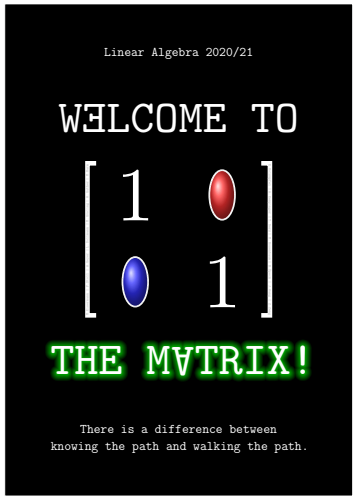
Dies ist nur die Saalversion ohne Erläuterungen.

Lineare Algebra

von klassischen Grundlagen zu aktuellen Anwendungen



erkennen.
beweisen.
anwenden.

Prof. Dr. Michael Eisermann

eiserm.de/lehre/LinA

Universität Stuttgart

WiSe 2025/26 und SoSe 2026
Stand 19. September 2026

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

Habe Mut, dich deines eigenen Verstandes zu bedienen!

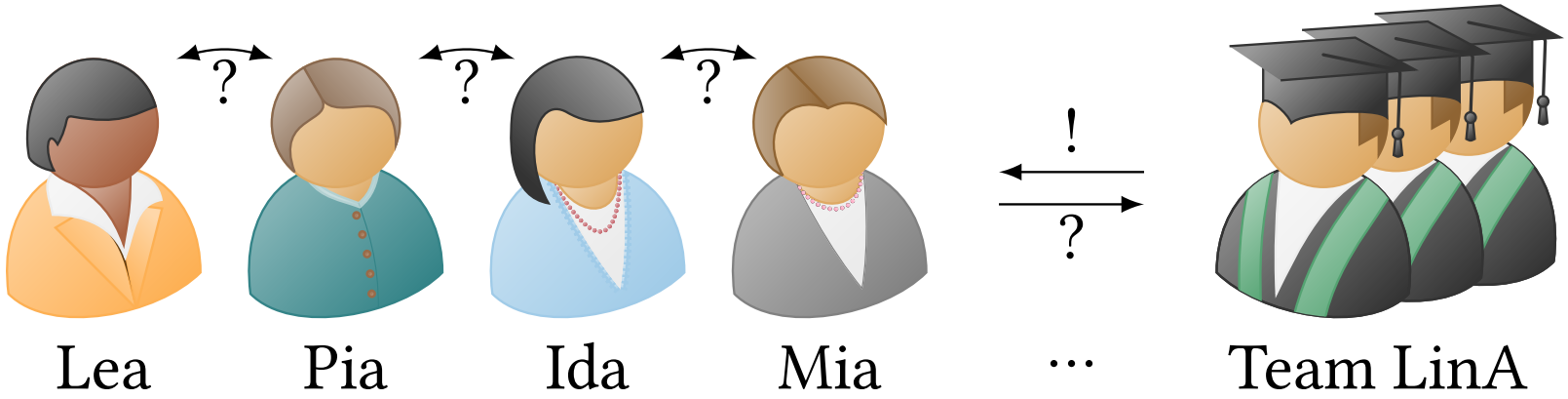
Much to learn, you still have.
This is just the beginning.

Ausführliche Erläuterungen bietet die Vollversion.

Herzlich willkommen zu Ihrer Linearen Algebra!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



L Lea, die lernbegeisterte Lehrer:in: „Wie kann ich das selbst *verstehen* und anderen *vermitteln*, mathematisch korrekt und didaktisch geschickt?“

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

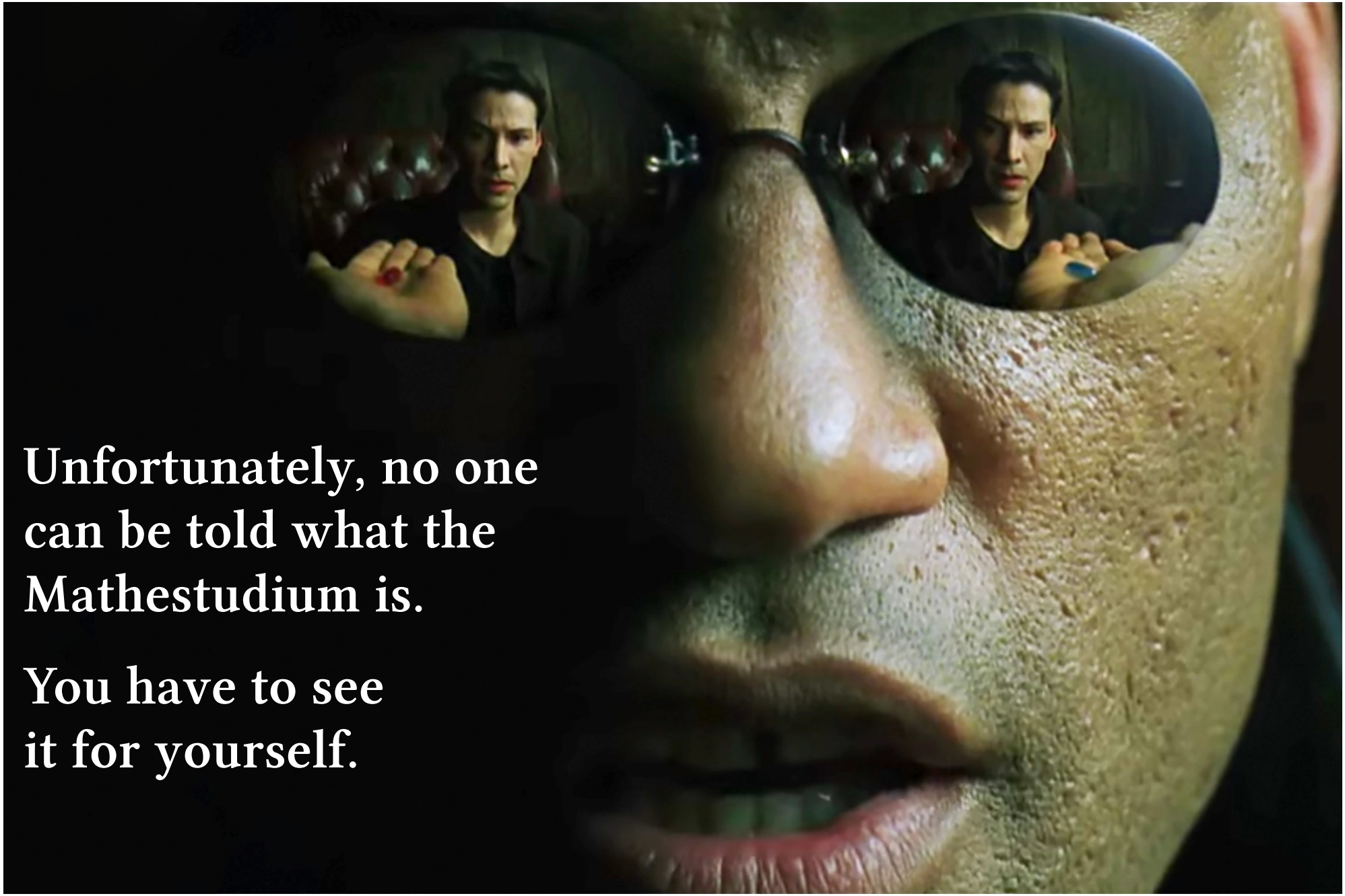
I Ida, die innovative Informatiker:in: „Wie *implementiere* ich mathematische Modelle und Methoden, korrekt und effizient?“

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

Herzlich willkommen zu Ihrer Linearen Algebra!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

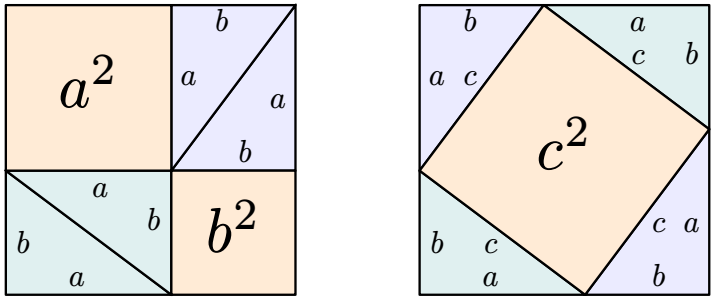


Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel A

Einleitung und Überblick



We choose to go to the moon in this decade and do the other things, not because they are easy, but because they are hard.

John F. Kennedy (1917–1963), Address at Rice University

Non quia difficilia sunt non audemus,
sed quia non audemus difficilia sunt.

Seneca (1–65), Moralische Briefe an Lucilius

Inhalt dieses Kapitels A

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

1. Herzlich willkommen im Studium!
2. Was macht Mathematik so besonders?
3. Was erwartet Sie in dieser Veranstaltung?

Schöne Mathematik – gute Vorlesung – faire Klausur

Dies ist nur die Saalversion ohne Erläuterungen.

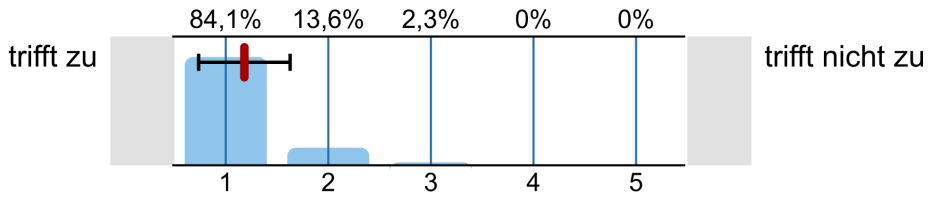
Ausführliche Erläuterungen bietet die Vollversion.

Gute Erfahrung unserer Linearen Algebra 2020/21

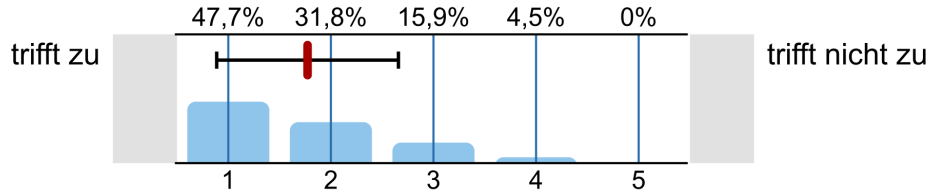
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

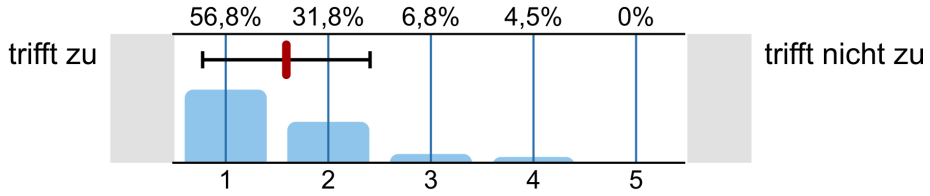
Alles in allem fühle ich mich gut betreut.



Die Veranstaltung fördert mein Interesse am Thema.

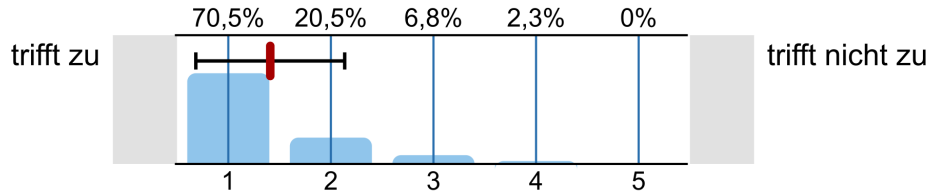


Ich werde zur regelmäßigen Bearbeitung aktueller Lehrinhalte motiviert.

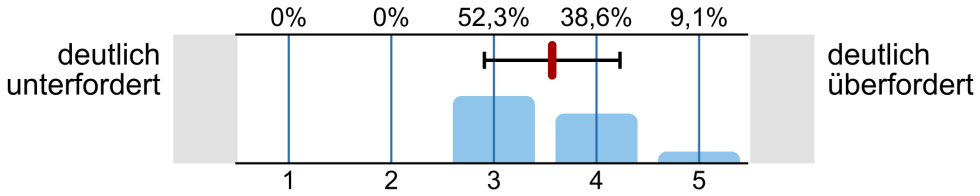


⚠ *Studieren heißt sich bemühen, kontinuierlich, Woche für Woche.*

Ich habe durch den Besuch dieser Veranstaltung viel gelernt.



Die Lehrveranstaltung hat mich ...



Unser Ilias-Kurs ist informativ und liebevoll gestaltet.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lineare Algebra 1 - WiSe 2025/26

Aktionen

Die Lineare Algebra gehört zum Beginn des Mathematikstudiums wie das Erlernen der Buchstaben zum Beginn der Grundschule: Es ist anfangs mühsam, aber nützt ein Leben lang! Lineare Methoden sind elegant und praktisch, daher werden sie überall gerne genutzt, sowohl innerhalb der Mathematik als auch in ihren zahlreichen Anwendungen, jüngst etwa in Quantencomputing, Data Science oder Künstlicher Intelligenz. Zugleich ist die Lineare Algebra eine wunderschöne Theorie, an der Sie vorbildlich lernen, wie moderne Mathematik aufgebaut wird. Die Vorlesung führt Sie in diese methodische und strukturelle Arbeitsweise ein.

Inhalt | Timeline | Info | Mitglieder | Lernfortschritt

Herzlich willkommen zur Linearen Algebra!

Startseite

In diesem Ilias-Kurs finden Sie Informationen und Online-Materialen zu unserer Veranstaltung:

- Die **Vorlesung** erklärt Ihnen die Begriffe und Methoden. Unterstützend bieten wir Ihnen unser Skript, erprobt und umfassend.
- Jede Woche lösen Sie hier in Ilias ein **hilfreiches Quiz**. Damit wiederholen Sie den aktuellen Vorlesungsstoff und sind so für die Übungen bestens vorbereitet.
- Zur **Übung** erstellen wir für Sie jede Woche ein Übungsblatt mit gut abgestimmten Aufgaben, die Sie bis zur Folgewoche lösen.
- Zusätzlich gibt es alle zwei Wochen eine **Vortragsübung**, in der Aufgaben vorgerechnet und erklärt werden.
- Im **Forum** können Sie anonym Ihre Fragen stellen und erhalten kompetente Auskunft.
- In den **Sprechstunden** haben Sie eine weitere gute Möglichkeit, einer erfahrenen Tutorin Fragen zu Ihren Erstsemestervorlesungen zu stellen.

V Q Ü S

Lineare Algebra 1 – Termine im Überblick

Vorlesung

- **Dienstag 9:45 - 11:15** Uhr in V47.01
- **Donnerstag 8:00 - 9:30** in V57.02 (alle zwei Wochen abwechselnd zur Vortragsübung, am 16.10., 30.10., ..., siehe Kalender)
- **Freitag 9:45 - 11:15** in V47.02

Die Vorlesung startet am Dienstag, den **14. Oktober**. In der ersten Woche haben wir drei (!) Vorlesungen: Di, Do, Fr, siehe Kalender.

Vortragsübung

- **Donnerstag 8:00 - 9:30** in V57.02 (alle zwei Wochen abwechselnd zur Vorlesung, am 23.10., ..., siehe Kalender)

Die erste Vortragsübung findet in der zweiten Woche statt, also am Donnerstag, den **23. Oktober**.

Quizze

Wöchentlich veranstalten wir ein Quiz jeweils von **Freitag 13:00 bis Dienstag 8:00**. Das erste Quiz startet in der ersten Woche, also am Freitag, den **17. Oktober** 2025.

Gruppenübungen

Die Gruppenübungen finden **dienstags und mittwochs** in verschiedenen Blöcken statt. Zeiten und Räume finden Sie im Übungsordner.

Die **Anmeldung zu den Übungen** läuft am **Mittwoch, den 15. Oktober** 2025, **von 9 bis 17 Uhr** hier in Ilias (nicht C@mpus). Treten Sie dazu einer der Ilias-Gruppen im Übungsordner bei.

Das erste Übungsblatt gibt es in Woche 1. Die Gruppenübungen starten in Woche 2, also am **21. und 22. Oktober**.

