/Beispielen. Diese illustrieren eindrücklich alle Feinheiten und Besonderheiten, die einem allzu eingeschränkten Blick sonst leicht entgehen würden.

Wo Divisionsringe oder Körper verlangt sind, sage ich dies dazu.

Bei theoretischen Grundlagen plädiere ich für logischen Minimalismus; nicht immer, aber hier; nicht dogmatisch, sondern aus guter Erfahrung: Wer nur das Allernötigste voraussetzt, kann zwar nur wenig damit tun, doch zum Glück auch nur wenig Unfug treiben und kaum Irrwege gehen.

Bei den Beispielen, Illustrationen und Anwendungen hingegen plädiere ich dafür, aus dem Vollen zu schöpfen, neben der Linearen Algebra auch die Analysis, die Numerik, die Physik und vieles mehr zu bewundern. Dazu habe ich im Folgenden einige Ausblicke zumindest skizziert.

Wir gehen den langen Weg und schmähen weder Satz noch Beispiel. Das ist mathematisch ehrlich und didaktisch hilfreich, so hoffe ich! Die Theorie strukturiert und vereinfacht, hier sollte alles klar sein. In den Anwendungen jedoch tobt das Leben, prall und verwirrend.

Manche Studierende skandieren „Wir wollen keine abstrakte Theorie, sondern nur Beispiele!“ Ich denke, die Mischung macht den Erfolg. Abstraktion strukturiert und vereinfacht: Eine allgemeine Tatsache ist oft leichter zu verstehen und zu erklären als ihre zahlreichen Spezialfälle.

Seien Sie versichert: Linearformen und Dualität sind nicht esoterisch, sondern allgegenwärtige Phänomene, in vielfältiger Erscheinung!

Sie sehen dies bereits in der Schule, wenn Sie eine Ebene $E \leq \mathbb{R}^3$ im euklidischen Raum beschreiben wollen oder bestimmen müssen: Dies gelingt auf zwei duale Weisen, explizit durch eine **Parametrisierung**

$$E = \{\, p_0 + t_1(p_1 - p_0) + t_2(p_2 - p_0) \mid t_1, t_2 \in \mathbb{R} \,\}$$

oder implizit als Lösungsmenge einer **Gleichung**

$$E = \{\, x \in \mathbb{R}^3 \mid a_1x_1 + a_2x_2 + a_3x_3 = b \,\}.$$

Beide Darstellungen lassen sich ineinander umrechnen, und jede hat ihre eigenen Vorzüge. Versuchen Sie etwa folgende Probleme zu lösen:

1. Geben Sie ein (beliebiges, willkürliches) Element $x \in E$ explizit an.
2. Prüfen Sie zu einem (vorgegebenen) Punkt $x \in \mathbb{R}^3$, ob $x \in E$ gilt.

Die erste Frage ist in der ersten Darstellung leicht, in der zweiten schwer. Für die zweite Frage ist es umgekehrt. Beide ergänzen sich wunderbar!

Wir betrachten lineare Abbildungen $f : V \to W$ über einem Ring R. Speziell beim Zielraum $W = R$ nennen wir dies eine **Linearform**.

Linearformen werden tatsächlich überall genutzt, wo gerechnet wird, meist ganz natürlich, ohne es zu merken oder besonders zu erwähnen. Ich nenne einige spektakuläre Anwendungen in Mathematik und Physik:

Algebraisch-numerische Anwendungen:

- Dualität zwischen Gleichungssystemen und Lösungsräumen
- Dualität in der linearen Optimierung (lineare Ungleichungen)

Analytisch-geometrische Anwendungen:

- mehrdimensionale Analysis, Differential- und Integralrechnung
- Differentialgeometrie, Riemannsche Metriken, Krümmung, etc.

Anwendungen in der Funktionalanalysis:

- Dualräume mit Topologie / Norm / Skalarprodukt
- Distributionen als Dualraum der Testfunktionen

Wie so oft wurden und werden viele „theoretische“ Entwicklungen der Mathematik angetrieben durch ganz handfeste „konkrete“ Bedürfnisse in den Anwendungen. Im vorliegenden Falle ist dies ganz genauso! Das Abstrakte hilft dem Konkreten, so wie es sein soll.

Anwendungen in der Physik:

- Distributionen als verallgemeinerte Funktionen
- Mechanik, Wegintegrale über Differentialformen
- Thermodynamik, Wegintegrale über Differentialformen
- Elektrodynamik, das Potential als Differentialform
- spezielle und allgemeine Relativitätstheorie
- Quantenmechanik, Bra und Ket als duale Objekte

Ich werde daher im Folgenden die grundlegenden Begriffe entwickeln und zugleich illustrative Beispiele skizzieren. Sie werden dabei sehen: Die Theorie ist leicht, die Beispiele sind komplex. So ist das Leben!

Linearformen

R101

Sei R ein Ring mit $0 \neq 1$, etwa $\mathbb{Z}/n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, K^{r\times r}, \ldots$.
Eine (homogene) lineare Gleichung über dem Ring R hat die Form

$$a_1x_1 + \cdots + a_nx_n = 0.$$

In Matrixnotation schreiben wir dies als Zeile mal Spalte:

$$a = \begin{bmatrix} a_1 & \ldots & a_n \end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad a \cdot x = a_1x_1 + \cdots + a_nx_n$$

Anschaulich ist x ein **Vektor** und dual hierzu ist a ein **Covektor**.
Insbesondere können wir a und x als **Linearformen** interpretieren:

$$\varphi_a : R^{n\times 1} \to R : x \mapsto a \cdot x \quad \text{vs} \quad \psi_x : R^{1\times n} \to R : a \mapsto a \cdot x$$

Albert Einstein (1879–1955) führte hierzu die **Summenkonvention** ein:
Covektor $a = (a^i)$ mal Vektor $x = (x_i)$ ergibt den Skalar $a^ix_i := \sum_i a^ix_i$.
Paul Dirac (1902–1984) erfand hierzu später die **Bra-Ket-Notation**:
Aus Bra $\langle a|$ und Ket $|x\rangle$ wird durch Auswertung der Skalar $\langle\, a \mid x \,\rangle$.

Linearformen

R102

Definition R1A: Linearformen auf einem linearen Raum V

Sei R ein Ring und $(V, +, \cdot)$ ein rechtslinearer Raum über R.

Eine **Linearform** auf V ist eine rechtslineare Abbildung $\varphi : V \to R$ in den Grundring R, das heißt für alle $u, v \in V$ und $\lambda, \mu \in R$ gilt

$$\varphi(u\lambda + v\mu) = \varphi(u)\lambda + \varphi(v)\mu.$$

Dasselbe gilt entsprechend für linkslineare Räume und Abbildungen.

Beispiel: Die Spur $\operatorname{tr} : R^{n\times n} \to R : (a_{ij}) \mapsto \sum_i a_{ii}$ ist eine Linearform, die Determinante $\det : R^{n\times n} \to R$ jedoch nicht für $n \geq 2$ (L2O).

Beispiel: Auf dem Funktionenraum $V = \mathscr{C}^1(\mathbb{R}, \mathbb{R})$ über $\mathbb{R}$ haben wir die folgenden Linearformen, auch **lineare Funktionale** genannt:

$$\begin{aligned} \delta_a &: V \to \mathbb{R} : f \mapsto \delta_a(f) = f(a), \\ \delta'_a &: V \to \mathbb{R} : f \mapsto \delta'_a(f) = -f'(a), \\ \iota_a &: V \to \mathbb{R} : f \mapsto \iota_a(f) = \textstyle\int_{x=0}^{a} f(x)\,\mathrm{d}x. \end{aligned}$$

Linearformen sind auch Vektoren.

R103

Definition R1B: der Dualraum V^* zum Raum V

Der **Dualraum** V^* von V ist die Menge aller Linearformen auf V:

$$V^* = \operatorname{Hom}_R(V, R) = \{\, \varphi : V \to R \mid \varphi \text{ ist rechtslinear} \,\}$$

Dies ist ein linkslinearer Raum $(V^*, +, \cdot)$ mit den Verknüpfungen

$$\begin{aligned} + &: V^* \times V^* \to V^* : (\varphi + \psi)(v) = \varphi(v) + \psi(v), \\ \cdot &: R \times V^* \to V^* : (\alpha\varphi)(v) = \alpha\varphi(v). \end{aligned}$$

Gleiches gilt bei Vertauschung von rechts und links.

Aufgabe: Rechnen Sie dies nach! Addition $+$ und Skalarmultiplikation $\cdot$ stehen hier für drei verschiedene Verknüpfungen: in R, in V und in V^*.

Bemerkung: Ist der Ring R kommutativ, zum Beispiel ein Körper, so brauchen wir links und rechts hier nicht weiter zu unterscheiden. Der allgemeine Fall lässt weniger Freiheit und schafft mehr Klarheit.

Linearformen sind auch Vektoren.

R104
Erläuterung

Lösung: Zunächst und vor allem ist die Wohldefiniertheit zu prüfen!
Sind $\varphi, \psi : V \to R$ rechtslinear, so auch $\varphi + \psi : V \to R$, denn für alle $u, v \in V$ und $\alpha, \lambda, \mu \in R$ gilt:

$$\begin{aligned} (\varphi + \psi)(u\lambda + v\mu) &\overset{\text{Def}}{=} \varphi(u\lambda + v\mu) + \psi(u\lambda + v\mu) \\ &\overset{\text{Lin}}{=} \varphi(u)\lambda + \varphi(v)\mu + \psi(u)\lambda + \psi(v)\mu \\ &\overset{\text{Lin}}{=} [\varphi(u) + \psi(u)]\lambda + [\varphi(v) + \psi(v)]\mu \\ &\overset{\text{Def}}{=} [(\varphi + \psi)(u)]\lambda + [(\varphi + \psi)(v)]\mu \end{aligned}$$

$$\begin{aligned} (\alpha\varphi)(u\lambda + v\mu) &\overset{\text{Def}}{=} \alpha[\varphi(u\lambda + v\mu)] \\ &\overset{\text{Lin}}{=} \alpha[\varphi(u)\lambda + \varphi(v)\mu] \\ &\overset{\text{Lin}}{=} \alpha\varphi(u)\lambda + \alpha\varphi(v)\mu \\ &\overset{\text{Def}}{=} [(\alpha\varphi)(u)]\lambda + [(\alpha\varphi)(v)]\mu \end{aligned}$$

Demnach sind die Addition $+ : V^* \times V^* \to V^* : (\varphi, \psi) \mapsto \varphi + \psi$ und die Skalarmultiplikation $\cdot : R \times V \to V : (\alpha, \varphi) \mapsto \alpha\varphi$ wohldefiniert.
Somit ist $\operatorname{Hom}_R(V, R)$ ein Unterraum von $(\operatorname{Abb}(V, R), +, \cdot)$. (I1A) QED

Der Zeilenraum $R^{1\times n}$ ist dual zum Spaltenraum $R^{n\times 1}$.

R105

Beispiel R1C: Spaltenraum $V = R^{n\times 1}$ und Zeilenraum $V^* \cong R^{1\times n}$

Sei R ein Ring und hierüber $V = R^{n\times 1}$ der Raum der Spaltenvektoren. Der Dualraum $V^* \cong R^{1\times n}$ ist isomorph zum Raum der Zeilenvektoren.

Genauer: Zu $a \in R^{1\times n}$ definieren wir $\varphi_a : V \to R$ durch $\varphi_a(x) = a \cdot x$.
(1) Die Abbildung φ_a ist rechtslinear, also $\varphi_a \in V^* = \mathrm{Hom}_R(V, R)$.
(2) Die Abbildung $\Phi : R^{1\times n} \to V^* : a \mapsto \varphi_a$ ist linkslinear.
(3) Sie ist zudem bijektiv, also ein Isomorphismus.

Aufgabe: Rechnen Sie die hier gemachten Behauptungen nach.

Lösung: Wir haben in §B1 nachgerechnet: Die Matrixmultiplikation $R^{p\times q} \times R^{q\times r} \to R^{p\times r}$, hier für $(p, q, r) = (1, n, 1)$, ist (1) rechtsdistributiv und (2) linksdistributiv, und die Skalarmultiplikation jeweils assoziativ.

(3) Jede rechtslineare Abbildung $\varphi : V \to R$ können wir eindeutig durch eine Matrix $a \in R^{1\times n}$ darstellen (K1E), also $\varphi = \varphi_a$. QED

🙂 Wir werden diese Dualität in R2E noch eleganter formulieren, nämlich gleichberechtigt in $R^{n\times 1} = V$ und $R^{1\times n} \cong V^*$.

Der Zeilenraum $R^{1\times n}$ ist dual zum Spaltenraum $R^{n\times 1}$.

R106
Erläuterung

Bemerkung: Sei R ein Ring und hierüber $V = R^{1\times n}$ der linkslineare Raum der Zeilenvektoren. Der Dualraum $V^* \cong R^{1\times n}$ ist isomorph zum rechtslinearen Raum der Spaltenvektoren. Der Beweis verläuft genauso. Bitte führen Sie dies zur Übung der Begriffe selbst sorgsam aus!

(Formal erhalten wir dieses Ergebnis durch Transposition von Matrizen. Dabei müssen wir allerdings zusätzlich auch alle Faktoren vertauschen: Das gelingt automatisch über jedem kommutativen Ring; über einem nicht kommutativen Ring benötigen wir einen Anti-Automorphismus.)

Wie versprochen sind Linearformen und Dualräume ein einfaches und grundlegendes Konzept. Einzig die Abstraktion mag etwas schrecken.

Zeilen- und Spaltenvektoren sind ein simples, doch hilfreiches Beispiel, doch längst noch nicht alles! Zur Illustration betone ich zudem Beispiele aus der Analysis, der Numerik, dem Obsthandel und der Physik.

Wem das doch zu naiv-angewandt und verwirrend-anschaulich ist, der möge dies zunächst übergehen später darauf zurückkommen.

Beispiel: numerische Integration nach Gauß–Legendre

R107
Erläuterung

Beispiel: Auf $V = \mathscr{C}([a, b], \mathbb{R})$ über $\mathbb{R}$ ist das Integral eine Linearform:

$$I : V \to \mathbb{R} : f \mapsto \int_{x=a}^{b} f(x)\,\mathrm{d}x$$

Diese wollen wir numerisch approximieren, möglichst gut und günstig. Sei $n \geq 1$. Zu Stützstellen $a \leq x_1 < x_2 < \cdots < x_n \leq b$ und Gewichten $(w_1, w_2, \ldots, w_n) \in \mathbb{R}$ definieren wir die **Abtastung** (engl. *sampling*)

$$S_x^w : V \to \mathbb{R} : f \mapsto (b-a) \sum_{i=1}^{n} w_i f(x_i).$$

Nach der affinen Transformation $\tau : \mathbb{R} \to \mathbb{R} : x \mapsto (2x - a - b)/(b - a)$ können wir vereinfachend $[a, b] = [-1, 1]$ annehmen.

Berühmte Beispiele sind die Mittelpunktsregel ($n = 1$, $x_1 = 0$, $w_1 = 1$), die Trapezregel ($n = 2$, $x = (-1, 1)$, $w = (1/2, 1/2)$), die Keplersche Fassregel ($n = 3$, $x = (-1, 0, 1)$, $w = (1/6, 4/6, 1/6)$) und viele weitere.

🙂 Gäbe es Linearformen noch nicht, wir erfänden sie hier neu!

Beispiel: numerische Integration nach Gauß–Legendre

R108
Erläuterung

🙂 Jedes S_x^w ist eine Linearform, also ein Element des Dualraums V^*. Wir suchen (x, w), sodass S_x^w das Integral I möglichst gut approximiert.

Newton–Cotes: Der erste und einfachste Fall entsteht, wenn wir die Stützstellen fest vorschreiben, etwa äquidistant $x_k = a + (b - a) \cdot k/n$. Dann können wir die Gewichte $w_1, \ldots, w_n \in \mathbb{R}$ so wählen, dass exakte Gleichheit $I(f) = S_x^w(f)$ für alle Polynome vom Grad $< n$ gilt. (Übung!) Die obige Trapezregel und die Fassregel sind genau von dieser Form.

Gauß–Legendre: Es erweist sich als vorteilhaft, die Stützstellen nicht äquidistant zu wählen, sondern je nach Bedarf ihre Lage zu optimieren. Es existiert genau eine Lösung (x, w), sodass Gleichheit $I(f) = S_x^w(f)$ für alle Polynome vom Grad $< 2n$ gilt. (Mehr hierzu in der Numerik!) Zudem ist Gleichheit bis Grad $\leq 2n$ nachweislich nicht möglich.

🙂 Das antwortet auf die eingangs gestellte Optimierungsfrage: Unter allen Abtastungen mit höchstens n Auswertungen ist Gauß–Legendre die beste Approximation, also wie gewünscht: möglichst gut und günstig.

Beispiel: Äpfel und Birnen

R109

Ein Obstladen führt Bestandslisten, etwa für Einkauf und Verkauf:

$$x = x_1\,\mathrm{Apfel} + x_2\,\mathrm{Birne} + x_3\,\mathrm{Citrone} + \dots$$

Solche Bestandslisten über $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bilden einen linearen Raum:

$$V = \langle\, \mathrm{Obst} \,\rangle_R^! \quad \text{mit Basis} \quad \mathrm{Obst} = \{\, \mathrm{Apfel}, \mathrm{Birne}, \mathrm{Citrone}, \dots \,\}$$

☹ Ein Skalarprodukt ist sinnlos, es würde Äpfel mit Birnen vergleichen:

$$\langle\, x \mid x \,\rangle = x_1^2\,\mathrm{Apfel}^2 + x_2^2\,\mathrm{Birne}^2 + x_3^2\,\mathrm{Citrone}^2 + \dots$$

Dual zu Bestandslisten sind Preislisten (in Euro):

$$a = a_1/\mathrm{Apfel} + a_2/\mathrm{Birne} + a_3/\mathrm{Citrone} + \dots$$

Auch Preislisten über R bilden einen linearen Raum:

$$V^* = \langle\, \mathrm{Obst}^{-1} \,\rangle_R^! \quad \text{mit Basis} \quad \mathrm{Obst}^{-1} = \{\, 1/\mathrm{Apfel}, 1/\mathrm{Birne}, \dots \,\}$$

🙂 Die Auswertung $B : V^* \times V \to R : (a, x) \mapsto a \cdot x$ ist bilinear über R.

Beispiel: Äpfel und Birnen

R110
Erläuterung

Diese Illustration klingt etwas albern, ist aber sprechend und nützlich. Dasselbe Phänomen finden Sie in der Physik, dort seriös ausgeführt.

Wir betrachten hierbei die Basiselemente $\mathrm{Apfel}, \mathrm{Birne}, \mathrm{Citrone}, \dots$ als physikalische Einheiten und führen sie daher in der Notation explizit mit.

Für den Covektor sind die physikalischen Einheiten dann die Kehrwerte $1/\mathrm{Apfel}, 1/\mathrm{Birne}, 1/\mathrm{Citrone}, \dots$. Das ist sehr natürlich und anschaulich.

Dies betont den Unterschied zwischen den beiden Räumen V und V^*: Sie messen verschiedene Dinge und sie verhalten sich verschieden.

Auf V haben wir kein sinnvolles Skalarprodukt. Stattdessen haben wir jedoch die Auswertung $B : V^* \times V \to R$ von Covektoren auf Vektoren.

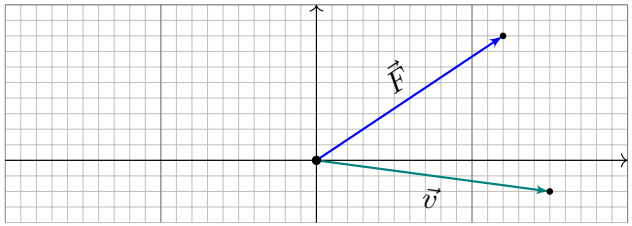
Diese Sichtweise ist zunächst nicht ganz so anschaulich und vertraut, doch sie ist eine universelle Konstruktion und bietet viele Vorteile:

Anders als Skalarprodukte benötigen wir hier keine zusätzliche Struktur: Zu jedem linearen Raum V haben wir den zugehörigen Dualraum V^* und die Auswertung B. Diese wollen wir nun nutzen lernen!

Beispiel: Leistung gleich Kraft mal Geschwindigkeit

R111

Aus der Schulphysik kennen wir die anschaulichen Merkregeln „Arbeit = Kraft mal Weg“ und „Leistung = Arbeit durch Zeit“.



Daraus folgt „Leistung = Kraft mal Geschwindigkeit“. Ausgeschrieben:

$$\Delta W = \vec{F} \bullet \Delta\vec{s}, \qquad \vec{v} = \frac{\Delta\vec{s}}{\Delta t}, \qquad P = \frac{\Delta W}{\Delta t} = \vec{F} \bullet \vec{v}$$

Letzteres sieht aus wie ein Skalarprodukt, ist aber eine Auswertung!

$$B \,:\, V^* \times V \to \mathbb{R} \,:\, (\vec{F}, \vec{v}) \mapsto \vec{F} \bullet \vec{v}$$

Hier ist $\vec{v} \in V = \mathbb{R}^{3\times1}$ ein Vektor und $\vec{F} \in V^* \cong \mathbb{R}^{1\times3}$ ein Covektor.

Beispiel: Leistung gleich Kraft mal Geschwindigkeit

R112
Erläuterung

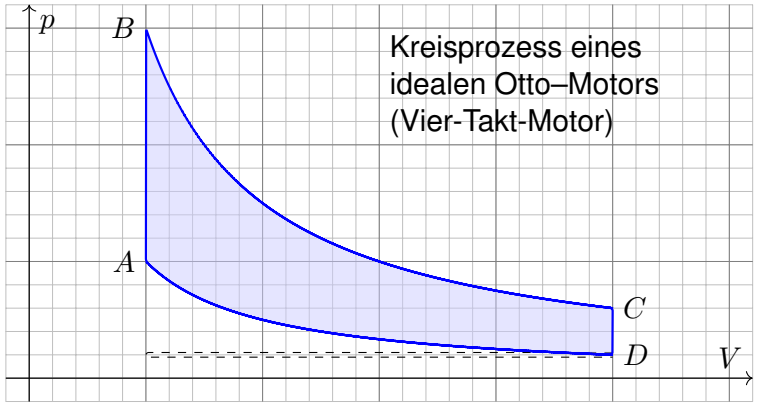
Wie im vorigen Beispiel sollten wir nicht Äpfel mit Birnen vergleichen! Die Verschiebung $\Delta\vec{s}$ und Geschwindigkeit $\vec{v} = \Delta\vec{s}/\Delta t$ sind Vektoren, die Kraft $\vec{F}$ wirkt hierauf als Covektor. Die Auswertung ergibt dann die Arbeit $\Delta W = \vec{F} \bullet \Delta\vec{s}$ bzw. die Leistung $P = \Delta W/\Delta t = \vec{F} \bullet \vec{v}$.

Auch hier sind die physikalischen Einheiten hilfreich zum Verständnis: Unsere beiden physikalischen Größen *Geschwindigkeit* $\vec{v}$ und *Kraft* $\vec{F}$ haben verschiedene „Dimensionen“ (ein sehr unglücklicher Name!), das heißt: verschiedene Maßeinheiten. Wir messen Geschwindigkeit in $1\,\mathrm{m/s}$ und Kraft in $1\,\mathrm{N} = 1\,\mathrm{kg\,m/s^2}$. Demnach liegen $\vec{v}$ und $\vec{F}$ nicht im selben Vektorraum: Wir können sie nicht einmal sinnvoll addieren! Die Auswertung $\vec{F} \bullet \vec{s}$ kann demnach kein Skalarprodukt sein.

Hingegen können wir wunderbar $\vec{F}$ auf $\vec{s}$ auswerten, und umgekehrt: Die zugehörigen Vektorräume V^* und V sind dual zueinander.

(Natürlich haben wir für Geschwindigkeitsvektoren ein Skalarprodukt. Dies nutzen wir insbesondere in der Formel für die kinetische Energie $E_\mathrm{kin} = \frac{1}{2} m \vec{v}^{\,2}$, wobei $\vec{v}^{\,2} = \langle\, \vec{v} \mid \vec{v} \,\rangle$ eine skalare Größe ergibt.)

Beispiel: Prozessgrößen in der Thermodynamik



In der Thermodynamik (etwa für ideale Gase) gibt es **Zustandsgrößen** wie den Druck p und das Volumen V: Diese beschreiben den Zustand $\gamma(t) = (p(t), V(t), \dots)$ des Systems in einem Zustandsraum $\Omega \subseteq \mathbb{R}^n$.

Daneben gibt es **Prozessgrößen** wie die geleistete Arbeit $\mathrm{d}W = p\,\mathrm{d}V$. Diese hängen ab von der Zustandsänderung, also $\partial_t\gamma = (\partial_t p, \partial_t V, \dots)$. Die Auswertung ergibt $\partial_t W = \mathrm{d}W(\partial_t\gamma) = p\,\partial_t V$ und $\Delta W = \int_\gamma \mathrm{d}W$.

Beispiel: Thermodynamik

Der hier skizzierte Kreisprozess eines **Otto–Motors** verläuft wie folgt. Verdichten: Der Kolben komprimiert Kraftstoff-Luft-Gemisch von D bis A. Arbeitstakt: Bei A wird das Gas gezündet, der Druck steigt schlagartig bis B an, dadurch dehnt sich der Kolben bis C aus und verrichtet Arbeit. Zwei weitere Takte: Ausstoß des Abgases, Ansaugen des Gemisches.

Der **Wirkungsgrad** des Motors ist die geleistete Arbeit dividiert durch die eingesetzte Verbrennungsenergie, also den Treibstoffverbrauch. Die oben skizzierte Formel liefert den zu maximierenden Wert ΔW. Solche praktischen Fragen der Optimierung von Maschinen und Motoren waren im 19. Jahrhundert der Ausgangspunkt.

Heute ist die **Thermodynamik** eine fundamentale Wissenschaft und hat überaus wichtige technische Anwendungen: Sie dient zum Verständnis von Kraftmaschinen (wie Motoren, Turbinen, etc.) und Arbeitsmaschinen (Pumpen, Verdichter) sowie in der Klimatechnik (Heizungen, Kühlung). Daran erahnen wir bereits, dass sie einerseits fundamental wichtig ist, andererseits mathematisch-konzeptuell erstaunlich anspruchsvoll.

Beispiel: Thermodynamik

Den Zustand $\gamma(t)$ des Systems zur Zeit $t \in [t_0, t_1]$ beschreiben wir dabei durch den Druck $p(t)$, das Volumen $V(t)$ und evtl. weitere Größen. Das entspricht einem Punkt $x = \gamma(t)$ im Zustandsraum $\Omega \subseteq \mathbb{R}^n$.

Eine **Zustandsfunktion** hängt nur vom Zustand des Systems ab, nicht jedoch von der Historie, also dem durchlaufenen Weg: Zum Beispiel ist die Wärmeenergie eines idealen Gases gleich $U = fpV = f\nu RT$. Hier ist $U =$ Wärmemenge, $p =$ Druck, $V =$ Volumen, $\nu =$ Stoffmenge, $R =$ universelle Gaskonstante, $T =$ absolute Temperatur. Der Faktor $f = 3/2$ entspricht der mikroskopischen Struktur eines einatomigen Gases wie Helium; für zweiatomige wie Wasserstoff gilt $f \approx 5/2$.

Eine **Prozessfunktion** hingegen hängt vom durchlaufenen Weg ab, wie etwa die geleistete Arbeit $\Delta W = \int_\gamma \mathrm{d}W$ in der obigen Formel. Den Verlauf des Prozesses beschreiben wir als Weg $\gamma : [t_0, t_1] \to \Omega$ im Zustandsraum. Der momentane Zustand ist $x = \gamma(t)$ und die Ableitung $\dot{x} = \partial_t\gamma(t)$ ist die momentane Änderungsgeschwindigkeit. Bei einem Kreisprozess gilt $\gamma(t_0) = \gamma(t_1)$ und dennoch $\Delta W \neq 0$!

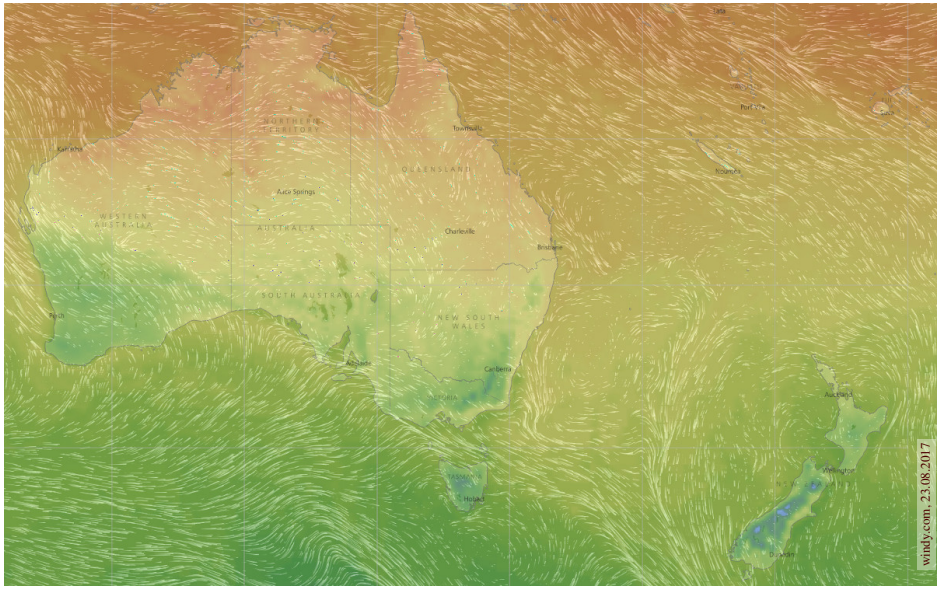
Beispiel: Thermodynamik

Angeheftet in jedem Punkt $x = (p, V, \dots)$ des Zustandsraumes $\Omega \subseteq \mathbb{R}^n$ ist der Tangentialraum $T_x\Omega \cong \mathbb{R}^n$ der Änderungsgeschwindigkeiten. Hierauf ist $\mathrm{d}W = p\,\mathrm{d}V : T_x\Omega \to \mathbb{R}$ eine Linearform, also $\mathrm{d}W \in T_x^*\Omega$. Wie hier zu sehen, hängt $(\mathrm{d}W)_x$ vom Punkt $x \in \Omega$ ab, zudem glatt. Daher sprechen wir genauer von einer **Differentialform**.

Prof. Hermann Karcher (Universität Bonn) erklärte die Situation sehr treffend in seiner Notiz *Differentialformen für die Thermodynamik*:

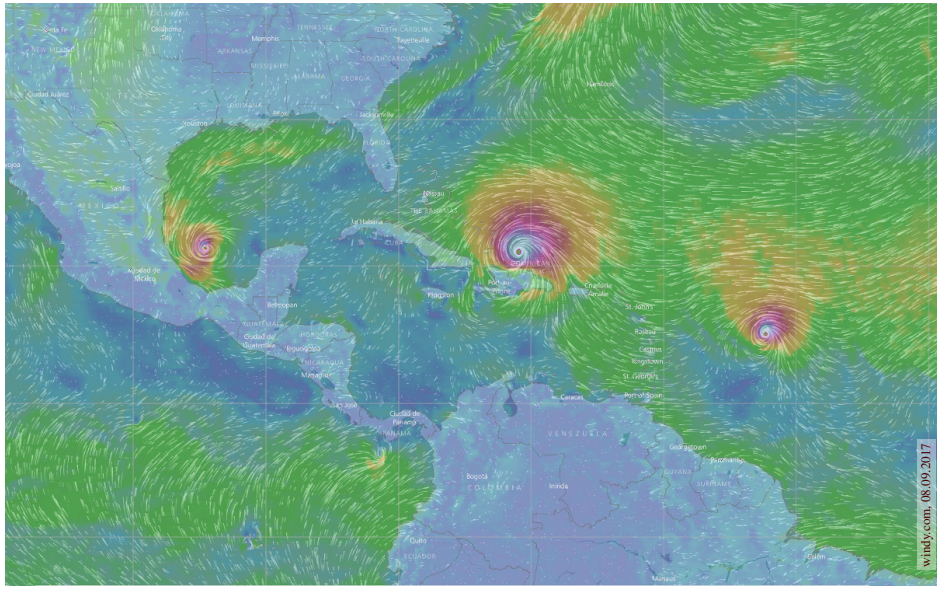
> *Die Vektoranalysis lebt davon, dass wir den Raum $\mathbb{R}^3$ nicht bloß als Vektorraum, sondern als euklidischen Raum, mit einem Skalarprodukt, betrachten und nutzen können. In der Thermodynamik gibt es jedoch kein Skalarprodukt, das eine physikalische Bedeutung hätte. Deshalb können Kurvenintegrale nicht Integranden haben, die Skalarprodukt aus einem Vektorfeld mit dem Tangentialvektor der Kurve sind. Wir müssen daher lernen, die Ableitung von Funktionen und deren Anwendung auf Tangentialvektoren von Kurven ohne ein bequemes Skalarprodukt zu beschreiben. Genau hierzu dienen Differentialformen.*

Skalarfelder und Vektorfelder



Skalarfeld $g : \mathbb{R}^2 \supset \Omega \to \mathbb{R} : (x, y) \mapsto g(x, y)$, z.B. Temperatur, Luftdruck.
Vektorfeld $f : \mathbb{R}^2 \supset \Omega \to \mathbb{R}^2 : (x, y) \mapsto (f_1(x, y), f_2(x, y))$, z.B. Wind, etc.

Skalarfelder und Vektorfelder



Vektorfelder treten in vielen naturwissenschaftlichen Modellen auf.
Hierbei gelten gewisse Gesetze, die wir verstehen und nutzen wollen.

Skalarfelder, Ableitung als Linearform

Wir betrachten zunächst ein ebenes **Skalarfeld**

$$g \;:\; \mathbb{R}^2 \supset \Omega \to \mathbb{R} \;:\; (x, y) \mapsto g(x, y).$$

Jedem Punkt $(x, y) \in \Omega$ wird eine Zahl $g(x, y) \in \mathbb{R}$ zugeordnet.
Wir können die Funktion g als eine Fläche über Ω veranschaulichen:
Der Wert $z = g(x, y)$ ist dann die Höhe über dem Punkt (x, y).

Wir nehmen an, dass g stetig partiell differenzierbar ist, kurz $\mathscr{C}^1$.
Die Ableitung $\partial_1 g(x, y) = \frac{\partial g}{\partial x}(x, y)$ ist die Steigung in x–Richtung.
Die Ableitung $\partial_2 g(x, y) = \frac{\partial g}{\partial y}(x, y)$ ist die Steigung in y–Richtung.
Dies definiert zwei neue Funktionen $\partial_1 g, \partial_2 g : \Omega \to \mathbb{R}$. Die **Ableitung**

$$g' = (\partial_1 g, \partial_2 g) \;:\; \Omega \to \mathbb{R}^2 \;:\; (x, y) \mapsto (\partial_1 g(x, y), \partial_2 g(x, y))$$

weist in Richtung des steilsten Anstiegs der Funktion g im Punkt (x, y).
Dies entspricht dem linearen Term der **Taylor–Entwicklung**

$$g(x + a) = g(x) + \textstyle\sum_{i=1}^{n} \partial_i g(x)\, a_i + \ldots$$

🙂 Die Ableitung g' in x ist eine Linearform: Ausgewertet auf einem Tangentialvektor $a \in T_x\Omega$ ergibt sie einen Skalar, den linearen Zuwachs.

Vektorfelder, Jacobi–Matrix, Divergenz, Rotation

Wir betrachten nun ein ebenes **Vektorfeld**

$$f \;:\; \mathbb{R}^2 \supset \Omega \to \mathbb{R}^2 \;:\; (x, y) \mapsto f(x, y) = (f_1(x, y), f_2(x, y)).$$

Jedem Punkt $(x, y) \in \Omega$ wird ein Vektor $f(x, y) \in \mathbb{R}^2$ zugeordnet, mit Komponenten $f_1(x, y) \in \mathbb{R}$ und $f_2(x, y) \in \mathbb{R}$. Seine **Jacobi–Matrix** ist

$$f' = \frac{\partial(f_1, f_2)}{\partial(x, y)} = \begin{pmatrix} \partial f_1/\partial x & \partial f_1/\partial y \\ \partial f_2/\partial x & \partial f_2/\partial y \end{pmatrix} = \begin{pmatrix} \partial_1 f_1 & \partial_2 f_1 \\ \partial_1 f_2 & \partial_2 f_2 \end{pmatrix}.$$

Wir definieren die **Quelldichte** oder **Divergenz** $\operatorname{div} f : \Omega \to \mathbb{R}$ durch

$$\operatorname{div} f := \partial_1 f_1 + \partial_2 f_2 = \frac{\partial f_1}{\partial x} + \frac{\partial f_2}{\partial y}.$$

Wir definieren die **Wirbeldichte** oder **Rotation** $\operatorname{rot} f : \Omega \to \mathbb{R}$ durch

$$\operatorname{rot} f := \partial_1 f_2 - \partial_2 f_1 = \frac{\partial f_2}{\partial x} - \frac{\partial f_1}{\partial y}.$$

🙂 Ausgewertet in einem Punkt $(x, y) \in \Omega$ sind dies Linearformen!

Duale Familien in V^* und V

Definition R1D: duale Familien

Vorgelegt sei eine Familie $(v_i)_{i\in I}$ im (rechts)linearen Raum V über R und eine Familie $(\varphi_i)_{i\in I}$ im (links)linearen Dualraum $V^* = \mathrm{Hom}_R(V,R)$.

Wir nennen diese Familien $(\varphi_i)_{i\in I}$ und $(v_i)_{i\in I}$ **dual** zueinander, falls gilt:

$$\varphi_i(v_j) = \delta_{i,j} := \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Daraus folgt sofort: (1) Die Familie $(v_i)_{i\in I}$ ist linear unabhängig in V, und (2) die Familie $(\varphi_i)_{i\in I}$ ist linear unabhängig im Dualraum V^*.

☺ Duale Familien bezeugen gegenseitig ihre lineare Unabhängigkeit.

Beweis: (1a) Aus $v = \sum_{j\in I} v_j\mu_j$ folgt $\varphi_i(v) \overset{\text{lin}}{=} \sum_{j\in I} \varphi_i(v_j)\mu_j \overset{\text{dual}}{=} \mu_i$.
(1b) Gilt speziell $v = 0$, so folgt $0 \overset{\text{lin}}{=} \varphi_i(v) \overset{(1a)}{=} \mu_i$ für alle $i \in I$.

(2a) Aus $\varphi = \sum_{i\in I} \lambda_i\varphi_i$ folgt $\varphi(v_j) \overset{\text{lin}}{=} \sum_{i\in I} \lambda_i\varphi_i(v_j) \overset{\text{dual}}{=} \lambda_j$.
(2b) Gilt speziell $\varphi = 0$, so folgt $0 \overset{\text{lin}}{=} \varphi(v_j) \overset{(2a)}{=} \lambda_j$ für alle $j \in I$.

Beispiel: Monome und Ableitungen

Aufgabe: Sei $\Omega =]-\varepsilon,\varepsilon[\subset \mathbb{R}$ ein reelles Intervall vom Radius $\varepsilon > 0$. Im $\mathbb{R}$–Vektorraum $V = \mathscr{C}^\infty(\Omega,\mathbb{R})$ betrachten wir die Monomfunktion

$$f_k : \Omega \to \mathbb{R} : x \mapsto x^k$$

mit Exponent $k \in \mathbb{N}$. Linearkombination ergibt $f(x) = \sum_{k\in\mathbb{N}} a_k x^k$. Ist $(f_k)_{k\in\mathbb{N}}$ linear unabhängig? Finden Sie eine duale Familie!