Sprechstunden

gemeinsam zur Analysis 1 und Linearen Algebra 1

In den Sprechstunden zur Analysis und Linearen Algebra haben Sie eine weitere gute Möglichkeit, Ihre Fragen zum Stoff und zu den Übungsaufgaben zu stellen.

- **Montag, 11:30 - 13:00** in V57 8.135
- **Donnerstag, 11:30 - 13:00** in V57 8.143

Kalender

1 4

Erste Vorlesung in V47.01
14. Okt 2025, 09:45 - 11:15

Anmeldung zu den Übungsgruppen
15. Okt 2025, 09:00 - 17:00

Vorlesung in V57.02
16. Okt 2025, 08:00 - 09:30

Quiz 1
17. Okt 2025 - 21. Okt 2025

Vorlesung in V47.02
17. Okt 2025, 09:45 - 11:15

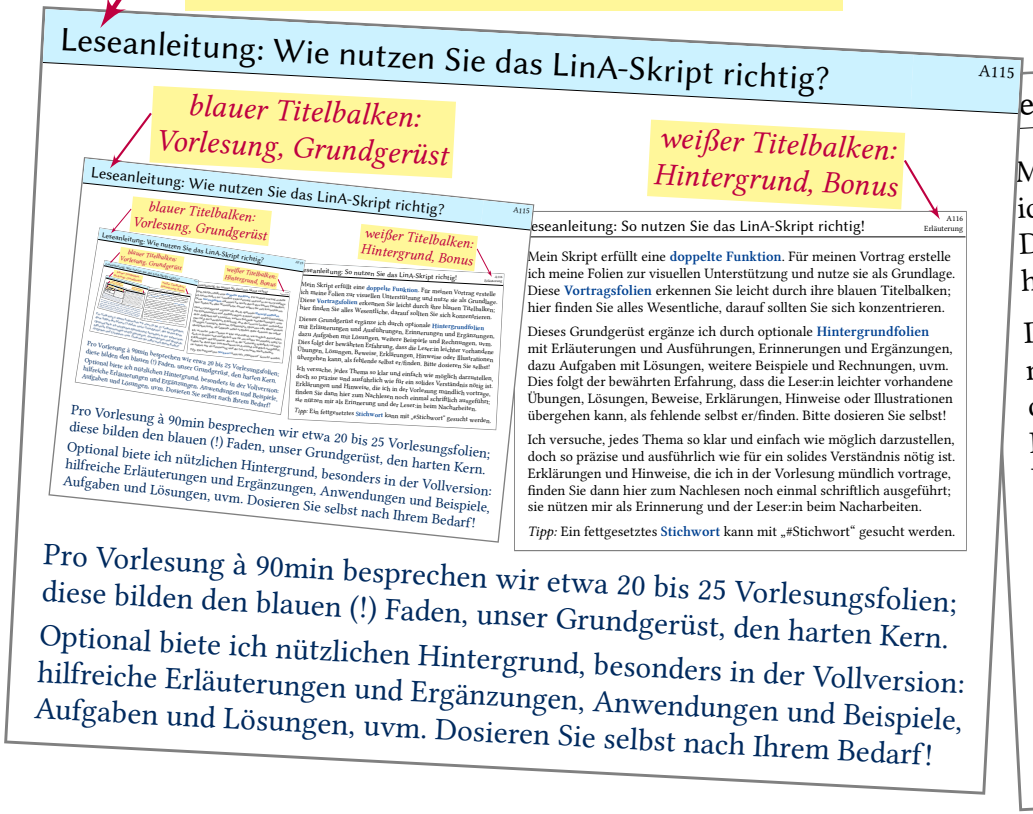
Leseanleitung: Wie nutzen Sie das LinA-Skript richtig?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

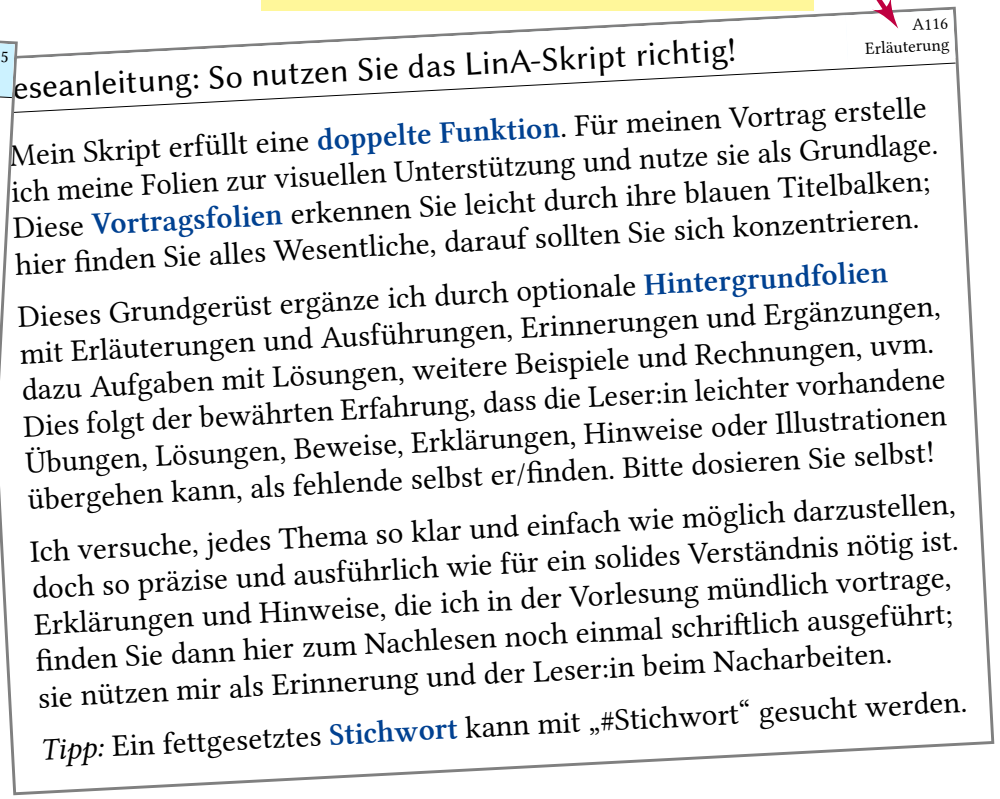
blauer Titelbalken: Vorlesung, Grundgerüst

weißer Titelbalken: Hintergrund, Bonus



Pro Vorlesung à 90min besprechen wir etwa 20 bis 25 Vorlesungsfolien; diese bilden den blauen (!) Faden, unser Grundgerüst, den harten Kern.

Optional biete ich nützlichen Hintergrund, besonders in der Vollversion: hilfreiche Erläuterungen und Ergänzungen, Anwendungen und Beispiele, Aufgaben und Lösungen, uvm. Dosieren Sie selbst nach Ihrem Bedarf!



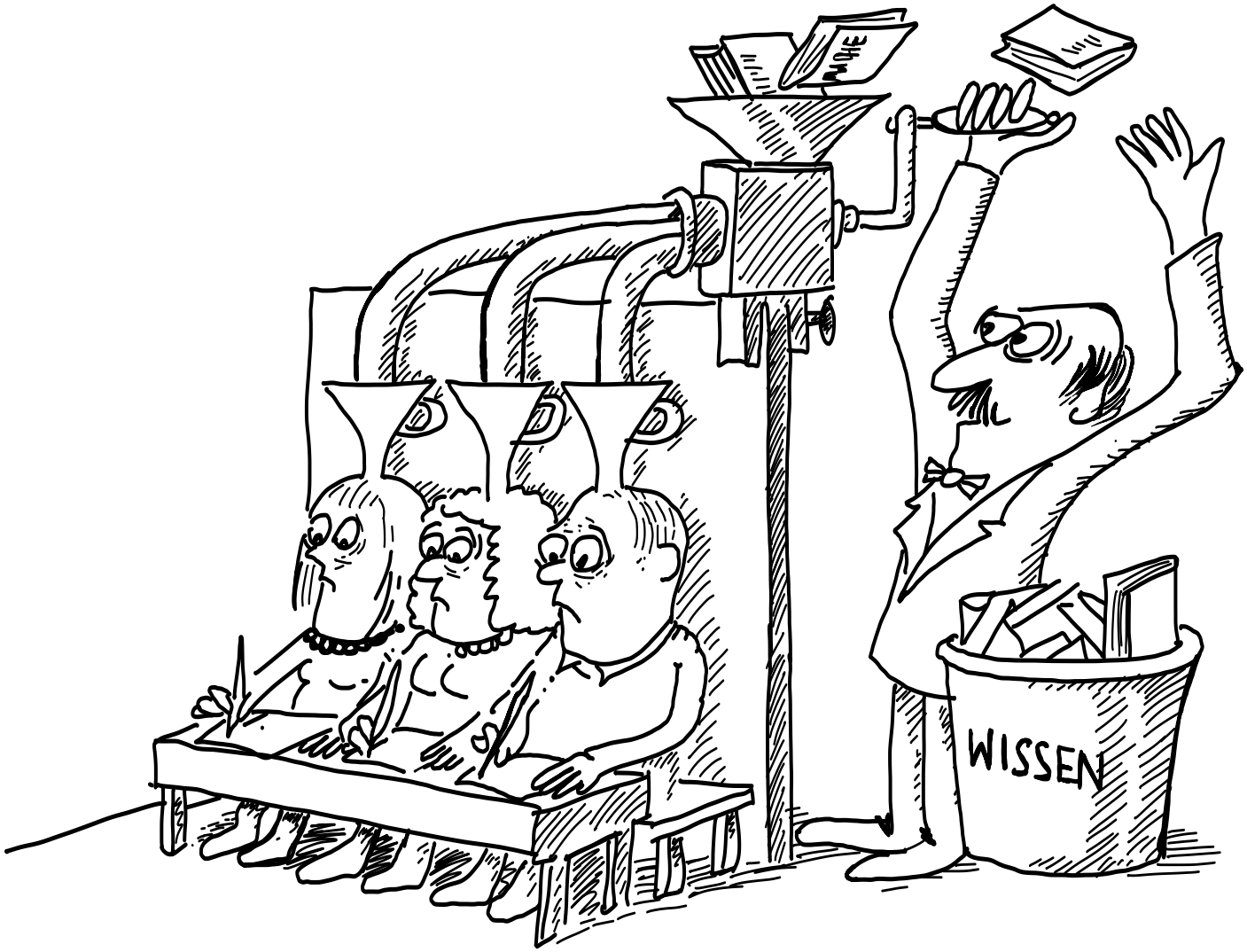
Mein Skript erfüllt eine **doppelte Funktion**. Für meinen Vortrag erstelle ich meine Folien zur visuellen Unterstützung und nutze sie als Grundlage. Diese **Vortragsfolien** erkennen Sie leicht durch ihre blauen Titelbalken; hier finden Sie alles Wesentliche, darauf sollten Sie sich konzentrieren.

Dieses Grundgerüst ergänze ich durch optionale **Hintergrundfolien** mit Erläuterungen und Ausführungen, Erinnerungen und Ergänzungen, dazu Aufgaben mit Lösungen, weitere Beispiele und Rechnungen, uvm. Dies folgt der bewährten Erfahrung, dass die Leser:in leichter vorhandene Übungen, Lösungen, Beweise, Erklärungen, Hinweise oder Illustrationen übergehen kann, als fehlende selbst er/finden. Bitte dosieren Sie selbst!

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 vortrage, finden Sie dann hier zum Nachlesen noch einmal schriftlich ausgeführt; sie nützen mir als Erinnerung und der Leser:in beim Nacharbeiten.

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

Aktives vs passives Lernen



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

3½ wirksame Regeln zum aktiven Lernen

- Fragen Sie, sich und andere!
- Rechnen reinigt die Seele!
- Machen Sie sich Skizzen!

Dies ist nur die Saalversion ohne Erläuterungen.

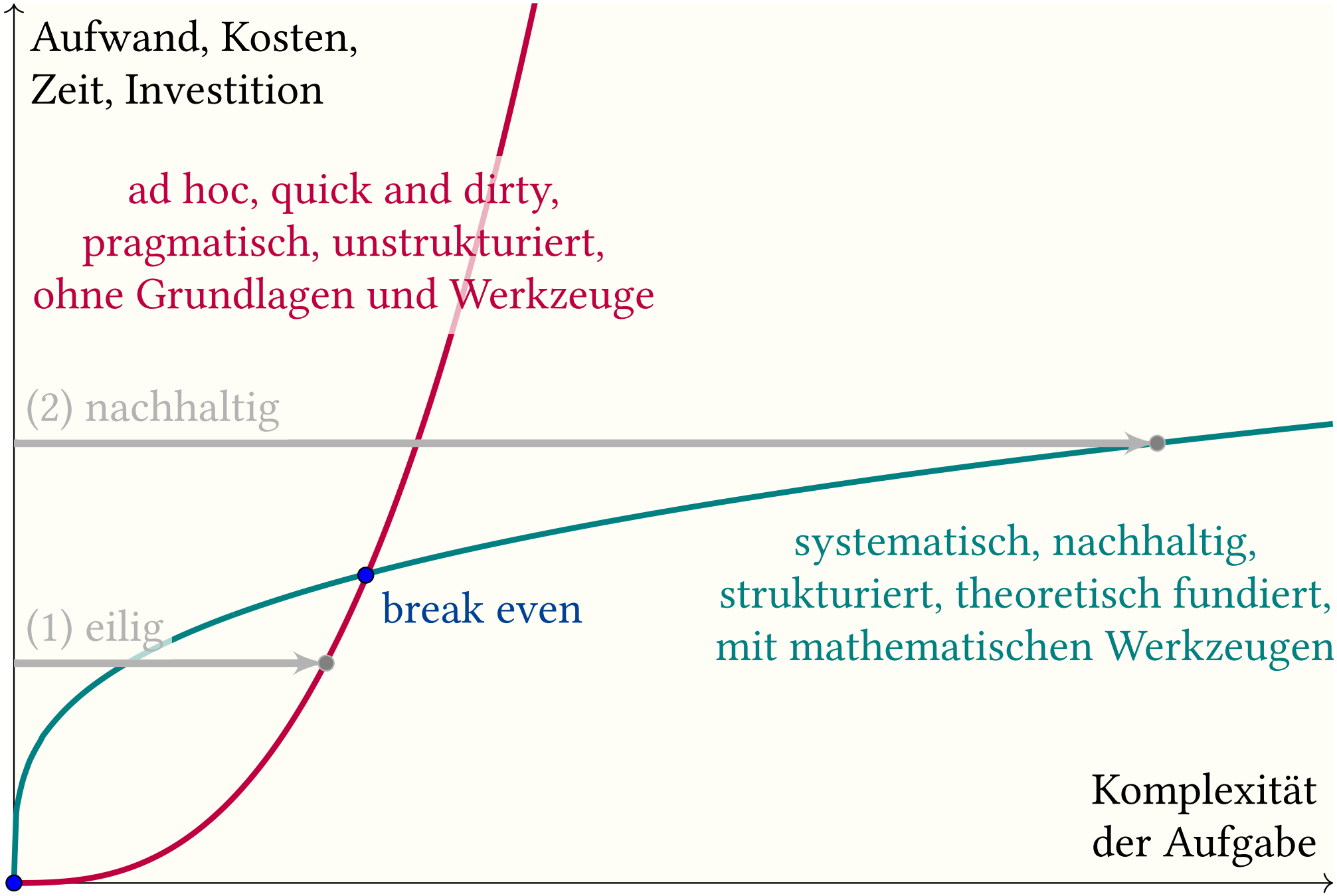
Ausführliche Erläuterungen bietet die Vollversion.

Ihr Studium: Investition vs Konsum. Langfrist vs Kurzfrist.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lohnt studieren? speziell Mathematik? kurz- vs langfristig?



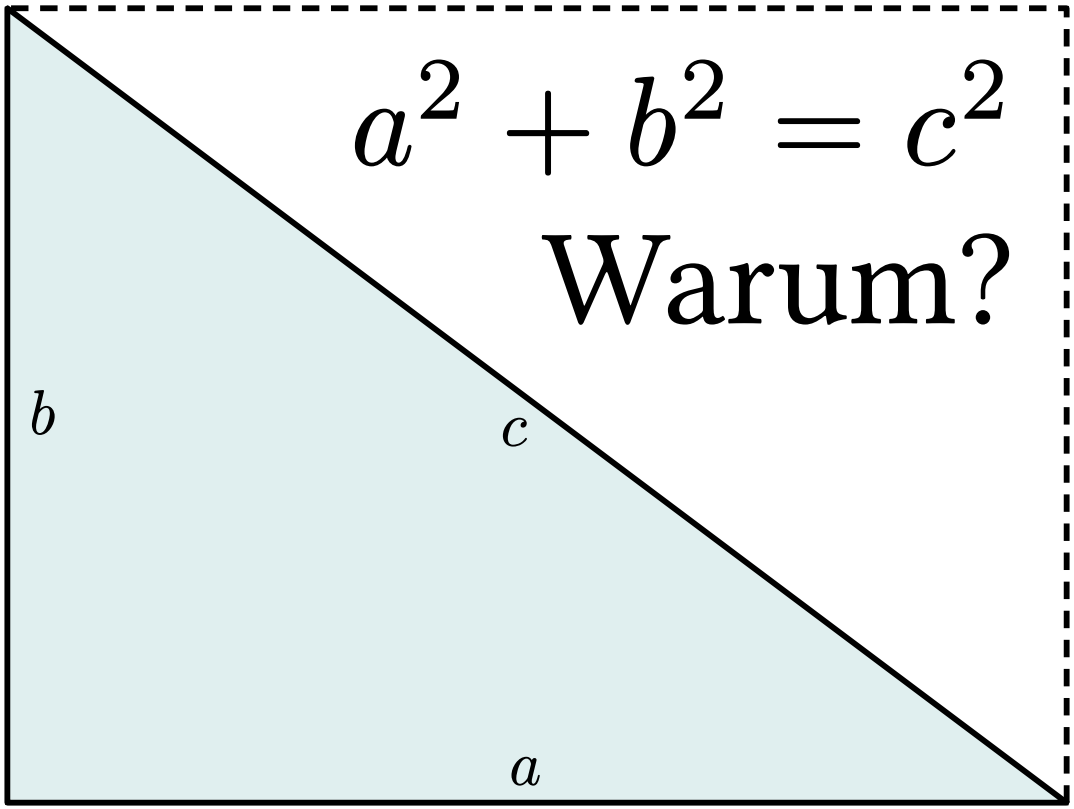
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Mathematik bedeutet: erkennen, beweisen, anwenden!

Dies ist nur die Saalversion ohne Erläuterungen.

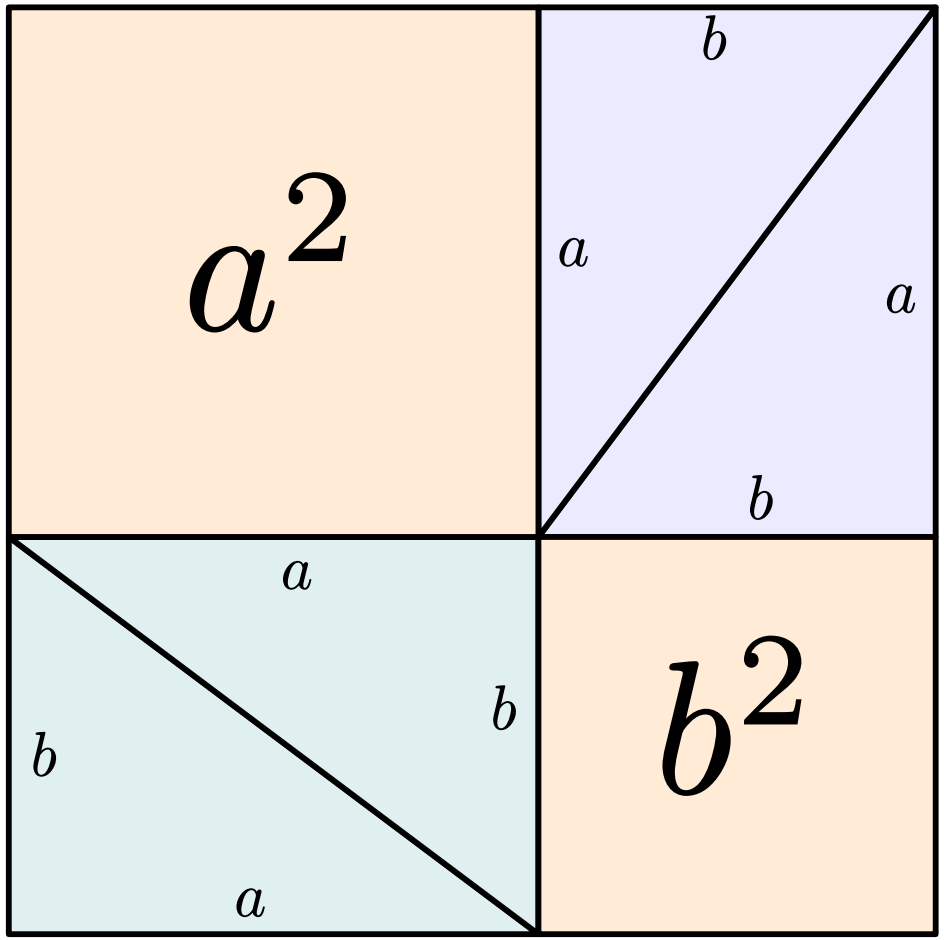
Ausführliche Erläuterungen bietet die Vollversion.

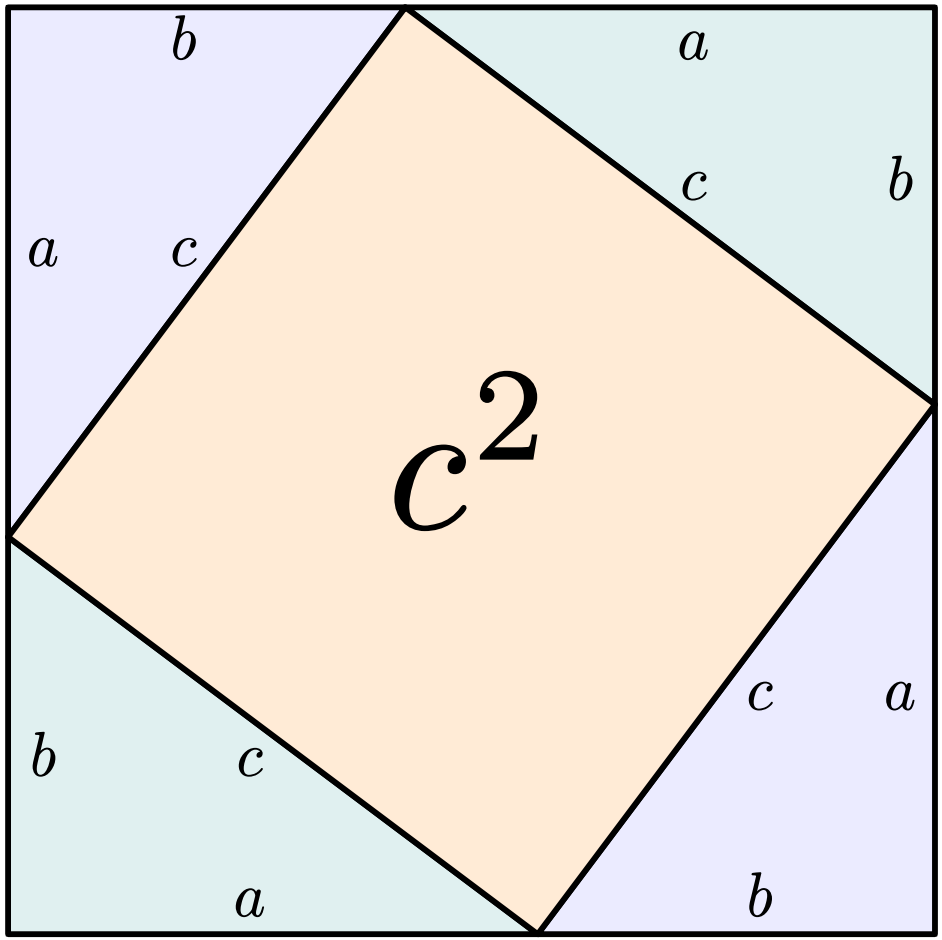


Pythagoras – Satz und Beweis – ohne Worte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: An einer Tafel stehen die Zahlen $1, 2, 3, \ldots, 1970$. Sie dürfen irgend zwei Zahlen wegwischen und dafür ihre Differenz anschreiben. Können Sie dies so ausführen, dass schließlich eine *gerade* Zahl verbleibt?

Beispiele: Wir experimentieren mutig mit kleinen Zahlenreihen $1, \ldots, n$:

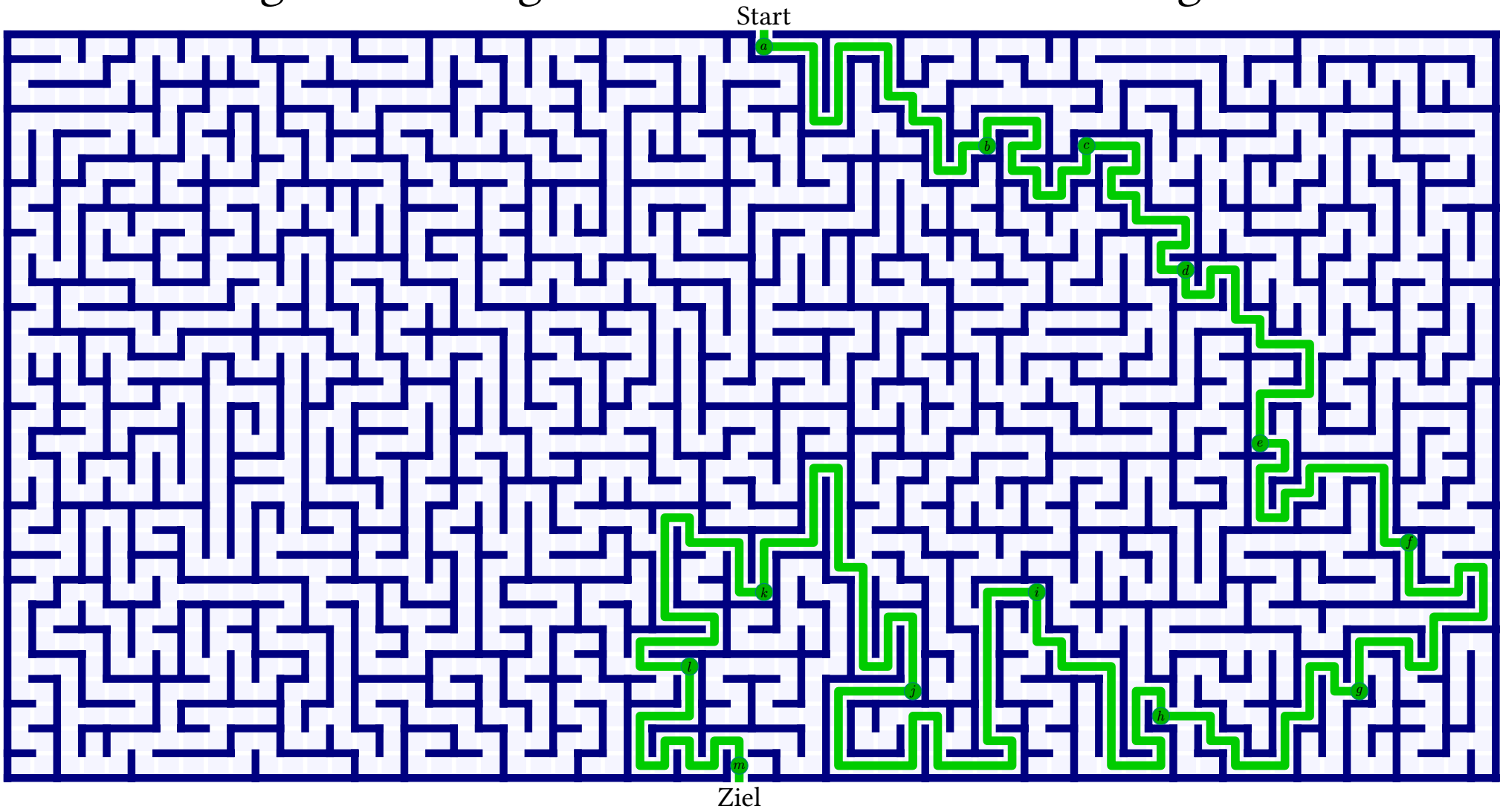
$$1, \cancel{2}, 3, 4, 5, \cancel{6} \mapsto 1, 3, \cancel{4}, \cancel{4}, 5 \mapsto 0, 1, \cancel{3}, \cancel{5} \mapsto \cancel{0}, 1, \cancel{2} \mapsto \cancel{1}, \cancel{2} \mapsto 1$$
$$1, 2, 3, 4, \cancel{5}, \cancel{6} \mapsto 1, 1, \cancel{2}, 3, \cancel{4} \mapsto 1, \cancel{1}, \cancel{2}, 3 \mapsto \cancel{1}, \cancel{1}, 3 \mapsto \cancel{0}, \cancel{3} \mapsto 3$$

$\pm$	g	u
g	g	u
u	u	g

Lösung: Nein! Die Anzahl ungerader Zahlen bleibt gleich oder nimmt um zwei ab. Anfangs ist sie 985, schließlich 1.

Arbeitsteilung zwischen Lehren und Lernen

Ich führe Argumente sorgsam vor. — Sie arbeiten alles gründlich nach.



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wie schreibt man griechische Buchstaben?

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

Dies ist nur die Saalversion ohne Erläuterungen.

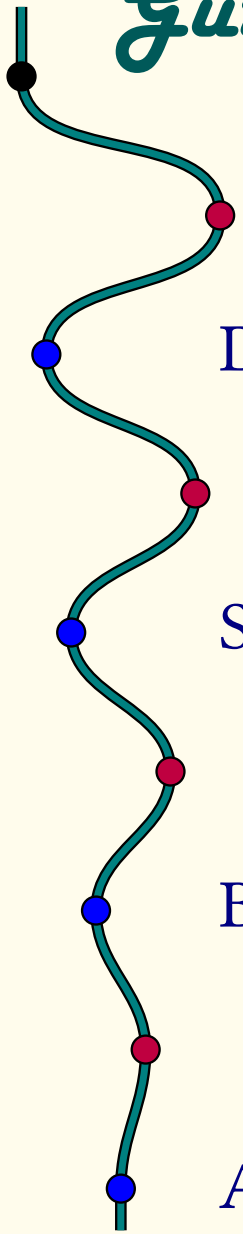
Ausführliche Erläuterungen bietet die Vollversion.