Lösung: Die Ableitung definiert zu jedem $k \in \mathbb{N}$ die Linearform

$$\varphi_k : f \mapsto \frac{1}{k!}\frac{\mathrm{d}^k f}{\mathrm{d}x^k}(0).$$

Somit ist $\varphi_k : V \to \mathbb{R}$ ein Element des Dualraums $V^* = \mathrm{Hom}_{\mathbb{R}}(V,\mathbb{R})$. Für alle Indizes $k,\ell \in \mathbb{N}$ gilt nach Konstruktion (und kurzer Rechnung)

$$\varphi_k(f_\ell) = \delta_{k,\ell} := \begin{cases} 1 & \text{falls } k = \ell, \\ 0 & \text{falls } k \neq \ell. \end{cases}$$

Daraus folgt sofort: Die Familie $(f_k)_{k\in\mathbb{N}}$ ist linear unabhängig in V, und die duale Familie $(\varphi_k)_{k\in\mathbb{N}}$ ist linear unabhängig im Dualraum V^*.

Beispiel: Monome und Ableitungen im $\mathbb{R}^n$

Beispiel R1E: Monome und Ableitungen im $\mathbb{R}^n$

Im euklidischen Raum $\mathbb{R}^n$ betrachten wir um 0 einen offenen Ball $\Omega = B(0,\varepsilon) := \{\, x \in \mathbb{R}^n \mid \|x\| < \varepsilon \,\}$ mit beliebig kleinem Radius $\varepsilon > 0$.

(1) Im $\mathbb{R}$–Vektorraum $V = \mathscr{C}^\infty(\Omega,\mathbb{R})$ betrachten wir die Monomfunktion

$$f_k : \Omega \to \mathbb{R} : x = (x_1,\dots,x_n) \mapsto x^k = x_1^{k_1}\cdots x_n^{k_n}$$

zum Multiindex $k = (k_1,\dots,k_n) \in \mathbb{N}^n$. Linearkombination ergibt die n–dimensionale Polynomfunktion $f(x) = \sum_{k\in\mathbb{N}^n} a_k x^k$ mit $a \in \mathbb{R}^{(\mathbb{N}^n)}$.

(2) Dual hierzu betrachten wir die Linearform $\varphi_k \in V^*$ gegeben durch

$$\varphi_k : V \to \mathbb{R} : f \mapsto \frac{(\partial^k f)(0)}{k!} \quad \text{mit } \partial^k = \partial_1^{k_1}\cdots\partial_n^{k_n} \text{ und } k! = k_1!\cdots k_n!$$

Für alle Multiindizes $k,\ell \in \mathbb{N}^n$ gilt nach Konstruktion $\varphi_k(f_\ell) = \delta_{k,\ell}$.

(3) Daraus folgt sofort: Die Familie $(f_k)_{k\in\mathbb{N}^n}$ ist linear unabhängig in V, und die duale Familie $(\varphi_k)_{k\in\mathbb{N}^n}$ ist linear unabhängig im Dualraum V^*.

Beispiel: Monome und Ableitungen im $\mathbb{R}^n$

Bemerkung: Beachten Sie die Wahl der Konstanten:
Dual zu $(f_k : x \mapsto x^k)_{k\in\mathbb{N}^n}$ ist wie oben $(\varphi_k : f \mapsto (\partial^k f)(0)/k!)_{k\in\mathbb{N}}$.
Dual zu $(g_k : x \mapsto x^k/k!)_{k\in\mathbb{N}^n}$ ist entsprechend $(\psi_k : f \mapsto (\partial^k f)(0))_{k\in\mathbb{N}}$.

Diese einfache Beobachtung ist der Ausgangspunkt eines wichtigen Kapitels der Analysis: die Theorie der Taylor–Polynome und –Reihen.

Zur Funktion $f \in \mathscr{C}^m(\Omega,\mathbb{R})$ um den Punkt 0 gehört das Taylor–Polynom

$$(T_m^0 f)(x) = \textstyle\sum_{|k|\leq m} c_k x^k \quad \text{mit Koeffizienten} \quad c_k = (\partial^k f)(0)/k!.$$

Dies ist das Polynom vom Grad $\leq m$ mit denselben Ableitungen wie f im Punkt 0. Entsprechendes gilt verschoben um jeden Punkt $a \in \mathbb{R}^n$. Für $m = 1$ beschreibt dies die Tangentialebene (affin-linear), für $m = 2$ die Schmiegequadrik (als quadratisches Polynom). Dies nutzt man zur Untersuchung kritischer Stellen, insbesondere Minima und Maxima.

Das Restglied $(\varepsilon_m^0 f)(x) = f(x) - (T_m^0 f)(x)$ gibt Auskunft über den Fehler im Punkt $x \in \Omega$. In günstigen Fällen gilt Konvergenz $|\varepsilon_m^0 f| \to 0$ für $m \to \infty$, und wir erhalten so die Darstellung von f als Taylor–Reihe.

Beispiel: Wirtinger–Ableitungen auf $\mathbb{C} = \mathbb{R}^2$

Beispiel R1F: Wirtinger Ableitungen

In der Zahlenebene $\mathbb{C} = \mathbb{R}^2$ betrachten wir $x, y \in \mathbb{R}$ als reelle Variablen, hieraus bilden wir die komplexen Variablen $z = x + \mathrm{i}y$ und $\overline{z} = x - \mathrm{i}y$. Genauer gesagt betrachten wir die Polynomringe $\mathbb{C}[x, y] \supseteq \mathbb{C}[z, \overline{z}]$.

(0) Wir definieren die **Wirtinger–Ableitungen** nach z und $\overline{z}$ durch

$$\partial_z := \tfrac{1}{2}\big(\partial_x - \mathrm{i}\partial_y\big) \quad \text{und} \quad \partial_{\overline{z}} := \tfrac{1}{2}\big(\partial_x + \mathrm{i}\partial_y\big).$$

(1) Folgende Regeln rechnet man durch Einsetzen direkt nach:

$$\partial_z(z) = 1, \quad \partial_z(\overline{z}) = 0, \quad \partial_{\overline{z}}(z) = 0, \quad \partial_{\overline{z}}(\overline{z}) = 1.$$

(2) Die vertrauten Ableitungen ∂_x, ∂_y sind linear und erfüllen Produkt- und Kettenregel; dasselbe gilt daher auch für $\partial_z, \partial_{\overline{z}}$.

(3) Für alle $n \in \mathbb{Z}$ gilt $\partial_z(z^n) = nz^{n-1}$ und $\partial_{\overline{z}}(z^n) = 0$ sowie entsprechend $\partial_{\overline{z}}(\overline{z}^n) = n\overline{z}^{n-1}$ und $\partial_z(\overline{z}^n) = 0$.

Aufgabe: Rechnen Sie die hier gemachten Behauptungen nach.

Beispiel: Wirtinger–Ableitungen auf $\mathbb{C} = \mathbb{R}^2$

Aufgabe: In der Ebene $\mathbb{R}^2$ betrachten wir um 0 einen offenen Ball $\Omega = B(0, \varepsilon) := \{\, z \in \mathbb{C} \mid |z| < \varepsilon \,\}$ mit beliebig kleinem Radius $\varepsilon > 0$. Im $\mathbb{C}$–Vektorraum $V = \mathscr{C}^\infty(\Omega, \mathbb{C})$ betrachten wir die Monomfunktion

$$f_{a,b} : \Omega \to \mathbb{C} : (x, y) \mapsto z^a \overline{z}^b$$

mit Exponenten $a, b \in \mathbb{N}$. Linearkombination ergibt die Polynome $f(x, y) = \sum_{a,b\in\mathbb{N}} c_{a,b}\, z^a \overline{z}^b$ mit komplexen Koeffizienten $c \in \mathbb{C}^{(\mathbb{N}^2)}$. Ist $(f_{a,b})_{(a,b)\in\mathbb{N}^2}$ linear unabhängig? Finden Sie eine duale Familie!

Lösung: Zu jedem Paar $(k, \ell) \in \mathbb{N}^2$ haben wir die Ableitungen

$$\varphi_{k,\ell} : f \mapsto \frac{1}{k!\ell!}(\partial_z^k \partial_{\overline{z}}^\ell f)(0)$$

Für alle Indizes $(k, \ell), (a, b) \in \mathbb{N}^2$ gilt nach Konstruktion

$$\varphi_{k,\ell}(f_{a,b}) = \begin{cases} 1 & \text{falls } (k, \ell) = (a, b), \\ 0 & \text{falls } (k, \ell) \neq (a, b). \end{cases}$$

Daraus folgt sofort: Die Familie $(f_{a,b})_{(a,b)\in\mathbb{N}^2}$ ist linear unabhängig in V, und die duale Familie $(\varphi_{k,\ell})_{(k,\ell)\in\mathbb{N}^2}$ ist linear unabhängig im Dualraum.

Beispiel: Laurent–Polynome und Cauchy–Wegintegral

Beispiel R1G: Laurent–Polynome und Cauchy–Wegintegral

In $\mathbb{C}$ betrachten wir $\Omega := B(0, \varepsilon) \smallsetminus \{0\} = \{\, z \in \mathbb{C} \mid 0 < |z| < \varepsilon \,\}$ mit Radius $\varepsilon > 0$. Im $\mathbb{C}$–Vektorraum $V = \mathscr{C}(\Omega, \mathbb{C})$ liegt die Monomfunktion

$$f_k : \Omega \to \mathbb{C} : z \mapsto z^k$$

mit Exponent $k \in \mathbb{Z}$. Zum Radius $0 < r < \varepsilon$ betrachten wir den Weg $\gamma : [0, 2\pi] \to \Omega : t \mapsto r\,\mathrm{e}^{\mathrm{i}t}$ und das zugehörige Cauchy–Wegintegral

$$\varphi : V \to \mathbb{C} : f \mapsto \frac{1}{2\pi\mathrm{i}} \oint_\gamma f(z)\,\mathrm{d}z := \frac{1}{2\pi\mathrm{i}} \int_{t=0}^{2\pi} f(\gamma(t))\gamma'(t)\,\mathrm{d}t.$$

Dies ist eine Linearform auf V. Die Auswertung von φ auf f_k ergibt

$$\varphi(f_k) = \frac{1}{2\pi\mathrm{i}} \int_{t=0}^{2\pi} r^k\,\mathrm{e}^{\mathrm{i}kt}\, r\mathrm{i}\,\mathrm{e}^{\mathrm{i}t}\,\mathrm{d}t = \frac{r^{k+1}}{2\pi} \int_{t=0}^{2\pi} \mathrm{e}^{\mathrm{i}(k+1)t}\,\mathrm{d}t = \begin{cases} 1 & \text{für } k = -1, \\ 0 & \text{für } k \neq -1. \end{cases}$$

Linearkombination ergibt das Laurent–Polynom $f(z) = \sum_{k\in\mathbb{Z}} c_k z^k$ mit $c \in \mathbb{C}^{(\mathbb{Z})}$. Die Koeffizienten rekonstruieren wir dank $c_k = \varphi(f(z)/z^{k+1})$.

Beispiel: Laurent–Polynome und Cauchy–Wegintegral

Der Weg $\gamma(t) = r\,\mathrm{e}^{\mathrm{i}t}$ durchläuft den Kreis vom Radius r um den Punkt 0. Der Geschwindigkeitsvektor $\gamma'(t) = r\mathrm{i}\,\mathrm{e}^{\mathrm{i}t}$ ist der um $\pi/2 \mathrel{\hat{=}} 90°$ nach links gedrehte Ortsvektor, also mit i multipliziert. Das Wegintegral $\oint_\gamma f(z)\,\mathrm{d}z$ durchläuft $z = \gamma(t)$ für $t \in [0, 2\pi]$, daher substituieren wir $\mathrm{d}z = \gamma'(t)\,\mathrm{d}t$.

Das erklärt die Definition des Wegintegral entlang γ wie oben gezeigt:

$$\oint_\gamma f(z)\,\mathrm{d}z := \int_{t=0}^{2\pi} f(\gamma(t))\gamma'(t)\,\mathrm{d}t.$$

Bemerkenswerterweise ist das Integral unabhängig vom Radius r: Das Ergebnis der Auswertung ist $\varphi(f_k) = 1$ für $k = -1$ und $= 0$ sonst. Das liegt daran, dass $f(z) = z^k$ die Stammfunktion $F(z) = z^{k+1}/(k+1)$ hat, außer für $k = -1$. Die Funktion $z \mapsto 1/z$ ist überaus interessant!

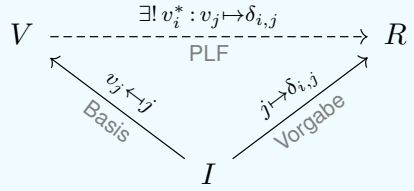
🙂 Dies ist der Ausgangspunkt einer sensationell schönen Theorie: Die komplexe Analysis untersucht komplex-differenzierbare Funktionen $f : \mathbb{C} \supseteq \Omega \to \mathbb{C}$. Hier ist das Cauchy–Wegintegral die Grundlage für die Darstellung durch Laurent–Reihen und Cauchys Residuensatz.

Die duale Familie $\mathcal{B}^*$ einer Basis $\mathcal{B}$

Satz R1H: die duale Familie $\mathcal{B}^* = (v_i^*)_{i\in I}$ einer Basis $\mathcal{B} = (v_i)_{i\in I}$

Sei V ein linearer Raum über R. (1) Zu jeder Basis $\mathcal{B} = (v_i)_{i\in I}$ von V existiert genau eine duale Familie $\mathcal{B}^* = (v_i^*)_{i\in I}$ in $V^* = \mathrm{Hom}_R(V, R)$.

Genauer: Dank dem Prinzip der linearen Fortsetzung (K1B) existiert zu jedem Index $i \in I$ genau eine lineare Abbildung $v_i^* : V \to R : v_j \mapsto \delta_{i,j}$.



(2) Ist I zudem endlich, so ist $\mathcal{B}^* = (v_i^*)_{i\in I}$ eine Basis von V^*.
Wir nennen dies kurzerhand die duale Basis zur Basis $\mathcal{B} = (v_i)_{i\in I}$.

(3) Ist I jedoch unendlich, so ist $\mathcal{B}^* = (v_i^*)_{i\in I}$ keine Basis von V^*.
Die Familie $(v_i^*)_{i\in I}$ in V^* ist linear unabhängig, aber nicht erzeugend.

Die duale Familie einer Basis

Beweis: (1) Existenz und Eindeutigkeit verdanken wir Satz K1B (PLF).
Die duale Familie $(v_i^*)_{i\in I}$ in V^* ist ebenfalls linear unabhängig (R1D).
Sie erzeugt den Dualraum V^* genau dann, wenn I endlich ist:

(2) Sei I endlich. Vorgelegt sei eine Linearform $\varphi : V \to R$.
Wir vergleichen φ mit der Linearkombination $\psi = \sum_{i\in I} \varphi(v_i) v_i^*$.
Für $j \in J$ gilt $\psi(v_j) \overset{\text{lin}}{=} \sum_{i\in I} \varphi(v_i) v_i^*(v_j) \overset{\text{dual}}{=} \varphi(v_j)$, also $\psi = \varphi$. (K1A)

(3) Die Abbildung $\varphi : V \to R : v \mapsto \sum_{i\in I} v_i^*(v)$ ist wohldefiniert und linear, also $\varphi \in V^*$: Sie ordnet jeder Linearkombination $v = \sum_{j\in I} v_j \mu_j$ mit $\mu \in R^{(I)}$ die (endliche!) Summe $\varphi(v) = \sum_{i\in I} \mu_i$ in R zu.

Angenommen, φ lässt sich als eine (endliche!) Linearkombination $\varphi = \sum_{i\in I} \lambda_i v_i^*$ mit $\lambda \in R^{(I)}$ darstellen. Dann folgt $\lambda_j = \varphi(v_j) = 1$ für jeden Index $j \in I$, und somit ist I endlich. QED

Beispiel: Der Teilraum $\mathrm{Poly}(\Omega, \mathbb{R}) \leq \mathscr{C}^\infty(\Omega, \mathbb{R})$ hat die Basis $(x^k)_{k\in\mathbb{N}^n}$.
Die duale Familie ist $(f_k^* : f \mapsto \partial^k f(0)/k!)_{k\in\mathbb{N}^n}$ in $\mathrm{Poly}(\Omega, \mathbb{R})^*$ (R1E).
Hier liegt $\varphi : \mathrm{Poly}(\Omega, \mathbb{R}) : f \mapsto f(1)$ nicht im Aufspann $\langle\, f_k^* \mid k \in \mathbb{N}^n \,\rangle_{\mathbb{R}}^!$.
Dasselbe gilt für die Auswertung $f \mapsto f(a)$ in jedem Punkt $a \neq 0$.

Beispiel: duale Familie einer Basis

Beispiel / Aufgabe: Im Vektorraum $V = \mathbb{R}^{2\times 1}$ über $\mathbb{R}$ vergleichen wir die beiden Basen $\mathcal{A} = (a_1, a_2)$ und $\mathcal{B} = (b_1, b_2)$ mit

$$a_1 = \begin{bmatrix}1\\0\end{bmatrix}, a_2 = \begin{bmatrix}0\\1\end{bmatrix} \quad \text{und} \quad b_1 = \begin{bmatrix}1\\0\end{bmatrix}, b_2 = \begin{bmatrix}1\\1\end{bmatrix}.$$

Bestimmen Sie die hierzu dualen Basen des Dualraums $V^* \cong \mathbb{R}^{1\times 2}$.

Lösung: Nach Definition der dualen Familie finden wir

$$a_1^* = \begin{bmatrix}1 & 0\end{bmatrix}, \; a_2^* = \begin{bmatrix}0 & 1\end{bmatrix} \quad \text{und} \quad b_1^* = \begin{bmatrix}1 & -1\end{bmatrix}, \; b_2^* = \begin{bmatrix}0 & 1\end{bmatrix}.$$

⚠ Beachten Sie die Tücke der Notation: Es gilt $a_1 = b_1$, doch $a_1^* \neq b_1^*$.

Merke: Die Konstruktion der Linearform $v_i^* : V \to R : v_j \mapsto \delta_{i,j}$
hängt nicht nur von v_i ab, sondern von der gesamten Basis $(v_i)_{i\in I}$.

Bemerkung: Zu der linear unabhängigen Familie $(a_1) = (b_1)$ in V existieren mehrere duale Familien in V^*, etwa $(a_1^*) \neq (b_1^*)$.
Zur Eindeutigkeit in Satz R1H benötigen wir eine Basis!

Beispiel: duale Familie einer Basis

Aufgabe: Sei $(a_1, \ldots, a_n)$ eine Basis im Spaltenraum $V = R^{n\times 1}$.
Wie berechnen Sie die duale Basis im Zeilenraum $V^* \cong R^{1\times n}$?

Lösung: Wir bilden die Matrix $A \in R^{n\times n}$ mit Spalten $a_1, \ldots, a_n$.
Gesucht ist die inverse Matrix $B \in R^{n\times n}$ mit Zeilen $b_1, \ldots, b_n$,
sodass $BA = 1_{n\times n}$ gilt, also $b_i \cdot a_j = \delta_{i,j}$ für alle Indizes i, j.

🙂 Über jedem Divisionsring R löst dies der Gauß–Algorithmus!

Aufgabe: Gegeben sei eine Basis $(v_i)_{i\in I}$ von V.
Wie berechnen Sie $v_i^*(v)$ für einen beliebigen Vektor $v \in V$?

Lösung: Jeder Vektor $v \in V$ schreibt sich eindeutig als Linearkombination $v = \sum_{j\in I} v_j \mu_j$ mit Koeffizienten $\mu \in R^{(I)}$.
Daraus folgt $v_i^*(v) \overset{\text{lin}}{=} \sum_{j\in I} v_i^*(v_j)\mu_j \overset{\text{dual}}{=} \mu_i$. Voilà!

🙂 Die Linearform v_i^* filtert den Koeffizienten μ_i heraus.

Beispiel: der Koordinatenraum $R^{(I)}$ und sein Dualraum R^I

Beispiel R1I: der Koordinatenraum $R^{(I)}$ und sein Dualraum R^I

Sei R ein Ring. Hierüber betrachten wir den rechtslinearen Raum

$$V = R^{(I)}.$$

Dann ist der Dualraum $V^* = \mathrm{Hom}_R(V, R)$ ein linkslinearer Raum, und dank PLF (K1B) haben wir den R–linearen Isomorphismus

$$V^* \cong R^I \;:\; \varphi \mapsto (\varphi(e_i))_{i\in I}$$

Zur kanonischen Basis $(e_i)_{i\in I}$ haben wir die duale Familie $(e_i^*)_{i\in I}$. Diese erzeugt V^* genau dann, wenn die Menge I endlich ist.

Speziell für $I = \{1, \dots, n\}$ finden wir erneut das Eingangsbeispiel von Spaltenvektoren $V = R^{n\times 1} \cong R^n$ und Zeilenvektoren $V^* \cong R^{1\times n} \cong R^n$.

Für $I = \mathbb{N}$ ist $V = R^{(\mathbb{N})} \cong R[X]$ der Raum aller Folgen mit endlichem Träger über R (aka Polynome). Hingegen ist $V^* \cong R^{\mathbb{N}} \cong R[[X]]$ der Raum aller Folgen über R (aka formale Potenzreihen).

Beispiel: der Koordinatenraum $R^{(I)}$ und sein Dualraum R^I

Zur Erinnerung: R^I ist der Raum aller Abbildungen $v : I \to R : i \mapsto v_i$, wobei Addition und Skalarmultiplikation punktweise erklärt sind. Darin ist $R^{(I)} = \{\, v \in R^I \mid \sharp\,\mathrm{supp}(v) < \infty \,\}$ der Unterraum aller Abbildungen $v : I \to R$ mit endlichem Träger $\mathrm{supp}(v) = \{\, i \in I \mid v_i \neq 0 \,\}$, siehe I1Q.

Ist R ein Körper oder ein Divisionsring, so hat jeder R–Vektorraum V eine Basis $(v_i)_{i\in I}$, ist also isomorph zu unserem Koordinatenraum $R^{(I)}$. Dieser einfache Koordinatenraum ist somit das zentrale Beispiel und über einem Divisionsring sogar repräsentativ für alle linearen Räume.

Jeder R–Vektorraum V sieht also aus wie ein Koordinatenraum $R^{(I)}$, und der Dualraum V^* ist demnach isomorph zu R^I. Das ist konkret. Mit diesen vertrauten Räumen haben wir durchgehend gearbeitet und schon viele gute Erfahrungen gemacht, so auch hier.

Nicht-kanonische Isomorphie zwischen V und V^*

Wie oben gesehen ist V ein rechtslinearer Raum über R und V^* ein linkslinearer Raum über R, oder umgekehrt. Im Allgemeinen kann es daher keinen Isomorphismus geben, selbst wenn beide Räume dieselbe Dimension haben. Mit etwas mehr Struktur gelingt dies jedoch:

Korollar R1J: nicht-kanonische Isomorphie zwischen V und V^*

Sei V ein rechtslinearer Raum über R mit Basis $\mathcal{B} = (v_1, \dots, v_n)$. Dann ist V^* ein linkslinearer Raum mit dualer Basis $\mathcal{B}^* = (v_1^*, \dots, v_n^*)$.

(1) Ist R kommutativ, so definiert die Basis $\mathcal{B}$ den Isomorphismus

$$(\Psi_{\mathcal{B}}, \Psi_{\mathcal{B}}^*) \;:\; V \cong V^* \;:\; \textstyle\sum_{i\in I} v_i\mu_i \rightleftarrows \sum_{i\in I} \mu_i v_i^*.$$

(2) Allgemein sei $\bar{}: R \to R : \lambda \mapsto \overline{\lambda}$ ein Anti-Automorphismus, $\overline{\lambda\mu} = \overline{\mu}\,\overline{\lambda}$ für alle $\lambda, \mu \in R$. Daraus erhalten wir den antilinearen Isomorphismus

$$(\Psi_{\mathcal{B}}, \Psi_{\mathcal{B}}^*) \;:\; V \cong V^* \;:\; \textstyle\sum_{i\in I} v_i\mu_i \rightleftarrows \sum_{i\in I} \overline{\mu_i} v_i^*.$$

Typische Beispiele sind die Konjugation auf $\mathbb{C}$ oder auf $\mathbb{H}$, ebenso auf dem Matrixring $R = K^{n\times n}$ die Transposition (und ggf. Konjugation).

Nicht-kanonische Isomorphie zwischen V und V^*

⚠ Der Isomorphismus $(\Psi_{\mathcal{B}}, \Psi_{\mathcal{B}}^*) : V \cong V^*$ ist nicht natürlich, insbesondere müssen wir links und rechts zurechtbiegen.

⚠ Der Isomorphismus $(\Psi_{\mathcal{B}}, \Psi_{\mathcal{B}}^*) : V \cong V^*$ ist nicht kanonisch, sondern hängt von der willkürlich gewählten Basis $\mathcal{B}$ ab.

⚠ Ohne Vorgabe einer Basis können wir herzlich wenig sagen.

Beispiel R1K

Wir betrachten die abelsche Gruppe $V = \mathbb{Z}/n$ mit $n \in \mathbb{N}_{\geq 2}$

(1) Als linearer Raum über dem Ring $\mathbb{Z}$ gilt $V^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) = 0$.

(2) Über dem Ring $\mathbb{Z}/n$ hingegen gilt $V^* = \mathrm{Hom}_{\mathbb{Z}/n}(\mathbb{Z}/n, \mathbb{Z}/n) \cong \mathbb{Z}/n$.

Aufgabe: Rechnen Sie dies sorgsam nach.

Skizze: (1) Jeder Gruppenhomomorphismus $\varphi : \mathbb{Z}/n \to \mathbb{Z}$ ist trivial, denn für $a = \varphi(1) \in \mathbb{Z}$ mit Ordnung n bleibt nur $a = 0$.

(2) Es gilt $\mathrm{Hom}_{\mathbb{Z}/n}(\mathbb{Z}/n, \mathbb{Z}/n) \cong \mathbb{Z}/n : \varphi \mapsto \varphi(1)$. Ausführlicher gesagt: Jede Gruppenhomomorphismus $\varphi : \mathbb{Z}/n \to \mathbb{Z}/n$ ist von der Form $\varphi : x \mapsto ax$ mit $a = \varphi(1)$. Diese Zuordnung ist ein Ringisomorphismus.

Der natürliche Homomorphismus von V zum Bidual V^{**}

Satz R1L: der natürliche Homomorphismus von V zum Bidual V^{**}

Sei V ein rechtslinearer Raum über dem Ring R.
Der Dualraum $V^* = \mathrm{Hom}_R(V,R)$ ist ein linkslinearer Raum.
Der Bidualraum $V^{**} = (V^*)^* = \mathrm{Hom}_R(V^*,R)$ ist wieder rechtslinear.

(0) Wir haben die natürliche Abbildung

$$\iota : V \to V^{**} : v \mapsto \iota(v) \quad \text{mit} \quad \iota(v)(\varphi) = \varphi(v).$$

(1) Diese Abbildung ι ist rechtslinear, $\iota \in \mathrm{Hom}_R(V, V^{**})$.

(2) Hat V eine Basis $(v_i)_{i\in I}$, so ist ι injektiv, $\iota : V \hookrightarrow V^{**}$.

(3) Hat V eine endliche Basis $(v_i)_{i\in I}$, so ist ι bijektiv, $\iota : V \xrightarrow{\sim} V^{**}$.

Beispiel: Für $V = R^{n\times 1}$ über R gilt $V^* \cong R^{1\times n}$ und dann $V^{**} \cong R^{n\times 1}$.
In dieser Darstellung ist der natürliche Isomorphismus ι die Identität.

Aufgabe: Weisen Sie die Aussagen des Satzes sorgsam nach!
Alle Daten liegen explizit vor. Es genügt gewissenhaftes Nachrechnen.

Der natürliche Homomorphismus von V zum Bidual V^{**}

Lösung: (0) Als erstes müssen wir die Definition von ι verstehen!

$$\iota : V \to V^{**} : v \mapsto \iota(v) \quad \text{mit} \quad \iota(v)(\varphi) = \varphi(v)$$

Die Abbildung $\iota(v) : V^* \to R : \varphi \mapsto \varphi(v)$ ist linkslinear (R1A).
Somit erhalten wir tatsächlich $\iota(v) \in \mathrm{Hom}_R(V^*,R) = (V^*)^* = V^{**}$.

(1) Die so definierte Abbildung $\iota : V \to V^{**} : v \mapsto \iota(v)$ ist rechtslinear:

$$\begin{aligned} \iota(u\lambda + v\mu)(\varphi) &\overset{\text{Def}}{=} \varphi(u\lambda + v\mu) \\ &\overset{\text{Lin}}{=} \varphi(u)\lambda + \varphi(v)\mu \\ &\overset{\text{Def}}{=} \iota(u)(\varphi)\lambda + \iota(v)(\varphi)\mu \end{aligned}$$

(2) Sei $(v_i)_{i\in I}$ eine Basis von V und $(v_i^*)_{i\in I}$ die duale Familie in V^* (R1H).
Dann ist die Familie $(v_i^{**} := \iota(v_i))_{i\in I}$ in V^{**} dual zu $(v_i^*)_{i\in I}$, also linear unabhängig (R1D). Somit ist $\iota : V \to V^{**} : \sum_i v_i\mu_i \mapsto \sum_i v_i^{**}\mu_i$ injektiv.

(3) Ist $(v_i)_{i\in I}$ eine endliche Basis von V, so auch $(v_i^*)_{i\in I}$ in V^* (R1H) und $(v_i^{**})_{i\in I}$ in V^{**} (R1H). Dank Eindeutigkeit gilt $\iota(v_i) = v_i^{**}$ (R1H).
Somit ist $\iota : V \to V^{**} : \sum_i v_i\mu_i \mapsto \sum_i v_i^{**}\mu_i$ bijektiv.

Der natürliche Homomorphismus von V zum Bidual V^{**}

In diesem Kapitel arbeiten wir durchweg über einem beliebigen Ring R.
Um Trivialitäten zu vermeiden, fordern wir lediglich $1 \neq 0$, also $R \neq \{0\}$.
Das ist schwindelerregend allgemein, doch zum Ausgleich betrachten wir meist nur freie Räume, also mit einer Basis, das vereinfacht enorm.

Über einem Körper oder Divisionsring ist jeder Vektorraum frei (J2B), unsere Sätze gelten in diesen Fällen also ohne jede Einschränkung.
Wie gesehen genügt für viele Sätze bereits die Annahme einer Basis, und die Beweise sind wörtlich dieselben; daher bleibt R allgemein.

Es gibt im Folgenden ein paar Aussagen, für die wir tatsächlich mehr benötigen; in diesen Fällen setze ich dann einen Divisionsring voraus.
Solange es weder Aussage noch Beweis verkompliziert, verzichte ich auf diese Einschränkung und formuliere so allgemein wie möglich.

Der natürliche Homomorphismus von V zum Bidual V^{**}

Anschauliche Interpretation

Wir stellen uns einen Vektor $v \in V$ als physikalische Größe vor, zum Beispiel eine Verschiebung oder eine Geschwindigkeit im $\mathbb{R}^3$. Doch wie können / sollen wir uns einen Covektor $u \in V^*$ vorstellen?

Jeder Covektor $u \in V^*$ ist ein **Messgerät** für Vektoren $v \in V$!
Die Messung ist die Auswertung von u auf v: Der Covektor u nimmt als Eingabe den Vektor v und gibt als Ausgabe den Skalar $u(v)$.

Hierzu haben wir bereits vielfältige Beispiele skizziert:

- Zeilenvektor u mal Spaltenvektor v
- Auswertung / Abtastung einer Funktion f
- Preisliste ausgewertet auf einer Bestandsliste
- Auswertung einer Kraft auf einer Geschwindigkeit
- Anwendung einer Ableitung auf einen Tangentialvektor
- Integral eines Covektorfeldes entlang eines Weges.

Anschauliche Interpretation

Wie können / sollen wir uns den Bidualraum V^{**} anschaulich vorstellen? Seine Elemente $\psi \in V^{**}$ sind Messgeräte für Covektoren $u \in V^*$, so weit, so klar. Doch was bedeuten solche „Cocovektoren“ konkret?

Das einfachste ist natürlich, Messgeräte zu messen und zu vergleichen, indem wir sie auf ein und dieselbe Datenlage $v \in V$ anwenden.
Das ist genau die oben erklärte Abbildung $\iota : V \to V^{**}$.

Die gute Nachricht des obigen Satzes R1L lautet:
(0) Zu jedem Vektor $v \in V$ erhalten wir so den Cocovektor $\iota(v)$.
(1) Die Zuordnung $\iota : V \to V^{**}$ ist eine lineare Abbildung.
(2) Hat V eine Basis $(v_i)_{i \in I}$, so ist ι injektiv, kurz $\iota : V \hookrightarrow V^{**}$.
(3) Hat V eine endliche Basis $(v_i)_{i \in I}$, so ist ι bijektiv, $\iota : V \xrightarrow{\sim} V^{**}$.

In endlicher Dimension verliert das Bidual V^{**} also seinen Schrecken:
Wir können uns *jeden* Cocovektor als einen Vektor $v \in V$ vorstellen.
Die Anwendung von $v \in V$ auf $u \in V^*$ ist die Auswertung $u(v)$.

Anschauliche Interpretation

Anschauliche Interpretation

Der Annulator einer Teilmenge / eines Teilraums

Definition R2A: der Annulator einer Teilmenge / eines Teilraums

Sei V ein linearer Raum über R und $V^* = \mathrm{Hom}_R(V, R)$ der Dualraum.
Der **Annulator** einer Teilmenge $X \subseteq V$ ist definiert durch

$$X^\circ := \{\, \varphi \in V^* \mid \forall v \in X : \varphi(v) = 0 \,\} \leq V^*.$$

Nach Konstruktion ist dies ein linearer Unterraum des Dualraums V^*.
Die Bedingung „$\varphi(v) = 0$ für alle $v \in X$“ schreiben wir kurz $\varphi(X) = 0$.

Bemerkung R2A: von X zum Teilraum $\langle\, X \,\rangle_R$

Aus $X \subseteq Y \subseteq U := \langle\, X \,\rangle_R$ folgt $X^\circ = Y^\circ = U^\circ \leq V^*$.

Aufgabe: Rechnen Sie diese Bemerkung sorgsam nach.

Lösung: Die Inklusionen $X^\circ \supseteq Y^\circ \supseteq U^\circ$ sind klar, ebenso $X^\circ \subseteq U^\circ$:
Für $\varphi \in X^\circ$ gilt $X \subseteq \ker(\varphi)$, und daraus folgt $U = \langle\, X \,\rangle_R \subseteq \ker(\varphi)$,
denn der Kern ist ein Unterraum (I1R). Das bedeutet $\varphi \in U^\circ$.

Der Annulator einer Teilmenge / eines Teilraums

Bemerkung: Beachten Sie die Ähnlichkeit, aber auch den Unterschied zum Orthogonalraum $X^\perp$ bezüglich einer Bilinearform $\langle - \mid - \rangle$ auf V:

$$X^\perp := \{\, u \in V \mid \forall v \in X : \langle\, u \mid v \,\rangle = 0 \,\} \leq V$$

Der Annulator X° der Teilmenge $X \subseteq X$ liegt im Dualraum V^*,
der Orthogonalraum $X^\perp$ hingegen ist immer ein Unterraum von V.
Im nächsten Abschnitt werden wir die beiden Sichtweisen versöhnen.

Gemäß $X^\perp = \langle\, X \,\rangle_R^\perp$ können wir auch hier zum erzeugten Teilraum $U = \langle\, X \,\rangle_R \leq V$ übergehen. Bei einem Skalarprodukt gilt $V = U \oplus U^\perp$, und wir nennen dann $U^\perp$ das orthogonale Komplement zu U in V.

🙂 Dualität ist, wie bereits eingangs motiviert, eine natürliche Verallgemeinerung von Bilinearformen und Skalarprodukten.
Auch das nächste Beispiel illustriert dies sehr eindrücklich.

Beispiel zum Annulator

Aufgabe: Gegeben sind die folgenden Vektoren in $V = \mathbb{R}^{3\times 1}$ über $\mathbb{R}$:

$$v_1 = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 1 \\ 0 \\ -2 \end{bmatrix}, \quad v_4 = \begin{bmatrix} 0 \\ 1 \\ 5 \end{bmatrix}$$

Bestimmen Sie zu $X = \{v_1, v_2, v_3, v_4\}$ den Annulator X° in $V^* \cong \mathbb{R}^{1\times 3}$.

Lösung: Wir schreiben die Spalten v_1, v_2, v_3, v_4 in die Matrix $A \in \mathbb{R}^{3\times 4}$.
Wir suchen $u \in \mathbb{R}^{1\times 3}$ mit $uA = 0$. Mit Spaltenoperationen bringen
wir A in reduzierte Spaltenstufenform $C = AT$ mit $T \in \mathrm{GL}_4\,\mathbb{R}$:

$$A = \begin{bmatrix} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 3 & -2 & 5 \end{bmatrix} \xrightarrow[\text{RSSF}]{\text{Gauß}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & 5 & 0 & 0 \end{bmatrix} = C$$

Demnach gilt $uA = 0$ genau dann, wenn $uC = 0$. Daraus lesen wir ab:

$$X^\circ = \langle\, u_1 \,\rangle_{\mathbb{R}}^! \quad \text{mit} \quad u_1 = \begin{bmatrix} -2 & 5 & -1 \end{bmatrix}$$

🙂 Hier addieren sich $\dim\langle\, X \,\rangle = 2$ und $\dim X^\circ = 1$ zu $\dim V = 3$.
Anschaulich ist $\langle\, X \,\rangle$ eine Ebene, und u_1 steht hierzu senkrecht.

Beispiel zum Annulator

⚠ Statt dem Rechtskern berechnen wir hier den Linkskern von A.

Meist schreiben wir lineare Gleichungssysteme in der vertrauten Konvention $Ax = b$ mit $x \in R^{n\times 1}$ und $b \in R^{m\times 1}$ als Spaltenvektoren und der Koeffizientenmatrix $A \in R^{m\times n}$. Mit Zeilenoperationen B2C bringen wir A in reduzierte *Zeilenstufenform* $B = SA$ mit $S \in \mathrm{GL}_m\, R$.
Statt $Ax = b$ lösen wir die äquivalente, leichtere Gleichung $SAx = Sb$.

Im vorliegenden Falle bietet sich jedoch die Schreibweise $uA = 0$ an, mit $u \in R^{1\times m}$ und $0 \in R^{1\times n}$ als Zeilenvektoren. Mit Spaltenoperationen bringen wir A in reduzierte *Spaltenstufenform* $C = AT$ mit $T \in \mathrm{GL}_n\, R$.
Statt $uA = 0$ lösen wir die äquivalente, leichtere Gleichung $uAT = 0$.
Das Gauß–Verfahren ist in beiden Situationen vollkommen analog.

Über jedem kommutativen Ring R können Sie die beiden Probleme und Lösungsverfahren ineinander transponieren: Aus $Ax = b$ wird $x^\mathsf{T} A^\mathsf{T} = b$ und umgekehrt. Ist R nicht-kommutativ, so gilt dies nicht, daher scheint mir hier die nötige Links-Rechts-Disziplin natürlich und hilfreich.

Dimension und Struktur des Annulators

Satz R2B: Dimension und Struktur des Annulators

Sei V ein R–linearer Raum und $U \leq V$ ein Unterraum.