Die Struktur der Mathematik hilft Ihnen!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Gute mathematische Kommunikation



Motivation — einführende Beispiele

Definition — Vereinbarung, Konvention, Notation

Gegen/Beispiele — Miss/Verständnis

Satz — Feststellung, Rechenregel, Algorithmus

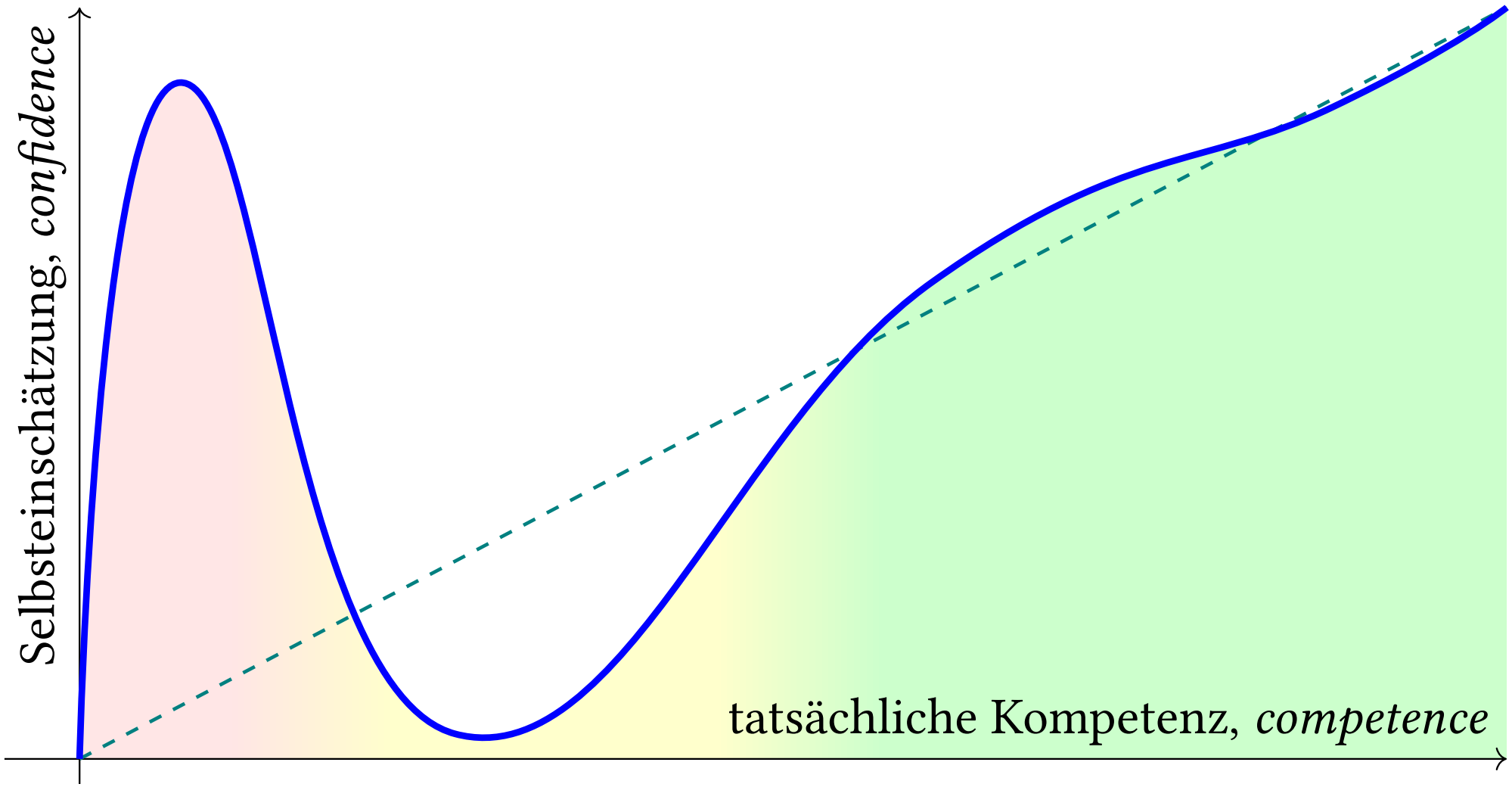
Gegen/Beispiele — Fehl/Anwendung

Beweis — Begründung, Rechenweg, Verfahren

kritischer Rückblick — Feinschliff

Anwendungen, Quiz, Übung, Prüfung, ...

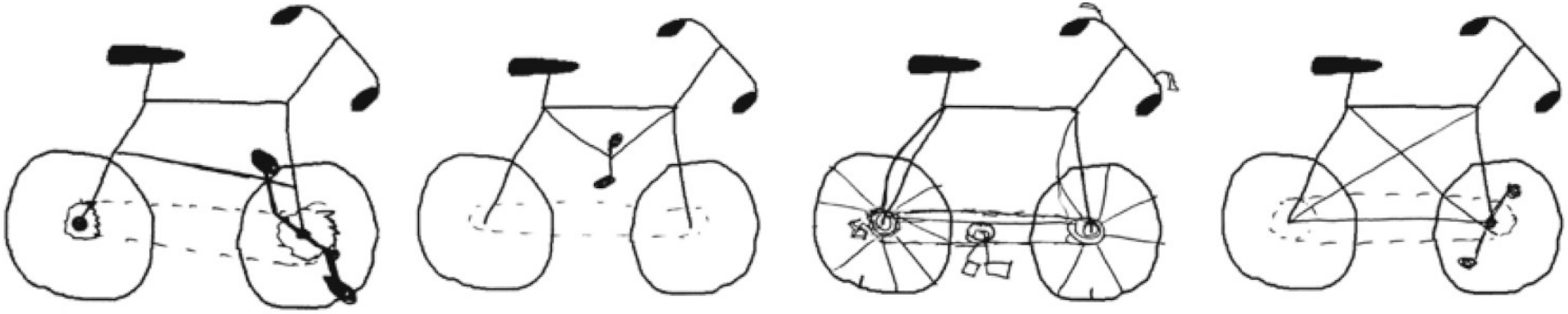
Der berühmt-berüchtigte Dunning–Kruger–Effekt



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wissen vs Können: die Illusion der Erklärtiefe



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel A

Bonusmaterial

Die zwei goldenen Regeln der Didaktik:
Erstens, sage nicht alles.

Inhalt dieses Kapitels A

5 Stolz und Vorurteil: Was ist und was soll Schulmathematik?

6 Landaus Dilemma: Mathematik, unvoreingenommen?

7 Gut gemeinte Ratschläge, vor allem an mich selbst

Dies ist nur die Saalversion ohne Erläuterungen.

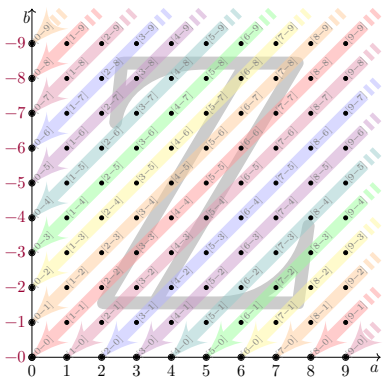
Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel B

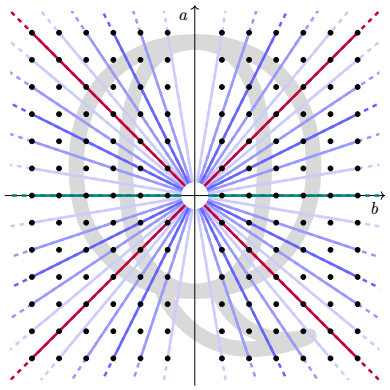
Aufbau des Zahlensystems und Arithmetik: natürliche, ganze und rationale Zahlen

$$(\mathbb{N}, 0, s): \quad 0 \xmapsto{s} 1 \xmapsto{s} 2 \xmapsto{s} 3 \xmapsto{s} 4 \xmapsto{s} 5 \xmapsto{s} 6 \xmapsto{s} 7 \xmapsto{s} 8 \xmapsto{s} 9 \xmapsto{s} \ldots$$



Bitte vergiss alles, was Du auf der Schule gelernt hast; denn Du hast es nicht gelernt. Bitte denke bei allem an das Schulpensum; denn Du hast es doch nicht vergessen.

Edmund Landau (1877–1938)



Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels B

1 Rechnen mit Mengen und Funktionen

2 Aufbau des Zahlensystems $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$

3 Arithmetik in $\mathbb{Z}$, Restring $\mathbb{Z}_n$ und Restklassenring $\mathbb{Z}/n\mathbb{Z}$

4 Aufgaben, Anwendungen, Fazit

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vorschau: praktische Beispiele, Fragen, Anwendungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Frage B0A: Aufbau unseres Zahlensystems

(0) Wie erklären Sie $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ und das Rechnen darin?

(1) Existiert zu $a, b \in \mathbb{Z}$ ein größter gemeinsamer Teiler $d \in \mathbb{Z}$?

(2) Ist jedes $n \in \mathbb{N}_{\geq 1}$ ein Produkt von Primzahlen? eindeutig?

(3) Ist $\sqrt{2}$ rational? irrational? und $\sqrt[3]{864}$? und $\log_{10}(99)$?

(4) Gibt es rationale Punkte $(x, y, z) \in \mathbb{Q}^3$ in der Ebene $x + y + z = 0$, die zudem auf der Sphäre $x^2 + y^2 + z^2 = 10^2$ von Radius 10 liegen?

Unwichtiges weglassen? Abstraktion vereinfacht!

Picasso

Le Taureau 1945

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lineare Gleichungssysteme lösen über $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

? Welche Rechenregeln benötigen wir dazu für $(\mathbb{K}, +, 0, -, \cdot, 1, {}^{-1})$?
Nur erfreulich wenige! (A) Die Addition bildet eine **abelsche Gruppe** $(\mathbb{K}, +, 0, -)$. Das heißt ausgeschrieben, für alle Elemente $a, b, c \in \mathbb{K}$ gilt:

(A0)	$a + b = b + a$	(A2)	$a + 0 = a = 0 + a$
(A1)	$(a + b) + c = a + (b + c)$	(A3)	$a + (-a) = 0 = (-a) + a$

(M) Die Multiplikation bildet ein **kommutatives Monoid** $(\mathbb{K}, \cdot, 1)$, dabei gilt $1 \neq 0$ und jedes Element $x \neq 0$ hat ein Inverses x^{-1}:

(M0)	$a \cdot b = b \cdot a$	(M2)	$a \cdot 1 = a = 1 \cdot a$
(M1)	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	(M3)	$x \cdot x^{-1} = 1 = x^{-1} \cdot x$

(D) Die Multiplikation ist beidseitig **distributiv** über die Addition:

$$\text{(DL)} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \overset{\text{(A)}}{\Longrightarrow} \quad \text{(L0)} \quad a \cdot 0 = 0$$

$$\text{(DR)} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c) \quad \overset{\text{(A)}}{\Longrightarrow} \quad \text{(R0)} \quad 0 \cdot a = 0$$

Wir nennen $(\mathbb{K}, +, 0, -, \cdot, 1, {}^{-1})$ einen **Körper**. Beispiele sind $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
Dem **CRing** $\mathbb{Z} \subset \mathbb{Q}$ fehlt nur (M3), dem **CHalbring** $\mathbb{N} \subset \mathbb{Z}$ zudem (A3).

Aussagenlogik: bequem und präzise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jeder Aussage A, wie „$2+3=1$“ oder „$2+3=5$“ können wir eindeutig einen Wahrheitswert $[A]$ zuordnen, entweder $0=$ falsch oder $1=$ wahr.

Operation	Bedeutung	Beispiele etwa in $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
$\neg A$	Es gilt nicht A.	Die Aussage $x \neq y$ bedeutet $\neg(x=y)$.
$A \wedge B$	Es gilt A und B.	$3 \leq x \leq 5$ bedeutet $(3 \leq x) \wedge (x \leq 5)$.
$A \vee B$	Es gilt A oder B.	$x = \pm 3$ bedeutet $(x=-3) \vee (x=+3)$.
$A \Rightarrow B$	Aus A folgt B.	$x=\pm 3 \Rightarrow x^2 = 9$ wenn… gilt, dann…
$A \Leftarrow B$	Aus B folgt A.	$x=\pm 3 \Leftarrow x^2 = 9$ …ist erfüllt, wenn…
$A \Leftrightarrow B$	Äquivalenz	$x=\pm 3 \Leftrightarrow x^2 = 9$ …genau dann, wenn…

Der Quantor „$\forall$“ bedeutet „für alle“: $\forall x \in \mathbb{R} : x^2 \geq 0$. $\forall x \in \mathbb{R} : x^2 > 0$.
Der Quantor „$\exists$“ bedeutet „es existiert“: $\exists x \in \mathbb{Q} : x^2 = 2$. $\exists x \in \mathbb{R} : x^2 = 2$.
Der Quantor „$\exists!$“ bedeutet „es existiert genau ein“: $\exists! x \in \mathbb{R}_{\geq 0} : x^2 = 2$.

Mengen und ihre Elemente

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Eine **Menge** M ist die Zusammenfassung ihrer Elemente, zum Beispiel

$$U := \{1, 3, 5, 7, 9\} \quad \text{oder} \quad V := \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}.$$

Wir schreiben $x \in M$, falls x ein Element von M ist, andernfalls $x \notin M$.

Die **Aufzählung** $M = \{a_1, \dots, a_n\}$ bedeutet: Genau dann gilt $x \in M$, wenn $x = a_1 \lor \dots \lor x = a_n$. Die **leere Menge** schreiben wir $\emptyset = \{\}$.

Eine **Teilmenge** $A \subseteq M$ erfüllt: Für jedes Element $x \in A$ gilt $x \in M$. Im Beispiel gilt $\{3, 5\} \subseteq U$, jedoch $\{3, 5\} \not\supseteq U$; wir schreiben $\{3, 5\} \subset U$.

Extensionalität: Mengengleichheit $A = B$ bedeutet $A \subseteq B$ und $A \supseteq B$. Beispielsweise gilt $\{1, 2\} = \{2, 1\}$ und ebenso $\{1, 2, 3\} = \{2, 1, 3, 3, 1\}$.

Schreibweise für Teilmengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

	Schreibweise	Inklusion	strikt
☺	(0) ästhetisch	$A \subseteq B$	$A \subset B$
😐	(1) narrensicher	$A \subseteq B$	$A \subsetneq B$
☹	(2) à la Bourbaki	$A \subset B$	$A \subsetneq B$

Teilmengen durch Aussonderung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Durch **Aussonderung** bilden wir die Teilmenge $A = \{\, x \in M \mid P(x) \,\}$.

$$[a,b]_{\mathbb{R}} := \{\, x \in \mathbb{R} \mid a \leq x \leq b \,\}, \qquad]a,b[_{\mathbb{R}} := \{\, x \in \mathbb{R} \mid a < x < b \,\},$$

$$[a,b[_{\mathbb{R}} := \{\, x \in \mathbb{R} \mid a \leq x < b \,\}, \qquad]a,b]_{\mathbb{R}} := \{\, x \in \mathbb{R} \mid a < x \leq b \,\}.$$

Beispiel: Wie lösen Sie quadratische Gleichungen über $\mathbb{R}$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Gegeben seien Koeffizienten $a, b, c \in \mathbb{R}$ mit $a \neq 0$. Dann gilt:

$$\underbrace{\{x \in \mathbb{R} \mid \overbrace{ax^2 + bx + c = 0}^{\text{quadratische Gleichung}}\}}_{\text{Lösungsmenge}} = \begin{cases} \left\{\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}\right\} & \text{falls } b^2 - 4ac \geq 0, \\ \emptyset & \text{falls } b^2 - 4ac < 0. \end{cases}$$

Lösung: 1. Fall: Sei $b^2 - 4ac \geq 0$. Sei $x \in \mathbb{R}$ eine reelle Zahl. Dann gilt:

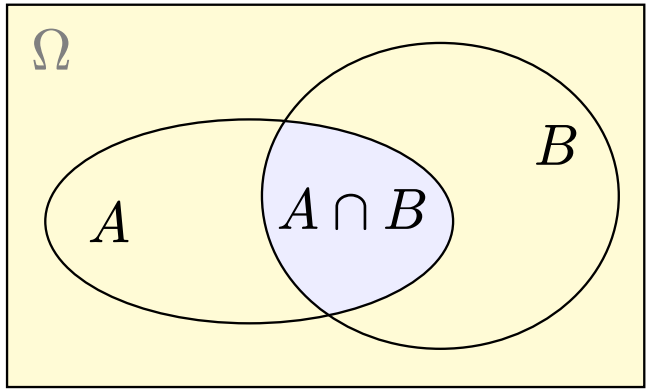
$$\begin{aligned}
& ax^2 + bx + c = 0 \\
\overset{(0)}{\Longleftrightarrow}\quad & x^2 + 2px + q = 0 && \text{mit } p := b/2a \text{ und } q := c/a \\
\overset{(1)}{\Longleftrightarrow}\quad & x^2 + 2px + p^2 = p^2 - q && \text{quadratische Ergänzung!} \\
\overset{(2)}{\Longleftrightarrow}\quad & (x+p)^2 = p^2 - q && = (b^2 - 4ac)/(4a^2) \geq 0 \\
\overset{(3)}{\Longleftrightarrow}\quad & x + p \in \{\pm\sqrt{p^2 - q}\} \\
\overset{(4)}{\Longleftrightarrow}\quad & x \in \{-p \pm \sqrt{p^2 - q}\}
\end{aligned}$$

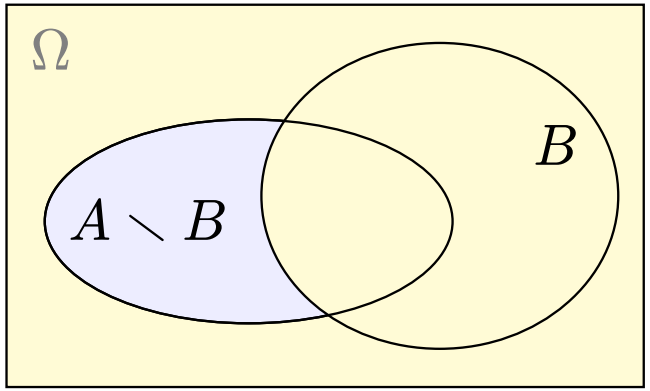
2. Fall: Sei $b^2 - 4ac < 0$. Dann existiert *keine* Lösung $x \in \mathbb{R}$. QED

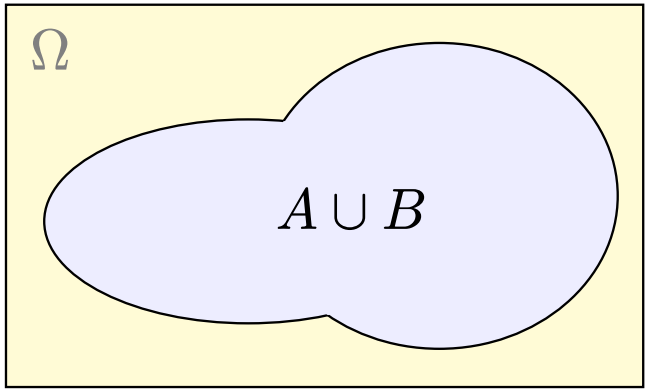
Schnittmenge, Komplement und Vereinigung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.