(1) Ist R ein Divisionsring, so gilt die Dimensionsformel

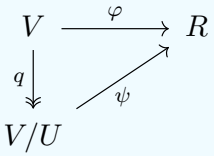
$$\boxed{\dim_R(U) + \dim_R(U^\circ) = \dim_R(V).}$$

(2) Allgemein über jedem Ring R gilt die folgende Implikation:

$$\boxed{V = U \oplus \langle\, v_1, \ldots, v_k \,\rangle^!_R \quad \Longrightarrow \quad U^\circ = \langle\, v_1^*, \ldots, v_k^* \,\rangle^!_R \leq V^*}$$

(3) Aus dem Quotienten $q : V \twoheadrightarrow V/U$ erhalten wir den Isomorphismus

$$\boxed{q^* \,:\, (V/U)^* \cong U^\circ \,:\, \psi \mapsto \psi \circ q.}$$



Letzteres folgt aus der linearen Faktorisierung über die Surjektion $q : V \twoheadrightarrow V/U$ (Satz I2E)

Dimension und Struktur des Annulators

Die Dimensionsformel (1) ist haben wir im vorigen Beispiel beobachtet. Die Gleichheit dort war tatsächlich kein Zufall, sondern gilt allgemein. Um allgemein von Dimension sprechen zu können, benötigen wir einen Divisionsring, wir denken insbesondere an Körper wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \ldots$.

Die Aussage (2) gilt allgemeiner über jedem Ring R, allerdings müssen wir eine Basis voraussetzen, hier in der Form $V = U \oplus \langle\, v_1, \ldots, v_k \,\rangle^!_R$. Wenn zudem U eine Basis hat, kurz $U = \langle\, v_i \mid i \in J \,\rangle^!_R$ mit $j = \sharp J$, dann folgt die Dimensionsformel (1), denn wir haben $\dim V = j + k$.

Für die Aussage (2) spielt jedoch die Struktur von U gar keine Rolle, wir benötigen lediglich ein Komplement mit einer endlichen Basis. Die griffige Formel lautet dann: Die Dimension des Annulators U° ist die Codimension des Unterraums U in V.

Die Aussage (3) ist die allgemeinste Formulierung dieser drei Aussagen, denn sie impliziert unmittelbar die Gleichung (2) und damit auch (1). Der Preis für diese Allgemeinheit ist die etwas höhere Abstraktion, doch diese Investition zahlt sich aus in Klarheit, Effizienz und Eleganz.

Dimension und Struktur des Annulators

Beweis: Übung!

Dimension und Struktur des Annulators

Rechenregeln für den Annulator

Satz R2C: Rechenregeln für den Annulator

Sei V ein R–linearer Raum und $V^* = \mathrm{Hom}_R(V,R)$ sein Dualraum.

(1a) Der Übergang zum Annulator kehrt alle Inklusionen um:

$$\boxed{A \subseteq B \subseteq V \quad\Longrightarrow\quad B^\circ \leq A^\circ \leq V^*}$$

(1b) Für den kleinsten bzw. größten Unterraum gilt dabei

$$\{0\}^\circ = V^* \quad\text{und}\quad V^\circ = \{0\}.$$

(2a) Für Summe und Schnitt von $A, B \leq V$ gilt:

$$\boxed{(A+B)^\circ = A^\circ \cap B^\circ \quad\text{und}\quad (A\cap B)^\circ \supseteq A^\circ + B^\circ}$$

(2b) Allgemein gilt für jede Familie $(A_i)_{i\in I}$ von Unterräumen $A_i \leq V$:

$$\textstyle(\sum_{i\in I} A_i)^\circ = \bigcap_{i\in I} A_i^\circ \quad\text{und}\quad (\bigcap_{i\in I} A_i)^\circ \supseteq \sum_{i\in I} A_i^\circ$$

Gleichheit gilt hier, falls R ein Divisionsring ist und die Menge I endlich.

Rechenregeln für den Annulator

Beweis: (1a) Sei $A \subseteq B \subseteq V$. Für $\varphi \in B^\circ$ gilt $\varphi(B) = 0$, also $\varphi(A) = 0$, und somit $\varphi \in A^\circ$. Das zeigt $B^\circ \leq A^\circ$. (1b) Diese Spezialfälle sind klar.

(2b) Wir zeigen $(\sum_{i\in I} A_i)^\circ = \bigcap_{i\in I} A_i^\circ$.

„$\subseteq$“: Aus $\varphi \in (\sum_{i\in I} A_i)^\circ$ folgt insbesondere $\varphi \in A_i^\circ$ für alle $i \in I$.

„$\supseteq$“: Aus $\varphi \in \bigcap_{i\in I} A_i^\circ$ folgt $\varphi \in A_i^\circ$ für alle $i \in I$, also $\varphi(A_i) = 0$, somit $\varphi(\sum_{i\in I} A_i) = 0$ dank Additivität von φ, und das heißt $\varphi \in (\sum_{i\in I} A_i)^\circ$.

(2b) Wir zeigen $(\bigcap_{i\in I} A_i)^\circ \supseteq \sum_{i\in I} A_i^\circ$.

„$\supseteq$“: Sei $\varphi \in \sum_{i\in I} A_i^\circ$, eine endliche Summe $\varphi = \sum_{i\in I} \varphi_i$ mit $\varphi_i \in A_i^\circ$. Auf $B = \bigcap_{i\in I} A_i$ gilt $\varphi_i(B) = 0$, also auch $\varphi(B) = 0$, somit $\varphi \in B^\circ$.

„$\subseteq$“: Sei I endlich. Wir betrachten $f : V \to \prod_{i\in I} V/A_i = \bigoplus_{i\in I} V/A_i$. Der Kern ist $\bigcap_{i\in I} A_i$. Wir nutzen nun $(\ker f)^\circ = \mathrm{im}(f^*)$, siehe R3K. QED

Beispiel: Sei $V = R^{(I)}$ und $A_i = \{\, v \in V \mid v_i = 0 \,\}$, also $V = A_i \oplus \langle\, e_i \,\rangle_R^!$. Dann gilt $B := \bigcap_{i\in I} A_i = \{\, v \in V \mid \forall i \in I : v_i = 0 \,\} = \{0\}$, also $B^\circ = V^*$. Hingegen gilt $A_i^\circ = \langle\, e_i^* \,\rangle_R^!$ (R2B), also $C := \sum_{i\in I} A_i^\circ = \langle\, e_i \mid i \in I \,\rangle_R^!$. Gleichheit $B^\circ = C$ gilt hier nur, falls die Menge I endlich ist! (R1I)

Rechenregeln für den Annulator

Satz R2C: Rechenregeln für den Annulator

(3a) Für direkte Summen gilt:

$$\boxed{V = A \oplus B \quad\Longrightarrow\quad V^* = B^\circ \oplus A^\circ}$$

(3b) Für allgemeine direkte Summen gilt:

$$V = \textstyle\bigoplus_{i\in I} V_i \quad\Longrightarrow\quad V^* = \prod_{i\in I} V_i^*$$

mit $V_i^* \cong (\sum_{j\neq i} V_j)^\circ$. Ist I zudem endlich, so folgt:

$$V = \textstyle\bigoplus_{i\in I} V_i \quad\overset{I \text{ endlich}}{\Longrightarrow}\quad V^* = \bigoplus_{i\in I} V_i^*$$

(4) Für jeden Unterraum $A \leq V$ gilt

$$\boxed{(A^\circ)^\circ \supseteq \iota(A).}$$

Gleichheit gilt im Falle $V = A \oplus B$ und $A = \langle\, v_1, \ldots, v_k \,\rangle_R^!$.

Rechenregeln für den Annulator

Beweis: (3b) Sei $V = \bigoplus_{i\in I} V_i$. Jede Linearform $\varphi : V \to R$ entspricht einer Familie $(\varphi_i)_{i\in I}$ von Linearformen $\varphi : V_i \to R$, und umgekehrt.

Für die Projektion $p_i : V \twoheadrightarrow V_i$ gilt $\ker p_i = \sum_{j\neq i} V_j$.
Dank R2B folgern wir $V_i^* \cong (\sum_{j\neq i} V_j)^\circ$.

Ist die Indexmenge I endlich, so gilt $\prod_{i\in I} V_i^* = \bigoplus_{i\in I} V_i^*$.
Diesen besonders sympathischen Fall haben wir in (3a) hervorgehoben.

(4) Die Inklusion $(A^\circ)^\circ \supseteq \iota(A)$ gilt immer und ist offensichtlich:
Für alle $v \in A$ und $\varphi \in A^\circ$ gilt nach Definition $\iota(v)(\varphi) = \varphi(v) = 0$.

Angenommen, es gilt zusätzlich $V = A \oplus B$ und $A = \langle\, v_1, \ldots, v_k \,\rangle_R^!$.
Dank (3) und R2B gilt dann $V^* = B^\circ \oplus A^\circ$ mit $B^\circ = \langle\, v_1^*, \ldots, v_k^* \,\rangle_R^!$.
Ebenso folgt $(V^*)^* = (A^\circ)^\circ \oplus (B^\circ)^\circ$ mit $(A^\circ)^\circ = \langle\, v_1^{**}, \ldots, v_k^{**} \,\rangle_R^!$.
Somit ist $\iota : A \hookrightarrow (A^\circ)^\circ : v_i \mapsto v_i^{**}$ ein Isomorphismus. QED

Beispiel: Zur Illustration betrachten wir $A = V = \langle\, v_i \mid i \in K \,\rangle_R^!$.
Hier gilt offensichtlich $A^\circ = \{0\} \leq V^*$ und demnach $(A^\circ)^\circ = V^{**}$.
Gleichheit $\iota(A) = (A^\circ)^\circ$ gilt nur, falls die Menge K endlich ist! (R1I)

Rechenregeln für den Annulator

🙂 Wir sehen, spüren und verstehen in diesen Sätzen deutlich, dass unendlich-dimensionale Räume oft nur schwache Aussagen zulassen.

Dennoch scheint mir das allgemeine Vorgehen und der so geschärfte Kontrast von endlicher vs unendlicher Dimension überaus lehrreich:

1. Wir lernen die Besonderheiten wahrzunehmen und wertzuschätzen, hier die Existenz endlicher Basen und ihrer guten Eigenschaften. Wir verstehen das Besondere besser im allgemeinen Kontext.
2. Der unendlich-dimensionale Fall wird in der Funktionalanalysis mit analytisch-topologischen Methoden „repariert“, soweit möglich. Auch diese Fortführung können wir hier bereits motivieren.

Rechenregeln für den Annulator

Vielleicht sind Sie dennoch unsicher, ob sich der erhöhte Aufwand lohnt, oder fragen sich, ob das alles nicht auch irgendwie einfacher geht.

In diesem Falle können Sie sich gerne selbst überzeugen, dass über einem Körper und in endlicher Dimension die Formulierungen nicht einfacher und die Beweise nicht kürzer werden. Es fallen lediglich ein paar lehrreiche Gegenbeispiele weg, was eher schade ist.

Ich denke, das allgemeine Vorgehen lohnt langfristig und bereits jetzt: Der schöne Spezialfall wird klarer verständlich im allgemeinen Kontext.

Anwendungsbeispiel der Rechenregeln

Aufgabe: Wir betrachten erneut folgende Vektoren in $V = \mathbb{R}^{3\times 1}$ über $\mathbb{R}$:

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ -2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 0 \\ 1 \\ 5 \end{bmatrix}$$

Diese erzeugen die Unterräume $A = \langle\, v_1 \,\rangle^!_{\mathbb{R}}$ und $B = \langle\, v_2 \,\rangle^!_{\mathbb{R}}$. Berechnen und vergleichen Sie $(A+B)^\circ$ und $A^\circ \cap B^\circ$ sowie $(A \cap B)^\circ$ und $A^\circ + B^\circ$.

Lösung: Wir haben $A + B = \langle\, v_1, v_2 \,\rangle^!_{\mathbb{R}}$ und finden $(A+B)^\circ = \langle\, u_1 \,\rangle^!_{\mathbb{R}}$ mit $u_1 = (-2, 5, -1) \in \mathbb{R}^{1\times 3} \cong V^*$ dank Gauß–Algorithmus (R203). Anschaulich ist $A + B$ eine Ebene, und u_1 steht hierzu senkrecht.

Dagegen gilt $A^\circ = \langle\, u_1, e_2^* \,\rangle^!_{\mathbb{R}}$, $B^\circ = \langle\, u_1, e_1^* \,\rangle^!_{\mathbb{R}}$ und $A^\circ \cap B^\circ = \langle\, u_1 \,\rangle^!_{\mathbb{R}}$. Geometrisch ist dies der Schnitt von zwei Ebenen in einer Geraden. Rechnerisch lohnt sich hier bereits die Gleichung $A^\circ \cap B^\circ = (A+B)^\circ$.

Weiter finden wir den Schnitt $A \cap B = \{0\}$, also $(A \cap B)^\circ = V^*$, sowie $A^\circ + B^\circ = \langle\, e_1^*, e_2^*, u_1 \,\rangle = V^*$. Das bestätigt $(A \cap B)^\circ = A^\circ + B^\circ$.

Anwendungsbeispiel der Rechenregeln

🙂 Die Rechenregeln R2c für den Annulator entsprechen intuitiv anschaulichen Gesetzmäßigkeiten für lineare Gleichungssysteme. Die abstrakte Formulierung fasst konkrete Anwendungen zusammen.

🙂 Die Schnittmenge $U_1 \cap \cdots \cap U_k$ von Unterräumen $U_1, \ldots, U_k \leq \mathbb{R}^n$ ist zunächst nicht leicht zu berechnen. Das ändert sich, wenn jeder als Kern $U_i = \ker M_i$ einer Matrix $M_i \in \mathbb{R}^{m_i \times n}$ gegeben ist. Dann ist

$$U_1 \cap \cdots \cap U_k = \ker M \quad \text{mit} \quad M = \begin{bmatrix} M_1 \\ \vdots \\ M_k \end{bmatrix} \in \mathbb{R}^{m\times n}.$$

Hier betrachten wir $V = \mathbb{R}^{1\times n}$ als Raum der Zeilenvektoren.
Die Zeilen der Matrix M_i spannen hierin den Unterraum $V_i \leq V$ auf.
Der Dualraum $V^* \cong \mathbb{R}^{n\times 1}$ ist dann der Raum der Spaltenvektoren.
Darin liegt der Unterraum $U_i = \ker M_i = \{\, u \in \mathbb{R}^{n\times 1} \mid M_i u = 0 \,\} = V_i^\circ$.

🙂 Wir nutzen dankend $U_1 \cap \cdots \cap U_k = (V_1 + \cdots + V_k)^\circ$: Wir wollen die linke Seite berechnen, die rechte beherrschen wir dank Gauß.

Bilinearformen und Dualität

Ist V ein rechtslinearer Raum über R, so ist der Dualraum $U = V^*$ linkslinear (R1B), und wir haben die gegenseitige **Auswertung**

$$B : U \times V \to R : (u, v) \mapsto u(v).$$

Dies ist eine Bilinearform, linkslinear in U und rechtslinear in V:

$$B(u, v + v') = B(u, v) + B(u, v'), \qquad B(u, v \cdot \mu) = B(u, v) \cdot \mu,$$
$$B(u + u', v) = B(u, v) + B(u', v), \qquad B(\lambda \cdot u, v) = \lambda \cdot B(u, v)$$

für alle Vektoren $u, u' \in U$ und $v, v' \in V$ und Skalare $\lambda, \mu \in R$.

Definition R2D: Bilinearform / Paarung

Sei U ein linkslinearer und V ein rechtslinearer Raum über R sowie

$$B : U \times V \to R : (u, v) \mapsto B(u, v).$$

Dies ist eine **Bilinearform**, falls für alle $u \in U$ und $v \in V$ gilt:

$$B_1(u) : V \to R : v \mapsto B(u, v) \quad \text{ist rechtslinear,}$$
$$B_2(v) : U \to R : u \mapsto B(u, v) \quad \text{ist linkslinear.}$$

Bilinearformen und Dualität

Definition R2D: Bilinearform / Paarung

Die Bilinearform B definiert lineare Abbildungen in die Dualräume:

$$B_1 : U \to V^* : u \mapsto B_1(u) = B(u, -) \quad \text{linkslinear,}$$
$$B_2 : V \to U^* : v \mapsto B_2(v) = B(-, v) \quad \text{rechtslinear.}$$

Der **Linkskern** oder das **Linksradikal** ist der Unterraum

$$\ker B_1 = {}^\perp V = \{ u \in U \mid \forall v \in V : B(u, v) = 0 \} \leq U.$$

Der **Rechtskern** oder das **Rechtsradikal** ist der Unterraum

$$\ker B_2 = U^\perp = \{ v \in V \mid \forall u \in U : B(u, v) = 0 \} \leq V.$$

Wir nennen B **nicht-ausgeartet**, wenn B_1 und B_2 injektiv sind:

- $\ker B_1 = \{0\}$: Zu jedem $u \in U \setminus \{0\}$ existiert $v \in V$ mit $B(u, v) \neq 0$.
- $\ker B_2 = \{0\}$: Zu jedem $v \in V \setminus \{0\}$ existiert $u \in U$ mit $B(u, v) \neq 0$.

Wir nennen B **perfekt**, wenn B_1 und B_2 Isomorphismen sind.

Beispiel: Zeilenraum $R^{1\times n}$ und Spaltenraum $R^{n\times 1}$

Beispiel R2E: Zeilenraum $R^{1\times n}$ und Spaltenraum $R^{n\times 1}$

Über dem Ring R betrachten wir $V = R^{n\times 1}$ als rechtslinearen Raum.
Hierzu ist der Dualraum $V^* = \mathrm{Hom}_R(V, R) \cong R^{1\times n}$ dann linkslinear.

Genauer haben wir die perfekte Paarung durch **Matrixmultiplikation**:

$$B : R^{1\times n} \times R^{n\times 1} \to R : (u, v) \mapsto B(u, v) = u \cdot v = \textstyle\sum_{i=1}^{n} u_{1,i} \cdot v_{i,1}$$

Dies definiert die beiden Isomorphismen R1C zu den Dualräumen:

$$B_1 : R^{1\times n} \xrightarrow{\sim} (R^{n\times 1})^* : u \mapsto B_1(u) = B(u, -)$$
$$B_2 : R^{n\times 1} \xrightarrow{\sim} (R^{1\times n})^* : v \mapsto B_2(v) = B(-, v)$$

☺ Dies präzisiert den Isomorphismus, den wir seit R1C gerne nutzen. Zudem wird dies nun wunderbar elegant und symmetrisch formuliert.

Zum Raum $V = R^{n\times 1}$ der Spaltenvektoren ist $V^* = \mathrm{Hom}_R(V, R)$ nicht *gleich* dem Raum $R^{1\times n}$ der Zeilenvektoren, doch immerhin kanonisch isomorph: Die obige Paarung stiftet den ersehnten Isomorphismus.

Beispiel: der Koordinatenraum $R^{(I)}$ und sein Dualraum R^I

Beispiel R2F: der Koordinatenraum $R^{(I)}$ und sein Dualraum R^I

Über dem Ring R betrachten wir $V = R^{(I)}$ als rechtslinearen Raum.
Hierzu ist der Dualraum $V^* = \mathrm{Hom}_R(V, R) \cong R^I$ dann linkslinear.

Hierzu haben wir die kanonische Paarung durch **Auswertung**:

$$B : R^I \times R^{(I)} \to R : (u, v) \mapsto B(u, v) = \textstyle\sum_{i\in I} u_i v_i$$

(1) Diese Bilinearform ist nicht-ausgeartet: B_1 ist bijektiv und B_2 injektiv.
(2) Genau dann ist B perfekt, also auch B_2 bijektiv, wenn I endlich ist.

Aufgabe: Rechnen Sie dies sorgsam nach!

Lösung: Wir nutzen die Definition und unsere vorigen Überlegungen:

(1a) Sei $u \in U \setminus \{0\}$. Es gilt $u_i \neq 0$ für ein $i \in I$, also $B(u, e_i) = u_i \neq 0$.
(1b) Sei $v \in V \setminus \{0\}$. Es gilt $v_i \neq 0$ für ein $i \in I$, also $B(e_i, v) = v_i \neq 0$.

(2a) Die Abbildung $B_1 : R^I \to (R^{(I)})^*$ ist immer ein Isomorphismus,
(2b) doch $B_2 : R^{(I)} \to (R^I)^*$ nur genau dann, wenn I endlich ist (R1I).

Perfekte Bilinearformen

☺ Perfekte Paarungen existieren nur in endlicher Dimension:

Satz R2G: perfekte Bilinearform

Sei R ein Divisionsring und hierüber $B : U \times V \to R$ eine Bilinearform.

(1) Ist B nicht-ausgeartet, so sind folgende Aussagen äquivalent:
(a) B ist perfekt. (b) $\dim_R(U) < \infty$. (c) $\dim_R(V) < \infty$.

Beweis: „(c) ⇒ (b,a)“: Sei $\dim_R(V) < \infty$. Nach Voraussetzung sind die Homomorphismen $B_1 : U \to V^*$ und $B_2 : V \to U^*$ injektiv. Daraus folgt:

$$\dim U \overset{\text{J2I}}{\leq} \dim V^* \underset{\text{(c)}}{\overset{\text{R1H}}{=}} \dim V \overset{\text{J2I}}{\leq} \dim U^* \underset{\text{(b)}}{\overset{\text{R1H}}{=}} \dim U$$

Demnach sind alle vier Dimensionen gleich.
Somit sind B_1 und B_2 bijektiv (J2I).

Ebenso beweist man „(b) ⇒ (c,a)“.

Die Implikation „(a) ⇒ (b,c)“ folgt aus der folgenden Verschärfung, die ich zwecks Klarheit und Betonung separat formuliere.

Perfekte Bilinearformen

Satz R2G: perfekte Bilinearform

(2) Sind $B_1 : U \to V^*$ und $B_2 : V \to U^*$ surjektiv, so gilt:
(a) $\dim_R(V) < \infty$, (b) $\dim_R(U) < \infty$, (c) B ist perfekt.

Beweis: (a) Sei $(v_i)_{i\in I}$ eine Basis von V (J2B). Wir nutzen $B_1 : U \twoheadrightarrow V^*$: Zu jedem $i \in I$ existiert $u_i \in U$ mit $B(u_i, -) = v_i^*$, also $B(u_i, v_j) = \delta_{i,j}$. Ebenso $B_2 : V \twoheadrightarrow U^*$: Die Familie $(u_i^*)_{i\in I}$ mit $u_i^* = B(-, v_i)$ erzeugt U^*.

Es existiert $\varphi \in U^*$ mit $\varphi(u_i) = 1$ für alle $i \in I$ (K1D). Hierzu existiert $\lambda \in R^{(I)}$ mit $\varphi = \sum_{i\in I} \lambda_i u_i^*$. Hierbei gilt $1 = \varphi(u_j) = \sum_{i\in I} \lambda_i u_i^*(u_j) = \lambda_j$ für alle $j \in I$. Also ist die Menge I endlich, das heißt $\dim_R(V) < \infty$.

(b) Ebenso zeigt man $\dim_R(U) < \infty$.

(c) Daraus schließen wir die Gleichheit aller vier Dimensionen:

$$\dim U \overset{\text{J2I}}{\geq} \dim V^* \underset{\text{(a)}}{\overset{\text{R1H}}{=}} \dim V \overset{\text{J2I}}{\geq} \dim U^* \underset{\text{(b)}}{\overset{\text{R1H}}{=}} \dim U$$

Somit sind B_1 und B_2 bijektiv (J2I). QED

Perfekte Bilinearformen

Das ist ein recht elegantes und bemerkenswertes Ergebnis:
Perfekte Paarungen existieren nur in endlicher Dimension!

Der Beweis ist nicht minder elegant und bemerkenswert.
Bitte gehen Sie alle Argumente noch einmal sorgsam durch, anschließend versuchen Sie es zur Kontrolle selbst ohne Vorlage.
Sie werden sehen, es ist eine wunderbare Übung zur Wiederholung.

Hier spielen alle Grundbegriffe erneut wunderbar zusammen:
lineare Räume und lineare Abbildungen, lineare Unabhängigkeit, Erzeugendensysteme, Basen, Basisauswahl und -Ergänzung, etc.
Es ist daher schön, dies im Rückblick aufzugreifen und zu vertiefen.

Wenn Ihnen das auch nach dem zweiten Lesen noch verwirrend scheint, dann sollten Sie genau diese Grundbegriffe dringend wiederholen!

Perfekte Bilinearformen

Definition R2H: Anti-Involution

(1) Sei $(R,+,\cdot)$ ein Ring. Ein **involutiver Anti-Automorphismus**

$$\bar{}\,:\, R\to R\,:\,\lambda\mapsto\overline{\lambda}$$

erfüllt $\overline{\lambda+\mu}=\overline{\lambda}+\overline{\mu}$ und $\overline{\lambda\cdot\mu}=\overline{\mu}\cdot\overline{\lambda}$ sowie $\overline{\overline{\mu}}=\mu$ für alle $\lambda,\mu\in R$.
Wir nennen dies auch kurz eine **Anti-Involution**, das ist bequemer.

(2) Sei $(U,+,\bullet)$ ein rechtslinearer Raum über R, mit Skalarmultiplikation

$$\bullet\,:\,U\times R\to U\,:\,(u,\lambda)\mapsto u\bullet\lambda.$$

Dann ist $(U,+,\bar{\bullet})$ ein linkslinearer Raum über R mit Skalarmultiplikation

$$\bar{\bullet}\,:\,R\times U\to U\,:\,(\lambda,u)\mapsto\lambda\,\bar{\bullet}\,u:=u\bullet\overline{\lambda}.$$

Wir schreiben diese Räume $(U,+,\bullet)$ und $(U,+,\bar{\bullet})$ kurz U und $\overline{U}$.

(3) Ebenso definieren wir zu jedem linkslinearen Raum U
den zugehörigen rechtslinearen Raum $\overline{U}$. Nach Konstruktion gilt $\overline{\overline{U}}=U$.

Beweis: (1) Auch wenn dies nicht explizit gefordert wird, folgt $\overline{1}=1$:

$$1\overset{\text{Inv}}{=}\overline{\overline{1}}\overset{\text{Ntr}}{=}\overline{1\cdot\overline{1}}\overset{\text{Anti}}{=}\overline{\overline{1}}\cdot\overline{1}\overset{\text{Inv}}{=}1\cdot\overline{1}\overset{\text{Ntr}}{=}\overline{1}$$

(2) Wir rechnen die Behauptung nach für $u\in U$ und $\lambda,\mu\in R$:

$$1\,\bar{\bullet}\,u\overset{\text{Def}}{=}u\bullet\overline{1}\overset{(1)}{=}u\bullet 1\overset{\text{rLin}}{=}u$$
$$(\lambda\cdot\mu)\,\bar{\bullet}\,u\overset{\text{Def}}{=}u\bullet(\overline{\lambda\cdot\mu})\overset{\text{Anti}}{=}u\bullet(\overline{\mu}\cdot\overline{\lambda})\overset{\text{rLin}}{=}(u\bullet\overline{\mu})\bullet\overline{\lambda}\overset{\text{Def}}{=}\lambda\,\bar{\bullet}\,(\mu\,\bar{\bullet}\,u)$$

Beispiele: Für jeden kommutativen Ring R können wir $\overline{\lambda}=\lambda$ nutzen und so die Skalare von rechts nach links umwälzen und umgekehrt.

Eine interessante Anti-Involution ist die Konjugation auf $\mathbb{C}$ oder auf $\mathbb{H}$.
(Da $\mathbb{C}$ kommutativ ist, ist dies auf $\mathbb{C}$ zugleich ein Automorphismus.)

Ist $(K,+,\cdot)$ ein Ring mit Anti-Involution $\lambda\mapsto\overline{\lambda}$, so auch der Matrixring $R=K^{n\times n}$ über R mit der Transposition-Konjugation $A\mapsto A^\dagger=\overline{A}^\mathsf{T}$.

☺ Anti-Involutionen sind uns bereits vertraut und sehr oft nützlich.
Es ist gut und hilfreich, hierfür einen griffigen Namen zu haben.

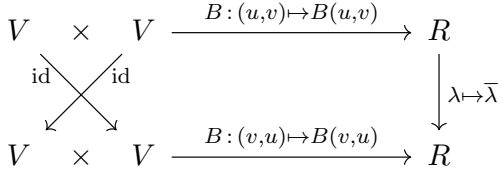
Bemerkung: Genau dann ist $B:U\times V\to R$ **sesquilinear**,

$$B(u,v+v')=B(u,v)+B(u,v'),\qquad B(u,v\bullet\mu)=B(u,v)\cdot\mu,$$
$$B(u+u',v)=B(u,v)+B(u',v),\qquad B(u\bullet\lambda,v)=\overline{\lambda}\cdot B(u,v),$$

wenn die Abbildung $B:\overline{U}\times V\to R$ **bilinear** ist,

$$B(u,v+v')=B(u,v)+B(u,v'),\qquad B(u,v\bullet\mu)=B(u,v)\cdot\mu,$$
$$B(u+u',v)=B(u,v)+B(u',v),\qquad B(\lambda\,\bar{\bullet}\,u,v)=\lambda\bullet B(u,v).$$

Gilt speziell $U=V$ und $B(u,v)=\overline{B(v,u)}$ für alle $u,v\in V$,
so nennen wir B **hermitesch** oder **konjugiert-symmetrisch**.



Die Konjugation auf dem Körper $\mathbb{C}$ der komplexen Zahlen mussten wir in das Skalarprodukt einführen, um positive Definitheit zu erreichen.

Das wirkt anfangs etwas lästig und scheint eine notdürftige Reparatur.
Hier nun sehen wir, wie sich alles elegant und natürlich zusammenfügt.

Wie versprochen zahlt sich unsere Links-Rechts-Disziplin sofort aus,
und das sogar für kommutative Ringe wie hier für den Körper $\mathbb{C}$!

Die gute Notation denkt für uns mit, sie verhindert Rechenfehler,
sie macht den Weg frei und nimmt uns einen Teil der Arbeit ab.

Aufgabe: Ist $B:U\times V\to R$ eine Bilinearform, so auch $B^\dagger:\overline{V}\times\overline{U}\to R$ mit $B^\dagger(v,u)=\overline{B(u,v)}$. Genau dann ist B hermitesch, wenn $B^\dagger=B$ gilt.

Lösung: Additivität ist klar. Für $u\in U$ und $v\in V$ sowie $\lambda,\mu\in R$ gilt:

$$B^\dagger(\lambda\,\bar{\bullet}\,v,u\,\bar{\bullet}\,\mu)\overset{\text{Def}}{=}B^\dagger(v\bullet\overline{\lambda},\overline{\mu}\bullet u)\overset{\text{Def}}{=}\overline{B(\overline{\mu}\bullet u,v\bullet\overline{\lambda})}$$
$$\overset{\text{Bil}}{=}\overline{\overline{\mu}\cdot B(u,v)\cdot\overline{\lambda}}\overset{\text{Anti}}{=}\overline{\overline{\lambda}}\cdot\overline{B(u,v)}\cdot\overline{\overline{\mu}}\overset{\text{Inv}}{=}\lambda\cdot B^\dagger(v,u)\cdot\mu$$

Das Standardskalarprodukt ist eine perfekte Paarung. R229

Beispiel R2I: das Standardskalarprodukt als perfekte Paarung

(1) Über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ betrachten wir $V = \mathbb{K}^n$ als rechtslinearen Raum.
Hierauf haben wir das Standardskalarprodukt

$$\langle - \mid - \rangle : V \times V \to \mathbb{K} : (u, v) \mapsto \langle u \mid v \rangle = \textstyle\sum_{i=1}^{n} \overline{u_i} \cdot v_i.$$

Somit ist die Abbildung $B : \overline{V} \times V \to \mathbb{K} : (u, v) \mapsto \langle u \mid v \rangle$ bilinear:

$$\begin{aligned} B(\lambda \mathbin{\bar{\cdot}} u, v) &\overset{\text{Def}}{=} B(u \cdot \overline{\lambda}, v) \overset{\text{Def}}{=} \textstyle\sum_{i=1}^{n} \overline{(u_i \cdot \overline{\lambda})} \cdot v_i \overset{\text{Anti}}{=} \sum_{i=1}^{n} (\lambda \cdot \overline{u_i}) \cdot v_i \\ &\overset{\text{Ass}}{=} \textstyle\sum_{i=1}^{n} \lambda \cdot (\overline{u_i} \cdot v_i) \overset{\text{Distr}}{=} \lambda \cdot \sum_{i=1}^{n} \overline{u_i} \cdot v_i \overset{\text{Def}}{=} \lambda \cdot B(u, v) \end{aligned}$$

Dies definiert Homomorphismen zu den Dualräumen:

$$\begin{aligned} B_1 &: \overline{V} \xrightarrow{\sim} V^* : u \mapsto B_1(u) = \langle u \mid - \rangle \\ B_2 &: V \xrightarrow{\sim} \overline{V}^* : v \mapsto B_2(v) = \langle - \mid v \rangle \end{aligned}$$

Diese sind injektiv dank positiver Definitheit des Skalarprodukts, daher bijektiv dank Satz R2G. Somit ist B eine perfekte Paarung.

Das Standardskalarprodukt ist eine perfekte Paarung. R230 Erläuterung

Wie üblich betrachten wir $V = \mathbb{K}^{n \times 1}$ als Raum der Spaltenvektoren und dual hierzu $V^* \cong \mathbb{K}^{1 \times n}$ als Raum der Zeilenvektoren (R1C).

Zudem haben wir das obige Skalarprodukt $B : V \times V \to \mathbb{K}$.
Die zugehörigen Isomorphismus haben dann die konkrete Form

$$\begin{aligned} B_1 &: \overline{\mathbb{K}^{n \times 1}} \xrightarrow{\sim} \mathbb{K}^{1 \times n} : u \mapsto \overline{u}^\intercal, \\ B_2 &: \mathbb{K}^{n \times 1} \xrightarrow{\sim} \overline{\mathbb{K}^{1 \times n}} : v \mapsto \overline{v}^\intercal. \end{aligned}$$

Nach Konstruktion gilt $\lambda \mathbin{\bar{\cdot}} u = u \cdot \overline{\lambda} \mapsto \lambda \cdot \overline{u}^\intercal$ und $\lambda \cdot v \mapsto \overline{v}^\intercal \cdot \overline{\lambda} = \lambda \mathbin{\bar{\cdot}} \overline{v}^\intercal$.

🙂 Die beiden Isomorphismen $B_1 : \overline{V} \xrightarrow{\sim} V^*$ und $B_2 : V \xrightarrow{\sim} \overline{V}^*$ entsprechen hier der vertrauten Transposition-Konjugation.

Bemerkung: In Diracs Bra-Ket-Notation wird aus dem Ket-Vektor $|v\rangle \in V$ der Bra-Covektor $\langle v| = |v\rangle^\dagger \in V^*$. Umgekehrt wird aus dem Bra-Covektor $\langle u| \in V^*$ der Ket-Vektor $|u\rangle = \langle u|^\dagger \in V$. Dies sind jeweils Anti-Isomorphismen, denn skalare Faktoren werden dabei konjugiert.

Skalarprodukt als nicht-ausgeartete Paarung R231

Beispiel R2I: Skalarprodukt als nicht-ausgeartete Paarung

(2) Sei V ein rechtslinearer Raum über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ mit Skalarprodukt

$$\langle - \mid - \rangle : V \times V \to \mathbb{K} : (u, v) \mapsto \langle u \mid v \rangle.$$

Wir betrachten dies als bilineare Abbildung

$$B : \overline{V} \times V \to \mathbb{K} : (u, v) \mapsto \langle u \mid v \rangle.$$

Dies definiert lineare Abbildungen in die Dualräume:

$$\begin{aligned} B_1 &: \overline{V} \to V^* : u \mapsto B_1(u) = \langle u \mid - \rangle \\ B_2 &: V \to \overline{V}^* : v \mapsto B_2(v) = \langle - \mid v \rangle \end{aligned}$$

Beide sind injektiv, also ist die Bilinearform B nicht-ausgeartet:

$$\forall v \in V \setminus \{0\} : \langle v \mid v \rangle > 0$$

Genau dann ist B perfekt, wenn V endlich-dimensional ist (R2G).

Skalarprodukt als nicht-ausgeartete Paarung R232 Erläuterung

In Teil (2) dieses Beispiels betrachten wir ein beliebiges Skalarprodukt, gemäß Definition P1L, auf einem Vektorraum V über $\mathbb{K} = \mathbb{R}, \mathbb{C}$

Dank positiver Definitheit ist dies eine nicht-ausgeartete Bilinearform, doch perfekt ist sie nur in endlicher Dimension, genau wie in Teil (1).

Wie angekündigt verallgemeinert die duale Paarung $B : V^* \times V \to R$ über R das Skalarprodukt $\langle - \mid - \rangle : V \times V \to \mathbb{K}$ über $\mathbb{K} = \mathbb{R}, \mathbb{C}$.

Mit diesem abschließenden Beispiel sehen Sie, wie sich die vertrauten Begriffe zu Skalarprodukten in diesen allgemeineren Kontext einbetten.

Bemerkung: In R1J haben wir zu jeder Basis $\mathcal{B}$ von V den antilinearen Isomorphismus $(\Psi_\mathcal{B}, \Psi_\mathcal{B}^*) : V \cong V^*$ konstruiert. Dieser ist jedoch nicht kanonisch, denn er hängt ab von der willkürlich gewählten Basis $\mathcal{B}$.

Im Gegensatz hierzu ist der Isomorphismus $B_1 : \overline{V} \xrightarrow{\sim} V^*$ kanonisch, sobald der Raum V mit einem Skalarprodukt B ausgestattet ist.

Übung: Es gilt $B_1 = \Psi_\mathcal{B}$ für jede Orthonormalbasis $\mathcal{B}$ von V.
Die Konstruktion aus R1J war also nicht vergebens.

Motivation: die Adjunktionsformel

Sei R ein Ring, hierüber V ein rechtslinearer Raum. Der Dualraum V^* ist dann linkslinear (R1B), und wir haben die **duale Paarung**

$$B_V : V^* \times V \to R : (\varphi, v) \mapsto \langle \varphi \mid v \rangle = \varphi(v).$$

Dieselbe Situation finden wir für jeden weiteren R–linearen Raum U:

$$B_U : U^* \times U \to R : (\psi, u) \mapsto \langle \psi \mid u \rangle = \psi(u)$$

Zu jeder linearen Abbildung $f : U \to V$ suchen wir eine duale Abbildung $f^* : V^* \to U^*$, sodass die folgende, vertraute **Adjunktionsformel** gilt:

$$\langle \varphi \mid f(u) \rangle = \langle f^*(\varphi) \mid u \rangle$$

für alle $\varphi \in V^*$ und $u \in U$. Dies gelingt auf genau eine Weise:

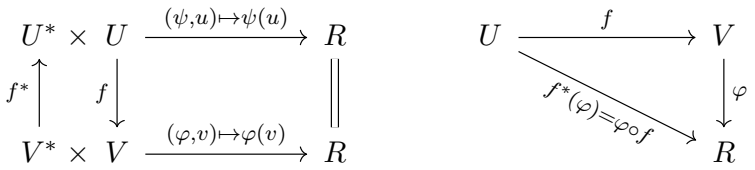
$$\boxed{f^*(\varphi) := \varphi \circ f}$$

Die Linearform φ auf V wird so zurückgezogen zu $\varphi \circ f$ auf U.
Die hier gefundene Formel erheben wir nun zur Definition.