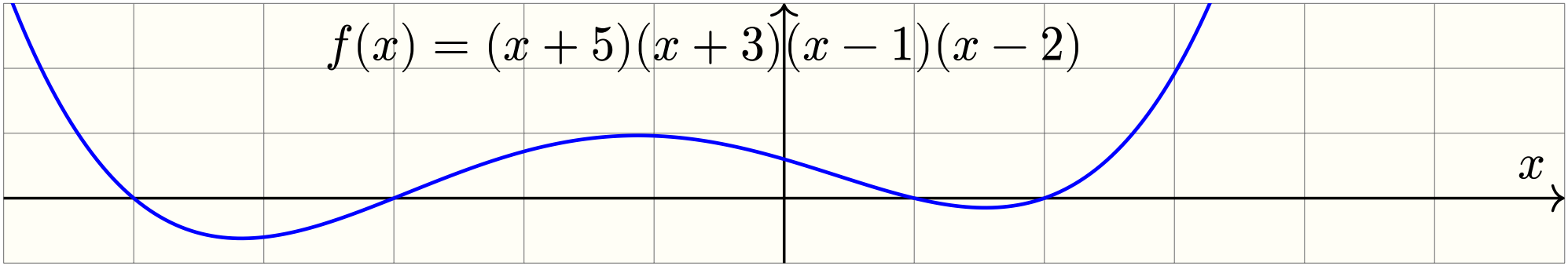
Schnittmenge: $S = A \cap B \quad := \{x \in \Omega \mid x \in A \wedge x \in B\}$

Komplement: $K = A \setminus B \quad := \{x \in \Omega \mid x \in A \wedge x \notin B\}$

Vereinigung: $V = A \cup B \quad := \{x \in \Omega \mid x \in A \vee x \in B\}$

Disjunkte Vereinigung $V = A \sqcup B$ bedeutet $V = A \cup B$ und $A \cap B = \emptyset$.

Anwendungsbeispiel: Lösungsmengen von Un/Gleichungen



$$P := \{\, x \in \mathbb{R} \mid f(x) > 0 \,\}$$
$$N := \{\, x \in \mathbb{R} \mid f(x) \leq 0 \,\}$$

$$P \;=\;]-\infty, -5[\, \cup\,]-3, 1[\, \cup\,]2, +\infty[$$ also $\subseteq$ und $\supseteq$!

$$N \;=\; \mathbb{R} \setminus P \;=\; [-5, -3] \cup [1, 2]$$ also $\subseteq$ und $\supseteq$!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

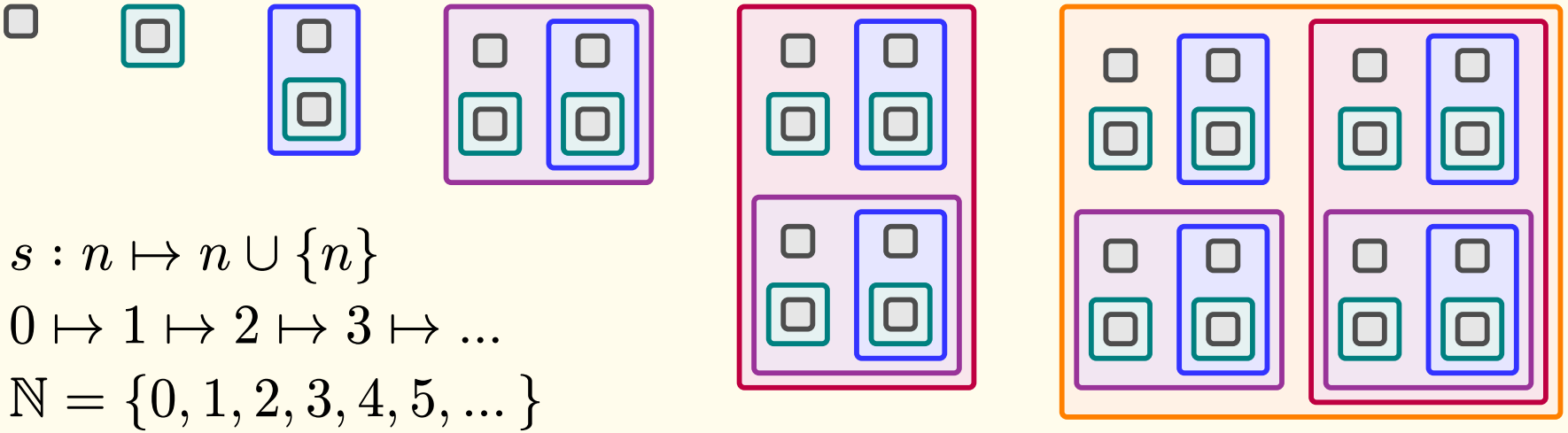
John von Neumanns Konstruktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

John von Neumanns Konstruktion

0	1	2	3	4	5
$\ddot{\shortparallel}$	$\ddot{\shortparallel}$	$\ddot{\shortparallel}$	$\ddot{\shortparallel}$	$\ddot{\shortparallel}$	$\ddot{\shortparallel}$
$\emptyset$	$\{0\}$	$\{0,1\}$	$\{0,1,2\}$	$\{0,1,2,3\}$	$\{0,1,2,3,4\}$



$$s : n \mapsto n \cup \{n\}$$

$$0 \mapsto 1 \mapsto 2 \mapsto 3 \mapsto \dots$$

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$$

der natürlichen Zahlen $(\mathbb{N}, 0, s)$

Designed 2024 by Michael Eisermann, University of Stuttgart

Kartesische Produkte von Mengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Der reelle Koordinatenraum $\mathbb{R}^n$ ist das kartesische Produkt

$$\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R} = \{ x = (x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{R} \}.$$

Allgemein, zu Mengen $A_1, \dots, A_n$ definieren wir ihr kartesisches **Produkt**

$$A = A_1 \times \cdots \times A_n := \{ x = (x_1, \dots, x_n) \mid x_1 \in A_1 \wedge \dots \wedge x_n \in A_n \}.$$

Gleichheit: Genau dann gilt $x = y$ in A, wenn $x_i = y_i$ in A_i für alle i gilt.

Kartesische Produkte von Mengen

Dies ist nur die Saalversion ohne Erläuterungen.

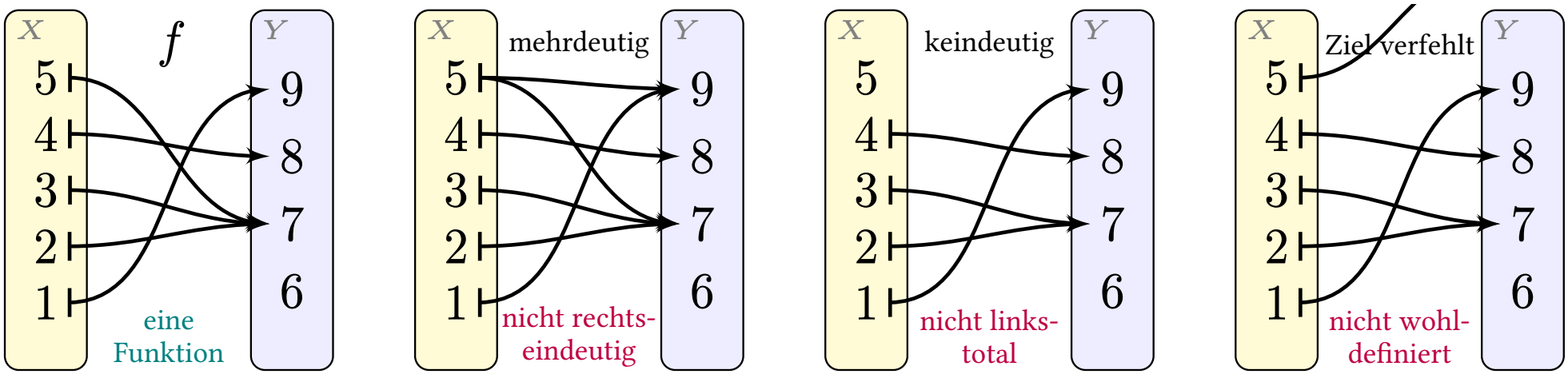
Ausführliche Erläuterungen bietet die Vollversion.

$$\{7, 8, 9\} \times \{\spadesuit, \heartsuit\} = \{(7, \spadesuit), (7, \heartsuit), (8, \spadesuit), (8, \heartsuit), (9, \spadesuit), (9, \heartsuit)\}$$

y			
$\heartsuit$	$(7, \heartsuit)$	$(8, \heartsuit)$	$(9, \heartsuit)$
$\spadesuit$	$(7, \spadesuit)$	$(8, \spadesuit)$	$(9, \spadesuit)$
x	7	8	9

Was *tut* eine Funktion? (aka Abbildung, Zuordnung)

Eine **Funktion** $f : X \to Y$ ordnet jedem Startelement $x \in X$ genau ein Zielelement $y \in Y$ zu, geschrieben $f : x \mapsto y$ oder $f(x) = y$.



Zu Teilmengen $A \subseteq X$ und $B \subseteq Y$ definieren wir die

$$\begin{array}{lll} \text{Bildmenge} & f(A) = f_*(A) := \{\, f(x) \mid x \in A \,\} & \subseteq Y, \\ \text{Urbildmenge} & f^{-1}(B) = f^*(B) := \{\, x \in X \mid f(x) \in B \,\} & \subseteq X. \end{array}$$

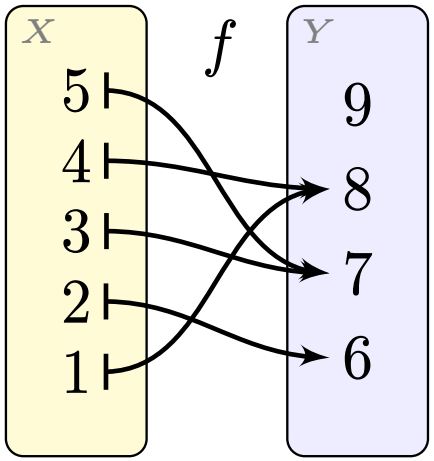
Im obigen Beispiel gilt $f(\{3,4,5\}) = \{7,8\}$ und $f^{-1}(\{7\}) = \{2,3,5\}$.
Die **Bildmenge** von f ist $\operatorname{Im}(f) := f(X) = \{\, f(x) \mid x \in X \,\} \overset{\text{Bsp}}{=} \{7,8,9\}$.

Dies ist nur die Saalversion ohne Erläuterungen.
Ausführliche Erläuterungen bietet die Vollversion.

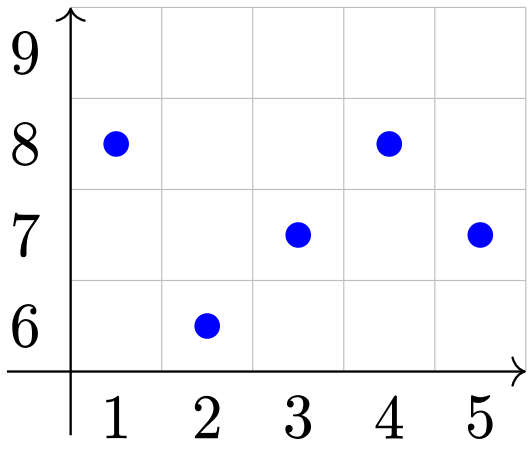
Extensionalität: Wann sind zwei Funktionen gleich?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Funktion $f : X \to Y$ als Graph
$F = \{\, (x, y) \in X \times Y \mid f(x) = y \}$



Aufgabe: Wie viele Funktionen $\{1, 2, 3, 4, 5\} \to \{6, 7, 8, 9\}$ gibt es?
Lösung: Die gesuchte Anzahl ist $\sharp\,\mathrm{Fun}(X, Y) = 4^5 = 2^{10} = 1024$.

Extensionalität: Funktionen $f : X \to Y$ und $f' : X' \to Y'$ sind **gleich**, wenn sie gleiche Startmenge $X = X'$ und gleiche Zielmenge $Y = Y'$ haben und gleich abbilden, also $f(x) = f'(x)$ für alle $x \in X$ erfüllen.

Was *ist* eine Funktion? (aka Abbildung, Zuordnung)

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition B1A: Funktion aka Abbildung

Eine **Funktion** $f : X \to Y$ ist ein Tripel $f = (X, F, Y)$ aus der Startmenge X, der Zielmenge Y und dem Funktionsgraphen $F \subseteq X \times Y$, wobei gilt:

$$\forall x \in X \;\; \exists! y \in Y : \; (x, y) \in F$$

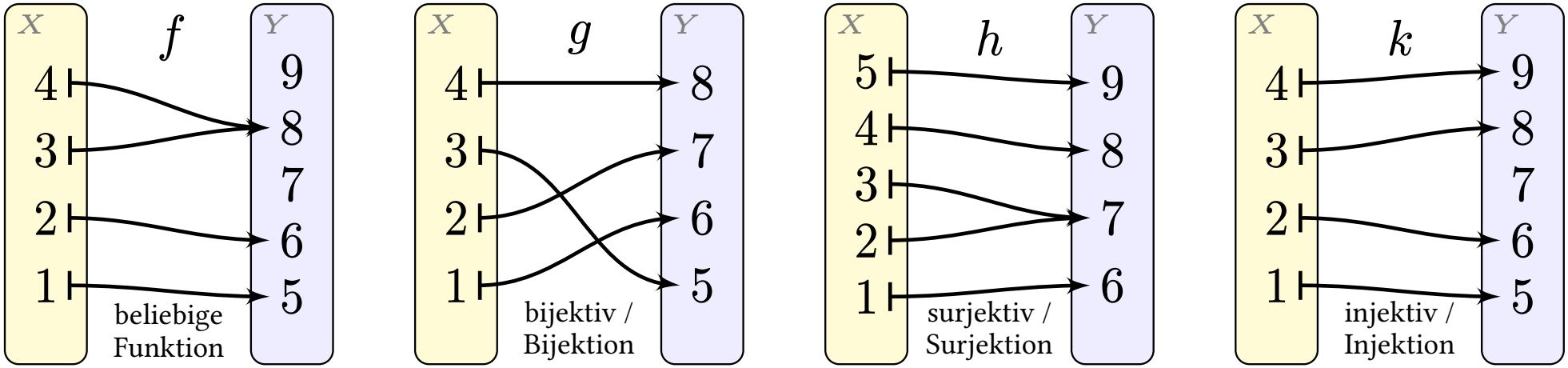
In Worten: Zu jedem Startelement $x \in X$ existiert genau ein Zielelement $y \in Y$ mit $(x, y) \in F$. Hierfür schreiben wir kurz $f : x \mapsto y$ oder $f(x) = y$.