Motivation: die Adjunktionsformel

Der duale Homomorphismus $f^* : V^* \to U^*$ zu $f : U \to V$

Wir können lineare Räume dualisieren und ebenso lineare Abbildungen:



Definition R3A: die duale Abbildung

(0) Jede lineare Abbildung $f : U \to V$ induziert ihre **duale Abbildung**

$$\boxed{f^* : V^* \to U^* : \varphi \mapsto \varphi \circ f.}$$

(1) Ist f rechtslinear, so ist f^* linkslinear, und umgekehrt. Wir erhalten

$$^* : \mathrm{Hom}_R(U, V) \to \mathrm{Hom}_R(V^*, U^*) : f \mapsto f^*.$$

(2) Die Dualisierung * ist ein Homomorphismus der additiven Gruppen.
(3) Ist der Ring R kommutativ, so ist die Dualisierung * sogar R–linear.

Der duale Homomorphismus $f^* : V^* \to U^*$ zu $f : U \to V$

Beweis: (0) Sind $f : U \to V$ und $\varphi : V \to R$ rechtslinear, so auch $\varphi \circ f$.
(1) Die Abbildung $f^* : V^* \to U^* : \varphi \mapsto \varphi \circ f$ ist linkslinear.
Für alle $\varphi, \psi \in V^*$ und $\lambda, \mu \in R$ gilt nämlich:

$$\begin{aligned} f^*(\lambda\varphi + \mu\psi) &\overset{\text{Def}}{=} (\lambda\varphi + \mu\psi) \circ f \\ &\overset{\text{DR}}{=} \lambda(\varphi \circ f) + \mu(\psi \circ f) \overset{\text{Def}}{=} \lambda f^*(\varphi) + \mu f^*(\psi) \end{aligned}$$

(2) Die Zuordnung $^* : \mathrm{Hom}_R(U, V) \to \mathrm{Hom}_R(V^*, U^*) : f \mapsto f^*$ ist additiv:

$$\begin{aligned} (f + g)^*(\varphi) &\overset{\text{Def}}{=} \varphi \circ (f + g) \\ &\overset{\text{DL}}{=} (\varphi \circ f) + (\varphi \circ g) \overset{\text{Def}}{=} f^*(\varphi) + g^*(\varphi) \end{aligned}$$

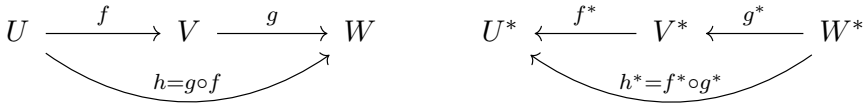
Das bedeutet $(f + g)^* = f^* + g^*$ für alle $f, g \in \mathrm{Hom}_R(U, V)$.
(3) Ist der Ring R zudem kommutativ, so gilt für alle $u \in U$ zudem:

$$\begin{aligned} (f\lambda)^*(\varphi)(u) &\overset{\text{Def}}{=} (\varphi \circ (f\lambda))(u) \overset{\text{Def}}{=} \varphi((f\lambda)(u)) \overset{\text{Def}}{=} \varphi(f(u)\lambda) \\ &\overset{\text{Lin}}{=} \varphi(f(u))\lambda \overset{\text{Def}}{=} (\varphi \circ f)(u)\lambda \overset{\text{Def}}{=} (\lambda f^*(\varphi))(u) \end{aligned}$$

Das bedeutet $(f\lambda)^* = \lambda f^*$: Die Dualisierung $f \mapsto f^*$ ist R–linear. QED

Komposition von Homomorphismen

Die Dualisierung kehrt alle Pfeile um:



Satz R3B: Funktorialität

(1) Dual zur Identität $\mathrm{id}_V : V \to V$ ist $\mathrm{id}_V^* = \mathrm{id}_{V^*} : V^* \to V^*$.

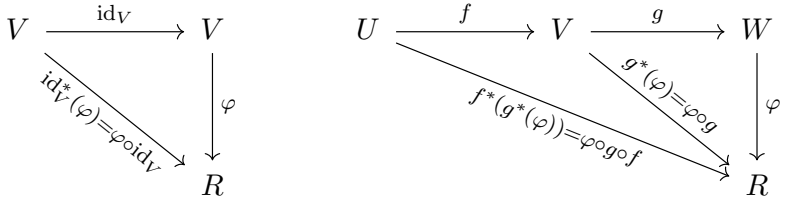
(2) Dual zur Komposition $h = g \circ f$ ist $h^* = f^* \circ g^*$.

🙂 Das sind zwei einfache, aber überaus nützliche Rechenregeln.
Vornehm zusammengefasst sagen wir hierzu abkürzend:
Die Dualisierung ist ein **kontravarianter Funktor**.

Das bedeutet: Jedem linearen Raum V wird sein dualer Raum V^* zugeordnet, und jeder linearen Abbildung $f : U \to V$ ihre duale Abbildung $f^* : V^* \to U^*$. Diese Zuordnung respektiert Identitäten gemäß $\mathrm{id}_V^* = \mathrm{id}_{V^*}$ und Kompositionen gemäß $(g \circ f)^* = f^* \circ g^*$.

Komposition von Homomorphismen

Aufgabe: Rechnen Sie diese Regeln sorgsam nach!



Lösung: (1) Für $\mathrm{id}_V : V \to V$ und alle $\varphi \in V^*$ gilt:

$$\mathrm{id}_V^*(\varphi) \overset{\text{Def}}{=} \varphi \circ \mathrm{id}_V \overset{\text{Id}}{=} \varphi$$

Das bedeutet $\mathrm{id}_V^* = \mathrm{id}_{V^*}$.

(2) Für $f : U \to V$ und $g : V \to W$ und alle $\varphi \in W^*$ gilt:

$$(g \circ f)^*(\varphi) \overset{\text{Def}}{=} \varphi \circ (g \circ f) \overset{\text{Ass}}{=} (\varphi \circ g) \circ f \overset{\text{Def}}{=} f^*(g^*(\varphi)) \overset{\text{Def}}{=} (f^* \circ g^*)(\varphi)$$

Das bedeutet $(g \circ f)^* = f^* \circ g^*$. QED

Komposition von Homomorphismen

Komposition von Homomorphismen

Dualität und Matrixdarstellung

Beispiel / Aufgabe: Wir betrachten $U = R^{n\times 1}$ und $V = R^{m\times 1}$ sowie die lineare Abbildung $f : U \to V : u \mapsto Au$ zur Matrix $A \in R^{m\times n}$.

Wir kennen die Dualräume $U^* \cong R^{1\times n}$ und $V^* \cong R^{1\times m}$ (R1C).
Beschreiben Sie $f^* : V^* \to U^*$ ebenfalls durch eine Matrix.

Lösung: Wir identifizieren jeden Zeilenvektor $v^* \in R^{1\times m} \cong V^*$ mit der zugehörigen Linearform $\varphi_{v^*} : V \to R : v \mapsto v^* \cdot v$, ebenso $R^{1\times n} \cong U^*$.
Dann gilt $f^*(\varphi_{v^*}) = \varphi_{v^*} \circ f : U \to R : u \mapsto Au \mapsto v^*(Au) = (v^*A)u$.

Satz R3C: Dualität und Matrixdarstellung

(1) Für $U = R^{n\times 1}$ und $V = R^{m\times 1}$ sowie $U^* \cong R^{1\times n}$ und $V^* \cong R^{1\times m}$ gilt:

$$f : U \to V : u \mapsto A \cdot u \quad \Longrightarrow \quad f^* : V^* \to U^* : v^* \mapsto v^* \cdot A$$

(2) Ist R ein Divisionsring, so können wir Dimensionen betrachten.
Dank K2J sind $\operatorname{rang}(f) = \operatorname{sr}(A)$ und $\operatorname{rang}(f^*) = \operatorname{zr}(A)$ gleich:

$$\operatorname{rang}(f) = \operatorname{rang}(f^*)$$

Dualität und Matrixdarstellung

⚠ Wenn wir über einem kommutativen Ring arbeiten, so ist es üblich, Matrizen immer links zu schreiben. Dann können wir transponieren, um auch U^* und V^* als Spaltenvektoren darzustellen. Damit gilt:

$$f : R^n \to R^m : u \mapsto A \cdot u \quad \Longrightarrow \quad f^* : R^m \to R^n : (v^*)^\intercal \mapsto A^\intercal \cdot (v^*)^\intercal$$

Die zu f duale Abbildung f^* wird in dieser Schreibweise durch die transponierte Matrix dargestellt. (Das ist möglich, wenn auch künstlich.)

⚠ Über $\mathbb{K} = \mathbb{R}, \mathbb{C}$ nutzen wir gemäß R2I den Anti-Isomorphismus durch Transposition-Konjugation, geschrieben $A \mapsto A^\dagger = \overline{A}^\intercal$:

$$f : \mathbb{K}^n \to \mathbb{K}^m : u \mapsto A \cdot u \quad \Longrightarrow \quad f^* : \mathbb{K}^m \to \mathbb{K}^n : (v^*)^\dagger \mapsto A^\dagger \cdot (v^*)^\dagger$$

Die zu f duale Abbildung f^* wird in dieser Schreibweise durch die transponiert-konjugierte Matrix dargestellt. (Auch das ist oft nützlich.)

🙂 Die natürliche Schreibweise zeigt unser obiger Satz R3C: Eine Transformation von Zeilen- zu Spaltenvektoren wird dabei vermieden. Sie ist möglich, manchmal nützlich, aber auch immer etwas künstlich.

Dualität und Matrixdarstellung

Satz R3D: Dualität und Matrixdarstellung

Seien U und V lineare Räume über R mit endlichen Basen $\mathcal{A} = (a_1, \dots, a_n)$ und $\mathcal{B} = (b_1, \dots, b_m)$. Dann haben wir:

$$\begin{array}{ccc} R^{n\times 1} & \xrightarrow[x\mapsto y = Ax]{A} & R^{m\times 1} \\ {\scriptstyle \Phi_{\mathcal{A}}}\downarrow\cong & & {\scriptstyle \Phi_{\mathcal{B}}}\downarrow\cong \\ U & \xrightarrow[u\mapsto v = f(u)]{f} & V \end{array} \qquad \begin{array}{ccc} R^{1\times n} & \xleftarrow[y^*A = x^* \leftarrow y^*]{A} & R^{1\times m} \\ {\scriptstyle \Phi_{\mathcal{A}^*}}\downarrow\cong & & {\scriptstyle \Phi_{\mathcal{B}^*}}\downarrow\cong \\ U^* & \xleftarrow[f^*(v^*) = u^* \leftarrow v^*]{f^*} & V^* \end{array}$$

Die Abbildung $f : U \to V$ und ihre duale Abbildung $f^* : V^* \to U^*$ werden durch dieselbe Matrix A dargestellt: Im ersten Falle wirkt A von links auf Spaltenvektoren, im zweiten Falle von rechts auf Zeilenvektoren.

⚠ Das ist die natürliche Darstellung mit Zeilen- und Spaltenvektoren. Falls gewünscht können wir anschließend (über einem kommutativen Ring!) Zeilenvektoren zu Spaltenvektoren transponieren.
In diesem Falle wird f durch A und f^* durch $A^\intercal$ dargestellt.

Dualität und Matrixdarstellung

Aufgabe: Alle Daten liegen explizit vor. Rechnen Sie es sorgsam nach!

Lösung: Hier gilt $\Phi_{\mathcal{A}} : x \mapsto u = \sum_j u_j x_{j,1}$ und $\Phi_{\mathcal{B}} : y \mapsto v = \sum_i v_i y_{i,1}$, entsprechend $\Phi_{\mathcal{A}^*} : x^* \mapsto u^* = \sum_j x^*_{1,j} u^*_j$ und $\Phi_{\mathcal{B}^*} : y^* \mapsto v^* = \sum_i y^*_{1,i} v^*_i$.

Für die Matrix $A = (a_{i,j})_{i,j}$ gilt nach Definition $f(u_j) = \sum_i v_i a_{i,j}$, also $f(\sum_j u_j x_{j,1}) = \sum_j \sum_i v_i a_{i,j} x_{j,1} = \sum_i v_i y_{i,1}$ mit $y_{i,1} = \sum_j a_{i,j} x_{j,1}$.
Dies entspricht der Matrixmultiplikation $x \mapsto y = A \cdot x$.

Auf der anderen Seite gilt $f^*(v^*_k)(u_j) = v^*_k(f(u_j)) = v^*_k(\sum_i v_i a_{i,j}) = a_{k,j}$, also $f^*(\sum_k y^*_{1,k} v^*_k)(u_j) = \sum_k y^*_{1,k} a_{k,j}$, somit $f^*(\sum_k y^*_{1,k} v^*_k) = \sum_j x^*_{1,j} u^*_j$ mit $x^*_{1,j} = \sum_k y^*_{1,k} a_{k,j}$. Dies entspricht $y^* \mapsto x^* = y^* \cdot A$.

Bemerkung: Ist R kommutativ, so können wir dies transponieren zu

$$(y^*)^\intercal \mapsto (x^*)^\intercal = A^\intercal \cdot (y^*)^\intercal.$$

Speziell über $R = \mathbb{R}, \mathbb{C}$ können wir dies transponieren-konjugieren zu

$$(y^*)^\dagger \mapsto (x^*)^\dagger = A^\dagger \cdot (y^*)^\dagger.$$

Dualität und Matrixdarstellung

Aufgabe: Wir betrachten die folgenden Sequenzen über $\mathbb{Z}$:

$$\mathbb{Z}^{2\times1} \xrightarrow[f]{\begin{bmatrix}0&0\\1&0\\0&1\end{bmatrix}} \mathbb{Z}^{3\times1} \xrightarrow[g]{\begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix}} \mathbb{Z}^{3\times1}, \qquad 0 \xrightarrow[h]{[0]} \mathbb{Z} \xrightarrow[k]{[2]} \mathbb{Z}$$

(1) Sind diese Sequenzen exakt, gilt hier also „Bild = Kern“?
(2) Wie sehen die dualen Sequenzen aus? Sind diese exakt?

Lösung: (1) Wir vergleichen Bild und Kern:
(a) Es gilt $\operatorname{im}(f) = \langle\, e_2, e_3 \,\rangle^!_{\mathbb{Z}} = \ker(g)$, also exakt.
(b) Hier gilt $\operatorname{im}(h) = \{0\} = \ker(k)$, also ebenfalls exakt.

(2) Die dualen Sequenzen können wir wie folgt darstellen:

$$\mathbb{Z}^{1\times2} \xleftarrow[f^*]{\begin{bmatrix}0&0\\1&0\\0&1\end{bmatrix}} \mathbb{Z}^{1\times3} \xleftarrow[g^*]{\begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix}} \mathbb{Z}^{1\times3}, \qquad 0 \xleftarrow[h^*]{[0]} \mathbb{Z} \xleftarrow[k^*]{[2]} \mathbb{Z}$$

(a) Die linke Sequenz ist exakt, denn $\operatorname{im}(g^*) = \langle\, e_1^* \,\rangle^!_{\mathbb{Z}} = \ker(f^*)$.
(b) Die rechte Sequenz ist nicht exakt, denn $\operatorname{im}(k^*) = 2\mathbb{Z} \neq \mathbb{Z} = \ker(h^*)$.

Dualität und Matrixdarstellung

Konkrete Beispiele wie diese zeigen eindrücklich: Nach Klärung der Grundbegriffe erhalten wir ganz handfeste Objekte und Rechnungen. Insbesondere mit Matrizen können wir wunderbar rechnen!

🙂 Wie im obigen Satz stellen wir die rechtslinearen Räume durch Spaltenvektoren dar und dual hierzu die linkslinearen Räume durch Zeilenvektoren. Wir „kippen“ also die Vektoren, dafür bleiben die Matrizen unverändert. Das vermeidet Fehler und ist narrensicher

Die Matrizen wirken allerdings verschieden: Im ersten Falle von links auf Spaltenvektoren, nach dem Dualisieren von rechts auf Zeilenvektoren!

🙂 Wer möchte kann alles transponieren und so die Matrizen immer von links wirken lassen; das war bisher unsere übliche Konvention.
(Über einem kommutativen Ring so wie hier $\mathbb{Z}$ ist dies erlaubt.)

⚠ Über dem Ring $\mathbb{Z}$ der ganzen Zahlen ist die Dualisierung nicht exakt: Aus exakten Sequenzen macht sie nicht-exakte Sequenzen.
Diesem Problem wollen wir nun auf den Grund gehen.

Dualität und Matrixdarstellung

Bemerkung: In Diracs Bra-Ket-Notation wird die lineare Abbildung A als Operator zwischen dem Bra-Covektor $\langle u|$ und dem Ket-Vektor $|v\rangle$ geschrieben, wie der Sandwichbelag zwischen den beiden Brothälften:

$$\langle\, u \mid A \mid v \,\rangle$$

Diese geschickte Notation entspricht sowohl der linearen Abbildung

$$f : V \to V : |v\rangle \mapsto A|v\rangle$$

auf den Ket-Vektoren als auch zugleich der dualen Abbildung

$$f^* : V^* \to V^* : \langle u| \mapsto \langle u|A$$

auf den Bra-Covektoren. Diese Schreibweise ist genial einfach.

Die gute Notation denkt für uns mit. Daher habe ich in Satz R3C die natürliche Schreibweise mit Zeilen- und Spaltenvektoren betont. Wir *können* zu Spaltenvektoren transponieren (und ggf. konjugieren), aber wir *müssen* es nicht, und meist *wollen* wir dies auch nicht.

Dualität und Matrixdarstellung

Satz R3E: Dualität und Bi/Sur/Injektivität

Seien $f : U \to V$ und $g : V \to U$ linear über dem Ring R.

(1) Ist $(f, g) : U \rightleftarrows V$ ein Retraktionspaar, so auch $(g^*, f^*) : U^* \rightleftarrows V^*$.
(2) Ist $(f, g) : U \cong V$ ein Isomorphismus, so auch $(g^*, f^*) : U^* \cong V^*$.
(3) Ist $f : U \to V$ bijektiv, so ist $f^* : V^* \to U^*$ bijektiv.
(4) Ist $f : U \to V$ surjektiv, so ist $f^* : V^* \to U^*$ injektiv.

Für die folgende Aussage sei R ein Divisionsring:
(5) Ist $f : U \to V$ injektiv, so ist $f^* : V^* \to U^*$ surjektiv.

Beweis: (1) Aus $g \circ f = \mathrm{id}_U$ folgt $f^* \circ g^* = \mathrm{id}_{U^*}$ dank Funktorialität R3B.
(2) Aus $g \circ f = \mathrm{id}_U$ und $f \circ g = \mathrm{id}_V$ folgt $f^* \circ g^* = \mathrm{id}_{U^*}$ und $g^* \circ f^* = \mathrm{id}_{V^*}$.
(3) Ist $f : U \to V$ linear und bijektiv, so auch $g = f^{-1} : V \to U$ (I1G).
Aus $(f, g) : U \cong V$ folgt $(g^*, f^*) : U^* \cong V^*$ dank (2), also ist f^* bijektiv.
(4) Seien $\varphi, \psi \in V^*$ mit $f^*(\varphi) = f^*(\psi)$, also $\varphi \circ f = \psi \circ f$.
Zu jedem $v \in V$ existiert ein $u \in U$ mit $f(u) = v$, also gilt
$\varphi(v) = \varphi(f(u)) = \psi(f(u)) = \psi(v)$. Das bedeutet $\varphi = \psi$.

(5) Sei R ein Divisionsring und hierüber $f : U \to V$ linear und injektiv.
Wir wollen zeigen, dass die duale Abbildung $f^* : V^* \to U^*$ surjektiv ist.
Hierzu konstruieren wir eine Retraktion $(f, g) : U \rightleftarrows V$ und nutzen (1).

Wir wählen eine Basis $(u_i)_{i \in J}$ von U. Wir setzen $v_i = f(u_i)$ für $i \in J$
und ergänzen die Familie $(v_i)_{i \in J}$ zu einer Basis $(v_i)_{i \in J \sqcup K}$ von V. (J2B)

Dank PLF (K1B) existiert $g : V \to U$ linear mit $v_i \mapsto u_i$ für $i \in J$ und
$v_i \mapsto 0$ für $i \in K$. Damit gilt $g \circ f = \mathrm{id}_U$, also $(f, g) : U \rightleftarrows V$.

Daraus folgt $f^* \circ g^* = \mathrm{id}_{U^*}$. Somit ist $f^* : V^* \to U^*$ surjektiv. QED

Ausführlich: Gegeben sei $\psi \in U^*$, also eine Linearform $\psi : U \to R$.
Wir definieren $\varphi : V \to R$ durch $\varphi = \psi \circ g$. Somit gilt $f^*(\varphi) = \psi$,
denn $f^*(\varphi) = (\psi \circ g) \circ f = \psi \circ (g \circ f) = \psi \circ \mathrm{id}_V = \psi$.

Erinnerung: f^* ist **r**echtsinvertierbar, also insbesondere sur**j**ektiv.
Ebenso ist g^* ist l**i**nksinvertierbar, also insbesondere **i**njektiv.

Die Aussagen (1–5) sind nach aufsteigender Schwierigkeit sortiert.
Die Beweise sind eine gute Fingerübung und Wiederholung der Begriffe.

Warum sind die Aussagen (1) und (2) so leicht zu beweisen?
Das liegt gerade an der Funktorialität R3B der Dualisierung:
Gleichungen wie $g \circ f = \mathrm{id}_U$ werden durch den Funktor *
in ebensolche Gleichungen $f^* \circ g^* = \mathrm{id}_{U^*}$ überführt.

Auch die Aussage (3) zu Bijektionen ist leicht zu beweisen, dank (2):
Jede bijektive lineare Abbildung $f : U \to V$ ist ein Isomorphismus (I1G),
lässt sich also zu einem Isomorphismenpaar $(f, g) : U \cong V$ ergänzen.
Das verdanken wir dem glücklichen Umstand, dass die Umkehrfunktion
$g = f^{-1}$ selbst wieder linear ist! Anschließend genügt (2).

Auch (4) ist noch leicht, allein für (5) müssen wir ernsthaft arbeiten.
Die Aussage ohne weitere Voraussetzungen wäre falsch; schon das
deutet bereits darauf hin, dass hier ernsthaft etwas zu beweisen ist:
Basisauswahl und Basisergänzung (J2B).

⚠ Benötigen wir für (5) wirklich einen Divisionsring oder ist dies ein
Artefakt eines ungeschickten Beweises? Hier hilft ein Gegenbeispiel:

Beispiel R3F

Über dem Ring $\mathbb{Z}$ betrachten wir den linearen Raum $V = \mathbb{Z}^{n \times 1}$ und

$$f : V \to V : v \mapsto Av \quad \text{mit} \quad A \in \mathbb{Z}^{n \times n}.$$

Dual hierzu haben wir $V^* \cong \mathbb{Z}^{1 \times n}$ und $f^* : V^* \to V^* : u \mapsto uA$.
(1) Genau dann ist f (bzw. f^*) injektiv, wenn $\det A \neq 0$ gilt.
(2) Genau dann ist f^* (bzw. f) surjektiv, wenn $\det A = \pm 1$ gilt.
Die beiden Eigenschaften (1) und (2) klaffen also auseinander!

Das kleinste Gegenbeispiel entsteht für $n = 1$ und $f : \mathbb{Z} \to \mathbb{Z} : v \mapsto 2 \cdot v$.
Dieser Homomorphismus ist injektiv, doch ihr dualer Homomorphismus
$f^* : \mathbb{Z} \to \mathbb{Z} : u \mapsto u \cdot 2$ ist nicht surjektiv, denn 1 wird nicht getroffen.

Dualität und Exaktheit

Satz R3G: Dualität und Exaktheit

Wir betrachten eine Sequenz von R–linearen Abbildungen und ihr Dual:

$$\cdots \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow \cdots$$
$$\cdots \longleftarrow U^* \xleftarrow{f^*} V^* \xleftarrow{g^*} W^* \longleftarrow \cdots$$

(1) Allgemein gilt:

$$\boxed{\operatorname{im}(f) \subseteq \ker(g) \implies \ker(f^*) \supseteq \operatorname{im}(g^*)}$$

(2) Haben wir zudem $W = \operatorname{im}(g) \oplus W'$, so folgt umgekehrt:

$$\boxed{\operatorname{im}(f) \supseteq \ker(g) \implies \ker(f^*) \subseteq \operatorname{im}(g^*)}$$

(3) Über jedem Divisionsring R ist die Voraussetzung (2) immer erfüllt.
Aus Exaktheit $\operatorname{im}(f) = \ker(g)$ folgt demnach Exaktheit $\ker(f^*) = \operatorname{im}(g^*)$.

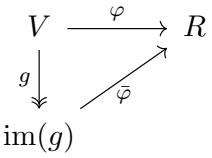
Dualität und Exaktheit

Nochmal die Daten zur Erinnerung:

$$\cdots \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow \cdots$$
$$\cdots \longleftarrow U^* \xleftarrow{f^*} V^* \xleftarrow{g^*} W^* \longleftarrow \cdots$$

Beweis: (1) Gegeben ist $\operatorname{im}(f) \subseteq \ker(g)$. Das bedeutet $g \circ f = 0$.
Dualisieren ergibt $f^* \circ g^* = 0$, und das bedeutet $\ker(f^*) \supseteq \operatorname{im}(g^*)$.

(2) Wir setzen nun $W = \operatorname{im}(g) \oplus W'$ voraus.
Aus $\operatorname{im}(f) \supseteq \ker(g)$ folgern wir $\ker(f^*) \subseteq \operatorname{im}(g^*)$:



Sei $\varphi \in \ker(f^*)$, also $\varphi \in V^*$ mit $0 = f^*(\varphi) = \varphi \circ f$.
Das bedeutet $\operatorname{im}(f) \subseteq \ker(\varphi)$, somit $\ker(g) \subseteq \ker(\varphi)$.

Dank Faktorisierung (Satz I2E) existiert $\bar{\varphi} : \operatorname{im}(g) \to R$ mit $\varphi = \bar{\varphi} \circ g$,
und dank $W = \operatorname{im}(g) \oplus W'$ eine Fortsetzung $\psi : W \to R$ mit $\psi|_{\operatorname{im}(g)} = \bar{\varphi}$.

Somit gilt $g^*(\psi) = \psi \circ g = \bar{\varphi} \circ g = \varphi$, also $\varphi \in \operatorname{im}(g^*)$. QED

Nochmal Dualität und Sur/In/Bijektivität

Beispiel R3H: nochmal Dualität und Sur/In/Bijektivität

Sei $f : U \to V$ linear über R und $f^* : V^* \to U^*$ dual hierzu.

(1) Ist f surjektiv, so ist f^* injektiv:

$$U \xrightarrow{f} V \xrightarrow{0} 0 \qquad \text{exakt}$$
$$U^* \xleftarrow{f^*} V^* \xleftarrow{0} 0 \qquad \text{exakt}$$

(2) Ist f injektiv mit $V = \operatorname{im}(f) \oplus V'$, so ist f^* surjektiv:

$$0 \xrightarrow{0} U \xrightarrow{f} V \qquad \text{exakt}$$
$$0 \xleftarrow{0} U^* \xleftarrow{f^*} V^* \qquad \text{exakt}$$

(3) Ist f bijektiv, so auch f^*:

$$0 \xrightarrow{0} U \xrightarrow{f} V \xrightarrow{0} 0 \qquad \text{exakt}$$
$$0 \xleftarrow{0} U^* \xleftarrow{f^*} V^* \xleftarrow{0} 0 \qquad \text{exakt}$$

Nochmal Dualität und Sur/In/Bijektivität

🙂 Die Schreibweise als exakte Sequenz bündelt nützliche Information.
Nun erhalten wir nützliche Rechenregeln für exakte Sequenzen.

⚠ In (2) ist die zusätzliche Voraussetzung $V = \operatorname{im}(f) \oplus V'$ zwar lästig, aber doch wesentlich. Andernfalls finden wir Gegenbeispiele:

$$0 \xrightarrow[h]{0} \mathbb{Z} \xrightarrow[k]{2} \mathbb{Z} \qquad \text{exakt}$$

$$0 \xleftarrow[h^*]{0} \mathbb{Z} \xleftarrow[k^*]{2} \mathbb{Z} \qquad \text{nicht exakt}$$

Hier erlaubt das Bild $\operatorname{im}(k) = 2\mathbb{Z}$ in $\mathbb{Z}$ kein Komplement. Tatsächlich ist die duale Sequenz nicht exakt, denn es gilt $\operatorname{im}(k^*) = 2\mathbb{Z} \neq \mathbb{Z} = \ker(h^*)$.

🙂 Über einem Divisionsring R ist die Voraussetzung (2) immer erfüllt.
Dualisierung überführt also exakte Sequenzen in exakte Sequenzen.

Beispiel: Einschränkung auf $U \leq V$

Beispiel R3I: Einschränkung auf $U \leq V$

(0) Die Inklusion $\iota = \mathrm{inc}_U^V : U \hookrightarrow V : u \mapsto u$ induziert die Einschränkung

$$\iota^* \,:\, V^* \to U^* \,:\, \varphi \mapsto \varphi \circ \iota = \varphi|_U.$$

(1) Ihr Kern ist der Annulator

$$\ker(\iota^*) = \{\, \varphi \in V^* \mid \varphi|_U = 0 \,\} = U^\circ.$$

(2) Wir erhalten so die exakte Sequenz

$$0 \longrightarrow U^\circ \xhookrightarrow{\mathrm{inc}} V^* \xrightarrow{\iota^*} U^*.$$

(3) Gilt zudem $V = U \oplus U'$, so erhalten wir die kurze exakte Sequenz

$$0 \longrightarrow U^\circ \xhookrightarrow{\mathrm{inc}} V^* \xrightarrow{\iota^*} U^* \longrightarrow 0.$$

(4) Über einem Divisionsring gilt Letzteres immer.

Beispiel: Einschränkung auf $U \leq V$

☺ Die Inklusion $\iota : U \hookrightarrow V$ und die Einschränkung $\iota^* : V^* \to U^*$ sind besonders nützlich, anschaulich und einfach zu verstehen.

Insbesondere finden wir hier erneut den Annulator $\ker(\iota^*) = U^\circ$. Auch dieser Begriff reiht sich so in unseren Werkzeugkasten ein.

Diesen Zusammenhang nutzen wir im folgenden Korollar und Anwendungsbeispiel zu den Rechenregeln für den Annulator.

Annulator des Kerns und Bild des Duals

Korollar R3J: Annulator des Kerns und Bild des Duals

Sei R ein Ring und $f : U \to V$ linear mit $V = \mathrm{im}(f) \oplus V'$.

(0) Ist R ein Divisionsring, so ist Letzteres immer erfüllt.

(1) Dank Satz R3G erhalten wir zwei exakte Sequenzen:

$$\ker(f) \xhookrightarrow{\iota} U \xrightarrow{f} V$$
$$\ker(f)^* \xleftarrow{\iota^*} U^* \xleftarrow{f^*} V^*$$

(2) Für $\iota^* : \varphi \mapsto \varphi \circ \iota$ gilt $\ker(\iota^*) = \ker(f)^\circ$. Daraus folgt

$$\boxed{(\ker f)^\circ = \mathrm{im}(f^*)}$$

Ohne die Voraussetzung $V = \mathrm{im}(f) \oplus W$ gilt im Allgemeinen nur

$$(\ker f)^\circ \supseteq \mathrm{im}(f^*).$$

Beispiel: Für $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto 2x$ gilt $(\ker f)^\circ = \mathbb{Z} \supsetneq 2\mathbb{Z} = \mathrm{im}(f^*)$.

Rechenregeln für den Annulator

☺ Mit unseren so geschärften Werkzeugen vollenden wir Satz R2C:

Beispiel R3K: Rechenregeln für den Annulator

Für jede Familie $(A_i)_{i\in I}$ von Unterräumen $A_i \leq V$ gilt:

$$(\textstyle\sum_{i\in I} A_i)^\circ = \bigcap_{i\in I} A_i^\circ \quad \text{und} \quad (\bigcap_{i\in I} A_i)^\circ \supseteq \sum_{i\in I} A_i^\circ$$

Gleichheit gilt hier, falls R ein Divisionsring ist und die Menge I endlich.

Beweis: Nach Satz R2C zeigen wir nur noch die letzte Aussage.

Für den Quotienten $f_i : V \twoheadrightarrow V/A_i$ gilt $\ker(f_i) = A_i$, also $\mathrm{im}(f_i^*) = A_i^\circ$. Da die Indexmenge I endlich ist, können wir dies zusammensetzen zu

$$f \,:\, V \to \textstyle\prod_{i\in I} V/A_i = \bigoplus_{i\in I} V/A_i \,:\, v \mapsto (f_i(v))_{i\in I}.$$

Hier gilt $\ker(f) = \bigcap_{i\in I} A_i$. Dank R3J gilt $(\ker f)^\circ = \mathrm{im}(f^*)$, wobei

$$f^* \,:\, \textstyle\bigoplus_{i\in I} (V/A_i)^* \to V^* \,:\, (\varphi_i)_{i\in I} \mapsto \sum_{i\in I} f_i^*(\varphi_i).$$

Daraus erhalten wir $(\bigcap_{i\in I} A_i)^\circ = (\ker f)^\circ = \mathrm{im}(f^*) = \sum_{i\in I} A_i^\circ$. QED

Kapitel S

Tensorprodukt

Was ist das Tensorprodukt? Da stellen wir uns ganz dumm.
Jeder weiß, dass man Vektoren untereinander zwar addieren kann,
aber allgemein nicht multiplizieren. Wir tun es einfach trotzdem!
Das universelle Ergebnis ist das Tensorprodukt.

frei nach Prof. Günter Harder

Inhalt dieses Kapitels S

Tensorprodukte: grundlegend & allgemein = schwierig?

Wir sind auf der Zielgeraden dieser Vorlesung zur Linearen Algebra.
Zum krönenden Abschluss behandeln wir das Tensorprodukt, zunächst über einem Körper (§S1), das vereinfacht, dann über beliebigen Ringen (§S2). Die Grundidee ist im Eingangszitat treffend zusammengefasst:

Wir multiplizieren Vektoren, naiv-mutig und so allgemein wie möglich.
(Ich zitiere hier frei aus meinem Gedächtnis, wie Prof. Günter Harder in seinen Bonner Algebra-Vorlesungen das Tensorprodukt resümierte.)
Etwas präziser gesagt, das Tensorprodukt realisiert folgendes Ziel:

> *Wir betrachten bilineare oder allgemein multilineare Abbildungen;*
> *mit dem Tensorprodukt können wir diese „universell linearisieren“.*

Wie alle neuen Werkzeuge kostet das Tensorprodukt anfangs Mühe, doch wie immer lohnt sich auch hier die langfristige Investition.
Um auch kurzfristig schon erste schöne Anwendungen zu zeigen, beginne ich über einem Körper mit dem „Tensorprodukt für Eilige.“

Tensorprodukte: grundlegend & allgemein = schwierig?

Zudem wage ich den Blick über den Tellerrand und diskutiere Anwendungen in der Quantenmechanik. Das zeigt zweierlei:

1. Die mathematischen Grundlagen sind vergleichsweise leicht.
2. Die Anwendungen sind erstaunlich vielseitig und komplex.

Schon die ersten Anwendungen sind spektakulär. Wer diese dennoch nicht wünscht oder braucht, kann die physikalische Einkleidung auch ignorieren und sich auf den mathematischen Kern konzentrieren. Abfragen werde ich es nicht, anbieten will ich es auf jeden Fall.

Erfahrungsgemäß ist es nämlich hilfreich, zu mathematischen Begriffen auch geometrische Anschauung und physikalische Intuition zu schulen. Dies dient der naturwissenschaftlich-technischen Allgemeinbildung und nützt auch direkt dem mathematischen Verständnis beim Lernen.

Mathematik (gr. μαθηματική τέχνη) ist die ‘Kunst des Erkennens’.

Woher kommen Tensoren?

Wie so viele fundamentale Begriffe wurden **Tensoren** ursprünglich in der Physik eingeführt und erst später mathematisch präzisiert. Das ist kein Makel, sondern Beleg ihrer tiefliegenden Bedeutung.

In der theoretischen Physik werden „Tensoren“ seit langem verwendet, da sie zur effizienten Modellbildung nützen und in Rechnungen helfen. Dabei werden diese „Tensoren“ zunächst ganz pragmatisch durch ihre **Rechenregeln** eingeführt… der Erfolg heiligt bekanntlich die Mittel.

Diesen Zugang „für Eilige“ möchte ich unten als erstes vorstellen. Das entspricht recht genau der ideengeschichtlichen Entwicklung, und auch heute noch antwortet es aus didaktisch-physikalischer Sicht sehr direkt und auch motivierend auf die Frage: Was sind Tensoren?

Wahre Begebenheit: Der Einstieg dieses Kapitels entstand auf die sorgenvolle Frage meines Sohnes, was er mit Tensoren anfangen soll… Wir wollen und können Tensoren anpacken und sofort damit rechnen!

Wo werden Tensoren genutzt?

Aus **mathematischer Sicht** dauerte es hingegen etwas länger, bis es Mathematiker/innen schließlich gelang, für diese „Tensoren“ eine befriedigende theoretische Grundlage zu finden und zu erklären.

Seither werden sie auch in der Mathematik recht vielseitig genutzt und angewendet, insbesondere in der Algebra und der Differentialgeometrie, zudem in den Ingenieurwissenschaften (etwa der Mechanik, Elastizität, Strömungslehre, Elektrodynamik, …) und der theoretischen Physik, von der Quantenmechanik bis zur Relativitätstheorie.

Dabei werden Tensoren meist zu Tensorfeldern verallgemeinert, die abkürzend-schludrig meist ebenfalls Tensoren genannt werden.

Ein Tensorfeld ordnet jedem Punkt des Raums einen Tensor zu. Viele naturwissenschaftliche Modelle und physikalische Theorien nutzen Tensorfelder, allen voran die allgemeine Relativitätstheorie, die damit die gekrümmte Geometrie der Raumzeit beschreibt. Das zugehörige mathematische Teilgebiet heißt Tensoranalysis.

Tensoren als Größen mit Indizes

Tensoren sind ein **Hilfsmittel** zur Beschreibung eines dahinterliegenden Objekts, das uns eigentlich interessiert, etwa eine lineare Abbildung oder eine Bilinearform uvm. Das Ergebnis unserer Rechnungen soll dabei invariant sein, also dasselbe in jedem Koordinatensystem.

0. Stufe: Wir beginnen viele unserer Rechnungen mit einem Skalar a: Dies ist einfach ein Element des Grundkörpers K, etwa $\mathbb{R}$ oder $\mathbb{C}$.

1. Stufe: Eine Folge $b = (b_1, \dots, b_k)$ solcher Skalare fassen wir zu einem neuen Objekt zusammen und rechnen damit als vektorielle Größe. Solch ein Vektor $b = (b_i)_i$ hat dabei einen einzigen Index i.

2. Stufe: Eine Folge von Vektoren $c = (c_{ij})_{ij}$ hat demnach zwei Indizes. Warum sagen wir nicht einfach „Matrix“? Tensoren sind allgemeiner!

3. Stufe: Ein Tensor $d = (d_{ijk})_{ijk}$ kann drei (oder mehr) Indizes haben, wie etwa das Levi-Civita-Symbol $\varepsilon_{ijk} = \operatorname{sign}(i, j, k)$ für $i, j, k \in \{1, 2, 3\}$. Die anfängliche Analogie mit Matrizen bricht daher schnell zusammen. Wir untersuchen Tensoren als eigene, universelle Konstruktion.

Wie erklären wir Tensoren mathematisch?

Tensoren sind ein vielseitiges und nützliches Werkzeug der Mathematik. Es lohnt sich daher, Zeit in diesen grundlegenden Begriff zu investieren, gerade zum Übergang von „koordinatengebunden“ zu „koordinatenfrei“. Das ist sehr präzise, doch abstrakt, und daher nicht allgemein beliebt.

Zur Motivation beginne ich mit meiner kurzen Vorschau „für Eilige“ und einer ersten spektakulären Anwendung in der Quantenmechanik: dem sogenannten No-Cloning-Theorem. Soviel Physik muss sein!