Die Menge aller Funktionen $f : X \to Y$ schreiben wir $\mathrm{Fun}(X, Y) = Y^X$.

Sur/in/bijektiv: Wie viele Lösungen hat $f(x) = y$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



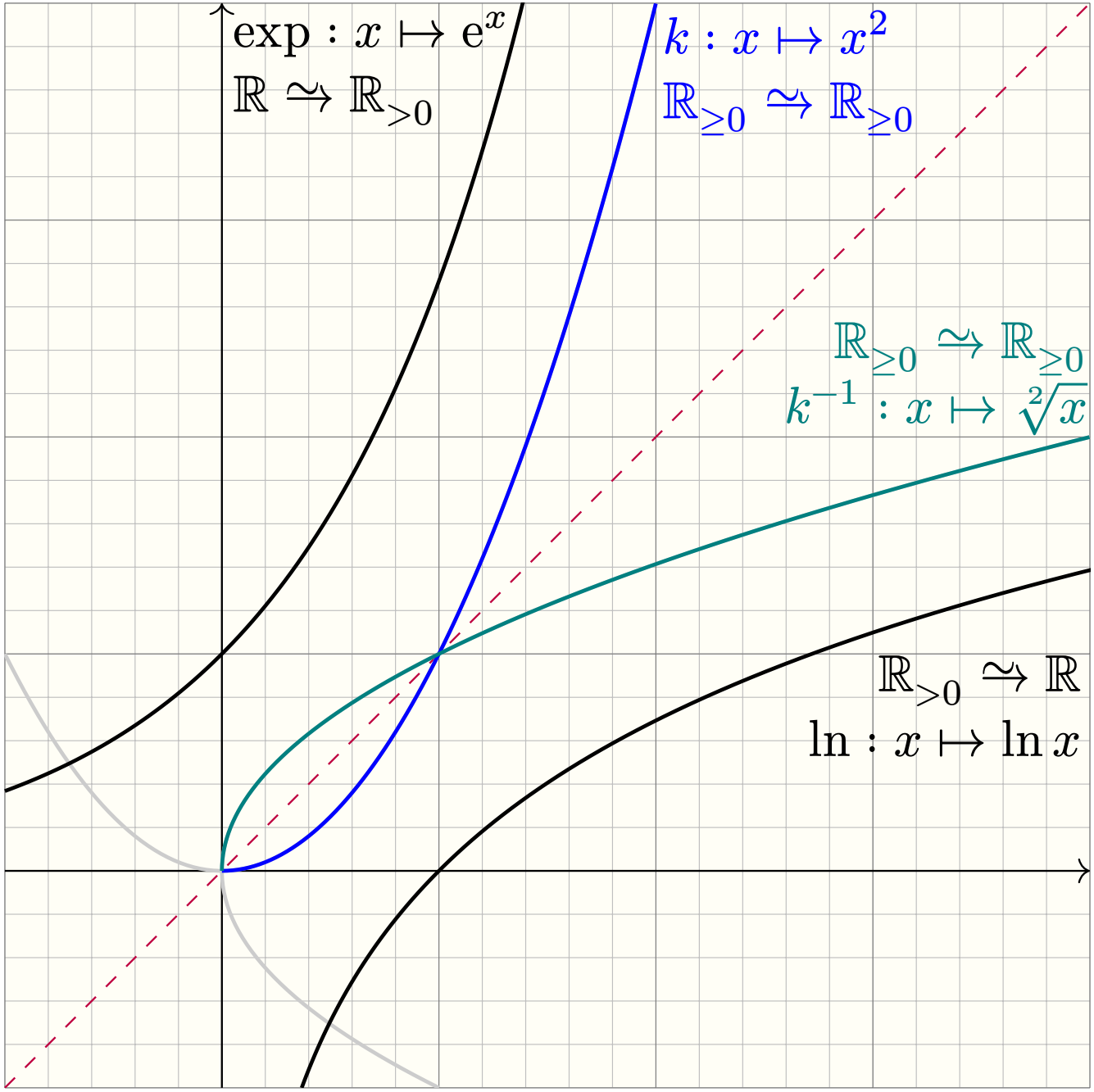
Definition B1B: bijektiv, surjektiv, injektiv

Wir nennen $f : X \to Y$ **bijektiv** / **surjektiv** / **injektiv**, wenn zu jedem $y \in Y$ genau / mindestens / höchstens ein $x \in X$ mit $f(x) = y$ existiert.

Injektiv bedeutet $f(a) = f(b) \Rightarrow a = b$, äquivalent $a \neq b \Rightarrow f(a) \neq f(b)$.

Genau dann wenn $f : X \to Y : x \mapsto f(x)$ bijektiv ist, ist die Umkehrung $f^{\mathsf{T}} : Y \to X : f(x) \mapsto x$ eine Funktion, die **Umkehrfunktion** f^{-1}.

Jede Bijektion können wir umkehren durch „Spiegelung“.



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Anwendungsbeispiel: Aufzählung ohne Dopplung

Dies ist nur die Saalversion ohne Erläuterungen.

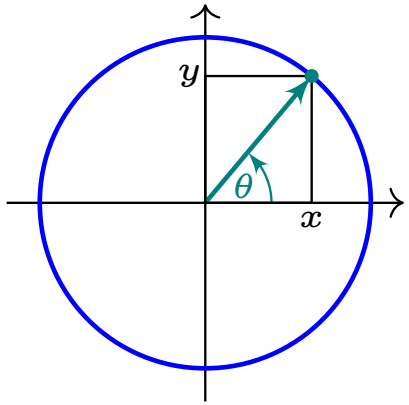
Ausführliche Erläuterungen bietet die Vollversion.

Bemerkung: Die Menge $M = \{x_1, \dots, x_n\}$ hat *höchstens* n Elemente.
Wie notieren wir, dass alle genannten Elemente *verschieden* sind?

$$M = \{x_1, \dots, x_n\}^! \quad \text{allgemein} \quad M = \{\, x_i \mid i \in I \}^!$$

Anwendungsbeispiel: Parametrisierung ohne Dopplung

$$\mathbb{S}^1 := \{\, (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \,\}.$$



$$\mathbb{S}^1 = \{\, (\cos\theta, \sin\theta) \mid \theta \in \mathbb{R} \,\} \quad (\subseteq, \supseteq)$$

$$\mathbb{S}^1 = \{\, (\cos\theta, \sin\theta) \mid \theta \in [0, 2\pi[\,\}^{!}$$

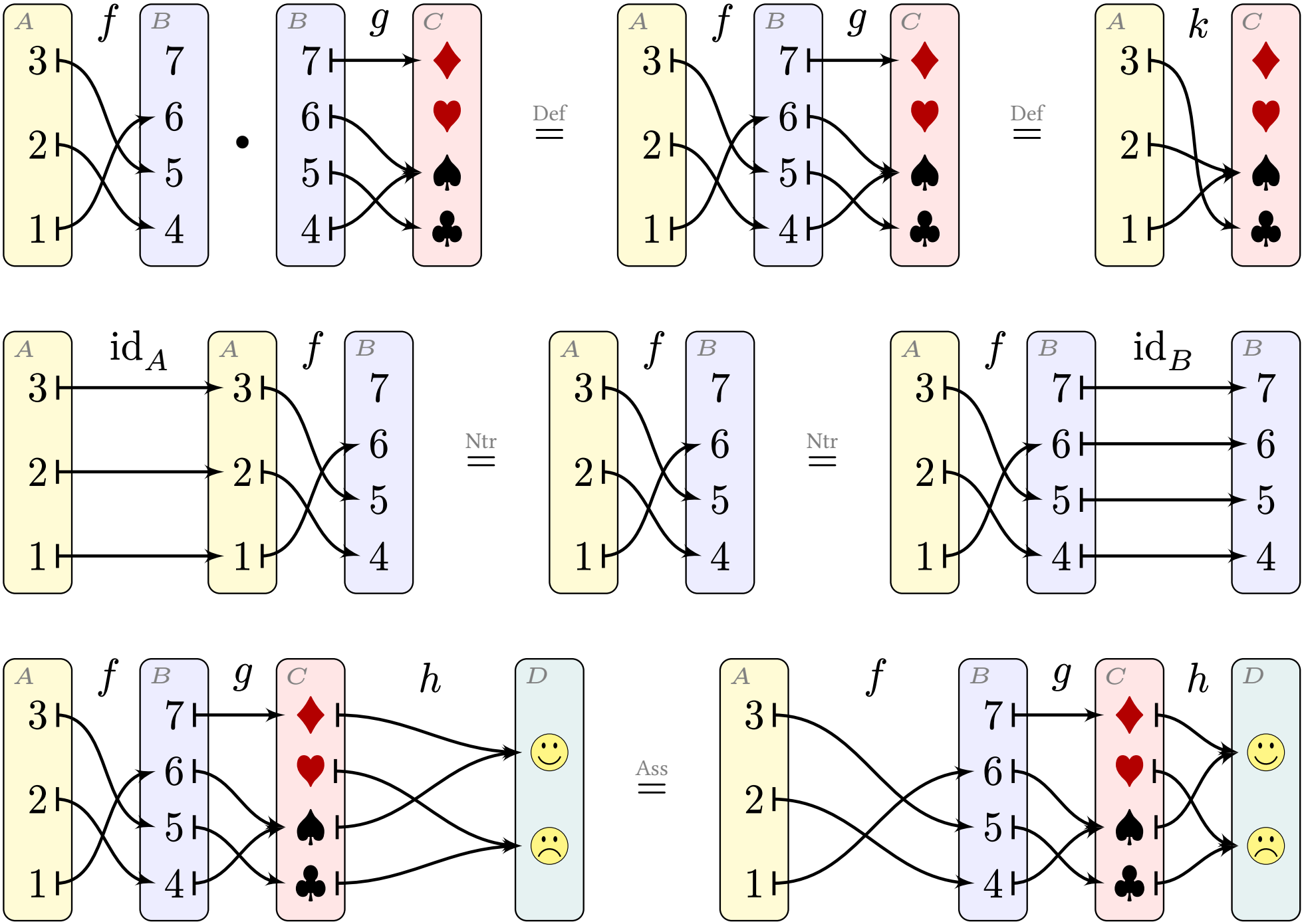
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Rechnen mit Mengen und Funktionen — die Kategorie Set

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

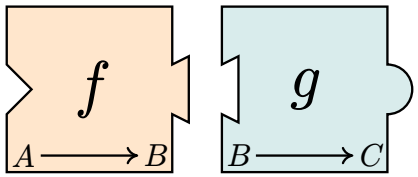


Rechnen mit Mengen und Funktionen — die Kategorie Set

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zur Teilmenge $A \subseteq B$ haben wir die **Inklusion** $\mathrm{inc} = \iota_A^B : A \to B : x \mapsto x$.
Speziell für $A = B$ erhalten wir die **Identität** $\mathrm{id}_A : A \to A : x \mapsto x$.



$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "k = f \bullet g = g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd} \qquad \begin{tikzcd} x \arrow[r, mapsto, "f"] \arrow[rr, bend right, mapsto, "k = f \bullet g = g \circ f"'] & y \arrow[r, mapsto, "g"] & z \end{tikzcd}$$

Satz B1c: Komposition, Neutralität, Assoziativität (aka Kategorie)

(0) Zwei Abbildungen $f : A \to B$ und $g : B \to C$ können wir verknüpfen zu $k = g \circ f = f \bullet g : A \to C$ mit $k(x) = g(f(x))$ für jedes Element $x \in A$.

(1) Neutralität: Für jede Abbildung $f : A \to B$ gilt $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$.

(2) Assoziativität: Für alle $f : A \to B$ und $g : B \to C$ und $h : C \to D$ gilt $(h \circ g) \circ f = h \circ (g \circ f)$.

Rechnen mit Mengen und Funktionen — die Kategorie Set

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Was ist hier zu beweisen? Beweisen Sie es!

Lösung: (2) Gilt Assoziativität?

$$
\begin{array}{lrcccc}
(h \circ g) \circ f : A \to D : & ((h \circ g) \circ f)(x) & \overset{\text{Def}}{=} & (h \circ g)(f(x)) & \overset{\text{Def}}{=} & h(g(f(x)) \\
h \circ (g \circ f) : A \to D : & (h \circ (g \circ f))(x) & \overset{\text{Def}}{=} & h((g \circ f)(x)) & \overset{\text{Def}}{=} & h(g(f(x))
\end{array}
$$

Dank Extensionalität gilt also $h \circ (g \circ f) = (h \circ g) \circ f$. $\boxed{\text{QED}}$

Übersichtliche Darstellung als Diagramm

$$\begin{tikzcd}
\mathbb{R} \arrow[r, "g", "x \mapsto x^2"'] \arrow[dr, "\mathrm{id}", "x \mapsto x"'] & \mathbb{R}_{\geq 0} \arrow[d, "f", "y \mapsto \sqrt{y}"'] \\
& \mathbb{R}
\end{tikzcd}$$

$\neq$

$f \circ g \neq \mathrm{id}_{\mathbb{R}}$

$$\begin{tikzcd}
\mathbb{R}_{\geq 0} \arrow[r, "f", "y \mapsto \sqrt{y}"'] \arrow[dr, "\mathrm{id}", "y \mapsto y"'] & \mathbb{R} \arrow[d, "g", "x \mapsto x^2"'] \\
& \mathbb{R}_{\geq 0}
\end{tikzcd}$$

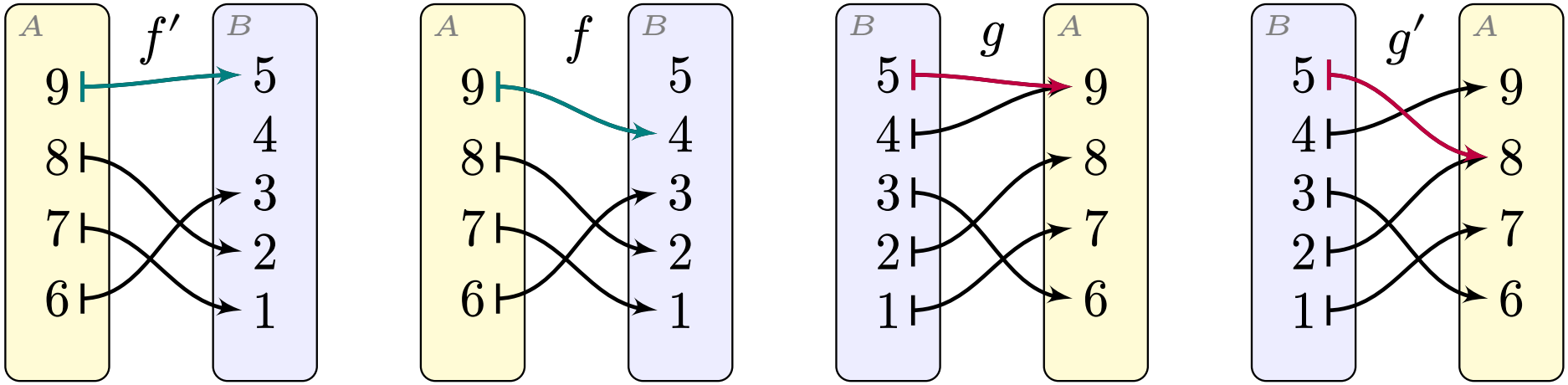
$=$

$g \circ f = \mathrm{id}_{\mathbb{R}_{\geq 0}}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Das Inverse ist eindeutig.



Satz B1D: Das Inverse ist eindeutig.

Wir nennen $g : B \to A$ **linksinvers** zu $f : A \to B$, falls $g \circ f = \mathrm{id}_A$ gilt.
Wir nennen $h : B \to A$ **rechtsinvers** zu $f : A \to B$, falls $f \circ h = \mathrm{id}_B$ gilt.