Zum Einstieg betone ich die **universelle Basiseigenschaft** S1B, die den Rechnungen zugrundeliegt und sofortigen Zugang ermöglicht.

Anschließend beschäftigen wir uns sorgsam und geduldig mit der mathematischen Grundlegung: Der richtige Ausgangspunkt ist hier die **universelle Abbildungseigenschaft** (S2E). Anschließend erarbeiten wir ihre segensreichen Konsequenzen wie die Basiseigenschaft S2G.

Dabei gehe ich den langen Weg und beginne so allgemein wie möglich: Wir legen das Thema breit an und spezialisieren dann schrittweise.

Erinnerung: das kartesische Produkt als direkte Summe

Satz S1A: das kartesische Produkt als direkte Summe

Gegeben seien zwei Vektorräume U und V über einem Körper K.

(1) Zu U, V haben wir das kartesische Produkt als **direkte Summe**:

$$U \times V := \{\, (u,v) \mid u \in U,\, v \in V \,\} = U' \oplus V'$$
$$\text{mit} \quad (i_1, p_1) : U \cong U' := U \times \{0\} : u \leftrightarrows (u,0)$$
$$\text{und} \quad (i_2, p_2) : V \cong V' := \{0\} \times V : v \leftrightarrows (0,v)$$

(2) Zu je zwei gegebenen Basen $(u_i)_{i\in I}$ von U und $(v_j)_{j\in J}$ von V ist ihre Aneinanderhängung $(w_k)_{k\in I \sqcup J}$ eine Basis des Raums $U \times V$, wobei $I \cap J = \emptyset$ und $w_i = (u_i, 0)$ für $i \in I$ und $w_j = (0, v_j)$ für $j \in J$.

(3) Insbesondere addieren sich die Dimensionen:

$$\dim(U' \oplus V') = \dim(U') + \dim(V')$$

🙂 Damit können wir konkret rechnen, denn alles liegt explizit vor!

Erinnerung: das kartesische Produkt als direkte Summe

Dieser Satz dient als freundliche Erinnerung und Zusammenfassung von zwei universell nützlichen Konstruktionen: Produkt vs Summe.

Aus mengentheoretischer Sicht konstruieren wir den Raum $U \times V$ als kartesisches Produkt mit koordinatenweiser Addition und Skalierung. Aus Sicht der linearen Räume betrachten wir dies als direkte Summe. genauer $U \times V = U' \oplus V'$ mit den Kopien U' und V' von U und V.

Allgemein unterscheiden wir das Produkt $\prod_{i\in I} V_i$ und die (externe / interne) direkte Summe $\bigoplus_{i\in I} V_i$. Allgemein gilt hierbei die Inklusion $\bigoplus_{i\in I} V_i \leq \prod_{i\in I} V_i$, und Gleichheit gilt für jede endliche Indexmenge I.

Die Konstruktion einer Basis durch Aneinanderhängen zeigt: Die Dimension der Summe ist die Summe der Dimensionen. Mit dieser Konstruktion können wir Vektorräume addieren. Als nächstes wollen wir Vektorräume auch multiplizieren.

Vorschau: das Tensorprodukt für Eilige

Definition S1B: das Tensorprodukt und seine Basiseigenschaft

Gegeben seien drei Vektorräume U, V und W über einem Körper K.

(1) Ein **Produkt** von U und V nach W ist eine K–bilineare Abbildung

$$\otimes : U \times V \to W : (u,v) \mapsto w = u \otimes v.$$

Das heißt ausgeschrieben für alle $u, u' \in U$ und $v, v' \in V$ und $\lambda \in K$:

$$(u+u') \otimes v = (u \otimes v) + (u' \otimes v), \qquad (\lambda u) \otimes v = \lambda(u \otimes v),$$
$$u \otimes (v+v') = (u \otimes v) + (u \otimes v'), \qquad u \otimes (v\lambda) = (u \otimes v)\lambda.$$

(2) Wir nennen $\otimes$ ein **Tensorprodukt** von U und V in den **Tensorraum** $W = U \otimes V$, falls zudem folgende **universelle Basiseigenschaft** gilt:

Zu je zwei gegebenen Basen $(u_i)_{i\in I}$ von U und $(v_j)_{j\in J}$ von V ist die Produktfamilie $(u_i \otimes v_j)_{(i,j)\in I\times J}$ eine Basis des Zielraums W.

(3) Insbesondere multiplizieren sich die Dimensionen:

$$\dim(U \otimes V) = \dim(U) \cdot \dim(V)$$

Vorschau: das Tensorprodukt für Eilige

🙂 Damit können wir konkret rechnen, denn wir haben eine Basis!

Diese Definition über die universelle Basiseigenschaft ist die schnellste, doch nicht unbedingt die beste. Wir optimieren und verallgemeinern sie später zur universellen Abbildungseigenschaft (Definition S2E).

Über einem Körper sind beide Eigenschaften äquivalent (Satz S2G), daher beginne ich hier mit dem einfacheren Spezialfall.

🙂 Satz S1A(1) konstruiert explizit den Vektorraum $U \times V = U' \oplus V'$. Daraus ziehen wir Folgerungen für (2) Basen und (3) Dimensionen.

Definition S1B erklärt die geforderten Eigenschaften (1) und (2). Wir beweisen später die Existenz (etwa durch Matrizen S1C oder Polynome S1D, oder ganz allgemein basisfrei als Quotienten S2I) und die Eindeutigkeit (bis auf eindeutige Isomorphie, Satz S2H).

🙂 Definition S1B enthält vorab schon genug Information, um sofort damit rechnen zu können, daher der Slogan „Tensorprodukt für Eilige“.

Wie rechnen wir mit Tensoren?

Aufgabe: (1) Nennen Sie eine Basis des Tensorraums $\mathbb{R}^2 \otimes \mathbb{R}^2$.
(2) Sind darin die Tensoren $(0,1) \otimes (1,0)$ und $(1,0) \otimes (0,1)$ gleich?

Lösung: (1) Wir wählen die Standardbasis (e_1, e_2) für $U = V = \mathbb{R}^2$.
Für den Tensorraum $W = U \otimes V$ erhalten wir daraus die Produktbasis

$$(e_1 \otimes e_1,\ e_1 \otimes e_2,\ e_2 \otimes e_1,\ e_2 \otimes e_2).$$

(2) Damit können wir die Tensoren $e_2 \otimes e_1$ und $e_1 \otimes e_2$ vergleichen:

$$e_2 \otimes e_1 = 0 \cdot (e_1 \otimes e_1) + 0 \cdot (e_1 \otimes e_2) + 1 \cdot (e_2 \otimes e_1) + 0 \cdot (e_2 \otimes e_2)$$
$$e_1 \otimes e_2 = 0 \cdot (e_1 \otimes e_1) + 1 \cdot (e_1 \otimes e_2) + 0 \cdot (e_2 \otimes e_1) + 0 \cdot (e_2 \otimes e_2)$$

☺ Die Tensoren $e_2 \otimes e_1$ und $e_1 \otimes e_2$ in $W = U \otimes V$ sind verschieden!

In diesem schönen Beispiel stört nur der numerische Zufall $2 \cdot 2 = 2 + 2$.
Erinnerung: Beim Tensorprodukt multiplizieren sich die Dimensionen.
Das Tensorprodukt $\mathbb{R}^3 \otimes \mathbb{R}^5$ etwa hat die Dimension $3 \cdot 5 = 15$,
die Summe $\mathbb{R}^3 \oplus \mathbb{R}^5$ hingegen hat die Dimension $3 + 5 = 8$.

Wie rechnen wir mit Tensoren?

☺ Definition S1B begründet das folgende Vergleichsverfahren:

Algo S1B: Vergleich von zwei Tensoren in $U \otimes V$

Eingabe: zwei Elemente w_1, w_2 des Tensorraums $U \otimes V$
Ausgabe: „gleich“ falls $w_1 = w_2$ oder „ungleich“ falls $w_1 \neq w_2$

1: Schreibe w_1 und w_2 in der gewählten Produktbasis von $U \otimes V$
2: Vergleiche diese Linearkombinationen koeffizientenweise

Mit diesem einfachen Trick haben wir die vorige Aufgabe gelöst,
und genau so gelingt es für jedes Tensorprodukt über einem Körper.

Dies betont die Bedeutung der universellen Basiseigenschaft S1B:
So können wir alle Elemente eindeutig darstellen und vergleichen.

Zum effektiven Rechnen gehört wie immer als allererster Schritt,
je zwei Elemente auf Un/Gleichheit prüfen zu können.

Wie rechnen wir mit Tensoren?

Definition S1B: einfache Tensoren

(4) Für Tensorprodukte vereinbaren wir folgende Sprechweisen.
Jedes Element $w \in U \otimes V$ des Tensorraums nennen wir einen **Tensor**.

Hat $w \in U \otimes V$ die besonders einfache Form $w = u \otimes v$ mit $u \in U$ und $v \in V$, so nennen wir den Tensor w **einfach** oder **elementar** oder **rein**.

Anders gesagt, die Menge der **einfachen Tensoren** ist das Bild der Produktabbildung $\otimes : U \times V \to U \otimes V$. Diese ist i.A. nicht surjektiv!

Der Tensorraum entsteht aus allen **Summen** einfacher Tensoren;
solche Summen sind im Allgemeinen keine einfachen Tensoren.

Der Tensorraum erlaubt immer eine **Basis** aus einfachen Tensoren,
zum Beispiel jede Produktbasis. Es gibt viele weitere Möglichkeiten.

Übung: Finden Sie in $\mathbb{R}^2 \otimes \mathbb{R}^2$ eine Basis aus vier Tensoren,
von denen *keiner* einfach ist. (Die nächste Aufgabe hilft dabei.)

Wie rechnen wir mit Tensoren?

Aufgabe: Im Tensorraum $W = \mathbb{R}^2 \otimes \mathbb{R}^2$ betrachten wir den allgemeinen Tensor $w = a \cdot (e_1 \otimes e_1) + b \cdot (e_1 \otimes e_2) + c \cdot (e_2 \otimes e_1) + d \cdot (e_2 \otimes e_2)$.
Genau dann ist w einfach, also $w = u \otimes v$, wenn $ad - bc = 0$ gilt.

Lösung: (1) Die Implikation „⇒“ ist klar, denn wir finden

$$\begin{aligned} w = u \otimes v &= (u_1 e_1 + u_2 e_2) \otimes (v_1 e_1 + v_2 e_2) \\ &= u_1 v_1 (e_1 \otimes e_1) + u_1 v_2 (e_1 \otimes e_2) + u_2 v_1 (e_2 \otimes e_1) + u_2 v_2 (e_2 \otimes e_2). \end{aligned}$$

Für diesen Tensor w gilt somit $ad - bc = u_1 v_1 \cdot u_2 v_2 - u_1 v_2 \cdot u_2 v_1 = 0$.

(2) Die Umkehrung „⇐“ ist interessanter. Der Fall $w = 0$ ist dabei klar.
Sei also $w \neq 0$, etwa $a \neq 0$. Für $u = ae_1 + ce_2$ und $v = 1e_1 + (b/a)e_2$
gilt dann $u \otimes v = w$. Die Fälle $b \neq 0$, $c \neq 0$, $d \neq 0$ sind analog.

Folgerung: Gilt $\dim U \geq 2$ und $\dim V \geq 2$, so ist die Produktabbildung $\otimes : U \times V \to U \otimes V$ nicht surjektiv, d.h. nicht jeder Tensor ist einfach.

Matrizen als vertrautes Beispiel

Beispiel S1C: Matrixmodell des Tensorprodukts

Wir betrachten $U = K^{p\times 1}$ und $V = K^{1\times q}$ sowie $W = K^{p\times q}$ mit

$$\cdot : K^{p\times 1} \times K^{1\times q} \to K^{p\times q} : (u, v) \mapsto u \cdot v.$$

Dieses Matrixprodukt bedeutet ausgeschrieben für $(p, q) = (3, 4)$:

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \cdot \boxed{\begin{bmatrix} v_1 & v_2 & v_3 & v_4 \end{bmatrix}} = \boxed{\begin{bmatrix} u_1v_1 & u_1v_2 & u_1v_3 & u_1v_4 \\ u_2v_1 & u_2v_2 & u_2v_3 & u_2v_4 \\ u_3v_1 & u_3v_2 & u_3v_3 & u_3v_4 \end{bmatrix}}$$

Es erfüllt die geforderten Eigenschaften eines Tensorprodukts:

1. Die Produktabbildung $\cdot$ ist bilinear über dem Grundkörper K.
2. Aus den Basen $(e_1, \dots, e_p)$ von $K^{p\times 1}$ und $(e_1^\intercal, \dots, e_q^\intercal)$ von $K^{1\times q}$ erhalten wir die Produktbasis $(e_{i,j} = e_i \cdot e_j^\intercal)_{i=1,\dots,p}^{j=1,\dots,q}$ von $K^{p\times q}$.

So unterscheiden wir $\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 1 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right]$ und $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ (S105).

Matrizen als vertrautes Beispiel

Notation: Für dieses **dyadische Produkt** nutzt man üblicherweise die bequeme Schreibweise $\otimes : K^p \times K^q \to K^{p\times q} : (u_i)_i \otimes (v_j)_j = (u_iv_j)_{i,j}$.

Dies verallgemeinern wir später zum Kronecker Produkt (S2P); hier sehen wir den Spezialfall $\otimes : K^{p\times 1} \times K^{1\times q} \to K^{p\times q}$.

Aufgabe: Einfache Tensoren sind genau die Matrizen vom Rang ≤ 1.

Lösung: „$\Rightarrow$“: Für $u \in K^{p\times 1}$ und $v \in K^{1\times q}$ hat $w = uv$ den Rang ≤ 1, denn alle Spalten der Matrix w sind Vielfache des Spaltenvektors u.

Ebenso: Alle Zeilen von w sind Vielfache des Zeilenvektors v.
Wir erinnern uns: Es gilt Zeilenrang gleich Spaltenrang. (K2J)

„$\Leftarrow$“: Hat $w \in K^{p\times q}$ den Rang 1, so enthält w einen Spaltenvektor $u \in K^{p\times 1} \setminus \{0\}$, und alle anderen Spalten sind Vielfache von u.

Also existiert ein Zeilenvektor $v \in K^{1\times q} \setminus \{0\}$, sodass $w = uv$ gilt.
Hat w den Rang 0, so gilt $w = 0$, also $w = uv$ mit $u = 0$ oder $v = 0$.

Matrizen als vertrautes Beispiel

Aufgabe: Hat die Matrixmultiplikation $\cdot : K^{p\times r} \times K^{r\times q} \to K^{p\times q}$ allgemein für $r \in \mathbb{N}$ die Eigenschaften eines Tensorprodukts?

Lösung: Nein. Das Produkt $\cdot : K^{p\times r} \times K^{r\times q} \to K^{p\times q}$ ist zwar bilinear, aber für $r \geq 2$ fehlt ihm die geforderte universelle Basiseigenschaft:

Zu Basen $(u_i)_{i\in I}$ von $U = K^{p\times r}$ und $(v_j)_{j\in J}$ von $V = K^{r\times q}$ ist die Produktfamilie $(u_i \otimes v_j)_{(i,j)\in I\times J}$ keine Basis des Raums $W = K^{p\times q}$.

Wir sehen dies bereits an den Dimensionen, denn die erwartete Multiplikativität $pr \cdot rq \overset{!}{=} pq$ ist wegen $p, q \geq 1$ nur für $r = 1$ möglich.

🙂 Für $r = 1$ erhalten wir gerade das obige Beispiel S1C. Für $r \geq 2$ erhalten wir Produkte, die nicht die universelle Basiseigenschaft haben. Für unsere Repertoire an Gegen/Beispielen ist das ebenso nützlich. Das Kronecker–Produkt S2P erweist sich hier als Tensorprodukt.

Matrizen als vertrautes Beispiel

Aufgabe: Zeigen Sie, dass für je zwei endlich-dimensionale Räume U und V über K ein Tensorprodukt $\otimes : U \times V \to U \otimes V$ existiert.

Lösung: Nach Wahl von Basen haben wir $U \cong K^p$ und $V \cong K^q$.
Für die Modellräume K^p und K^q haben wir das obige Tensorprodukt

$$\otimes : K^p \times K^q \to K^{p\times q} : (u_i)_i \otimes (v_j)_j = (u_iv_j)_{i,j}.$$

Die Komposition $U \times V \xrightarrow{\sim} K^p \times K^q \to K^{p\times q}$ ist bilinear und hat die universelle Basiseigenschaft, ist also ein Tensorprodukt von U und V.

🙂 Diese Konstruktion ist zwar korrekt, doch irgendwie „quick and dirty“. Die Wahl einer Basis ist immer ein Akt der Willkür, ganz besonders hier. Zudem gelingt dieser Trick zunächst nur in endlicher Dimension.

🙂 Wir werden in Satz S2I eine allgemeine und basisfreie Konstruktion ausführen, statt „quick and dirty“ ist sie „long-lasting and elegant“.

Polynome als vertrautes Beispiel

Beispiel S1D: Polynommodell des Tensorprodukts

Wir betrachten $U = K[X]$ und $V = K[Y]$ und $W = K[X,Y]$ mit

$$\cdot : K[X] \times K[Y] \to K[X,Y] : (u,v) \mapsto u \cdot v.$$

Dieses Polynomprodukt bedeutet ausgeschrieben:

$$\left[\sum_{i\in\mathbb{N}} u_i X^i\right] \cdot \left[\sum_{j\in\mathbb{N}} v_j Y^j\right] \;=\; \sum_{(i,j)\in\mathbb{N}^2} u_i v_j X^i Y^j$$

Es erfüllt die geforderten Eigenschaften eines Tensorprodukts:

1. Die Produktabbildung $\cdot$ ist bilinear über dem Grundkörper K.
2. Aus den Monombasen $(X^i)_{i\in\mathbb{N}}$ von $K[X]$ und $(Y^j)_{j\in\mathbb{N}}$ von $K[Y]$ erhalten wir die Produktbasis $(X^iY^j)_{(i,j)\in\mathbb{N}^2}$ von $K[X,Y]$.

Dasselbe gilt endlich-dimensional für $U = K[X]_{<p}$ und $V = K[Y]_{<q}$ mit $W = \langle\, X^iY^j \mid i < p,\, j < q \,\rangle_K^!$ und entspricht dem obigen Matrixmodell.

So interpretieren wir $(0,1) \otimes (1,0)$ als $(0X^0 + 1X^1) \cdot (1Y^0 + 0Y^1) = X$, hingegen $(1,0) \otimes (0,1)$ als $(1X^0 + 0X^1) \cdot (0Y^0 + 1Y^1) = Y$ (S105).

Polynome als vertrautes Beispiel

🙂 Die Definition S1B über die universelle Basiseigenschaft funktioniert problemlos auch für unendlich-dimensionale Räume, wie hier zu sehen.

Aufgabe: Hat die Polynommultiplikation $\cdot : K[X] \times K[X] \to K[X]$ in einer Variablen ebenfalls die Eigenschaften eines Tensorprodukts?

Lösung: Nein. Das Produkt $\cdot : K[X] \times K[X] \to K[X]$ ist zwar bilinear, aber ihm fehlt leider die geforderte universelle Basiseigenschaft:

⚠ Zu den Basen $(X^i)_{i\in\mathbb{N}}$ von $U = K[X]$ und $(X^j)_{j\in\mathbb{N}}$ von $V = K[X]$ ist die Produktfamilie $(X^{i+j})_{(i,j)\in\mathbb{N}^2}$ keine Basis des Raums $W = K[X]$.

⚠ Die beiden Familien $(X^{i+j})_{(i,j)\in\mathbb{N}^2}$ und $(X^k)_{k\in\mathbb{N}}$ beschreiben zwar dieselben Teilmengen in $K[X]$, sind aber dennoch sehr verschieden. Die zweite ist linear unabhängig, sogar eine Basis, die erste nicht!

🙂 Die Forderungen an das Tensorprodukt bedeuten anschaulich: (1) Es ist tatsächlich ein Produkt, also bilinear. (2) Dieses Produkt ist so frei wie möglich, das heißt, es erfüllt die universelle Basiseigenschaft.

Polynome als vertrautes Beispiel

Die Frage, wann ein Tensor einfach ist, führt uns in diesem konkreten Beispiel zurück auf die allgegenwärtige Zerlegung von Polynomen:

Übung: Wir betrachten $\cdot : K[X]_{\le p} \times K[X]_{\le q} \to K[X]_{\le p+q}$ für $p = q = 1$.
(1) Über $K = \mathbb{Q}$: Das Polynom $R = X^2 - 2 \in \mathbb{Q}[X]_{\le 2}$ liegt nicht im Bild.
(2) Über $K = \mathbb{R}$: Das Polynom $S = X^2 + 1 \in \mathbb{R}[X]_{\le 2}$ liegt nicht im Bild.

Polynome als vertrautes Beispiel

Die universelle Basiseigenschaft S1B(2) bezieht sich auf eine Basis, und diese dürfen wir willkürlich wählen. War ist mit anderen Basen?

Übung: Gilt die universelle Basiseigenschaft für ein Paar von Basen, so gilt sie für jedes Paar von Basen. Wie zeigen Sie das geschickt?
(Die universelle Abbildungseigenschaft S2E klärt dies elegant!)

Exkurs: von klassischer Physik zur Quantenphysik

Die **klassische Physik** beschreibt den Zustand eines Systems durch deterministische Größen, etwa Massen $m_k \in \mathbb{R}$ mit Positionen $u_k \in \mathbb{R}^3$ und Geschwindigkeiten $v_k \in \mathbb{R}^3$ wie in **Newtons Himmelsmechanik:**

$$\dot{u}_k = v_k, \quad \dot{v}_k = f_k(u) := \sum\nolimits_{j \neq k} \gamma\, m_j \frac{u_j - u_k}{\|u_j - u_k\|^3}.$$

Warum diese Beschreibung? Weil sie erfolgreich erklärt und vorhersagt!

Die **Quantenmechanik** beschreibt jeden Zustand durch einen Vektor

$$s \in V$$

in einem $\mathbb{C}$–Vektorraum und Operationen durch lineare Abbildungen. Als kleinste Informationseinheit kann ein **Bit** nur den Zustand 0 oder 1 annehmen. Die Quantenmechanik erlaubt zudem **Überlagerungen**:

$$s = \alpha\,|0\rangle + \beta\,|1\rangle$$

Warum diese Beschreibung? Weil sie erfolgreich erklärt und vorhersagt!

Exkurs: von klassischer Physik zur Quantenphysik

Die Koeffizienten $\alpha, \beta \in \mathbb{C}$ mit $(\alpha, \beta) \neq (0, 0)$ heißen auch **Amplituden**. Alle möglichen Zustandsvektoren $s = \alpha\,|0\rangle + \beta\,|1\rangle$ und der Nullvektor 0 bilden somit einen zweidimensionalen $\mathbb{C}$–Vektorraum $V \cong \mathbb{C}^2$.

Dieser trägt zudem ein Skalarprodukt mit Orthonormalbasis $(|0\rangle, |1\rangle)$. Die Absolutquadrate $|\alpha|^2$ und $|\beta|^2$ entsprechen Wahrscheinlichkeiten, dazu normieren wir den Zustand s, sodass $1 = \|s\| = |\alpha|^2 + |\beta|^2$ gilt.

Damit modelliert die Quantenmechanik Zufall, Superposition, Wellenphänomene und vieles mehr. Die hierzu verwendeten Rechenregeln formulieren wir in S1F als **Postulate der Quantenmechanik**.

Wie die Physiker/innen historisch, experimentell und theoretisch zu dieser raffinierten und sonderbaren Beschreibung gekommen sind, ist eine faszinierende Geschichte, leider auch lang und gewunden.

Ich will hier die Vogelperspektive einnehmen und mit ein paar groben Pinselstrichen skizzieren, wie unsere mathematischen Werkzeuge der Linearen Algebra hierbei wunderbar zum Einsatz kommen.

Anwendung: Tensoren im Quantencomputing

Wir betrachten zwei Teilchen, jedes mit zwei **Basiszuständen** $|0\rangle, |1\rangle$. Das zusammengesetzte Zwei-Teilchen-System hat vier Basiszustände:

$$|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle$$

Jeder Zustand ist eine **Überlagerungen** dieser Basiszustände, also

$$s = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

mit Koeffizienten $(\alpha, \beta, \gamma, \delta) \in \mathbb{C}^4 \setminus \{0\}$. Die möglichen Zustände und der Nullvektor bilden somit einen vierdimensionalen $\mathbb{C}$–Vektorraum.

🙂 Allgemein: Aus n einzelnen Teilchen mit Zustandsräumen $V_1, \ldots, V_n$ entsteht das n–Teilchen-System mit Zustandsraum $V = V_1 \otimes \cdots \otimes V_n$.

⚠ Hierbei werden die Dimensionen nicht addiert, sondern multipliziert. Die Zustände der Teilchen bestehen nicht unabhängig nebeneinander, wie in $V_1 \oplus \cdots \oplus V_n$, sondern sind i.A. verschränkt (engl. *entangled*).

⚠ Superposition ist ein fundamentales Prinzip der Quantenmechanik ohne klassische Entsprechung und daher ohne anschauliche Intuition.

Anwendung: Tensoren im Quantencomputing

Klassisch genügt zur Zustandsbestimmung von n Bits die Kenntnis der n Zustände $z_1, \ldots, z_n \in \{0, 1\}$. Dies ist ein Vektor $z \in \{0, 1\}^n$. Die Menge der möglichen Zustände hat somit $N = 2^n$ Elemente, Damit arbeiten klassische, binäre Computer sehr erfolgreich.

In der Quantenmechanik ist der Zustandsraum eines Systems ein $\mathbb{C}$–Vektorraum V. Ist $(v_1, \ldots, v_N)$ eine Basis, so können nicht nur diese Basiszustände auftreten, sondern auch Überlagerungen (Superpositionen), also alle $\mathbb{C}$–Linearkombinationen $s = \sum_{k=1}^{N} \alpha_k v_k$.

Die Zustandsbestimmung von n Quantenbits (Qubits) bedeutet somit die Kenntnis aller $N = 2^n$ komplexen Koeffizienten $\alpha_1, \ldots, \alpha_N \in \mathbb{C}$. Man kann sich fragen, wo die Natur die zusätzliche Speicher- und Rechenkapazität dafür hernimmt, aber so sind wohl die Spielregeln.

Dieses exponentielle Wachstum macht die Berechnung oder Simulation von Quantensystemen mit klassischen Computern nahezu unmöglich. Umgekehrt schlug Richard Feynman 1982 vor, dies zur Entwicklung von Quantencomputern zu nutzen. Sie werden es wohl noch erleben.

Sind Anwendungsbeispiele ein Fluch oder ein Segen?

So manche/r stöhnt vermutlich: „Jetzt übertreibt der Prof: Wir müssen nicht nur Lineare Algebra lernen, jetzt auch noch Quantenmechanik!“

Ja, bitte nehmen Sie mögliche Anwendungen interessiert zur Kenntnis! Der Blick über den Tellerrand lohnt sich, gerade an der Uni Stuttgart.

Sind solche Exkurse übertrieben? ablenkend? oder gar überfordernd? Ich nenne drei Gründe für akademische Neugier und Abenteuerlust:

1. Wir sollten uns freuen, dass mathematische Begriffe und Techniken so überraschend vielseitig anwendbar sind: Was Sie in einem Gebiet lernen, können Sie in vielen anderen Gebieten wiederverwenden.

2. Speziell im Fall des Quantencomputing ist realistisch absehbar, dass dies Ihr Leben nachhaltig beeinflussen wird. Ich will daher nicht kommentarlos an diesem wichtigen Anwendungsbeispiel vorübergehen.

3. Das Studium mathematischer Grundlagen ist fundamental wichtig. Wir wollen abstrahieren, um zahlreiche Einzelfälle zusammenzufassen, zugleich auch motivieren, konkretisieren, illustrieren. Nur so geht es!

Sind Anwendungsbeispiele ein Fluch oder ein Segen?

Der Spagat zwischen diesen beiden Polen ist eine fragile Kunst: Einerseits die abstrakten Grundlagen: einfach, elegant, allgemein. Andererseits die konkreten Einzelfälle: verwirrend, sonderbar, speziell.

Manche vertauschen hier die Adjektive, das halte ich für einen Fehler. Abstraktion strukturiert und vereinfacht: Eine allgemeine Tatsache ist oft leichter zu verstehen und zu erklären als ihre zahlreichen Spezialfälle.

Studierende fordern zu Recht motivierende Beispiele, Querverbindung zwischen den Themen und auch Bezug zu möglichen Anwendungen. Wir sollten uns also über jede Gelegenheit freuen, wo dies gelingt!

Be careful what you wish for, it might just come true!

Wird der Wunsch nach Beispielen und Anwendungen ernsthaft erfüllt, so fangen erfahrungsgemäß leider auch immer einige an zu jammern: Der Ruf nach Anwendungsbeispielen entsprang nicht ihrer Neugier, sondern der naiven Sehnsucht nach Einfachheit. Die ist oft unerfüllbar: Ehrliche Anwendungen sind meist nicht leichter zu verstehen, sondern komplizierter als die übergeordnete Theorie. Sie benötigen beides!

Sind Anwendungsbeispiele ein Fluch oder ein Segen?

Ich bin überzeugt, naturwissenschaftlich-technische Neugier und Allgemeinbildung sind wichtige Bildungsziele unserer Universität. Dazu möchte ich Gelegenheiten bieten, als wohlmeinendes Angebot.

Man kann das Pferd zum Wasser führen, aber nicht zum Trinken zwingen.

Ich weiß auch, dass unser Bildungssystem zumeist nicht Neugier und Lernfreude fördert, sondern Auswendiglernen und Nachbeten erzwingt.

Intrinsische Motivation gelingt nur aufwändig mit viel Mühe und Geduld, extrinsische Zwänge hingegen sind sofort und kostengünstig zu haben.

Auch hier macht die Mischung den Erfolg. Einseitige Lerndressur führt junge Menschen leider zu fatalem Desinteresse an ihrer Bildung:

Ein gutes Pferd springt nur so hoch, wie es muss.

Kurzum, bevor Sie fragen: Dieser Abschnitt ist nicht klausurrelevant. Bitte nutzen Sie Ihre Freiheiten weise und entscheiden Sie selbst!

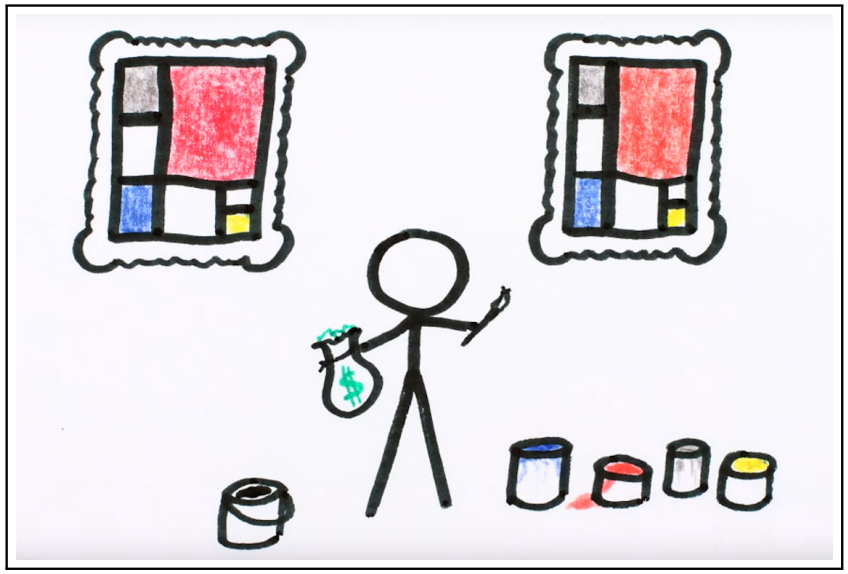
Habe Mut, dich deines eigenen Verstandes zu bedienen!

Sind Anwendungsbeispiele ein Fluch oder ein Segen?

Zum Spannungsfeld von Theorie und Anwendung, zur Wechselwirkung von Grundlagenforschung und technischer Umsetzung zitiere ich Albert Einstein aus seiner Rede anlässlich der Eröffnung der 7. Deutschen Funkausstellung in Berlin 1930 (siehe `youtu.be/VqvGRVM2jk8`).

Verehrte An- und Abwesende!
Wenn Ihr den Rundfunk höret, so denkt auch daran, wie die Menschen in den Besitz dieses wunderbaren Werkzeuges der Mitteilung gekommen sind. Der Urquell aller technischen Errungenschaften ist die göttliche Neugier und der Spieltrieb des bastelnden und grübelnden Forschers und nicht minder die konstruktive Phantasie des technischen Erfinders.
[…]
Sollen sich auch alle schämen, die gedankenlos sich der Wunder der Wissenschaft und Technik bedienen und nicht mehr davon geistig erfasst haben als die Kuh von der Botanik der Pflanzen, die sie mit Wohlbehagen frisst.

Anwendung: das No-Cloning-Theorem



Als wunderschönes Video von MinutePhysics, `youtu.be/owPC60Ue0BE`.

Anwendung: das No-Cloning-Theorem

A single quantum cannot be cloned

If a photon of definite polarization encounters an excited atom, there is typically some nonvanishing probability that the atom will emit a second photon by stimulated emission. Such a photon is guaranteed to have the same polarization as the original photon. But is it possible by this or any other process to amplify a quantum state, that is, to produce several copies of a quantum system (the polarized photon in the present case) each having the same state as the original? If it were, the amplifying process could be used to ascertain the exact state of a quantum system: in the case of a photon, one could determine its polarization by first producing a beam of identically polarized copies and then measuring the Stokes parameters[1]. We show here that the linearity of quantum mechanics forbids such replication and that this conclusion holds for all quantum systems.

Abstract des vielzitierten Artikels von W.K. Wootters, W.H. Zurek:
A single quantum cannot be cloned. Nature 299 (1982) 802–803

In *Nature* ist selbst eine kurze Notiz eine beachtliche Publikation;
zur Geschichte siehe `en.wikipedia.org/wiki/No-cloning_theorem`.

Anwendung: das No-Cloning-Theorem

Das berühmte **No-Cloning-Theorem** der Quantenmechanik besagt:

Es ist unmöglich, ein quantenmechanisches System perfekt auf ein zweites zu kopieren, ohne dabei das erste zu verändern.

Dies beruht auf einer einfachen Rechnung der Linearen Algebra:

Satz S1E: das No-Cloning-Theorem

Sei V ein K–Vektorraum der Dimension $\dim V \geq 2$ und $e \in V \setminus \{0\}$.
Dann existiert keine K–lineare Abbildung $T : V \otimes V \to V \otimes V$ mit

$$T\big[\,|v\rangle \otimes |e\rangle\,\big] = |v\rangle \otimes |v\rangle$$

für alle möglichen Zustände $v \in V$.

🙂 Es genügen die grundlegenden Rechenregeln aus Definition S1B.
Die *Rechnung* ist erschütternd einfach, die physikalische *Interpretation* ebenso erschütternd tiefsinnig, siehe hierzu das oben zitierte Video.

Übung: Versuchen Sie es bitte zunächst selbst, bevor Sie weiterlesen.

Anwendung: das No-Cloning-Theorem

Beweis: Angenommen, es gäbe solch eine lineare Abbildung T.
Wir wählen eine Basis $(a, b, \dots)$ von V und betrachten den Zustand

$$s = (|a\rangle + |b\rangle) \otimes |e\rangle \qquad \in V \otimes V.$$

Rechenweg 1: Wir multiplizieren erst aus und wenden dann T an.

$$\begin{aligned} T(s) &\overset{(a)}{=} T\big[\,(|a\rangle + |b\rangle) \otimes |e\rangle\,\big] \\ &\overset{\text{Bil}}{=} T\big[\,(|a\rangle \otimes |e\rangle) + (|b\rangle \otimes |e\rangle)\,\big] \\ &\overset{\text{Lin}}{=} T\big[\,|a\rangle \otimes |e\rangle\,\big] + T\big[\,|b\rangle \otimes |e\rangle\,\big] \\ &\overset{\text{Def}}{=} (|a\rangle \otimes |a\rangle) + (|b\rangle \otimes |b\rangle) \end{aligned}$$

Rechenweg 2: Wir wenden erst T an und multiplizieren dann aus.

$$\begin{aligned} T(s) &\overset{(a)}{=} T\big[\,(|a\rangle + |b\rangle) \otimes |e\rangle\,\big] \\ &\overset{\text{Def}}{=} (|a\rangle + |b\rangle) \otimes (|a\rangle + |b\rangle) \\ &\overset{\text{Bil}}{=} (|a\rangle \otimes |a\rangle) + (|a\rangle \otimes |b\rangle) + (|b\rangle \otimes |a\rangle) + (|b\rangle \otimes |b\rangle) \end{aligned}$$

Der Koeffizientenvergleich (dank S1B) führt zum Widerspruch. QED

EPR: das Einstein–Podolsky–Rosen–Paradox

Wir betrachten unser Zwei-Teilchen-System $V = V_1 \otimes V_2$ im Zustand

$$s = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle.$$

Die Basiszustände bilden die Orthonormalbasis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$.

$A = \begin{bmatrix} 0&0&0&0\\ 0&0&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix}$
Alice misst $a \in \{0,1\}$.

Wkt	0	1
0	$\lvert\alpha\rvert^2$	$\lvert\beta\rvert^2$
1	$\lvert\gamma\rvert^2$	$\lvert\delta\rvert^2$

$B = \begin{bmatrix} 0&0&0&0\\ 0&1&0&0\\ 0&0&0&0\\ 0&0&0&1 \end{bmatrix}$
Bob misst $b \in \{0,1\}$.

Mit A misst Alice das erste Teilchen und erhält den Messwert $a \in \{0,1\}$.
Das zerlegt $V = \mathrm{E}_0 \oplus \mathrm{E}_1$ in die Eigenräume $\mathrm{E}_a = \mathbb{C}|a\rangle \otimes V_2$ und somit $s = s_0 + s_1$ in $s_0 = \alpha\,|00\rangle + \beta\,|01\rangle \in \mathrm{E}_0$ und $s_1 = \gamma\,|10\rangle + \delta\,|11\rangle \in \mathrm{E}_1$.
Postulate der Messung (S1F): Alice misst den Wert $a \in \{0,1\}$ mit Wkt

$$p_a = \frac{\|s_a\|^2}{\|s\|^2} = \frac{|\alpha|^2 + |\beta|^2 \text{ bzw. } |\gamma|^2 + |\delta|^2}{|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2}.$$

Durch die Messung des Wertes a kollabiert der Zustand von s zu s_a.

EPR: das Einstein–Podolsky–Rosen–Paradox

Sie kennen solche **Vierfeldertafeln** aus der Schule. In der Stochastik stellen Sie so die gemeinsamen Wkten von zwei Ereignissen A und B übersichtlich dar, hier entsprechend für unsere beiden Zufallsvariablen. Damit beantworten Sie Fragen zu Korrelation und Unabhängigkeit.

In unserem Beispiel werden jeweils nur zwei Werte angenommen, nämlich 0 oder 1; diese Miniatur ist der kleinste interessante Fall. Ganz genauso beschreiben wir jedes endlich-dimensionale System; den unendlich-dimensionalen Fall führt die Funktionalanalysis fort.

Die komplexen Koeffizienten $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ werden auch **Amplituden** genannt und entsprechen den Wahrscheinlichkeiten $|\alpha|^2, |\beta|^2, |\gamma|^2, |\delta|^2$. Damit diese sich zu 1 summieren, dividieren wir durch das Normquadrat

$$\|s\|^2 = |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2.$$

Das kann ganz am Ende geschehen. Oft nimmt man dies schon anfangs vorweg, indem man den Zustandsvektor s auf Länge $\|s\| = 1$ normiert. Genau so habe ich für unsere obige Tabelle alles vorsorglich normiert.

EPR: das Einstein–Podolsky–Rosen–Paradox

Wir betrachten zwei unabhängige Teilchen, also einen **reinen Tensor**:

$$\begin{aligned} s = u \otimes v &= (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle \end{aligned}$$

Zur Vereinfachung normieren wir zu $|\alpha_0^2| + |\alpha_1^2| = |\beta_0^2| + |\beta_1^2| = 1$.
Das erste Teilchen transportieren wir zu Alice, das zweite zu Bob.

$A = \begin{bmatrix} 0&0&0&0\\ 0&0&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix}$
Alice misst $a \in \{0,1\}$.

Wkt	0	1
0	$\lvert\alpha_0^2\rvert \cdot \lvert\beta_0^2\rvert$	$\lvert\alpha_0^2\rvert \cdot \lvert\beta_1^2\rvert$
1	$\lvert\alpha_1^2\rvert \cdot \lvert\beta_0^2\rvert$	$\lvert\alpha_1^2\rvert \cdot \lvert\beta_1^2\rvert$

$B = \begin{bmatrix} 0&0&0&0\\ 0&1&0&0\\ 0&0&0&0\\ 0&0&0&1 \end{bmatrix}$
Bob misst $b \in \{0,1\}$.

Alice misst den Zustand und findet den Wert $a \in \{0,1\}$ mit Wkt $|\alpha_a|^2$.
Dadurch kollabiert der Zustand von s zu $s_a = \alpha_a(\beta_0|a0\rangle + \beta_1|a1\rangle)$.
Daraufhin misst Bob und findet den Wert $b \in \{0,1\}$ mit Wkt $|\beta_b|^2$.
Fazit: Die Messergebnisse von Alice und Bob sind unabhängig.

🙂 Das entspricht unserer Intuition: klassisch, unabhängig.

EPR: das Einstein–Podolsky–Rosen–Paradox

Wir bringen unsere beiden Teilchen in den **verschränkten Zustand**

$$s = \frac{1}{\sqrt{2}} \cdot |00\rangle + 0 \cdot |01\rangle + 0 \cdot |10\rangle + \frac{1}{\sqrt{2}} \cdot |11\rangle.$$

Dieser Zustand lässt sich nicht als reiner Tensor $u \otimes v$ darstellen.
Das erste Teilchen transportieren wir zu Alice, das zweite zu Bob.

$A = \begin{bmatrix} 0&0&0&0\\ 0&0&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix}$
Alice misst $a \in \{0,1\}$.

Wkt	0	1
0	50%	0%
1	0%	50%

$B = \begin{bmatrix} 0&0&0&0\\ 0&1&0&0\\ 0&0&0&0\\ 0&0&0&1 \end{bmatrix}$
Bob misst $b \in \{0,1\}$.

Alice misst den Zustand und findet $a \in \{0,1\}$, jeweils mit gleicher Wkt.
Bob misst den Zustand und findet $b \in \{0,1\}$, jeweils mit gleicher Wkt.
Hier sind die Messergebnisse von Alice und Bob immer identisch!
Wie kann das sein, instantan über beliebig große Distanzen?

⚠ Der Wesenskern der Quantenmechanik ist die Superposition.
Dafür gibt es keine klassische Entsprechung oder Anschauung.

Warum gilt diese einfache Rechnung als paradox?
Das liegt ganz allein an der physikalischen Interpretation:

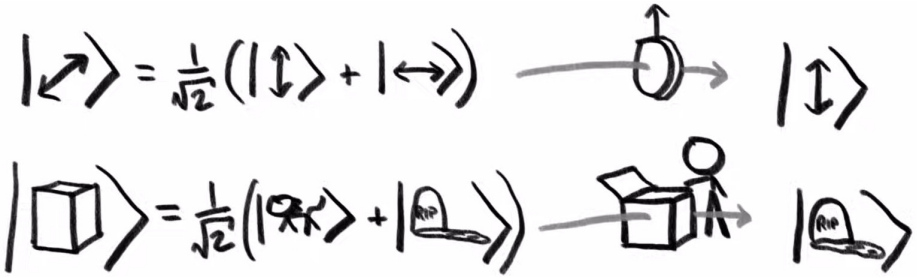
Alice und Bob können beliebig weit entfernt sein! Alice' Messung entspricht einem Münzwurf, mit Ergebnis 0 für Kopf und 1 für Zahl. Auch Bobs Messung entspricht einem Münzwurf. Diese sind jedoch nicht unabhängig, sondern beide Ergebnisse stimmen immer überein.

Wie kann das sein? Wird hier Information von Alice zu Bob übertragen, und zwar instantan und somit schneller als Lichtgeschwindigkeit? Einstein wollte sich mit dieser „spukhaften Fernwirkung“ nicht abfinden. Aus dieser Sicht wird die obige Rechnung als „paradox“ bezeichnet.

Das Phänomen ist sicherlich unerwartet und unintuitiv, aber Experimente bestätigen genau diese Vorhersage. Information wird hier nicht übertragen, denn Alice kann ihren Wert zwar messen, doch nicht willkürlich vorgeben.

Auch hier ist die *Rechnung* erschütternd einfach, vor allem dank des zugrundeliegenden, sehr eleganten Tensorkalküls. Die physikalische *Interpretation* jedoch ist ebenso erschütternd tiefsinnig und schwierig.

If people do not believe that mathematics is simple,
it is only because they do not realize how complicated life is.
John von Neumann (1903–1957)



Video von 3Blue1Brown und MinutePhysics, `youtu.be/MzRCDLre1b4`, und ebenso sehenswert von Veritasium, `youtu.be/ZuvK-od647c`.

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*
(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

Warum erzähle ich Ihnen das hier, in der Linearen Algebra?
Ist Quantenmechanik nicht viel zu schwer und unanschaulich?

Ja, Quantenmechanik ist unanschaulich, doch von fundamentaler Bedeutung: physikalisch, mathematisch, technisch, philosophisch, ...

Vor allem aber können wir an solchen Anwendungen viel lernen, vielleicht sogar etwas Physik, ganz sicher aber viel Mathematik!

Ich präsentiere Ihnen diesen faszinierenden Exkurs, um zu illustrieren, dass Sie die mathematischen Grundlagen Ihrer Linearen Algebra sehr vielseitig anwenden können, in der Physik und auch überall sonst.

Ich betone dabei nochmals: Die Mathematik ist zunächst nicht einfach, doch in Ihrer Reichweite und mit Übung gut erlernbar und verständlich. Es lohnt sich daher in solide mathematische Grundlagen zu investieren.

Abstraktion strukturiert und vereinfacht: Eine allgemeine Tatsache ist oft leichter zu verstehen und zu erklären als ihre zahlreichen Spezialfälle. In den Anwendungen hingegen tobt das Leben, prall und verwirrend.

Die obigen Miniaturen zum No-Cloning-Theorem und dem EPR-Paradox zeigen eindrücklich: Die mathematischen Grundlagen der Rechnungen sind „einfache Lineare Algebra“, wie Physiker/innen gerne sagen.

Und das zu Recht. Die (abstrakten) mathematischen Werkzeuge muss man nur einmal erlernen, sie kosten anfangs etwas Geduld und Mühe, doch das ist gut investiert: sie lassen sich überall (konkret) anwenden.

Definition S1F: Postulate der Quantenmechanik

Die Quantenmechanik wird durch folgende Postulate zusammengefasst:

1. Der Zustand eines Systems wird beschrieben durch einen Vektor $\psi \in V$ in einem Hilbert–Raum V über $\mathbb{C}$, genannt Zustandsraum.
2. Jede physikalisch messbare Größe, kurz Observable genannt, wird beschrieben durch einen hermiteschen Operator $A : V \to V$.
3. Das Ergebnis jeder Messung von A ist ein Eigenwert $a \in \mathbb{R}$ von A. (Wenn wir $\dim V < \infty$ annehmen, so wissen wir $V = \bigoplus_{a\in\mathbb{R}} \mathrm{E}_a$.)
4. Die Wkt des Messwerts a im Zustand ψ ist $\mathbf{P}(a|\psi) = \|\psi_a\|^2/\|\psi\|^2$ gemäß der orthogonalen Zerlegung $V = \mathrm{E}_a \oplus \mathrm{E}_a^\perp$ und $\psi = \psi_a + \psi'_a$.
5. Nach der Messung von a befindet sich das System im Zustand ψ_a. Das ist die orthogonale Projektion von V auf den Eigenraum E_a.
6. Die Schrödinger–Gleichung $\mathrm{i}\hbar\,\partial_t\psi(t) = H(t)\psi(t)$ beschreibt die zeitliche Entwicklung; die Observable $H(t)$ ist die Gesamtenergie.

🙂 Die Postulate (1–5) präzisieren die grundlegenden Rechenregeln der Quantenmechanik in der vertrauten Sprache der Linearen Algebra!

So formulierte Werner Heisenberg 1925 seine **Matrizenmechanik** und Erwin Schrödinger im selben Jahre seine **Wellenmechanik**; dafür erhielten sie 1932 bzw. 1933 den Nobelpreis für Physik.

⚠ Zur Vereinfachung möchte ich im Folgenden $\dim V < \infty$ annehmen. Die zur Quantenmechanik nötige Mathematik liegt dann vollständig im Rahmen der **Linearen Algebra**. Der allgemeine Fall ist noch viel faszinierender, benötigt aber stärkere Werkzeuge der **Analysis**.

Diese Postulate der Quantenmechanik kann man wohl kaum intuitiv verstehen, wohl aber gut nutzen: Sie beschreiben die Experimente!

I think I can safely say that nobody understands quantum mechanics.
Richard P. Feynman, *The Character of Physical Law* (1965)

Ich betone nochmals: Die wesentliche Schwierigkeit liegt nicht in der mathematischen Formulierung, dazu haben Sie nun alle Werkzeuge. Das Verrückte ist einzig und allein die physikalische Interpretation.

Aufgabe: Lösen Sie die Schrödinger–Gleichung im Falle $\dim V < \infty$. Der Schrödinger–Hamilton–Operator $H : V \to V$ sei zeitlich konstant:

$$\boxed{\mathrm{i}\hbar\,\partial_t\psi(t) = H\psi(t), \quad \psi(t_0) = \psi^0}$$

Lösung: Dank Spektralsatz existiert eine Orthonormalbasis $(v_1, \dots, v_n)$ von V aus Eigenvektoren, also $Hv_k = E_k v_k$ mit $E_k \in \mathbb{R}$ für $k = 1, \dots, n$.

Wir untersuchen nun $\psi : \mathbb{R} \to V : t \mapsto \psi(t)$ als zeitabhängigen Zustand. Zu jedem Zeitpunkt $t \in \mathbb{R}$ zerlegen wir den Zustand $\psi(t) = \sum_k \psi_k(t) v_k$ als Summe orthogonaler Eigenvektoren, also $\psi_k(t) = \langle\, v_k \mid \psi(t) \,\rangle \in \mathbb{C}$.

Die allgemeine Schrödinger–Gleichung $\mathrm{i}\hbar\,\partial_t\psi(t) = H(t)\psi(t)$ wird nun entkoppelt zu $\mathrm{i}\hbar\,\partial_t\psi_k(t) = E_k\psi_k(t)$. Aus $\psi(t_0) = \sum_k \psi^0_k v_k$ folgt somit:

$$\boxed{\psi(t) = \textstyle\sum_k \mathrm{e}^{-\mathrm{i}(t-t_0)E_k/\hbar}\,\psi^0_k v_k}$$

Alternative: Mit der Matrix-Exponentialfunktion (N3B) können wir die eindeutige Lösung zusammenfassen durch $\psi(t) = \mathrm{e}^{\mathrm{i}(t-t_0)H/\hbar}\,\psi(t_0)$.

🙂 Die explizite Lösung gelingt überraschend leicht: Wir benötigen dazu nur eine Orthonormalbasis $(v_1, \dots, v_n)$ von V aus Eigenvektoren von H.

Wie der Schrödinger–Operator H genau aussieht, hängt vom konkreten Modell ab. Die Lösungsmethode hingegen ist universell anwendbar!

🙂 Wir erkennen hier eine erstaunlich simple zeitliche Entwicklung: Die Amplitude $\psi_k(t) = \mathrm{e}^{-\mathrm{i}(t-t_0)E_k/\hbar}\,\psi^0_k$ bleibt im Betrag immer gleich, nur die Phase ändert sich um den Faktor $\mathrm{e}^{-\mathrm{i}(t-t_0)E_k/\hbar} \in \mathbb{S}^1 = \mathrm{U}_1\,\mathbb{C}$.

Die Geschwindigkeit $E_k/\hbar$ dieser Phasenänderung ist die Energie E_k des Eigenzustands v_k geteilt durch eine universelle Naturkonstante, das Plancksche Wirkungsquantum $\hbar = h/2\pi \approx 1.055 \cdot 10^{-34}\mathrm{Js}$.

🙂 Die Wkten $|\psi_k(t)|^2 \in [0, 1]$ ändern sich nicht, lediglich die Phase! Die Phase ist nicht direkt messbar, spielt aber dennoch eine wichtige Rolle: Bei der Addition (Überlagerung, Superposition) führt sie zu Verstärkung oder Auslöschung; man spricht hier von Interferenz. Die Wkten $|\psi_k(t)|^2 \in [0, 1]$ alleine genügen dafür nicht!

Aufgabe: Sei V ein $\mathbb{C}$–Vektorraum mit Skalarprodukt $\langle - \mid - \rangle$ und $\dim V = n < \infty$ und hierauf $A : V \to V$ ein hermitescher Operator.

Wir interpretieren V als Zustandsraum und A als Observable.
Berechnen Sie gemäß den Postulaten der Quantenmechanik (S1F) Erwartung und Varianz des Operators A im gegebenen Zustand $\psi \in V$.

Lösung: Dank Spektralsatz existiert eine Orthonormalbasis $(v_1, \ldots, v_n)$ von V aus Eigenvektoren, also $Av_i = a_i v_i$ mit $a_i \in \mathbb{R}$ für $i = 1, \ldots, n$.

Wir zerlegen den Zustand $\psi = \sum_{i=1}^n \psi_i v_i$ in eine Summe orthogonaler Eigenvektoren. Die Koeffizienten hierfür sind $\psi_i = \langle v_i \mid \psi \rangle \in \mathbb{C}$ (P1O).

Die Betragsquadrate $|\psi_i^2|$ entsprechen Wkten. Wir normieren daher den Zustand ψ und erhalten so die Gesamtwkt $1 = \|\psi\|^2 = \sum_{i=1}^n |\psi_i^2|$.

Bei vorgegebenem Zustand $\psi \in V$ mit $\|\psi\| = 1$ interpretieren wir die Messung durch den hermiteschen Operator A als Zufallsvariable.

(Etwas nachlässig doch bequem bezeichne ich im Folgenden beides, den Operator A und die Zufallsvariable A, mit demselben Symbol.)

Die Erwartung μ der Messung durch A ist demnach:

$$\begin{aligned}\mu = \mathbf{E}(A) &= \textstyle\sum_i a_i |\psi_i^2| = \sum_i a_i \langle \psi_i \mid \psi_i \rangle = \sum_i a_i \langle \psi \mid \psi_i \rangle \\ &= \textstyle\sum_i \langle \psi \mid A\psi_i \rangle = \big\langle \psi \,\big|\, \sum_i A\psi_i \big\rangle = \big\langle \psi \,\big|\, A \sum_i \psi_i \big\rangle \\ &= \langle \psi \mid A\psi \rangle = \langle \psi \mid A \mid \psi \rangle =: \langle A \rangle\end{aligned}$$

Hierbei ist $\langle A \rangle$ die bequeme Kurzschreibweise zum gegebenen Zustand ψ. Die Erwartung von A^2 ist entsprechend:

$$\mathbf{E}(A^2) = \langle A^2 \rangle = \langle \psi \mid A^2 \mid \psi \rangle = \langle A\psi \mid A\psi \rangle$$

Daraus erhalten wir wie üblich die Varianz der Zufallsvariable A als Erwartung der quadratischen Abweichung vom Mittelwert:

$$\begin{aligned}\sigma^2 = \mathbf{V}(A) &= \mathbf{E}((A-\mu)^2) = \mathbf{E}(A^2 - 2\mu A + \mu^2) \\ &= \mathbf{E}(A^2) - 2\mu\mathbf{E}(A) + \mu^2 = \mathbf{E}(A^2) - \mathbf{E}(A)^2 = \langle A^2 \rangle - \langle A \rangle^2\end{aligned}$$

🙂 Hier verbinden sich Lineare Algebra, Skalarprodukte und Wahrscheinlichkeitsrechnung wunderbar einfach und elegant.

🙂 Zusammenfassend erhalten wir das folgende schöne Ergebnis:

Satz S1G: Erwartung und Varianz

Sei V ein Hilbert–Raum über $\mathbb{C}$; zur Vereinfachung gelte $\dim V < \infty$.

Gegeben sei ein hermitescher Endomorphismus $A : V \to V$ und ein Vektor $\psi \in V$. Nach den Postulaten der Quantenmechanik (S1F) interpretieren wir die Messung durch A als eine Zufallsvariable.

(1) Erwartung und Varianz sind dann gegeben durch:

$$\begin{aligned}\mu = \mathbf{E}(A) &= \langle A \rangle := \langle \psi \mid A \mid \psi \rangle \\ \mathbf{E}(A^2) &= \langle A^2 \rangle = \langle \psi \mid A^2 \mid \psi \rangle = \langle A\psi \mid A\psi \rangle \\ \sigma^2 = \mathbf{V}(A) &= \mathbf{E}(A^2) - \mathbf{E}(A)^2 = \langle A^2 \rangle - \langle A \rangle^2\end{aligned}$$

Dieser Satz gilt sinngemäß genauso in unendlicher Dimension; die dazu nötige technische Ausführung diskutieren wir hier nicht.

🙂 Mögliche Messwerte sind die Eigenwerte von A, und ihre Wkten sind verteilt gemäß ψ. Der Erwartungswert $\mu \in \mathbb{R}$ ist der Schwerpunkt dieser Verteilung, und die Streuung $\sigma \in \mathbb{R}_{\geq 0}$ misst die typische Breite.

🙂 Bitte beachten Sie den geschickten und fließenden Übergang von „koordinatengebundener“ zu „koordinatenfreier“ Formulierung: Unsere Rechnungen nutzen eine Eigenbasis von A, das Ergebnis jedoch nicht!

⚠ Auf dem Zustandsraum V arbeiten wir im Allgemeinen mit mehreren verschiedenen hermiteschen Operatoren $A, B, \ldots$. Es hat daher meist keinen rechten Sinn, sich auf eine Basis festzulegen: Jeder hermitesche Operator erlaubt zwar eine Eigenbasis, doch bei jedem Wechsel des Operators müssen wir im Allgemeinen auch die Basis wechseln.

🙂 In konkreten Rechnungen ist meist die Wahl einer Basis hilfreich; genau so haben wir oben die Erwartung definiert und berechnet.

🙂 Für die Ergebnisse sind basisfreie Formulierungen am schönsten; genau so haben wir den obigen Satz S1G formuliert.

Wann können wir mit einem „scharfen“ Messergebnis rechnen?
Darauf antwortet die folgende Ergänzung des obigen Satzes:

Satz S1G: Erwartung und Varianz

(2) Genau dann gilt $\mathbf{V}(A) = 0$, wenn ψ ein Eigenzustand von A ist.
In diesem Fall ist $\mathbf{E}(A) = \mu$ der zugehörige Eigenwert, also $A\psi = \mu\psi$.

Aufgabe: Beweisen Sie diese Äquivalenz.

Lösung: „⇐“: Angenommen, $\psi \in V \setminus \{0\}$ erfüllt $A\psi = \mu\psi$ mit $\mu \in \mathbb{R}$. Zudem gelte $\|\psi\| = 1$. Dann gilt $\mathbf{E}(A) = \langle\, \psi \mid A \mid \psi \,\rangle = \mu$ und ebenso $\mathbf{E}(A^2) = \langle\, \psi \mid A^2 \mid \psi \,\rangle = \mu^2$, also $\mathbf{V}(A) = \mathbf{E}(A^2) - \mathbf{E}(A)^2 = 0$.

„⇒“: Als Kontraposition zeigen wir: Ist ψ kein Eigenzustand, so gilt $\mathbf{V}(A) > 0$. Zunächst normieren wir $\|\psi\| = 1$. Da A hermitesch ist und $\dim V < \infty$, zerfällt V in die orthogonale Summe von Eigenräumen. Wir zerlegen $\psi = \sum_{k=1}^{m} \psi_k$ in Eigenzustände $\psi_k \neq 0$ mit $A\psi_k = \lambda_k \psi_k$ und $\lambda_k \neq \lambda_\ell$ für $k \neq \ell$. Gilt dabei $m \geq 2$, so folgt für die Varianz $\mathbf{V}(A) = \mathbf{E}((A-\mu)^2) = \sum_{k=1}^{m} (\lambda_k - \mu)^2 \|\psi_k^2\| > 0$.

Satz S1H: Unschärferelation, Heisenberg 1927, Robertson 1929

Sei V ein Hilbert–Raum über $\mathbb{C}$; zur Vereinfachung gelte $\dim V < \infty$.
Gegeben seien hermitesche Operatoren $A, B : V \to V$. Ihr Kommutator $[A, B] = AB - BA$ misst somit die Abweichung von der Kommutation.
Für jeden Zustand $\psi \in V$ gilt dann die Ungleichung

$$\mathbf{V}(A)\,\mathbf{V}(B) \;\geq\; \frac{1}{4}\big|\langle\, [A,B] \,\rangle\big|^2.$$

Im Falle $\mathbf{E}(A) = \mathbf{E}(B) = 0$ bedeutet das ausgeschrieben:

$$\langle\, \psi \mid A^2 \mid \psi \,\rangle\, \langle\, \psi \mid B^2 \mid \psi \,\rangle \;\geq\; \frac{1}{4}\big|\langle\, \psi \mid [A,B] \mid \psi \,\rangle\big|^2$$

Beweis: Zur Vereinfachung der Rechnung zentrieren wir A und B zu $A' = A - \mathbf{E}(A)$ und $B' = B - \mathbf{E}(B)$. Damit verschieben wir die beiden Erwartungswerte zu 0, doch Varianz und Kommutator ändern sich nicht. Wir können und werden im Folgenden $\mathbf{E}(A) = \mathbf{E}(B) = 0$ annehmen.

Wir nutzen Hermitizität und die Cauchy–Schwarz–Ungleichung:

$$\begin{aligned}\langle\, A^2 \,\rangle\, \langle\, B^2 \,\rangle \;&=\; \langle\, \psi \mid A^2\psi \,\rangle\, \langle\, \psi \mid B^2\psi \,\rangle \;=\; \langle\, A\psi \mid A\psi \,\rangle\, \langle\, B\psi \mid B\psi \,\rangle \\ &\geq\; \big|\langle\, A\psi \mid B\psi \,\rangle\big|^2 \;=\; \big|\langle\, \psi \mid AB\,\psi \,\rangle\big|^2 \;=\; \big|\langle\, AB \,\rangle\big|^2.\end{aligned}$$

Wir zerlegen $AB = \frac{1}{2}\{A,B\} + \frac{1}{2}[A,B]$ in die Summanden

$$\{A,B\} = AB + BA \quad \text{und} \quad [A,B] = AB - BA.$$

Der Antikommutator $\{A,B\}$ ist hermitesch, also $\langle\, \{A,B\} \,\rangle$ reell, der Kommutator $[A,B]$ ist antihermitesch, also $\langle\, [A,B] \,\rangle$ imaginär.

$$\big|\langle\, AB \,\rangle\big| \;=\; \Big|\frac{1}{2}\langle\, \{A,B\} \,\rangle + \frac{1}{2}\langle\, [A,B] \,\rangle\Big| \;\geq\; \frac{1}{2}\big|\langle\, [A,B] \,\rangle\big|$$

Zusammengefasst erhalten wir die allgemeine Unschärferelation:

$$\langle\, A^2 \,\rangle\, \langle\, B^2 \,\rangle \;\geq\; \frac{1}{4}\big|\langle\, [A,B] \,\rangle\big|^2$$

Das beweist die behauptete Ungleichung. QED

Auch hier ist die mathematische Behandlung vergleichsweise leicht, die physikalische Interpretation jedoch erwies sich als revolutionär:

Falls die beiden hermiteschen Operatoren A und B kommutieren, also $[A,B] = 0$ erfüllen, so lassen sie sich simultan diagonalisieren (M4B).

Andernfalls gilt $[A,B] \neq 0$, und die Unschärferelation S1H besagt, dass beide Messwerte nicht gleichzeitig exakt bestimmt sind.

Diese Unschärfe beruht nicht auf einem technisch behebbaren Mangel eines ungenügenden Messinstruments, sondern ist prinzipieller Natur!

Heisenbergs ursprüngliche Formulierung einer Unschärferelation betraf Ort x und Impuls p eines Teilchens: In geeigneter Darstellung gilt dabei $p = (\hbar/\mathrm{i})\partial_x$, daraus folgt $[x,p] = \mathrm{i}\hbar$, also $\sigma(x) \cdot \sigma(p) \geq \hbar/2$. Das heißt:

Es ist prinzipiell unmöglich, den Ort und den Impuls eines Teilchens gleichzeitig beliebig genau zu messen. Anders gesagt bedeutet das:

Es ist unmöglich, einen quantenmechanischen Zustand herzustellen, bei dem der Ort und der Impuls beliebig genau definiert sind.

Motivierendes Beispiel: die Multiplikation von Matrizen

Unser Vorbild ist die **Multiplikation** von Matrizen passender Größe:

$$\mu : K^{a\times b} \times K^{b\times c} \to K^{a\times c} : (u,v) \mapsto w = u \bullet v, \quad w_{i,k} = \textstyle\sum_{j=1}^{b} u_{i,j} \cdot v_{j,k}$$

Hier ist $U = K^{a\times b}$ ein linearer Raum über dem Ring $R = K^{a\times a}$ von links und über dem Ring $S = K^{b\times b}$ von rechts, und beide sind kompatibel:

$$(r \bullet u) \bullet s = r \bullet (u \bullet s) \quad \text{für alle } r \in R,\ u \in U,\ s \in S$$

Wir sagen U ist ein (R,S)**–linearer Raum** oder ein (R,S)**–Bimodul**.
Ebenso $V = K^{b\times c}$ über (S,T) und $W = K^{a\times c}$ über (R,T) mit $T = K^{c\times c}$.

Die Produktabbildung μ ist biadditiv, sogar (R,S,T)**–bilinear**:

$$\begin{aligned}
\mu(u+u',v) &= (u+u')\bullet v = (u\bullet v)+(u'\bullet v) = \mu(u,v)+\mu(u',v),\\
\mu(u,v+v') &= u\bullet(v+v') = (u\bullet v)+(u\bullet v') = \mu(u,v)+\mu(u,v'),\\
\mu(r\bullet u,v) &= (r\bullet u)\bullet v = r\bullet(u\bullet v) = r\bullet\mu(u,v),\\
\mu(u,v\bullet t) &= u\bullet(v\bullet t) = (u\bullet v)\bullet t = \mu(u,v)\bullet t\\
\mu(u\bullet s,v) &= (u\bullet s)\bullet v = u\bullet(s\bullet v) = \mu(u,s\bullet v),
\end{aligned}$$

für alle Vektoren $u,u' \in U$, $v,v' \in V$ und Skalare $r \in R$, $s \in S$, $t \in T$.

Motivierendes Beispiel: die Multiplikation von Matrizen

Wir betrachten Matrizen als zentrales Beispiel und extrahieren daraus die folgenden allgemeinen Begriffe. Die so entstehende Darlegung zu Tensorprodukten wird einerseits recht „einfach und konkret“ verlaufen: Was wir am zentralen Beispiel erkennen, formulieren wir nun allgemein.

Sie können, wenn Sie möchten, die folgenden Definitionen und Sätze auch ohne diese Einbettung in den konkreten Beispielkontext lesen. Das macht logisch keinen Unterschied, psychologisch hingegen schon: Die Darstellung wirkt dann vermutlich eher „abstrakt und schwierig“.

Ich plädiere dafür, wie bei nahezu allen mathematischen Themen, zunächst von einem gut gewählten, konkreten Beispiel auszugehen. Daraus schälen wir dann den allgemeingültigen, wahren Kern heraus. Von diesem höheren Standpunkt schreiten wir dann zu Anwendungen.

Allgemein gilt der Erfahrungsgrundsatz: Ein gut verstandenes Beispiel nützt Ihnen mehr als drei schlecht verstandene Sätze. Umgekehrt gilt: Ein gut verstandener Satz bündelt 1000 Beispiele. Nutzen Sie beides!

Beidseitig lineare Räume aka Bimoduln

Definition S2A: beidseitig linearer Raum aka Bimodul

(1) Seien R,S Ringe. Ein (R,S)**–linearer Raum** $(U,+,\bullet,\bar\bullet)$ ist linkslinear über R und rechtslinear über S und beide Operationen sind kompatibel:

$$(r\bullet u)\bar\bullet s = r\bullet(u\bar\bullet s) \quad \text{für alle } r\in R,\ u\in U,\ s\in S$$

Wir nennen U auch **linear über** (R,S) oder einen (R,S)**–Bimodul**.
Zur Betonung schreiben wir ${}_RU_S$ für den (R,S)–linearen Raum U.

(2) Seien U und U' lineare Räume über (R,S). Eine (R,S)**–lineare Abbildung** $f : U \to U'$ ist linkslinear über R und rechtslinear über S:

$$f(u+v) = f(u)+f(v), \quad f(r\bullet u) = r\bullet f(u), \quad f(u\bar\bullet s) = f(u)\bar\bullet s$$

für alle $u,v\in U$, $r\in R$, $s\in S$. Zusammenfassend schreiben wir:

$$\boxed{\operatorname{Hom}_{(R,S)}(U,U') = \{\, f : U\to U' \text{ linear über } (R,S) \,\}}$$

Es gelten die üblichen Rechenregeln für Homomorphismen (I1G).

Beidseitig lineare Räume aka Bimoduln

Ausführlich haben wir hier zwei Skalarmultiplikationen (I1B):

$$\bullet : R\times U \to U : (r,u)\mapsto r\bullet u$$
$$\bar\bullet : U\times S \to U : (u,s)\mapsto u\bar\bullet s$$

Wir fordern einerseits, dass $(U,+,\bullet)$ linkslinear über $(R,+,\cdot)$ ist:

$$\begin{aligned}
r\bullet(u+u') &= (r\bullet u)+(r\bullet u'), & 1_R\bullet u &= u,\\
(r+r')\bullet u &= (r\bullet u)+(r'\bullet u), & (r\cdot r')\bullet u &= r\bullet(r'\bullet u).
\end{aligned}$$

Wir fordern andererseits, dass $(U,+,\bar\bullet)$ rechtslinear über $(S,+,\cdot)$ ist:

$$\begin{aligned}
(u+u')\bar\bullet s &= (u\bar\bullet s)+(u'\bar\bullet s), & u\bar\bullet 1_S &= u,\\
u\bar\bullet(s+s') &= (u\bar\bullet s)+(u\bar\bullet s'), & u\bar\bullet(s'\cdot s) &= (u\bar\bullet s')\bar\bullet s.
\end{aligned}$$

Dies gelte für alle Skalare $r,r'\in R$, $s,s'\in S$ und alle Vektoren $u,u'\in U$.

⚠ Zudem fordern wir die Verträglichkeit $(r\bullet u)\bar\bullet s = r\bullet(u\bar\bullet s)$.

🙂 Die Linearität über (R,S) ist demnach äquivalent zur Linkslinearität über dem Ring $R\times S^{\mathrm{op}}$ und ebenso zur Rechtslinearität über $R^{\mathrm{op}}\times S$.

Beidseitig lineare Räume aka Bimoduln

Beispiel S2B: Links-Rechts-Symmetrie

Sei $(R,+,\cdot)$ ein kommutativer Ring und $(U,+,\bullet)$ linkslinear über R mit

$$\bullet : R\times U\to U : (r,u)\mapsto r\bullet u.$$

Dann ist $(U,+,\bar\bullet)$ ein rechtslinearer Raum über R mit

$$\bar\bullet : U\times R\to U : (u,s)\mapsto u\mathbin{\bar\bullet} s := s\bullet u.$$

Dies ist eine Rechtsoperation, denn für alle $u\in U$ und $s,s'\in R$ gilt

$$(u\mathbin{\bar\bullet}s')\mathbin{\bar\bullet}s \overset{\text{Def}}{=} s\bullet(s'\bullet u) \overset{\text{lOp}}{=} (s\cdot s')\bullet u \overset{\text{Com}}{=} (s'\cdot s)\bullet u \overset{\text{Def}}{=} u\mathbin{\bar\bullet}(s'\cdot s).$$

Damit ist $(U,+,\bullet,\bar\bullet)$ sogar ein (R,R)–linearer Raum (Bimodul), denn

$$(r\bullet u)\mathbin{\bar\bullet}s \overset{\text{Def}}{=} s\bullet(r\bullet u) \overset{\text{lOp}}{=} (s\cdot r)\bullet u \overset{\text{Com}}{=} (r\cdot s)\bullet u \overset{\text{lOp}}{=} r\bullet(s\bullet u) \overset{\text{Def}}{=} r\bullet(u\mathbin{\bar\bullet}s).$$

Dasselbe gilt, wenn wir mit einem rechtslinearen Raum beginnen.

Wir nennen die Links-Rechts-Operation mit $r\bullet u = u\mathbin{\bar\bullet} r$ **kommutativ**.
Das ist die Standardkonvention, sofern nichts anderes vereinbar wird.

Beidseitig lineare Räume aka Bimoduln

In Beispiel S2B haben wir eine Linksoperation vorausgesetzt mit

$$r\bullet(u+u') = (r\bullet u)+(r\bullet u'), \qquad 1_R\bullet u = u,$$
$$(r+r')\bullet u = (r\bullet u)+(r'\bullet u), \qquad (r\cdot r')\bullet u = r\bullet(r'\bullet u).$$

Wir definieren die Rechtsoperation $u\mathbin{\bar\bullet}s := s\bullet u$ und folgern daraus

$$(u+u')\mathbin{\bar\bullet}s = (u\mathbin{\bar\bullet}s)+(u'\mathbin{\bar\bullet}s), \qquad u\mathbin{\bar\bullet}1_S = u,$$
$$u\mathbin{\bar\bullet}(s+s') = (u\mathbin{\bar\bullet}s)+(u\mathbin{\bar\bullet}s'), \qquad u\mathbin{\bar\bullet}(s'\cdot s) = (u\mathbin{\bar\bullet}s')\mathbin{\bar\bullet}s.$$

Die ersten drei sind leicht nachzurechnen: Versuchen Sie es als Übung!
Oben habe ich nur die letzte und einzig kritische Gleichung gezeigt,
denn hier benötigen wir entscheidend die Kommutativität von R.

🙂 Über jedem kommutativen Ring, speziell über jedem Körper,
ist es bequem, die Skalare auf beiden Seiten schreiben zu können.
Die obige Überprüfung rechtfertigt, dass wir dies problemlos dürfen.

🙂 So reiht sich die vertraute kommutative Notation harmonisch
in den allgemeinen, nicht-notwendig-kommutativen Kontext ein.

Beidseitig lineare Räume aka Bimoduln

🙂 Es gibt gute Gründe, auch nicht-kommutative Ringe zu betrachten:

Beispiel: Sei K ein Ring. Dann ist $U=K^{p\times q}$ ein (R,S)–linearer Raum über dem Ring $R=K^{p\times p}$ von links und dem Ring $S=K^{q\times q}$ von rechts.

Beispiel: $V=K^{n\times 1}$ ist rechtslinear über K und linkslinear über $K^{n\times n}$.
Ebenso ist $K^{1\times n}$ ist linkslinear über K und rechtslinear über $K^{n\times n}$.

🙂 Diese erste Beispielgruppe nutzen wir schon lange erfolgreich in der Matrizenrechnung: Hier unterscheiden wir natürlich links und rechts!

Als Skalare können wir immer den Ring $\mathbb{Z}$ der ganzen Zahlen einsetzen:

Beispiel: Ist U linkslinear über R, so auch $(R,\mathbb{Z})$–linear. (I1K)
Ist R kommutativ, so ist U linear über (R,R) dank $u\bullet r := r\bullet u$. (S2B)

Beispiel: Ist U rechtslinear über R, so auch $(\mathbb{Z},R)$–linear. (I1K)
Ist R kommutativ, so ist U linear über (R,R) dank $r\bullet u := u\bullet r$. (S2B)

🙂 Letzteres nutzen wir ebenso intuitiv: Über einem kommutativen Ring,
etwa einem Körper, müssen wir links und rechts nicht unterscheiden.

Beidseitig lineare Räume aka Bimoduln

Beispiel S2C: Links-Rechts-Vertauschung

(1) Seien R,S kommutative Ringe und $(U,+,\bullet,\bullet)$ linear über (R,S).
Dann erhalten wir den (S,R)–linearen Raum ${}_R\overline{U}_S = {}_S\overline{U}_R$ mit

$$\bullet : S\times U\to U \quad : (s,u)\mapsto s\mathbin{\bar\bullet}u := u\bullet s,$$
$$\bar\bullet : U\times R\to U \quad : (u,r)\mapsto u\mathbin{\bar\bullet}r := r\bullet u.$$

(2) Allgemein seien Anti-Involutionen (R2H) auf R und S gegeben:

$$\bar{}\, : R\to R : r\mapsto \overline{r} \quad\text{und}\quad \bar{}\, : S\to S : s\mapsto \overline{s}.$$

Dann erhalten wir den (S,R)–linearen Raum ${}_R\overline{U}_S = {}_S\overline{U}_R$ mit

$$\bullet : S\times U\to U \quad : (s,u)\mapsto s\mathbin{\bar\bullet}u := u\bullet \overline{s},$$
$$\bar\bullet : U\times R\to U \quad : (u,r)\mapsto u\mathbin{\bar\bullet}r := \overline{r}\bullet u.$$

Für jeden kommutativen Ring ist die Identität eine Anti-Involution.
Wir erhalten so die Vertauschung (1) als Spezialfall von (2).

Bilineare Abbildungen und interner Ausgleich

Definition S2D: bilineare Abbildung und interner Ausgleich

Gegeben seien Ringe R, S, T und lineare Räume ${}_RU_S, {}_SV_T, {}_RW_T$.
Eine Abbildung $B : U \times V \to W$ heißt (R,T)**–bilinear**, falls gilt:

1. Für jedes $v \in V$ ist $U \to W : u \mapsto B(u,v)$ linkslinear über R.
2. Für jedes $u \in U$ ist $V \to W : v \mapsto B(u,v)$ rechtslinear über T.

Wir nennen B **ausgeglichen** über S (engl. *balanced*), falls gilt:

3. $B(u \cdot s, v) = B(u, s \cdot v)$ für alle $u \in U$, $v \in V$, $s \in S$.