(1) Gilt beides, so folgt $g = h$, denn

$$g \overset{\text{rNtr}}{=} g \circ \mathrm{id}_B \overset{\text{rInv}}{=} g \circ (f \circ h) \overset{\text{Ass}}{=} (g \circ f) \circ h \overset{\text{lInv}}{=} \mathrm{id}_A \circ h \overset{\text{lNtr}}{=} h.$$

Wir nennen f und g dann **invers** zueinander, geschrieben $(f, g) : A \cong B$.

(2) Die Abbildung f heißt **invertierbar**, falls zu f eine Inverse g existiert.
Dank (1) ist g eindeutig durch f bestimmt, und wir schreiben $f^{-1} := g$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Rechenregeln für die Inversion: einfach und nützlich

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz B1E: Rechenregeln für Inverse

(R) Reflexivität: Wir haben $(\mathrm{id}_A, \mathrm{id}_A) : A \cong A$, also $\mathrm{id}_A^{-1} = \mathrm{id}_A$.

(S) Symmetrie: Aus $(f, g) : A \cong B$ folgt $(g, f) : B \cong A$, also $(f^{-1})^{-1} = f$.

(T) Transitivität: Aus $(f, f^{-1}) : A \cong B$ und $(g, g^{-1}) : B \cong C$ folgt dank Komposition $(g \circ f, f^{-1} \circ g^{-1}) : A \cong C$, also gilt $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Beweis: Aussagen (R) und (S) sind trivial. Für (T) genügt Nachrechnen:

$$\begin{aligned}
(f^{-1} \circ g^{-1}) \circ (g \circ f) &\overset{\text{Ass}}{=} ((f^{-1} \circ g^{-1}) \circ g) \circ f \overset{\text{Ass}}{=} (f^{-1} \circ (g^{-1} \circ g)) \circ f \\
&\overset{\text{Inv}}{=} (f^{-1} \circ \mathrm{id}_B) \circ f \overset{\text{Ntr}}{=} f^{-1} \circ f \overset{\text{Inv}}{=} \mathrm{id}_A \\
(g \circ f) \circ (f^{-1} \circ g^{-1}) &\overset{\text{Ass}}{=} ((g \circ f) \circ f^{-1}) \circ g^{-1} \overset{\text{Ass}}{=} (g \circ (f \circ f^{-1})) \circ g^{-1} \\
&\overset{\text{Inv}}{=} (g \circ \mathrm{id}_B) \circ g^{-1} \overset{\text{Ntr}}{=} g \circ g^{-1} \overset{\text{Inv}}{=} \mathrm{id}_C
\end{aligned}$$

Bijektiv vs invertierbar in der Kategorie Set.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz B1G: Bijektiv bedeutet invertierbar.

(0) Gilt $(f, g) : A \rightleftarrows B$ und $g \circ f = \mathrm{id}_A$, so ist f injektiv und g surjektiv.

(1) Genau dann ist eine Abbildung f invertierbar, wenn sie bijektiv ist. In diesem Falle ist die Umkehrabbildung $f^\top$ die beidseitige Inverse zu f.

Beweis:

(0a) f ist injektiv: Gilt $f(x) = f(\tilde{x})$, so folgt $x = g(f(x)) = g(f(\tilde{x})) = \tilde{x}$.

(0b) g ist surjektiv: Zu $x \in A$ sei $y = f(x)$; dann gilt $g(y) = g(f(x)) = x$.

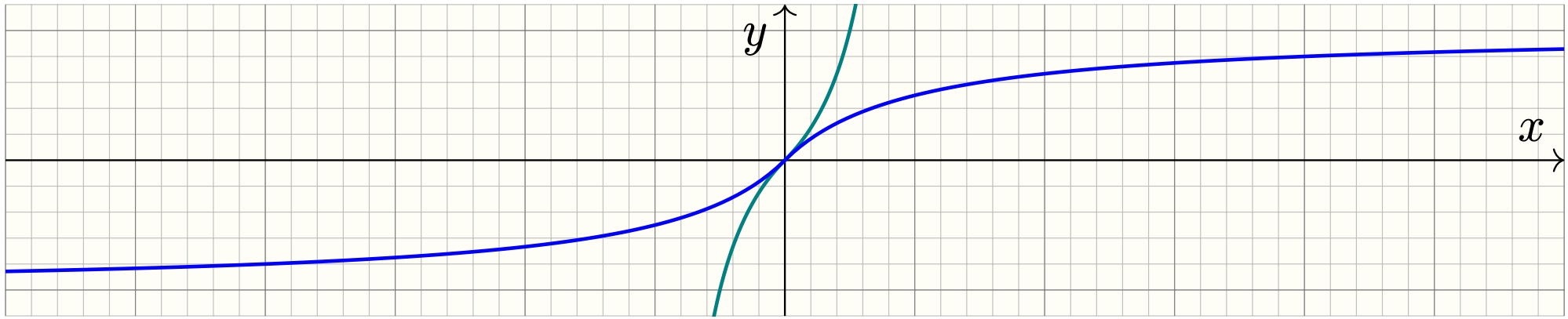
(1a) „$\Rightarrow$“: Ist $f : A \to B$ invertierbar, so existiert $g : B \to A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Demnach ist f injektiv dank (0a) und surjektiv dank (0b).

(1b) „$\Leftarrow$“: Ist f bijektiv, so ist die Umkehrung $g = f^\top$ eine Abbildung (B1A) und invers zu f.

Eine Bijektion zwischen reeller Gerade und offenem Intervall

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Aufgabe: Gibt es eine Bijektion $\mathbb{R} \cong \,]-1,1[$?

Beispiel B1H: reelle Gerade und offenes Intervall

Es gilt $\mathbb{R} \cong \,]-1,1[$, explizit $(f,g) : \mathbb{R} \cong \,]-1,1[$ vermöge der Abbildungen

$$f : \mathbb{R} \to \,]-1,1[\, : x \mapsto x/(1+|x|),$$
$$g : \,]-1,1[\, \to \mathbb{R} : y \mapsto y/(1-|y|).$$

Eine Bijektion zwischen reeller Gerade und offenem Intervall

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: Nachrechnen! (1) Die Abbildungen f und g sind wohldefiniert:
(1a) Für jedes $x \in \mathbb{R}$ gilt $|f(x)| = |x|/(1+|x|) < 1$, also $f(x) \in \,]-1,1[$.
(1b) Für jedes $y \in \,]-1,1[$ erfüllt der Nenner die Bedingung $1-|y| > 0$.

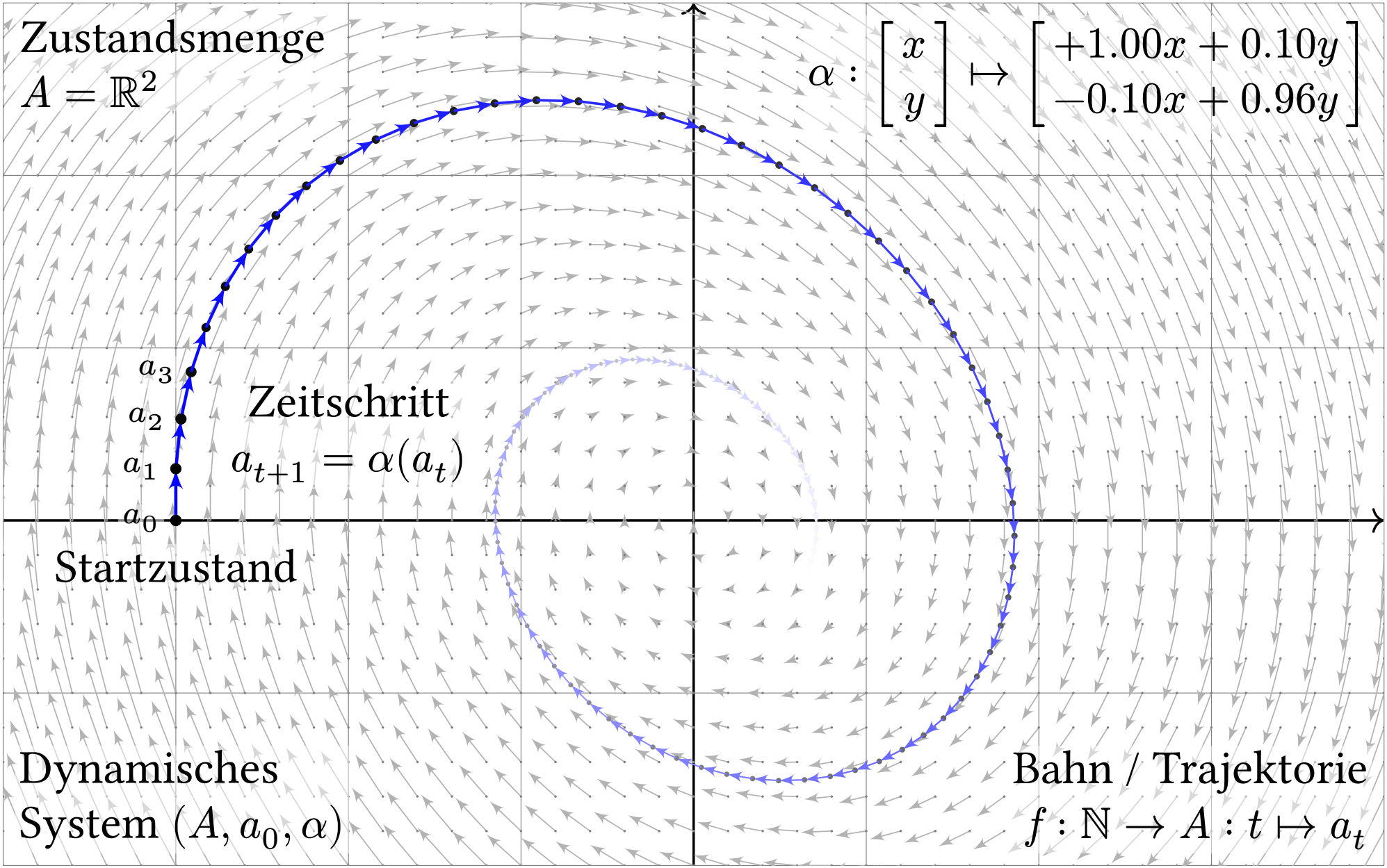
(2) Zudem sind sie invers zueinander, wie wir geduldig nachrechnen:

$$g(f(x)) \overset{\text{Def}}{=} \frac{x/(1+|x|)}{1-\big|x/(1+|x|)\big|} \overset{\mathbb{R}}{=} \frac{x}{1+|x|-|x|} \overset{\mathbb{R}}{=} x, \quad \text{also } g \circ f = \mathrm{id}_{\mathbb{R}}$$

$$f(g(y)) \overset{\text{Def}}{=} \frac{y/(1-|y|)}{1+\big|y/(1-|y|)\big|} \overset{\mathbb{R}}{=} \frac{y}{1-|y|+|y|} \overset{\mathbb{R}}{=} y, \quad \text{also } f \circ g = \mathrm{id}_{]-1,1[}$$

Damit haben wir die Behauptung $(f,g) : \mathbb{R} \cong \,]-1,1[$ bewiesen. $\boxed{\text{QED}}$

Anwendungsausblick: dynamische Systeme



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Grundlage aller Mathematik und Anwendung ist das Zahlensystem:

$$\begin{aligned}
\mathbb{N} &= \{0, 1, 2, 3, \dots\} \\
\mathbb{Z} &= \{a - b \mid a, b \in \mathbb{N}\} \\
\mathbb{Q} &= \{z/n \mid z, n \in \mathbb{Z},\ n \neq 0\} \\
\mathbb{R} &= \text{„}\mathbb{Q} \text{ und alle Grenzwerte“} \\
\mathbb{C} &= \{x + \mathrm{i}y \mid x, y \in \mathbb{R}\},\ \ \mathrm{i}^2 = -1
\end{aligned}$$

L Lea, die lernbegeisterte Lehrer:in: „Wie kann ich das selbst *verstehen* und anderen *vermitteln*, mathematisch korrekt und didaktisch geschickt?“

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

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

M Mia, die methodische Mathematiker:in: „Wie kann ich diese Objekte *definieren* und *konstruieren*, ihre Rechenregeln *formulieren* und *beweisen*?“

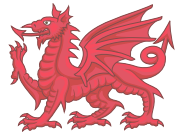
Was sind die natürlichen Zahlen $0, 1, 2, 3, \ldots$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Was bedeutet Zählen?

$$0 \xmapsto{s} 1 \xmapsto{s} 2 \xmapsto{s} 3 \xmapsto{s} 4 \xmapsto{s} 5 \xmapsto{s} \ldots ???$$



Here be Dragons

Durchaus möglich, aber hier unerwünscht:

$$0 \longmapsto 1 \longmapsto 2 \longmapsto 3 \longmapsto 4 \longmapsto 5 \longmapsto \ldots$$

¬D0

$$0 \longmapsto 1 \longmapsto 2 \longmapsto 3 \longmapsto 4 \longmapsto 5 \longmapsto \ldots$$

¬D1

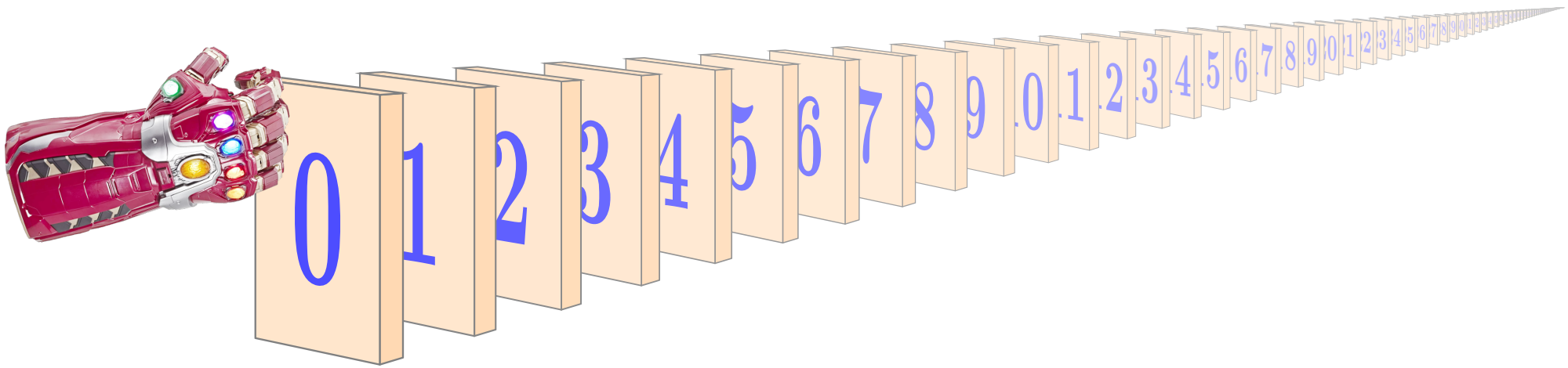
$$\begin{array}{l} 0 \longmapsto 1 \longmapsto 2 \longmapsto 3 \longmapsto 4 \longmapsto \ldots \\ \omega \longmapsto \omega{+}1 \mapsto \omega{+}2 \mapsto \omega{+}3 \mapsto \omega{+}4 \mapsto \ldots \end{array} \qquad \infty$$

¬D2

Die Dedekind–Peano–Axiome für natürliche Zahlen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Definition B2A: Axiome der natürlichen Zahlen

Ein **Zählsystem** $(N,\ 0 \in N,\ \nu : N \to N)$ erfüllt:

D0: Die Null ist kein Nachfolger: $0 \notin \nu(N)$

D1: Die Abbildung ν ist injektiv: $\forall p, q \in N : p \neq q \Rightarrow \nu(p) \neq \nu(q)$

D2: Vollständige Induktion: $\forall E \subseteq N : 0 \in E \wedge \nu(E) \subseteq E \Rightarrow E = N$

Modelle der natürlichen Zahlen

$$\text{null} \mapsto | \mapsto || \mapsto ||| \mapsto |||| \mapsto ||||| \mapsto |||||| \mapsto ||||||| \mapsto |||||||| \mapsto \ldots$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Modelle der natürlichen Zahlen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Binärsystem:

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

Dezimalsystem:

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

Ein Universalwerkzeug: Dedekinds Rekursionssatz

$$\begin{tikzcd}
\{0\} \arrow[r, hook, "\mathrm{inc}"] \arrow[d, "f"] & N \arrow[r, "\nu"] \arrow[d, "f"] & N \arrow[d, "f"] \\
\{a_0\} \arrow[r, hook, "\mathrm{inc}"] & A \arrow[r, "\alpha"] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
0 \arrow[r, mapsto, "\nu"] \arrow[d, mapsto, "f"] & 1 \arrow[r, mapsto, "\nu"] \arrow[d, mapsto, "f"] & 2 \arrow[r, mapsto, "\nu"] \arrow[d, mapsto, "f"] & 3 \arrow[r, mapsto, "\nu"] \arrow[d, mapsto, "f"] & \dots \\
a_0 \arrow[r, mapsto, "\alpha"] & a_1 \arrow[r, mapsto, "\alpha"] & a_2 \arrow[r, mapsto, "\alpha"] & a_3 \arrow[r, mapsto, "\alpha"] & \dots
\end{tikzcd}$$

$n+1 \mapsto a_{n+1}$
$= \alpha(a_n)$

Satz B2B: Rekursion „$a_{n+1} = \alpha(a_n)$“, Dedekind 1888

Sei $(A,\ a_0 \in A,\ \alpha : A \to A)$ ein dynamisches System.