Gelten alle drei Bedingungen, so nennen wir B kurz (R,S,T)**–bilinear**:

$$\mathrm{Bil}_{(R,S,T)}(U,V;W) = \{\, B : U \times V \to W \text{ bilinear über } (R,S,T) \,\}$$

Beispiel: Sei R kommutativ und U, V, W lineare Räume über R (S2B).
Ist $B : U \times V \to W$ bilinear über (R,R), dann auch über (R,R,R):

$$\begin{aligned} B(u \cdot r, v) &\overset{\text{Sym}}{=} B(r \cdot u, v) \overset{\text{lLin}}{=} r \cdot B(u,v) \\ &\overset{\text{Sym}}{=} B(u,v) \cdot r \overset{\text{rLin}}{=} B(u, v \cdot r) \overset{\text{Sym}}{=} B(u, r \cdot v) \end{aligned}$$

Bilineare Abbildungen und interner Ausgleich

Beispiel: Die Matrixmultiplikation ist bilinear, wie auf Seite S201 erklärt; das war unser motivierendes Beispiel, das wir als Leitbild voranstellen:

$$\mu : K^{a\times b} \times K^{b\times c} \to K^{a\times c} : (u,v) \mapsto w = u \cdot v, \quad w_{i,k} = \textstyle\sum_{j=1}^{b} u_{i,j} \cdot v_{j,k}$$

Hier operieren die Ringe $R = K^{a\times a}$ und $S = K^{b\times b}$ und $T = K^{c\times c}$ auf den Räumen ${}_RU_S = K^{a\times b}$ und ${}_SV_T = K^{b\times c}$ und ${}_RW_T = K^{a\times c}$.
Die Produktabbildung $\mu : U \times V \to W$ ist (R,S,T)–bilinear, denn es gilt

$$\begin{aligned} \mu(u+u',v) &= \mu(u,v) + \mu(u',v), & \mu(r \cdot u, v) &= r \cdot \mu(u,v), \\ \mu(u, v+v') &= \mu(u,v) + \mu(u,v'), & \mu(u, v \cdot t) &= \mu(u,v) \cdot t, \\ & & \mu(u \cdot s, v) &= \mu(u, s \cdot v) \end{aligned}$$

für alle Vektoren $u, u' \in U$, $v, v' \in V$ und Skalare $r \in R$, $s \in S$, $t \in T$.

🙂 Wir wollen nun jede bilineare Abbildung $\mu : U \times V \to Z$ linearisieren: Uns genügt *eine* einzige, universelle bilineare Abbildung $\tau : U \times V \to W$, um *jede* bilineare Abbildung $\mu : U \times V \to Z$ auf eine lineare Abbildung $f : W \to Z$ zu reduzieren, sodass $\mu = f \circ \tau$ gilt.

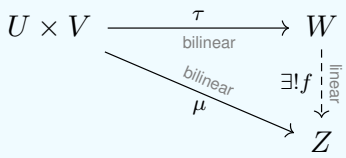
Das Tensorprodukt und seine universelle Eigenschaft

Definition S2E: Tensorprodukt

Gegeben seien Ringe R, S, T und lineare Räume ${}_RU_S$ und ${}_SV_T$.

(1) Ein **Produkt** des Paars (U,V) über (R,S,T) mit Werten in ${}_RZ_T$ ist eine (R,S,T)–bilineare Abbildung $\mu : U \times V \to Z$.

(2) Ein **Tensorprodukt** des Paars (U,V) über (R,S,T) ist ein Produkt $\tau : U \times V \to W$ mit der folgenden universellen Abbildungseigenschaft:



Jedes Produkt $\mu : U \times V \to Z$ faktorisiert eindeutig über τ, das heißt es existiert genau eine (R,T)–lineare Abbildung $f : W \to Z$ mit $\mu = f \circ \tau$.

Diese Forderung ist äquivalent zur Bijektivität der natürlichen Abbildung

$$\Phi_\tau^Z : \mathrm{Hom}_{(R,T)}(W,Z) \to \mathrm{Bil}_{(R,S,T)}(U,V;Z) : f \mapsto \mu = f \circ \tau.$$

Das Tensorprodukt und seine universelle Eigenschaft

🙂 In anderen Worten bedeutet das: (1) τ ist ein Produkt und (2) jedes Konkurrenzprodukt μ faktorisiert eindeutig über τ.

🙂 Die Bijektivität von Φ_τ^Z bedeutet, dass wir jede bilineare Abbildung $\mu : U \times V \to Z$ in eine lineare Abbildung $f : W \to Z$ umrechnen können.

🙂 In Satz S2H zeigen wir die Eindeutigkeit bis auf Isomorphie.
Für *das* Tensorprodukt von U, V über (R,S,T) schreiben wir dann

$$\otimes : U \times V \to U \otimes_S V : (u,v) \mapsto u \otimes v.$$

In dieser Schreibweise gilt $\mu(u,v) = f(u \otimes v)$ für alle $u \in U$ und $v \in V$.

⚠ Das Symbol „$\otimes$“ hat hier zwei Bedeutungen: Einerseits ist $u \otimes v$ das Tensorprodukt der beiden Vektoren $u \in U$ und $v \in V$ im Raum $U \otimes_S V$. Andererseits ist $U \otimes_S V$ das Tensorprodukt der beiden Räume U und V.

Wenn der Ring S aus dem Kontext klar ist, müssen wir ihn nicht explizit wiederholen. Erfahrungsgemäß ist dies jedoch anfangs meist hilfreich.

Das Tensorprodukt und seine universelle Eigenschaft

Definition S2E: einfache Tensoren

(3) Für Tensorprodukte vereinbaren wir folgende Sprechweisen.
Jedes Element $w \in U \otimes V$ des Tensorraums nennen wir einen **Tensor**.

Hat $w \in U \otimes V$ die besonders einfache Form $w = u \otimes v$ mit $u \in U$ und $v \in V$, so nennen wir den Tensor w **einfach** oder **elementar** oder **rein**.

Anders gesagt, die Menge der **einfachen Tensoren** ist das Bild der Produktabbildung $\otimes : U \times V \to U \otimes V$. Diese ist i.A. nicht surjektiv!

Der Tensorraum entsteht aus allen **Summen** einfacher Tensoren; solche Summen sind im Allgemeinen keine einfachen Tensoren.

Wir haben dies zuvor bereits im Anschluss an Definition S1B diskutiert und illustriert. Wir werden diese Frage später wiederholt aufgreifen.

Das Tensorprodukt und seine universelle Eigenschaft

☺ Über einem Körper K können wir jedes Tensorprodukt sehr konkret erklären durch die **universelle Basiseigenschaft**, siehe Definition S1B.

☹ Für lineare Räume über beliebigen Ringen verfügen wir meist nicht über Basen, daher ist diese Sichtweise hier nicht mehr hilfreich.

☺ Wir vollziehen daher den nötigen Perspektivwechsel und nutzen zur allgemeinen Definition S2E die **universelle Abbildungseigenschaft**.

⚠ Statt einer expliziten Definition durch Konstruktion (wie etwa in S1A) folgen wir der inneren Logik und den äußeren Zwängen und formulieren eine implizite Definition durch eine charakterisierende Eigenschaft.

Das ist mathematisch gesehen der beste Weg: effizient und elegant.
Beim ersten Kontakt ist es ungewohnt und bedarf der Gewöhnung;
wie immer gelingt dies am besten durch aktive Einübung.

Die elegante Definition S2E mittels UAE zieht sofort Arbeit nach sich:
Existenz und Eindeutigkeit müssen anschließend noch gezeigt werden.
Auch mit diesen Konstruktionen üben Sie Verständnis und Anwendung.

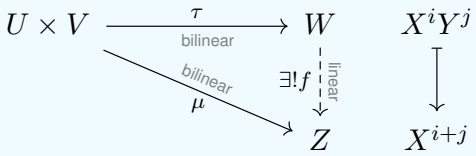
Das Tensorprodukt und seine universelle Eigenschaft

Beispiel S2F: Polynommodell

Sei K ein kommutativer Ring. Wir betrachten $U = V = K[X]$ und vergleichen zwei Produkte nach $W = K[X,Y]$ und $Z = K[X]$:

$$\begin{aligned} \tau &: K[X] \times K[X] \to K[X,Y] &&: (u,v) \mapsto u(X)v(Y). \\ \mu &: K[X] \times K[X] \to K[X] &&: (u,v) \mapsto u(X)v(X). \end{aligned}$$

Das erste Produkt τ hat die universelle Abbildungseigenschaft (S2G).
Wir wenden dies speziell auf das Konkurrenzprodukt μ an:



Das zweite Produkt μ faktorisiert eindeutig über τ gemäß $\mu = f \circ \tau$.

Für jedes solche f gilt $f(X^iY^j) = f(\tau(X^i, X^j)) = \mu(X^i, X^j) = X^{i+j}$.
Dank PLF (K1B) existiert $f : W \to Z : X^iY^j \mapsto X^{i+j}$ linear über K.

Das Tensorprodukt und seine universelle Eigenschaft

☺ Wir rechnen gleich in Satz S2G allgemein nach, dass unser Beispiel $\tau : U \times V \to W$ tatsächlich die universelle Abbildungseigenschaft hat.

Zur Illustration vergleichen wir τ mit dem zweiten Produkt $\mu : U \times V \to Z$ und konstruieren explizit die lineare Abbildung $f : W \to Z$ mit $\mu = f \circ \tau$.

Alle Daten liegen explizit vor, daher gelingt uns diese Rechnung leicht:
Sowohl die Eindeutigkeit als auch die Existenz von f sind offensichtlich.

☺ Hinter diesem schön einfachen Beispiel steht ein nützliches Prinzip über jedem kommutativen Ring, insbesondere über jedem Körper:

Für Räume mit Basis ist die universelle Abbildungseigenschaft S2E des Tensorprodukts äquivalent zur universellen Basiseigenschaft S1B.

Der folgende Satz formuliert dies detailliert aus.

Das Prinzip der bilinearen Fortsetzung

Satz S2G: Prinzip der bilinearen Fortsetzung

Gegeben seien Ringe R, T sowie lineare Räume ${}_RU$ und V_T und ${}_RW_T$.

(1) Gegeben seien Basen $(u_i)_{i\in I}$ von U und $(v_j)_{j\in J}$ von V sowie eine beliebige Familie $(w_{i,j})_{(i,j)\in I\times J}$ in W, die Gram–Matrix. Dann existiert genau eine bilineare Abbildung $\tau : U \times V \to W : (u_i, v_j) \mapsto w_{i,j}$, nämlich

$$\tau\Big(\sum_{i\in I} r_i u_i,\ \sum_{j\in J} v_j t_j\Big) = \sum_{(i,j)\in I\times J} r_i\, w_{i,j}\, t_j$$

für alle Linearkombinationen mit Koeffizienten $r \in R^{(I)}$ und $t \in T^{(J)}$.

(2) Sei zudem $R = T$ kommutativ und U, V, W linear über R (S2B). Genau dann ist $\tau : U \times V \to W$ ein Tensorprodukt, erfüllt also die universelle Eigenschaft S2E, wenn $(w_{i,j})_{(i,j)\in I\times J}$ eine Basis von W ist.

⚠ Warnung vor Missverständnis: Ist $\tau : U \times V \to W$ bilinear, so bildet τ die Basisvektoren $(u_i, 0)$ und $(0, v_j)$ von $U \times V$ alle auf 0 in W ab.

Das Prinzip der bilinearen Fortsetzung

Beweis: (1a) Eindeutigkeit: Sind $\tau, \tau' : U \times V \to W : (u_i, v_j) \mapsto w_{i,j}$ bilinear, so folgt $\tau = \tau'$, denn für alle $u = \sum_i r_i u_i$ und $v = \sum_j v_j t_j$ gilt:

$$\tau\big(\textstyle\sum_i r_i u_i, \sum_j v_j t_j\big) \overset{\text{Bil}}{=} \sum_i \sum_j r_i \tau(u_i, v_j) t_j \overset{\text{Vor}}{=} \sum_{i,j} r_i\, w_{i,j}\, t_j$$
$$\overset{\text{Vor}}{=} \sum_i \sum_j r_i \tau'(u_i, v_j) t_j \overset{\text{Bil}}{=} \tau'\big(\textstyle\sum_i r_i u_i, \sum_j v_j t_j\big)$$

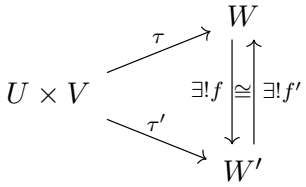
(1b) Existenz: Diese Formel definiert eine Abbildung $\tau : U \times V \to W$, sie erfüllt $(u_i, v_j) \mapsto w_{i,j}$ für alle $(i, j) \in I \times J$ und ist (R, T)–bilinear.

(2a) „⇐“: Sei $(w_{i,j})_{(i,j)\in I\times J}$ eine Basis von W. Sei $\mu : U \times V \to Z$ bilinear. Dank PLF (K1B) existiert genau eine R–lineare Abbildung $f : W \to Z$ mit $f(w_{i,j}) = \mu(u_i, v_j)$. Dank (1a) gilt dann $\mu = f \circ \tau$.

(2b) „⇒“: Angenommen $\tau : U \times V \to W$ erfüllt die UAE (S2E). Der R–lineare Raum $W' = R^{(I\times J)}$ hat die R–Basis $(e_{i,j})_{(i,j)\in I\times J}$. Dank (1b) existiert $\tau' : U \times V \to W' : (u_i, v_j) \mapsto e_{i,j}$ bilinear über R. Dank (2a) ist τ' ein Tensorprodukt, erfüllt also ebenfalls die UAE.

Der folgende Satz konstruiert den R–Isomorphismus $f' : W' \xrightarrow{\sim} W$ mit $\tau = f' \circ \tau'$. Somit ist $(w_{i,j} = f'(e_{i,j}))_{(i,j)\in I\times J}$ eine R–Basis von W. QED

Das Tensorprodukt ist eindeutig bis auf Isomorphie.



Eindeutigkeit trotz Wahlfreiheit: Alice und Bob konstruieren ihre Tensorprodukte wie sie mögen. Je zwei Tensorprodukte lassen sich eindeutig übersetzen.

Satz S2H: Eindeutigkeit des Tensorprodukts

Gegeben seien Ringe R, S, T sowie lineare Räume ${}_RU_S$ und ${}_SV_T$.

Dann sind je zwei Tensorprodukte $\tau : U \times V \to W$ und $\tau' : U \times V \to W'$ eindeutig isomorph: Es existiert genau ein (R, T)–Isomorphismus $(f, f') : W \cong W'$, für den $\tau' = f \circ \tau$ und $\tau = f' \circ \tau'$ gilt.

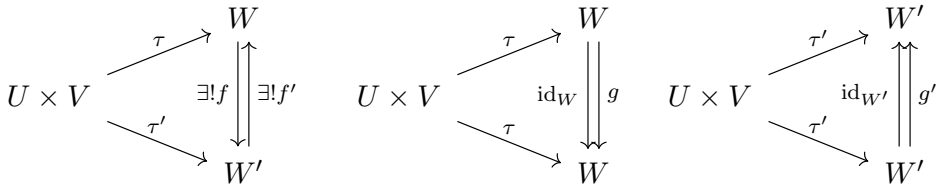
Für *das* Tensorprodukt von U, V über (R, S, T) schreiben wir fortan

$$\otimes : U \times V \to U \otimes_S V : (u, v) \mapsto u \otimes v.$$

Wir schreiben kurz $U \otimes V$, falls der Ring S aus dem Kontext hervorgeht.

Das Tensorprodukt ist eindeutig bis auf Isomorphie.

Beweis: Wir konstruieren (f, f') durch vierfache Anwendung der UAE:



(a) Dank der UAE des Tensorprodukts τ angewendet auf τ' existiert genau eine (R, T)–lineare Abbildung $f : W \to W'$ mit $\tau' = f \circ \tau$.

(b) Dank der UAE des Tensorprodukts τ' angewendet auf τ existiert genau eine (R, T)–lineare Abbildung $f' : W' \to W$ mit $\tau = f' \circ \tau'$.

(c) Für $g = f' \circ f : W \to W$ gilt $g \circ \tau = \tau = \mathrm{id}_W \circ \tau$, also $g = \mathrm{id}_W$ dank Eindeutigkeit / UAE des Tensorprodukts τ angewendet auf τ.

(d) Für $g' = f \circ f' : W' \to W'$ gilt $g' \circ \tau' = \tau' = \mathrm{id}_{W'} \circ \tau'$, also $g' = \mathrm{id}_{W'}$ dank Eindeutigkeit / UAE des Tensorprodukts τ' angewendet auf τ'.

Somit gilt $f' \circ f = \mathrm{id}_W$ und $f \circ f' = \mathrm{id}_{W'}$, also $(f, f') : W \cong W'$. QED

Erinnerung: die Rechenregeln für Tensoren

Gegeben seien Ringe R, S, T und lineare Räume ${}_RU_S$ und ${}_SV_T$.
Wir wissen, dass das Tensorprodukt $U \otimes V$ eindeutig ist, genauer:
Je zwei Tensorprodukte sind eindeutig isomorph. Wir wollen nun die Existenz eines solchen Tensorprodukts zeigen. Hierzu müssen wir eine Konstruktion durchführen. Zuvor erinnern wir uns nochmal an unser Ziel:

(1) Wir nennen $\otimes : U \times V \to W$ ein **Produkt**, falls gilt:

$$\begin{aligned} (u+u')\otimes v &= u\otimes v + u'\otimes v, & (r\cdot u)\otimes v &= r\cdot(u\otimes v),\\ u\otimes(v+v') &= u\otimes v + u\otimes v', & u\otimes(v\cdot t) &= (u\otimes v)\cdot t,\\ (u\cdot s)\otimes v &= u\otimes(s\cdot v) \end{aligned}$$

für alle Vektoren $u, u' \in U$, $v, v' \in V$ und Skalare $r \in R$, $s \in S$, $t \in T$.

(2) Für ein **Tensorprodukt** fordern wir genau diese Eigenschaften, doch sonst keine weiteren, also überflüssigen Relationen (UAE).

🙂 Das ist die Forderung der universellen Abbildungseigenschaft!
Genau so wollen wir daher in der folgenden Konstruktion vorgehen.

Erinnerung: die Rechenregeln für Tensoren

Satz S2ı: Existenz des Tensorprodukts
Zu (U, V) über (R, S, T) existiert ein Tensorprodukt $\tau : U \times V \to W$.

Dieser abstrakte Existenzsatz ist zwar beruhigend, doch für sich alleine noch längst nicht so hilfreich, wie wir es gerne hätten und benötigen.

Hermann Weyl schrieb hierzu in seinem Artikel *Über die neue Grundlagenkrise der Mathematik* 1921 die weisen Worte:

Ein Existenzsatz verkündet
„das Vorhandensein eines Schatzes,
ohne jedoch zu verraten, an welchem Ort. […]
Nicht das Existenztheorem ist das Wertvolle,
sondern die im Beweise geführte Konstruktion.“

🙂 Die folgende Konstruktion erlaubt uns, den Schatz zu heben!
Sie liefert eine explizite Präsentation durch Erzeuger und Relationen, und erlaubt uns damit eine genauere Untersuchung der Feinstruktur.

Existenz des Tensorprodukts durch explizite Konstruktion

Satz S2ı: Existenz des Tensorprodukts
Zu (U, V) über (R, S, T) existiert ein Tensorprodukt $\tau : U \times V \to W$.

Wir betrachten die Menge $U \times V$ aller Paare (u, v) mit $u \in U$ und $v \in V$.
Sei $F = \mathbb{Z}^{(U\times V)}$ der $\mathbb{Z}$–lineare Raum mit Basis $U \times V$: Jedes Element $\sigma \in F$ ist eine $\mathbb{Z}$–Linearkombination $\sigma = \sigma_1 \cdot (u_1, v_1) + \cdots + \sigma_n \cdot (u_n, v_n)$ von Paaren $(u_i, v_i) \in U \times V$ mit Koeffizienten $\sigma_i \in \mathbb{Z}$. Hierin setzen wir

$$G := \left\langle \begin{array}{l|l} (u+u',v)-(u,v)-(u',v) & u,u'\in U\\ (u,v+v')-(u,v)-(u,v') & v,v'\in V\\ (u\cdot s,v)-(u,s\cdot v) & s\in S \end{array} \right\rangle_{\mathbb{Z}} \leq F.$$

(0) Wir erhalten die Quotientenabbildung $q : F \twoheadrightarrow W := F/G : \sigma \mapsto [\sigma]$.
(1) Die abelsche Gruppe W wird zu einem (R, T)–linearen Raum durch

$$\begin{aligned} \cdot &: R \times W \to W \;:\; r\cdot[(u,v)] = [(r\cdot u, v)],\\ \cdot &: W \times T \to W \;:\; [(u,v)]\cdot t = [(u, v\cdot t)]. \end{aligned}$$

(2) Damit ist $\tau : U \times V \to W : (u, v) \mapsto u \otimes v := [(u, v)]$ ein Produkt
(3) und erfüllt zudem die universelle Abbildungseigenschaft S2E.

Existenz des Tensorprodukts durch explizite Konstruktion

🙂 Wir präsentieren hier $W = F/G$ durch **Erzeuger** und **Relationen**:
Dazu beginnen wir mit einem freien Objekt F, ohne jegliche Relationen, und erzwingen die gewünschten Relationen G durch Quotientenbildung.

⚠ Wir müssen nun noch sorgsam und geduldig nachrechnen, dass diese Konstruktion das gewünschte Ziel tatsächlich erreicht.
Genau dies ist Gegenstand des folgenden Beweises.

🙂 Das ist eigentlich Routinearbeit – nachdem man es ein paar Mal durchexerziert hat. In diesem Zusammenhang schrieb Hermann Weyl:

Nicht im Beweis einer gegebenen Konstruktion,
sondern in der Erfindung der Konstruktion liegt
in den meisten Fällen die eigentliche Schwierigkeit.

Da dieser routinierte Nachweis für Sie eine der ersten Gelegenheiten ist, und Sie genau diese Sorgfalt und Routine erst noch erlernen sollen, möchte ich hier ein gutes Vorbild geben und dies für Sie vorführen.
Zudem können wir so Verständnisschwierigkeiten klären.

Existenz des Tensorprodukts durch explizite Konstruktion

Lösung: (1) Auf $F = \mathbb{Z}^{U\times V}$ haben wir die Linksoperation

$$\bullet : R \times F \to F \,:\, r \bullet (u,v) = (r \bullet u, v).$$

Für jeden Skalar $r \in R$ gilt $r \bullet G \subseteq G$, denn dies gilt auf den Erzeugern:

$$\begin{aligned} r \bullet [(u+u',v) - (u,v) - (u',v)] &= (r\bullet u + r \bullet u', v) - (r\bullet u, v) - (r \bullet u', v) \\ r \bullet [(u, v+v') - (u,v) - (u,v')] &= (r \bullet u, v+v') - (r\bullet u, v) - (r \bullet u, v') \\ r \bullet [(u\bullet s, v) - (u, s\bullet v)] &= ((r\bullet u)\bullet s, v) - ((r\bullet u), s \bullet v) \end{aligned}$$

Somit erhalten wir auf $W = F/G$ die wohldefinierte Linksoperation

$$\bullet : R \times W \to W \,:\, r \bullet [(u,v)] = [(r\bullet u, v)].$$

Ebenso operiert der Ring T von rechts auf $W = F/G$ vermöge

$$\bullet : W \times T \to W \,:\, [(u,v)] \bullet t = [(u, v\bullet t)].$$

Damit ist W ein (R,T)–Modul: Rechnen Sie es nach!

Existenz des Tensorprodukts durch explizite Konstruktion

(1a) Die Linksoperation $\bullet : R \times F \to F : r \bullet (u,v) = (r\bullet u, v)$ erfüllt

$$1_R \bullet (u,v) = (u,v) \quad \text{und} \quad (r\cdot r') \bullet (u,v) = r \bullet (r' \bullet (u,v)).$$

Demnach folgt für $\bullet : R \times W \to W$ ebenso

$$1_R \bullet [(u,v)] = [(u,v)] \quad \text{und} \quad (r\cdot r') \bullet [(u,v)] = r \bullet (r' \bullet [(u,v)]).$$

Die Operation ist zudem links-distributiv auf F, also auch auf W:

$$r \bullet [\sigma + \sigma'] = [r\bullet\sigma + r\bullet\sigma'] = [r\bullet\sigma] + [r\bullet\sigma'] = r\bullet[\sigma] + r\bullet[\sigma']$$

Die Operation ist *nicht* rechts-distributiv auf F, sondern erst auf W:

$$\begin{aligned} (r+r') \bullet [(u,v)] &= [(r\bullet u + r' \bullet u, v)] \\ &= [(r\bullet u, v)] + [(r'\bullet u, v)] = r \bullet [(u,v)] + r' \bullet [(u,v)] \end{aligned}$$

(1b) Für die Rechtsoperationen $\bullet : F \times T \to F : (u,v)\bullet t = (u, v\bullet t)$ und $\bullet : W \times T \to W : [(u,v)] \bullet t = [(u, v\bullet t)]$ gilt entsprechend dasselbe.

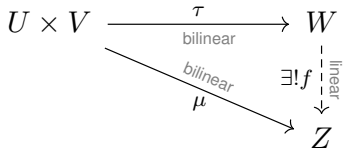
(1c) Beide sind kompatibel, offensichtlich auf F, somit auch auf W.

Existenz des Tensorprodukts durch explizite Konstruktion

(2) Unser $\tau : U \times V \to W : (u,v) \mapsto u \otimes v := [(u,v)]$ ist ein Produkt: Für alle $u,u' \in U$, $v,v' \in V$, $r \in R$, $s \in S$, $t \in T$ gilt nach Konstruktion

$$\begin{aligned} (u+u')\otimes v &= u\otimes v + u'\otimes v, & (r\bullet u)\otimes v &= r\bullet(u\otimes v), \\ u\otimes(v+v') &= u\otimes v + u\otimes v', & u\otimes(v\bullet t) &= (u\otimes v)\bullet t, \\ (u\bullet s)\otimes v &= u\otimes(s\bullet v). \end{aligned}$$

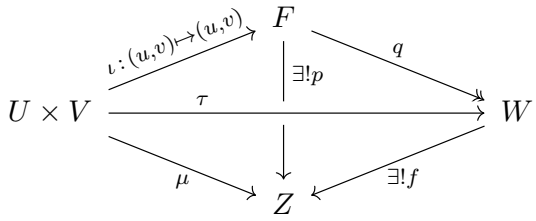
(3) Unser Produkt τ hat die universelle Abbildungseigenschaft S2E:



Sei $\mu : U \times V \to Z$ ein weiteres Produkt. Wir zeigen, dass genau eine (R,T)–lineare Abbildung $f : W \to Z$ mit $\mu = f \circ \tau$ existiert.

Existenz des Tensorprodukts durch explizite Konstruktion

(3a) Eindeutigkeit: Vorgelegt seien $f, g : W \to Z$ mit $\mu = f\circ\tau = g\circ\tau$, also $f(u\otimes v) = f(\tau(u,v)) = g(\tau(u,v)) = g(u\otimes v)$ für $(u,v) \in U\times V$. Daraus folgt $f = g$, denn W wird erzeugt von $(u\otimes v)_{(u,v)\in U\times V}$ (K1A).



(3b) Wir nutzen $F = \mathbb{Z}^{(U\times V)}$ mit Basis $U \times V$ über $\mathbb{Z}$. Dank PLF (K1B) existiert genau eine $\mathbb{Z}$–lineare Abbildung $p : F \to Z : (u,v) \mapsto \mu(u,v)$. Da μ ein Produkt ist, gilt $\ker(p) \supseteq G$. Demnach induziert p die $\mathbb{Z}$–lineare Abbildung $f : W \to Z$ mit $p = f\circ q$ (I2E). Somit gilt $f(u\otimes v) = \mu(u,v)$ für alle $u \in U$ und $v \in V$. Insbesondere ist f damit linear über (R,T), denn $f(r\bullet(u\otimes v)\bullet t) = \mu(r\bullet u, v\bullet t) = r\bullet\mu(u,v)\bullet t = r\bullet f(u\otimes v)\bullet t$. Homogenität gilt für alle einfachen Tensoren, also für alle Tensoren.

Die einfachen Tensoren erzeugen den Tensorraum.

Korollar S2J: Einfache Tensoren erzeugen alle Tensoren.

Vorgelegt seien Ringe R, S, T sowie lineare Räume ${}_RU_S$ und ${}_SV_T$.

(1) Die einfachen Tensoren $u \otimes v$ erzeugen den Tensorraum $U \otimes_S V$.

Jeder Tensor $w \in U \otimes_S V$ ist eine endliche Summe $w = \sum_{k=1}^{\ell} u_k \otimes v_k$ einer Länge $\ell \in \mathbb{N}$ mit Faktoren $u_1, \dots, u_\ell \in U$ und $v_1, \dots, v_\ell \in V$.

Beweis: (1) Dies folgt aus der Konstruktion von Satz S2I. QED

⚠ Diese Darstellung von w ist im Allgemeinen nicht eindeutig!

⚠ Nicht einmal die Länge ℓ dieser Summe ist eindeutig!

$$\begin{aligned} w = u \otimes v &= (u_1 + u_2) \otimes (v_1 + v_2) \\ &= (u_1 \otimes v_1) + (u_1 \otimes v_2) + (u_2 \otimes v_1) + (u_2 \otimes v_2). \end{aligned}$$

🙂 Minimale Länge $\ell = 0$ entspricht dem Nullelement $w = 0$ in $U \otimes_S V$.

🙂 Minimale Länge $\ell = 1$ entspricht einfachen Tensoren $w = u \otimes v \neq 0$.

Zu $w \in U \otimes V$ ist der **Tensorrang** $\operatorname{rang}(w)$ die Minimale Länge $\ell \in \mathbb{N}$ aller Summendarstellungen $w = \sum_{k=1}^{\ell} u_k \otimes v_k$ durch einfache Tensoren.

Die einfachen Tensoren erzeugen den Tensorraum.

Korollar S2J: Einfache Tensoren erzeugen alle Tensoren.

(2) Angenommen, $(u_i)_{i \in I}$ erzeugt U über R und $(v_j)_{j \in J}$ erzeugt V über T, dann wird der Tensorraum $U \otimes_S V$ über (R, T) erzeugt von

$$(u_i \otimes v_i)_{(i,j) \in I \times J}.$$

Jeder Tensor $w \in U \otimes_S V$ ist eine Summe $w = \sum_{k=1}^{\ell} r_k u_{i_k} \otimes v_{j_k} t_k$ mit endlicher Länge $\ell \in \mathbb{N}$ sowie $r_1, \dots, r_\ell \in R$ und $t_1, \dots, t_\ell \in T$.

Beweis: (2) Gemäß (1) ist jeder Tensor $w \in U \otimes_S V$ eine Summe einfacher Tensoren $u \otimes v$. Dabei gilt $u = \sum_{m=1}^{M} r_m u_{i_m}$ mit $r_m \in R$ und $v = \sum_{n=1}^{N} v_{j_n} t_n$ mit $t_n \in T$, also $u \otimes v = \sum_{m,n} r_m u_{i_m} \otimes v_{j_n} t_n$. QED

🙂 So konstruieren wir geeignete Erzeugendensysteme von $U \otimes_S V$, am besten möglichst kurz und somit effizient für unsere Rechnungen.

🙂 In günstigen Fällen erhalten wir sogar eine Basis (S2G), insbesondere über einem kommutativen Ring $R = S = T$.

Universelle Eigenschaft, Eindeutigkeit und Existenz

Das Tensorprodukt illustriert ein allgemein sehr nützliches Vorgehen:

1. Die universelle Eigenschaft S2E präzisiert, was wir eigentlich wollen.
2. Die Eindeutigkeit S2H zeigt, dass unser Ziel damit charakterisiert ist.
3. Die Konstruktion S2I zeigt, dass / wie unser Wunsch erfüllbar ist.

Damit verfügen wir über zwei sich ergänzende Werkzeuge:

🙂 Die Präsentation F/G ist konkret, leider meist schwer zu nutzen.

🙂 Die universelle Eigenschaft ist abstrakt, dafür meist leicht zu nutzen.

Mathematische Objekte (wie lineare Räume, ...) lassen sich meist am besten verstehen und nutzen, wenn wir beide Sichtweisen anwenden: intern, konkret, Rechnen mit Elementen (Basen, Matrizen, ...) und extern, abstrakt, mit Abbildungen (Homomorphismen, PLF, ...).

Je nach Anwendung nutzen wir mehr die eine oder die andere, meist jedoch benötigen Sie beide Sichtweisen für die erfolgreiche Lösung.

Universelle Eigenschaft, Eindeutigkeit und Existenz

Mathematische Objekte betrachten wir oft auf diese zwei Arten, da sie zueinander komplementär sind und sich wunderbar ergänzen. Das gilt nicht nur, aber ganz besonders für algebraische Objekte, wie Monoide und Gruppen, Ringe und Körper, oder hier lineare Räume:

Menge X mit Struktur	**Objekt X mit Morphismen**
interne Beschaffenheit von X	externe Eigenschaften von X
Beziehung zwischen Elementen	Beziehung zu anderen Objekten
Datenstruktur, Implementierung	Verhalten, Semantik, Axiome
Was ist X? Wie ist X aufgebaut?	Was tut X? Was leistet X für uns?
konkret und theoretisch	abstrakt und angewandt
explizite Bauanleitung	bequeme Bedienungsanleitung
Erzeuger und Relationen	universelle Eigenschaft
Konstruktion $\Rightarrow$ Existenz	Definition $\Rightarrow$ Eindeutigkeit

Satz S2K: Assoziativität des Tensorprodukts

Gegeben seien drei lineare Räume ${}_RU_S$ und ${}_SV_T$ und ${}_TW_Q$.
(0) Genau wie für zwei Faktoren (U,V) bzw. (V,W) erklären wir auch für drei Faktoren (U,V,W) das Tensorprodukt:

$$\tau : U \times V \times W \to U \otimes_S V \otimes_T W$$

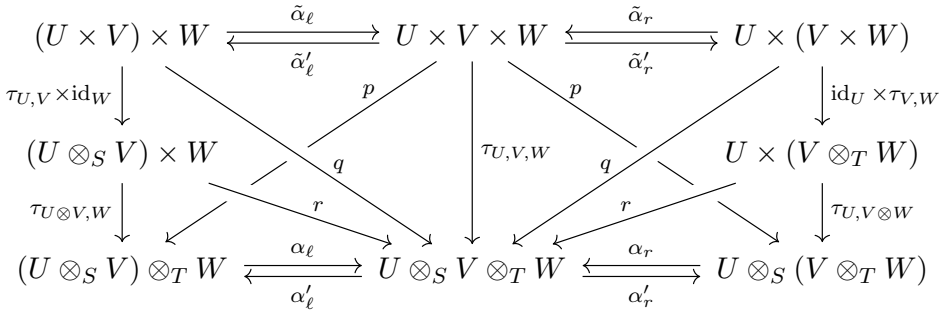
(1) Hierzu existieren eindeutig die natürlichen (R,Q)–Isomorphismen

$$\begin{array}{ccccc} (U \otimes_S V) \otimes_T W & \cong & U \otimes_S V \otimes_T W & \cong & U \otimes_S (V \otimes_T W), \\ (u \otimes v) \otimes w & \leftrightarrows & u \otimes v \otimes w & \leftrightarrows & u \otimes (v \otimes w). \end{array}$$

Die *Eindeutigkeit* ist klar (K1A), denn die einfachen Tensoren erzeugen den Tensorraum (S2J). Die *Existenz* der ersehnten Abbildungen muss jedoch sorgsam nachgewiesen werden, und zwar durch Konstruktion!

⚠ Wir können nicht einfach irgend etwas auf den einfachen Tensoren vorschreiben, sondern müssen zudem auch alle Relationen erfüllen. Ein drastisches Gegenbeispiel ist das No-Cloning-Theorem S1E!

Aufgabe: Beweisen Sie die Existenz durch Konstruktion dank UAE!



Wir haben $(\tilde\alpha_\ell, \tilde\alpha'_\ell) : (U \times V) \times W \cong U \times V \times W : ((u,v),w) \leftrightarrows (u,v,w)$. Die Komposition $p = \tau_{U\otimes V,W} \circ (\tau_{U,V} \times \mathrm{id}_W) \circ \tilde\alpha'$ ist (R,S,T,Q)–trilinear, induziert dank UAE also $\alpha'_\ell : u \otimes v \otimes w \mapsto (u \otimes v) \otimes w$, wie ersehnt.

Die Komposition $q = \tau_{U,V,W} \circ \tilde\alpha$ ist (R,S,T)–bilinear in $U \times V$, induziert dank UAE also r. Letzteres ist (R,T,Q)–linear, induziert dank UAE also $\alpha_\ell : (u \otimes v) \otimes w \mapsto u \otimes v \otimes w$, wie ersehnt. Demnach gilt $\alpha'_\ell \circ \alpha_\ell = \mathrm{id}$ und $\alpha_\ell \circ \alpha'_\ell = \mathrm{id}$ auf den einfachen Tensoren, also auf allen Tensoren (S2J).

Ausführung

Wir diskutieren vertraute Rechenregeln, hier für das Tensorprodukt: Assoziativität, Kommutativität, Neutrales und Distributivität.
Unter diesen ist die Assoziativität die aufwändigste; wir führen sie detailliert aus, die weiteren Rechnungen sind dann leichtere Übungen.

Kommutativität des Tensorprodukts

Satz S2L: Kommutativität des Tensorprodukts

Gegeben seien Ringe R, S, T und lineare Räume ${}_RU_S$ und ${}_SV_T$.

(1) Ist $R = S = T$ kommutativ, so haben wir den Isomorphismus

$$U \otimes_S V \cong V \otimes_S U \;:\; u \otimes v \leftrightarrows v \otimes u.$$

(2) Zu gegebenen Anti-Involutionen auf R, S, T haben wir ebenso

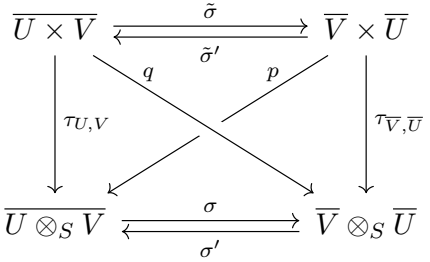
$$\overline{U \otimes_S V} \cong \overline{V} \otimes_S \overline{U} \;:\; u \otimes v \leftrightarrows v \otimes u.$$

Typische Anwendungsbeispiele dieses allgemeineren Falls sind die Konjugation auf $\mathbb{C}$ oder $\mathbb{H}$ oder die Transposition auf Matrizen.

Aufgabe: Konstruieren Sie diese Isomorphismen dank UAE.

Kommutativität des Tensorprodukts

Lösung: Es genügt statt (1) gleich den allgemeineren Fall (2) zu zeigen. Die Konstruktion verläuft von oben nach unten in folgendem Diagramm:



Neutrales zum Tensorprodukt

Satz S2M: Neutrales zum Tensorprodukt

Gegeben seien Ringe R, S, T und lineare Räume ${}_RU_S$ und ${}_SV_T$.

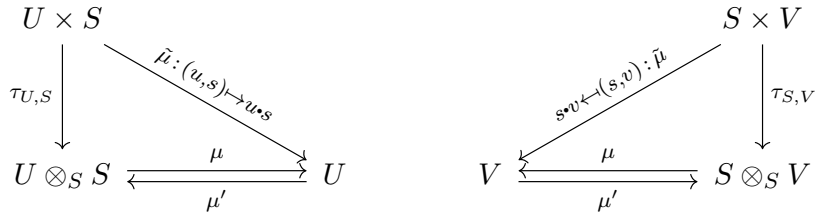
Dann wirkt der Raum ${}_SS_S$ neutral bezüglich des Tensorprodukts:

$$U \otimes_S S \cong U \;:\; u \otimes s \leftrightarrows u \bullet s$$
$$S \otimes_S V \cong V \;:\; s \otimes v \leftrightarrows s \bullet v$$

Aufgabe: Konstruieren Sie diese Isomorphismen dank UAE.

Neutrales zum Tensorprodukt

Lösung: Die Konstruktion verläuft von oben nach unten:



Zum (R, S)–linearen Raum U ist die Skalarmultiplikation von rechts $\tilde{\mu} : U \times S \to U : (u, s) \mapsto u \bullet s$ bilinear über (R, S, S). Dank UAE S2E induziert sie die (R, S)–lineare Abbildung $\mu : U \otimes_S S : u \otimes s \mapsto u \bullet s$.

Umgekehrt ist auch $\mu' : U \to U \otimes_S S : u \mapsto u \otimes 1_S$ linear über (R, S), denn es gilt $\mu'(r \bullet u) = (r \bullet u) \otimes 1_S = r \bullet (u \otimes 1_S) = r \bullet \mu'(u)$ und $\mu'(u \bullet s) = (u \bullet s) \otimes 1_S = u \otimes s = \mu'(u) \bullet s$ für $u \in U$, $r \in R$, $s \in S$.

Nach Konstruktion gilt $\mu' \circ \mu = \mathrm{id}$ und $\mu \circ \mu' = \mathrm{id}$ auf den einfachen Tensoren, also auf allen Tensoren (S2J).

Distributivität des Tensorprodukts

Satz S2N: Distributivität des Tensorprodukts

Gegeben seien Ringe R, S, T und lineare Räume ${}_R(U_i)_S$ und ${}_S(V_j)_T$.

(1) Dann ist das Tensorprodukt distributiv über die direkte Summe:

$$(U_1 \oplus U_2) \otimes V \cong (U_1 \otimes V) \oplus (U_2 \otimes V)$$
$$U \otimes (V_1 \oplus V_2) \cong (U \otimes V_1) \oplus (U \otimes V_2)$$

(2) Dies gilt ganz allgemein sogar für beliebige direkte Summen:

$$(\bigoplus_{i\in I} U_i) \otimes (\bigoplus_{j\in J} V_j) \;\cong\; \bigoplus_{(i,j)\in I\times J}(U_i \otimes V_j)$$
$$\sum_{(i,j)\in I\times J}(u_i \otimes v_j) \;\leftrightarrows\; \sum_{(i,j)\in I\times J}(u_i \otimes v_j)$$

Alle Tensorprodukte werden hier über dem mittleren Ring S gebildet.
Ich schreibe statt $\otimes_S$ lieber $\otimes$, um die Symmetrie zu $\oplus$ zu betonen.

Distributivität des Tensorprodukts

Eigenschaften des Tensorprodukts

Eigenschaften des Tensorprodukts

Eigenschaften der direkten Summe

Übung: Auch die direkte Summe $(U, V) \mapsto U \oplus V$ ist bis auf Isomorphie assoziativ und kommutativ, und der Nullraum 0 ist beidseitig neutral.

Eigenschaften der direkten Summe

Eigenschaften der direkten Summe

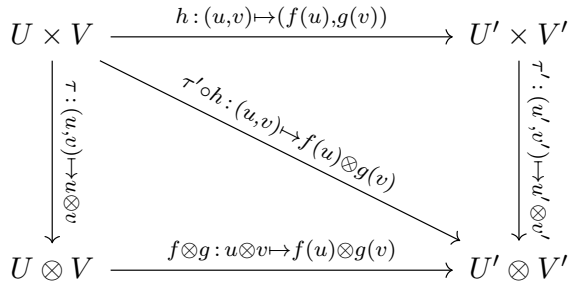
Eigenschaften der direkten Summe

Satz S2O: Funktorialität

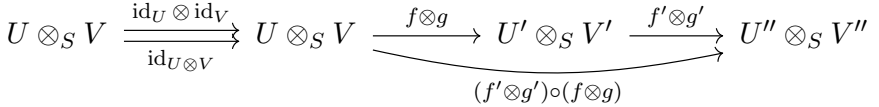
(0) Sei $f : U \to U'$ linear über (R, S) und $g : V \to V'$ linear über (S, T). Dann induzieren f und g eine eindeutige (R, T)–lineare Abbildung

$$f \otimes g \; : \; U \otimes_S V \to U' \otimes_S V' \; : \; u \otimes v \mapsto f(u) \otimes g(v).$$

Beweis: Die Konstruktion nutzt die universelle Eigenschaft S2E:



Die Komposition $\tau' \circ h$ ist bilinear über (R, S, T) und induziert dank der UAE von τ die ersehnte (R, T)–lineare Abbildung $f \otimes g$. QED



Satz S2O: Funktorialität

(1) Für die Identitäten gilt $\mathrm{id}_U \otimes \mathrm{id}_V = \mathrm{id}_{U \otimes V}$.

(2) Seien $f : U \to U'$ und $f' : U' \to U''$ linear über (R, S) sowie $g : V \to V'$ und $g' : V' \to V''$ linear über (S, T). Dann gilt:

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$$

Aufgabe: Was ist hier zu zeigen? Zeigen Sie es!

Lösung: Die beiden (R, T)–linearen Abbildungen links und rechts sind bereits konstruiert, wir müssen sie nur noch vergleichen. Die Gleichheit gilt auf den einfachen Tensoren, also auf allen Tensoren (S2J).

Definition S2P: Kronecker–Produkt

Für $A \in R^{m' \times m}$ und $B \in R^{n' \times n}$ definieren wir das **Kronecker–Produkt**

$$A \otimes B := \begin{bmatrix} a_{1,1}B & \dots & a_{1,m}B \\ \vdots & & \vdots \\ a_{m',1}B & \dots & a_{m',m}B \end{bmatrix} \in R^{(m'n') \times (mn)}.$$

Ausgeschrieben bedeutet das:

$$A \otimes B = \begin{bmatrix} a_{1,1}b_{1,1} & \dots & a_{1,1}b_{1,n} & \dots & a_{1,m}b_{1,1} & \dots & a_{1,m}b_{1,n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{1,1}b_{n',1} & \dots & a_{1,1}b_{n',n} & \dots & a_{1,m}b_{n',1} & \dots & a_{1,m}b_{n',n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m',1}b_{1,1} & \dots & a_{m',1}b_{1,n} & \dots & a_{m',m}b_{1,1} & \dots & a_{m',m}b_{1,n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m',1}b_{n',1} & \dots & a_{m',1}b_{n',n} & \dots & a_{m',m}b_{n',1} & \dots & a_{m',m}b_{n',n} \end{bmatrix}$$

Übung: Es gibt Spezialfälle, in denen das Kronecker–Produkt gleich dem üblichen Matrixprodukt ist. Welche sind das? (Matrixmodell S1C)

Satz S2P: Kronecker–Produkt

Sei $R = S = T$ kommutativ, $\mathcal{A} = (u_1, \dots, u_m)$ eine Basis von U und $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V. Dank S2G erhalten wir daraus die Produktbasis $\mathcal{A} \otimes \mathcal{B} = (u_1 \otimes v_1, \dots, u_1 \otimes v_n, \dots, u_m \otimes v_1, \dots, u_m \otimes v_n)$.

Für Basen $\mathcal{A}' = (u'_1, \dots, u'_{m'})$ von U' und $\mathcal{B}' = (v'_1, \dots, v'_{n'})$ von V' nutzen wir ebenso die lexikographische Ordnung für die Produktbasis $\mathcal{A}' \otimes \mathcal{B}' = (u'_1 \otimes v'_1, \dots, u'_1 \otimes v'_{n'}, \dots, u'_{m'} \otimes v'_1, \dots, u'_{m'} \otimes v'_{n'})$.

Für je zwei R–lineare Abbildungen $f : U \to U'$ und $g : V \to V'$ gilt dann:

$$\mathrm{M}^{\mathcal{A}' \otimes \mathcal{B}'}_{\mathcal{A} \otimes \mathcal{B}}(f \otimes g) = \mathrm{M}^{\mathcal{A}'}_{\mathcal{A}}(f) \otimes \mathrm{M}^{\mathcal{B}'}_{\mathcal{B}}(g)$$

☺ Damit haben wir für $f \otimes g$ eine konkrete Darstellung als Matrix. Für Matrizen haben wir unsere bewährten, effizienten Werkzeuge.

Übung: Es gilt $A \otimes (B \otimes C) = (A \otimes B) \otimes C$ aber i.A. $A \otimes B \neq B \otimes A$; Gleichheit gilt nach geeigneter Permutation der Basis (Zeilen&Spalten).

Bei Transposition gilt $(A \otimes B)^\mathsf{T} = A^\mathsf{T} \otimes B^\mathsf{T}$, bei gleicher Reihenfolge!

Beim Kronecker–Produkt erfüllt die Spur $\mathrm{tr}(A \otimes B) = \mathrm{tr}(A) \cdot \mathrm{tr}(B)$. Für $A \in K^{m \times m}$ und $B \in K^{n \times n}$ gilt $\det(A \otimes B) = \det(A)^n \det(B)^m$.

Für die Spektren gilt: Aus $\sigma(A) = \{\lambda_1, \dots, \lambda_m\}$ und $\sigma(B) = \{\mu_1, \dots, \mu_n\}$ folgt $\sigma(A \otimes B) = \{\, \lambda_i \mu_j \mid i = 1, \dots, m,\ j = 1, \dots, n \,\}$.

Für die zugehörigen Eigenräume gilt $\mathrm{E}(A; \lambda) \otimes \mathrm{E}(B; \mu) \subseteq \mathrm{E}(A \otimes B; \lambda\mu)$, somit gilt $\mathrm{E}(A \otimes B; \nu) \supseteq \bigoplus_{\lambda\mu = \nu} \mathrm{E}(A; \lambda) \otimes \mathrm{E}(B; \mu)$, aber i.A. nicht „⊆“.

Gegenbeispiel: Wir betrachten $A = B = \left[\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right]$. Dann ist neben $e_1 \otimes e_1$ auch $e_1 \otimes e_2 - e_2 \otimes e_1$ ein Eigenvektor von $A \otimes B$ zum Eigenwert λ^2.

Genau wie für zwei Faktoren erklären wir das n–fache Tensorprodukt

$$T = {}_{R_0}(U_1)_{R_1} \otimes {}_{R_1}(U_2)_{R_2} \otimes \cdots \otimes {}_{R_{n-1}}(U_n)_{R_n}.$$

Gegeben seien hierzu Ringe $R_0, R_1, R_2, \dots, R_n$ und lineare Räume $U_1, U_2, \dots, U_n$, wobei U_i linear über (R_{i-1}, R_i) ist, wie oben vermerkt.

Übung zur Wiederholung: Formulieren Sie die Definitionen S2D / S2E und die anschließenden Sätze für das mehrfache Tensorprodukt.

🙂 Alle Definitionen und Sätze verlaufen parallel zum vorigen Fall $n = 2$.

Warum, so fragen Sie, habe ich das nicht gleich allgemein ausgeführt? Nun ja, beim ersten Durchgang kostet schon der einfachste Fall $n = 2$ die wissbegierig Lernenden viel Mühe, und die zusätzliche Schreibarbeit für den allgemeinen Fall $n \in \mathbb{N}$ ist dabei nur Ballast ohne Mehrwert.

🙂 Beim zweiten Durchgang ist der allgemeine Fall dann leicht, daher formuliere ich die Ausführung als lehrreiche Übung zur Wiederholung.

Definition S2Q: multilineare Abbildung und interner Ausgleich

Sei $R = (R_0, R_1, \dots, R_n)$ eine Familie von Ringen und $U = (U_1, \dots, U_n)$ eine Familie linearer Räume über R, wobei U_i linear über (R_{i-1}, R_i) ist. Sei $\mu\colon \prod_{i=1}^n U_i \to W$ eine Abbildung in einen (R_0, R_n)–linearen Raum.

(1) Wir nennen μ **multiadditiv**, falls μ additiv in jedem U_i ist:

$$\mu(\dots, u_i + u_i', \dots) = \mu(\dots, u_i, \dots) + \mu(\dots, u_i', \dots)$$

(2) Wir nennen μ **multihomogen** über $R = (R_0, \dots, R_n)$ falls gilt:

$$\begin{aligned} \mu(r_0 \cdot u_1, u_2, \dots, u_n) &= r_0 \cdot \mu(u_1, u_2, \dots, u_n) \\ \mu(\dots, u_i \cdot r_i, u_{i+1}, \dots) &= \mu(\dots, u_i, r_i \cdot u_{i+1}, \dots) \\ \mu(u_1, \dots, u_{n-1}, u_n \cdot r_n) &= \mu(u_1, \dots, u_{n-1}, u_n) \cdot r_n \end{aligned}$$

in jeder Stelle i, für alle Skalare $r_i \in R_i$ und Vektoren $u_i \in U_i$.
Gilt (1) und (2), so nennen wir μ kurz **R–multilinear**:

$$\mathrm{Mul}_R(U; W) = \{\, \mu\colon \textstyle\prod_{i=1}^n U_i \to W \text{ multilinear über } R \,\}$$

Beispiel: Gegeben sei ein kommutativer Ring R und lineare Räume $U_1, \dots, U_n, W$ über R (S2B). Wir betrachten eine n–stellige Abbildung

$$\mu : U_1 \times U_2 \times \cdots \times U_n \to W.$$

Genau dann ist μ multihomogen über $(R, R, \dots, R)$, wenn gilt:

$$\mu(\dots, r \cdot u_i, \dots) = r \cdot \mu(\dots, u_i, \dots)$$

in jeder Stelle i, für alle Skalare $r \in R$ und Vektoren $u_i \in U_i$.

Übung: Beweisen Sie diese Äquivalenz (zunächst für $n = 2, 3, \dots$).

🙂 Über jedem kommutativen Ring R erhalten so den vertrauten Begriff der Multilinearität, wie wir ihn etwa von der Determinante (L2A) kennen.

⚠ Für nicht-kommutative Ringe müssen wir behutsamer vorgehen. Hier ist die oben formulierte Definition S2D bzw. S2Q die richtige.

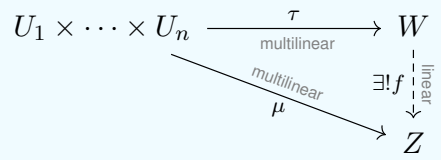
🙂 Im kommutativen Fall stimmen beide Definitionen überein.

Definition S2R: das mehrfache Tensorprodukt

Sei $R = (R_0, \dots, R_n)$ eine Familie von Ringen und $U = (U_1, \dots, U_n)$ eine Familie linearer Räume, wobei U_i linear über (R_{i-1}, R_i) ist.

(1) Ein **Produkt** $\mu\colon \prod_{i=1}^n U_i \to Z$ ist eine R–multilineare Abbildung.

(2) Ein **Tensorprodukt** von U über R ist ein Produkt $\tau\colon \prod_{i=1}^n U_i \to W$ mit der folgenden universellen Abbildungseigenschaft:



Jedes Produkt $\mu\colon \prod_{i=1}^n U_i \to Z$ faktorisiert eindeutig über τ:
Es gibt genau eine (R_0, R_n)–lineare Abbildung $f : W \to Z$ mit $\mu = f \circ \tau$.

Diese Forderung ist äquivalent zur Bijektivität der natürlichen Abbildung

$$\Phi_\tau^Z \;:\; \mathrm{Hom}_{(R_0,R_n)}(W, Z) \to \mathrm{Mul}_R(U; Z) \;:\; f \mapsto \mu = f \circ \tau.$$

Satz S2S: Prinzip der multilinearen Fortsetzung

Seien $U_1, \dots, U_n, W$ lineare Räume über dem kommutativen Ring R. Zu $i = 1, \dots, n$ sei $(u_{i,j})_{j \in J_i}$ eine Basis von U_i sowie $(w_j)_{j \in J}$ eine beliebige Familie in W, indiziert durch $J = J_1 \times \cdots \times J_n$.

(1) Dann existiert genau eine R–multilineare Abbildung

$$\tau : U_1 \times \cdots \times U_n \to W : (u_{1,j_1}, \dots, u_{n,j_n}) \mapsto w_{j_1,\dots,j_n}, \quad \text{nämlich}$$
$$\tau\Big(\sum_{j_1 \in J_1} \lambda_{1,j_1} u_{1,j_1}, \dots, \sum_{j_n \in J_n} \lambda_{n,j_n} u_{n,j_n} \Big) = \sum_{j \in J} \lambda_{1,j_1} \cdots \lambda_{n,j_n} w_j$$

für alle Linearkombinationen mit Koeffizienten $\lambda_i \in R^{(J_i)}$ für $i = 1, \dots, n$.

(2) Genau dann ist τ ein Tensorprodukt, erfüllt also die universelle Abbildungseigenschaft S2E, wenn $(w_j)_{j \in J}$ eine Basis von W ist.

Übung: Beweisen Sie dies nach dem Vorbild von Satz S2G.
Schließen Sie daraus das folgende schöne Anwendungsbeispiel.

Beispiel S2T: Polynommodell des mehrfachen Tensorprodukts

Sei K ein kommutativer Ring. Wir betrachten $U_1 = \cdots = U_n = K[X]$ und hierzu die vertraute Polynommultiplikation

$$\tau : K[X] \times \cdots \times K[X] \to K[X_1, \dots, X_n]$$
$$(u_1, \dots, u_n) \mapsto u_1(X_1) \cdots u_n(X_n).$$

Dieses Produkt τ hat die universelle Abbildungseigenschaft (S2S).

Satz S2U: Eindeutigkeit des mehrfachen Tensorprodukts

Sei $R = (R_0, \dots, R_n)$ eine Familie von Ringen und $U = (U_1, \dots, U_n)$ eine Familie linearer Räume, wobei U_i linear über (R_{i-1}, R_i) ist.

Dann sind zu diesen Räumen je zwei Tensorprodukte $\tau : \prod_{i=1}^n U_i \to W$ und $\tau' : \prod_{i=1}^n U_i \to W'$ eindeutig isomorph: Es existiert genau ein (R_0, R_n)–Isomorphismus $(f, f') : W \cong W'$ mit $\tau' = f \circ \tau$ und $\tau = f' \circ \tau'$.

Übung: Beweisen Sie dies nach dem Vorbild von Satz S2H.

Satz S2V: Existenz des mehrfachen Tensorprodukts

Sei $R = (R_0, \dots, R_n)$ eine Familie von Ringen und $U = (U_1, \dots, U_n)$ eine Familie linearer Räume, wobei U_i linear über (R_{i-1}, R_i) ist.

Zu U über R existiert ein Tensorprodukt $\tau : \prod_{i=1}^n U_i \times V \to W$.

Übung: Beweisen Sie dies nach dem Vorbild von Satz S2I.
Aus dieser länglichen, aber expliziten Konstruktion folgt sofort:

Korollar S2W: Einfache Tensoren erzeugen alle Tensoren.

Die einfachen Tensoren $u_1 \otimes \cdots \otimes u_n$ mit $u_1 \in U_1, \dots, u_n \in U_n$ erzeugen den Tensorraum $U_1 \otimes \cdots \otimes U_n$. Ausführlich bedeutet das:

Jeder beliebige Tensor $w \in U_1 \otimes \cdots \otimes U_n$ ist eine endliche Summe $w = \sum_{k=1}^{\ell} u_{1,k} \otimes \cdots \otimes u_{n,k}$ mit einer gewissen Länge $\ell \in \mathbb{N}$ und geeigneten Faktoren $u_{i,k} \in U_i$ für $i = 1, \dots, n$ und $k = 1, \dots, \ell$.

Reellifizierung und Komplexifizierung

Beispiel S3A: Reellifizierung und Komplexifizierung

(1a) Jeder $\mathbb{C}$–Vektorraum $V_{\mathbb{C}}$ wird zu einem $\mathbb{R}$–Vektorraum $V_{\mathbb{R}}$ durch Einschränkung der Skalare von $\mathbb{C}$ zu $\mathbb{R}$, also die Einschränkung von

$$\bullet : V \times \mathbb{C} \to V \qquad \text{zu} \qquad \bullet : V \times \mathbb{R} \to V.$$

(1b) Ist $(v_j)_{j\in J}$ eine $\mathbb{C}$–Basis von V, so ist $(v_j \bullet 1, v_j \bullet \mathrm{i})_{j\in J}$ eine $\mathbb{R}$–Basis von V. Für die Dimensionen folgt $\dim_{\mathbb{R}}(V) = 2\dim_{\mathbb{C}}(V)$.

(1c) Jede $\mathbb{C}$–lineare Abbildung $f : V \to V'$ ist auch $\mathbb{R}$–linear.

(2a) Zu jedem $\mathbb{R}$–Vektorraum $U_{\mathbb{R}}$ erhalten wir den $\mathbb{C}$–Vektorraum

$$V_{\mathbb{C}} := (U_{\mathbb{R}}) \otimes_{\mathbb{R}} ({}_{\mathbb{R}}\mathbb{C}_{\mathbb{C}}).$$

(2b) Ist $(u_j)_{j\in J}$ eine $\mathbb{R}$–Basis von $U_{\mathbb{R}}$, so ist $(v_j = u_j \otimes 1)_{j\in J}$ eine $\mathbb{C}$–Basis von $V_{\mathbb{C}}$. Für die Dimensionen folgt $\dim_{\mathbb{R}}(U) = \dim_{\mathbb{C}}(V)$.

(2c) Jede $\mathbb{R}$–lineare Abbildung $f_{\mathbb{R}} : U_{\mathbb{R}} \to U'_{\mathbb{R}}$ induziert eine zugehörige $\mathbb{C}$–lineare Abbildung $g_{\mathbb{C}} = f_{\mathbb{R}} \otimes \mathrm{id}_{\mathbb{C}} : V_{\mathbb{C}} = U_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}_{\mathbb{C}} \to U'_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}_{\mathbb{C}} = V'_{\mathbb{C}}$.

Reellifizierung und Komplexifizierung

Die Übergang von $\mathbb{C}$ nach $\mathbb{R}$ ist leicht, hier genügt die Einschränkung. Umgekehrt ist die Erweiterung von $\mathbb{R}$ nach $\mathbb{C}$ keineswegs offensichtlich!

Warum wollen wir das? Der Körper $\mathbb{C}$ hat bessere Eigenschaften, insbesondere zerfällt jedes Polynom über $\mathbb{C}$ in Linearfaktoren.

Diesen Trick haben wir daher schon oft angewendet, mangels allgemeiner Werkzeuge jedoch zunächst noch recht umständlich:

Wir stellen $f_{\mathbb{R}} : U_{\mathbb{R}} \to U'_{\mathbb{R}}$ als eine reelle Matrix $A \in \mathbb{R}^{m\times n}$ dar, und betrachten diese dann als eine komplexe Matrix $A \in \mathbb{C}^{m\times n}$.

Hier sehen Sie nun, was wirklich dahinter steckt: Mit dem Tensorprodukt können wir die Komplexifizierung allgemein und basisfrei erklären!

So erhalten wir nicht nur die komplexifizierte Matrix, sondern auch die $\mathbb{C}$–lineare Abbildung $g_{\mathbb{C}} = f_{\mathbb{R}} \otimes \mathrm{id}_{\mathbb{C}} : V_{\mathbb{C}} = U_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}_{\mathbb{C}} \to U'_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}_{\mathbb{C}} = V'_{\mathbb{C}}$

Dieser Trick funktioniert allgemein für jede Ringerweiterung $S \le R$. Dies führt uns zum folgenden allgemeinen Satz.

Erweiterung des Grundrings

Satz S3B: Erweiterung des Grundrings

Seien $S \le R$ Ringe und U_S ein (rechts)linearer Raum über S.

(1) Die **Erweiterung der Skalare** ergibt einen linearen Raum über R:

$$V_R := (U_S) \otimes_S ({}_S R_R)$$

(2) Wir haben die natürliche S–lineare Abbildung (i.A. keine Einbettung)

$$\iota : U_S \xrightarrow{\sim} U_S \otimes_S S \xrightarrow{\mathrm{id}\otimes \mathrm{inc}} U_S \otimes_S R = V_R : u \mapsto v = u \otimes 1_R.$$

(3) Freie Räume bleiben frei: Ist $(u_i)_{i\in I}$ eine Basis von U_S über S, dann ist $(v_i = u_i \otimes 1_R)_{i\in I}$ eine Basis von V_R über R, und ι ist injektiv.

(4) Jede S–lineare Abbildung $f_S : U_S \to U'_S$ induziert eine zugehörige R–lineare Abbildung $g_R = f_S \otimes \mathrm{id}_R : V_R = U_S \otimes_S R_R \to U'_S \otimes_S R_R = V'_R$.

(5) Die darstellenden Matrizen sind dieselben in $S^{m\times n} \le R^{m\times n}$.

Dasselbe gilt entsprechend für linkslineare Räume.

Die Erweiterung des Grundrings ist funktoriell.

$$U \xrightarrow{\mathrm{id}_U} U \xrightarrow{f} U' \xrightarrow{f'} U'' \qquad (f'\circ f)$$

$$U \otimes_S R \underset{\mathrm{id}_{U\otimes R}}{\overset{\mathrm{id}_U\otimes \mathrm{id}_R}{\rightrightarrows}} U \otimes_S R \xrightarrow{f\otimes \mathrm{id}_R} U' \otimes_S R \xrightarrow{f'\otimes \mathrm{id}_R} U'' \otimes_S R \qquad (f'\otimes \mathrm{id}_R)\circ(f\otimes \mathrm{id}_R)=(f'\circ f)\otimes \mathrm{id}_R$$

Satz S3B: Die Erweiterung des Grundrings ist funktoriell.

(6) Für die Identität $\mathrm{id}_U : U \to U$ gilt

$$\mathrm{id}_U \otimes \mathrm{id}_R = \mathrm{id}_{U\otimes R} = \mathrm{id}_V : V \to V.$$

(7) Für $f : U \to U'$ und $f' : U' \to U''$ und $f' \circ f : U \to U''$ gilt

$$(f' \otimes \mathrm{id}_R) \circ (f \otimes \mathrm{id}_R) = (f' \circ f) \otimes \mathrm{id}_R\,.$$

Übung: Alle Daten liegen explizit vor. Rechnen Sie es nach!

Tensorieren mit $\mathbb{Q}$

Aufgabe: Welche $\mathbb{Q}$–Dimension hat $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$? allgemein $(\mathbb{Z}/n) \otimes_{\mathbb{Z}} \mathbb{Q}$?

Satz S3C: Tensorieren mit $\mathbb{Q}$

(1) Dank S2M haben wir den Isomorphismus

$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} : (a \otimes b) \mapsto ab.$$

(2) Für alle $n \in \mathbb{N}_{\geq 1}$ hingegen gilt

$$(\mathbb{Z}/n) \otimes_{\mathbb{Z}} \mathbb{Q} = 0.$$

Beweis: (2) Die einfachen Tensoren erzeugen den Tensorraum (S2J) und $[a] \otimes b = [a] \otimes (n \cdot b/n) = ([a] \cdot n) \otimes (b/n) = 0 \otimes (b/n) = 0$. QED

Anwendungsbeispiel: Für jede endlich erzeugte abelsche Gruppe

$$V \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_t$$

mit $n_1, \ldots, n_t \geq 2$ extrahiert Tensorieren mit $\mathbb{Q}$ den freien Anteil:

$$V \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^r \quad \text{und} \quad r = \dim_{\mathbb{Q}}(V \otimes_{\mathbb{Z}} \mathbb{Q}).$$

Tensorieren mit $\mathbb{Q}$

☺ Unter diesem Isomorphismus wird die kanonische Basis $(e_1, \ldots, e_r)$ von $\mathbb{Z}^r$ abgebildet auf die kanonische Basis $(e_1, \ldots, e_r)$ von $\mathbb{Q}^r$.

Der Torsionsteil $\mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_t$ hingegen wird auf 0 abgebildet. Hierzu nutzen wir (2) und die Distributivität des Tensorprodukts (S2N).

⚠ Die natürliche Abbildung ι ist im Allgemeinen keineswegs injektiv. Wir illustrieren Ringerweiterungen hier mit dem Übergang von $\mathbb{Z}$ zu $\mathbb{Q}$:

Über $\mathbb{Z}$ kann das Tensorieren mit $\mathbb{Q}$ einige Information vernichten. Manchmal möchten wir genau das, so wie hier illustriert.

☺ Über einem Körper wie $\mathbb{Q}$ hat jeder lineare Raum eine Basis. Über dem Ring wie $\mathbb{Z}$ hingegen gilt diese Eigenschaft leider nicht.

Zur Vereinfachung können wir daher über $\mathbb{Z}$ mit $\mathbb{Q}$ tensorieren; wir verlieren dabei Information, aber gewinnen stärkere Sätze.

Diese grundlegende Beobachtung führt uns zu folgender Definition.

Der Rang einer abelschen Gruppe

Wie können wir den „Rang“ einer abelschen Gruppen erklären?

Definition S3D: Rang einer abelschen Gruppe

Sei $(V, +)$ eine abelsche Gruppe, also ein $\mathbb{Z}$–linearer Raum.
Der **Rang** von V, genauer der **$\mathbb{Q}$–Rang**, ist dann definiert durch

$$\operatorname{rang}_{\mathbb{Q}}(V) := \dim_{\mathbb{Q}}(V \otimes_{\mathbb{Z}} \mathbb{Q}).$$

Dasselbe gilt für jeden Körper $\mathbb{K}$, etwa $\mathbb{K} = \mathbb{F}_p = \mathbb{Z}/p$ mit p prim:

$$\operatorname{rang}_{\mathbb{K}}(V) := \dim_{\mathbb{K}}(V \otimes_{\mathbb{Z}} \mathbb{K}).$$

Anwendungsbeispiel: Für jede endlich erzeugte abelsche Gruppe

$$V \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_t$$

mit $n_1, \ldots, n_t \geq 2$ gilt $\operatorname{rang}_{\mathbb{Q}}(V) = r$ wie oben und zudem

$$\operatorname{rang}_{\mathbb{F}_p}(V) = r + \sharp\{\, i \in \{1, \ldots, t\} \mid p \mid n_i \,\}.$$

Der Rang einer abelschen Gruppe

Wir gehen hier von $\mathbb{Z}$ zu einem Körper $\mathbb{K}$ über, die natürlichen Kandidaten hierzu sind neben dem Bruchkörper $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z})$ vor allem die Quotientenkörper $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p = \mathbb{F}_p$ für p prim.

Der Vorteil eines Körpers $\mathbb{K}$ ist, wie oben motiviert, dass wir allgemein über Basen verfügen und von der Dimension über $\mathbb{K}$ sprechen könnnen. Unsere gründliche Arbeit zu Vektorräumen zahlt sich hier aus!

Beispiel: Für $V = \mathbb{Z}^7 \oplus \mathbb{Z}_2^4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3^2 \oplus \mathbb{Z}_9$ gilt $\operatorname{rang}_{\mathbb{Q}}(V) = 7$ sowie $\operatorname{rang}_{\mathbb{F}_2}(V) = 12$ und $\operatorname{rang}_{\mathbb{F}_3}(V) = 10$ und $\operatorname{rang}_{\mathbb{F}_p}(V) = 7$ für alle $p \geq 5$.

Für die Rechnung benötigen wir das Tensorprodukt $(\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q)$. Dies führt uns zu dem nächsten schönen Satz.

Das Tensorprodukt $(\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q)$

Aufgabe: Wie viele Elemente hat $(\mathbb{Z}/5) \otimes_{\mathbb{Z}} (\mathbb{Z}/9)$?

Lösung: Wir finden $5 \cdot 2 \equiv 1 \bmod 9$. In $(\mathbb{Z}/5) \otimes (\mathbb{Z}/9)$ folgt daraus:

$$[a] \otimes [b] = [a] \otimes (5 \cdot 2 \cdot [b]) = ([a] \cdot 5) \otimes (2 \cdot [b]) = 0 \otimes (2 \cdot [b]) = 0$$

Daher gilt $(\mathbb{Z}/5) \otimes_{\mathbb{Z}} (\mathbb{Z}/9) = 0$. Was steckt allgemein dahinter?

Satz S3E: das Tensorprodukt $(\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q)$

Für $p, q \in \mathbb{N}$ und $r = \operatorname{ggT}(p, q)$ haben wir den Isomorphismus

$$(\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q) \;\cong\; (\mathbb{Z}/r) \;:\; [a]_p \otimes [b]_q \mapsto [ab]_r, \quad [c]_p \otimes [1]_q \mapsfrom [c]_r$$

Wichtiger Spezialfall: Gilt $\operatorname{ggT}(p, q) = 1$, so folgt $(\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q) = 0$.

Aufgabe: Warum ist die Umkehrfunktion $[c]_p \otimes [1]_q \mapsfrom [c]_r$ wohldefiniert?

Lösung: Dank Bézout (A2I) existieren $u, v \in \mathbb{Z}$ mit $r = pu + qv$, also $[r]_r \mapsto [r]_p \otimes [1]_q = ([v]_p \cdot q) \otimes [1]_q = [v]_p \otimes (q \cdot [1]_q) = [v]_p \otimes [0]_q = 0$.

Das Tensorprodukt $\mathbb{Z}/p \otimes_{\mathbb{Z}} \mathbb{Z}/q$

☺ Beim Tensorprodukt multiplizieren sich die Dimensionen (S1B).
Naiv würde man daher für $(\mathbb{Z}/5) \otimes_{\mathbb{Z}} (\mathbb{Z}/9)$ vielleicht $5 \cdot 9 = 45$ Elemente vermuten; das gilt tatsächlich für das kartesische Produkt $(\mathbb{Z}/5) \times (\mathbb{Z}/9)$.

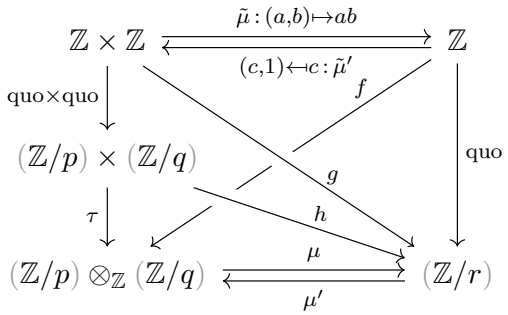
⚠ Das Tensorprodukt hingegen verhält sich deutlich anders!
Hierzu rechnen wir sorgfältig mit Erzeugern und Relationen.

⚠ Dieselbe Notation $[\dots]$ für Äquivalenzklassen bedeutet hier dreimal Verschiedenes! Zur Betonung habe ich die Indizes p, q, r hinzugefügt.

Aufgabe: Führen Sie die Konstruktion des ersehnten Isomorphismus $(\mu, \mu') : (\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q) \cong (\mathbb{Z}/r) : [a] \otimes [b] \rightleftarrows [ab]$ detailliert aus.

Das Tensorprodukt $\mathbb{Z}/p \otimes_{\mathbb{Z}} \mathbb{Z}/q$

Beweis: Wir nutzen auch hier die universelle Abbildungseigenschaft:



Das Tensorprodukt $\mathbb{Z}/p \otimes_{\mathbb{Z}} \mathbb{Z}/q$

Die Abbildung $\tilde{\mu} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (a, b) \mapsto ab$ ist bilinear. Die Komposition $g = \operatorname{quo} \circ \tilde{\mu}$ erfüllt zudem $g(p, 0) = g(0, q) = 0$. Somit induziert g die Abbildung $h : (\mathbb{Z}/p) \times (\mathbb{Z}/q) \to (\mathbb{Z}/r) : ([a], [b]) \mapsto [ab]$, ebenfalls bilinear. Dank UAE erhalten wir $\mu : (\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q) \to (\mathbb{Z}/r) : [a] \otimes [b] \mapsto [ab]$.

Die Abbildung $f : \mathbb{Z} \to (\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q) : c \mapsto [c] \otimes [1]$ erfüllt $\ker(f) \supseteq r\mathbb{Z}$, wie wir oben dank Bézout–Koeffizienten bereits nachgerechnet haben. Sie induziert somit $\mu' : (\mathbb{Z}/r) \to (\mathbb{Z}/p) \otimes_{\mathbb{Z}} (\mathbb{Z}/q) : [c] \mapsto [c] \otimes [1]$.
Damit gilt $\mu' \circ \mu = \mathrm{id}$ und $\mu \circ \mu' = \mathrm{id}$. (Nachrechnen!) QED

Darstellung von Homomorphismen

Satz S3F: Darstellung von Homomorphismen

Seien U, V rechtslineare Räume über dem Ring R. Wir betrachten dazu

$$\Phi \,:\, V \otimes_R U^* \to \mathrm{Hom}_R(U,V) \,:\, \Phi(v\otimes\varphi)(u) = v \bullet \varphi(u).$$

(1) Hat U eine endliche Basis $(u_1,\ldots,u_n)$, so ist Φ bijektiv mit Inverser

$$\Psi \,:\, \mathrm{Hom}_R(U,V) \to V \otimes_R U^* \,:\, f \mapsto \textstyle\sum_{j=1}^n f(u_j)\otimes u_j^*.$$

(2) Hat V eine endliche Basis $(v_1,\ldots,v_m)$, so ist Φ bijektiv mit Inverser

$$\Psi \,:\, \mathrm{Hom}_R(U,V) \to V \otimes_R U^* \,:\, f \mapsto \textstyle\sum_{i=1}^m v_i\otimes f^*(v_i^*).$$

(3) Gilt (1) und (2) mit R kommutativ, so ist $(e_{i,j} = \Phi(v_i\otimes u_j^*))_{i=1,\ldots,m}^{j=1,\ldots,n}$ eine Basis von $\mathrm{Hom}_R(U,V) \cong R^{m\times n}$, wie von Matrizen vertraut.

(4) Ist R ein Körper, so ist Φ injektiv, und das Bild in $\mathrm{Hom}_R(U,V)$ sind genau die Homomorphismen mit endlichem Rang:

$$\textstyle\sum_{i=1}^r v_i\otimes\varphi_i \;\mapsto\; \sum_{i=1}^r \Phi(v_i\otimes\varphi_i)$$

Darstellung von Homomorphismen

☺ Diese Schreibweise ist übersichtlich und effizient, insbesondere wenn der Rang r klein ist gegenüber den Dimensionen m und n.

Beispiel S3G: Singulärwertzerlegung

Die obige Darstellung kennen wir von der Singulärwertzerlegung:

$$\textstyle\sum_{i=1}^r \sigma_i(v_i\otimes u_i^*) \;\mapsto\; \sum_{i=1}^r \sigma_i\,\Phi(v_i\otimes u_i^*)$$

Hierzu betrachten wir eine lineare Abbildung $f : U \to V$ über $\mathbb{K} = \mathbb{R}, \mathbb{C}$. Die beiden Vektorräume U und V tragen jeweils ein Skalarprodukt.

Zu f sind $\sigma_1 \geq \cdots \geq \sigma_r \geq 0$ die Singulärwerte, die Singulärvektoren $v_1,\ldots,v_r \in V$ und $u_1,\ldots,u_r \in U$ bilden zwei orthonormale Familien, und $u_i^* = \langle\, u_i \mid - \,\rangle \in U^*$ ist die zu u_i gehörige Linearform.

Damit schreibt sich die lineare Abbildung f gemäß

$$f \,:\, U \to V \,:\, u \mapsto \textstyle\sum_{i=1}^r \sigma_i v_i \cdot \langle\, u_i \mid u \,\rangle.$$

Speziell für die euklidischen Räume $U = \mathbb{K}^m$ und $V = \mathbb{K}^n$ erhalten wir die Matrixdarstellung $\mathrm{M}(f) = \sum_{i=1}^r \sigma_i v_i u_i^\dagger$ bezüglich der Standardbasen.

Darstellung von Homomorphismen

Aufgabe: Alle Daten liegen explizit vor. Rechnen Sie Satz S3F nach!
(0) Warum ist Φ wohldefiniert? (1,2) Gilt $\Phi\circ\Psi = \mathrm{id}$ und $\Psi\circ\Phi = \mathrm{id}$?
(3) Warum sind Φ und Ψ nun R–linear? (4) Was sind Kern und Bild?

Darstellung von Homomorphismen