Sei $(N,\ 0 \in N,\ \nu : N \to N)$ ein Zählsystem.

Dann existiert genau eine Abbildung $f : N \to A$ als **rekursive Folge** mit Startwert $f(0) = a_0$ und der Rekursionsgleichung $f \circ \nu = \alpha \circ f$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Einzigkeit der natürlichen Zahlen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd}
\{0\} \arrow[r, hook, "\mathrm{inc}"] \arrow[d, shift right, "f"'] & N \arrow[r, "\nu"] \arrow[d, shift right, "f"'] & N \arrow[d, shift right, "f"'] \\
\{0'\} \arrow[r, hook, "\mathrm{inc}"] \arrow[u, shift right, "f'"'] \arrow[ur, phantom, "\cong"] & N' \arrow[r, "\nu'"] \arrow[u, shift right, "f'"'] \arrow[ur, phantom, "\cong"] & N' \arrow[u, shift right, "f'"'] \arrow[ur, phantom, "\cong"]
\end{tikzcd}$$

Korollar B2c: Einzigkeit der natürlichen Zahlen

Zu je zwei Modellen $(N, 0, \nu)$ und $(N', 0', \nu')$ der natürlichen Zahlen existiert genau ein Isomorphismus $(f, f') : (N, 0, \nu) \cong (N', 0', \nu')$.

Wir fixieren fortan ein Standardmodell $(\mathbb{N}, 0, s)$.

Die Addition $(a,b) \mapsto a+b$ natürlicher Zahlen $a,b \in \mathbb{N}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$+$	$0 \mapsto$	$1 \mapsto$	$2 \mapsto$	$3 \mapsto$	$4 \mapsto$	$5 \mapsto$	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$\ldots \mapsto$
0	$0 \mapsto$	$1 \mapsto$	$2 \mapsto$	$3 \mapsto$	$4 \mapsto$	$5 \mapsto$	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$\ldots \mapsto$
1	$1 \mapsto$	$2 \mapsto$	$3 \mapsto$	$4 \mapsto$	$5 \mapsto$	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$10 \mapsto$	$\ldots \mapsto$
2	$2 \mapsto$	$3 \mapsto$	$4 \mapsto$	$5 \mapsto$	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$10 \mapsto$	$11 \mapsto$	$\ldots \mapsto$
3	$3 \mapsto$	$4 \mapsto$	$5 \mapsto$	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$10 \mapsto$	$11 \mapsto$	$12 \mapsto$	$\ldots \mapsto$
4	$4 \mapsto$	$5 \mapsto$	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$10 \mapsto$	$11 \mapsto$	$12 \mapsto$	$13 \mapsto$	$\ldots \mapsto$
5	$5 \mapsto$	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$10 \mapsto$	$11 \mapsto$	$12 \mapsto$	$13 \mapsto$	$14 \mapsto$	$\ldots \mapsto$
6	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$10 \mapsto$	$11 \mapsto$	$12 \mapsto$	$13 \mapsto$	$14 \mapsto$	$15 \mapsto$	$\ldots \mapsto$
7	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$10 \mapsto$	$11 \mapsto$	$12 \mapsto$	$13 \mapsto$	$14 \mapsto$	$15 \mapsto$	$16 \mapsto$	$\ldots \mapsto$
8	$8 \mapsto$	$9 \mapsto$	$10 \mapsto$	$11 \mapsto$	$12 \mapsto$	$13 \mapsto$	$14 \mapsto$	$15 \mapsto$	$16 \mapsto$	$17 \mapsto$	$\ldots \mapsto$
9	$9 \mapsto$	$10 \mapsto$	$11 \mapsto$	$12 \mapsto$	$13 \mapsto$	$14 \mapsto$	$15 \mapsto$	$16 \mapsto$	$17 \mapsto$	$18 \mapsto$	$\ldots \mapsto$
$\vdots$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\ddots \mapsto$

Dies ist eine unendliche Tabelle!

? Wie konstruieren wir die Addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$? Wir definieren die linke Spalte $a + 0 := a$ und rekursiv jede weitere $a + s(n) := s(a+n)$.

Die Multiplikation $(a, b) \mapsto a \cdot b$ natürlicher Zahlen $a, b \in \mathbb{N}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

Dies ist eine unendliche Tabelle!

? Wie konstruieren wir die Multiplikation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$? Wir definieren die linke Spalte $a \cdot 0 := 0$ und rekursiv jede weitere $a \cdot s(n) := (a \cdot n) + a$.

Die Potenzierung $(a, b) \mapsto a^b$ natürlicher Zahlen $a, b \in \mathbb{N}$

$\hat{}$	$0 \mapsto$	$1 \mapsto$	$2 \mapsto$	$3 \mapsto$	$4 \mapsto$	$5 \mapsto$	$6 \mapsto$	$7 \mapsto$	$8 \mapsto$	$9 \mapsto$	$\ldots \mapsto$
0	$1 \mapsto$	$0 \mapsto$	$0 \mapsto$	$0 \mapsto$	$0 \mapsto$	$0 \mapsto$	$0 \mapsto$	$0 \mapsto$	$0 \mapsto$	$0 \mapsto$	$\ldots \mapsto$
1	$1 \mapsto$	$1 \mapsto$	$1 \mapsto$	$1 \mapsto$	$1 \mapsto$	$1 \mapsto$	$1 \mapsto$	$1 \mapsto$	$1 \mapsto$	$1 \mapsto$	$\ldots \mapsto$
2	$1 \mapsto$	$2 \mapsto$	$4 \mapsto$	$8 \mapsto$	$16 \mapsto$	$32 \mapsto$	$64 \mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\ldots \mapsto$
3	$1 \mapsto$	$3 \mapsto$	$9 \mapsto$	$27 \mapsto$	$81 \mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\ldots \mapsto$
4	$1 \mapsto$	$4 \mapsto$	$16 \mapsto$	$64 \mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\ldots \mapsto$
5	$1 \mapsto$	$5 \mapsto$	$25 \mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\ldots \mapsto$
6	$1 \mapsto$	$6 \mapsto$	$36 \mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\ldots \mapsto$
7	$1 \mapsto$	$7 \mapsto$	$49 \mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\ldots \mapsto$
8	$1 \mapsto$	$8 \mapsto$	$64 \mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\ldots \mapsto$
9	$1 \mapsto$	$9 \mapsto$	$81 \mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\mapsto$	$\ldots \mapsto$
$\vdots$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\vdots \mapsto$	$\ddots \mapsto$

Dies ist eine unendliche Tabelle!

? Wie konstruieren wir die Potenzierung $\hat{} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$? Wir definieren die linke Spalte $a^0 := 1$ und dann rekursiv jede weitere $a^{s(n)} := (a^n) \cdot a$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Rechenregeln für die natürlichen Zahlen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

Assoziativität, **Ass**$(\mathbb{N}, +)$: $(a + b) + c = a + (b + c)$

Neutralität, **Ntr**$(\mathbb{N}, +, 0)$: $0 + a = a$ und $a + 0 = a$

Wir sagen dazu kurz: $(\mathbb{N}, +, 0)$ ist ein **Monoid**. Es ist zudem kommutativ:

Kommutativität, **Com**$(\mathbb{N}, +)$: $a + b = b + a$

Die Multiplikation erfreut sich der selben drei Eigenschaften:

Assoziativität, **Ass**$(\mathbb{N}, \cdot)$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Neutralität, **Ntr**$(\mathbb{N}, \cdot, 1)$: $1 \cdot a = a$ und $a \cdot 1 = a$

Wir sagen dazu kurz: $(\mathbb{N}, \cdot, 1)$ ist ein **Monoid**. Es ist zudem kommutativ:

Kommutativität, **Com**$(\mathbb{N}, \cdot)$: $a \cdot b = b \cdot a$

Die Multiplikation ist **distributiv** über die Addition:

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

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

Wir sagen kurz: $(\mathbb{N}, +, 0, \cdot, 1)$ ist ein **kommutativer Halbring**.

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

Beweise Induktion

Satz B2E: grundlegende Rechenregeln für die natürlichen Zahlen

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

(1) Die Addition ist kürzbar, das heißt aus $a + b = a + c$ folgt $b = c$.
Wir schreiben wir $a \leq b$ in $\mathbb{N}$, falls ein $a' \in \mathbb{N}$ existiert mit $a + a' = b$.
Dank Kürzbarkeit ist a' eindeutig, und wir schreiben $a' =: b - a$.

(2) Die Multiplikation ist kürzbar: Aus $a \cdot b = a \cdot c$ und $a \neq 0$ folgt $b = c$.
Wir schreiben $a \mid b$ in $\mathbb{N}$, falls ein $a' \in \mathbb{N}$ existiert mit $a \cdot a' = b$.
Im Falle $a \neq 0$ ist a' eindeutig, und wir schreiben $a' =: b/a$.

(3) Es gilt $a^{m+n} = a^m \cdot a^n$ und $a^{m \cdot n} = (a^m)^n$ und $(a \cdot b)^n = a^n \cdot b^n$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Nachweis der Rechenregeln durch vollständige Induktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(0a) Zur Assoziativität **Ass**$(\mathbb{N}, +)$ betrachten wir die Erfüllungsmenge

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

Induktionsanfang: Gilt $0 \in E$? Ja, denn

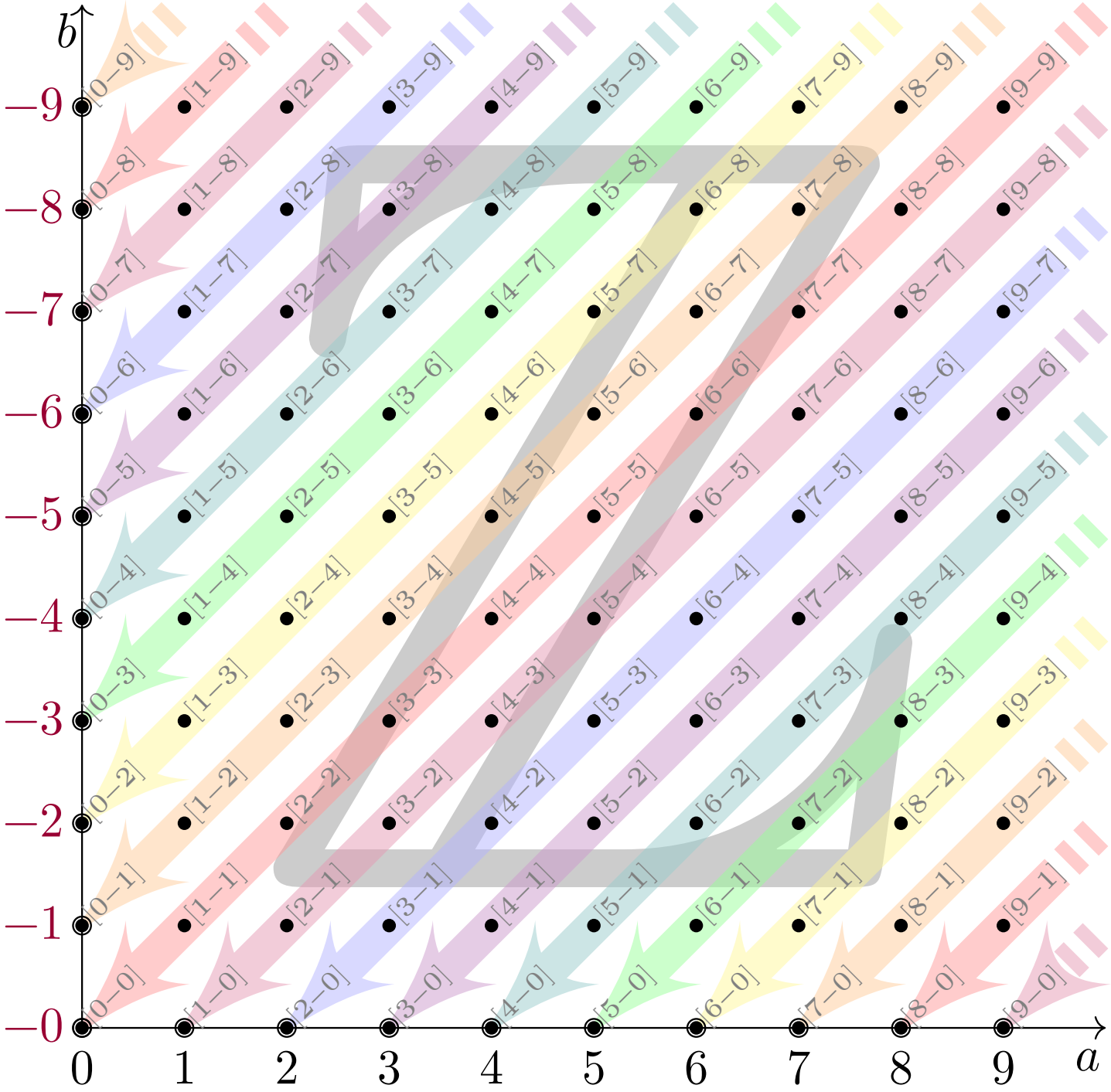
$$a + (b + 0) \overset{\text{Def}}{=} a + b \overset{\text{Def}}{=} (a + b) + 0.$$

Induktionsschritt: Folgt aus $n \in E$ stets $s(n) \in E$? Ja, 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 Induktionsaxiom D2 folgt $E = \mathbb{N}$. Die Addition ist also assoziativ.

Konstruktion der ganzen Zahlen $[a-b] \in \mathbb{Z}$



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

In $\mathbb{N}$ können wir Gleichungen wie $3 = 5 + x$ aufstellen, aber nicht lösen.
In $\mathbb{Z} \supseteq \mathbb{N}$ hingegen finden wir $x = [3-5] = [2-4] = \ldots = [0-2] = -2$.

Wunsch: Wir erweitern die natürlichen Zahlen $\mathbb{N}$ zu den ganzen Zahlen

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

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: neu	$-[a-b]$	$=$	$[b-a]$
Produkt:	$[a-b] \cdot [c-d]$	$=$	$[(ac+bd) - (ad+bc)]$

Ergebnis: Nach diesen Wünschen gelingt die Konstruktion von $\mathbb{Z}$.

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

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Addition erfreut sich nun folgender Eigenschaften für alle $a, b, c \in K$:

Assoziativität,	**Ass**$(K, +)$:	$(a + b) + c = a + (b + c)$
Neutralität,	**Ntr**$(K, +, 0)$:	$0 + a = a$ und $a + 0 = a$
Negation, neu	**Inv**$(K, +, 0, -)$:	$(-a) + a = 0$ und $a + (-a) = 0$

Wir sagen dazu: $(K, +, 0, -)$ ist eine **Gruppe**. Sie ist zudem kommutativ:

Kommutativität,	**Com**$(K, +)$:	$a + b = b + a$

Die Multiplikation distribuiert über die Addition gemäß **DL** und **DR**.

Die Multiplikation erfreut sich weiterhin folgender Eigenschaften:

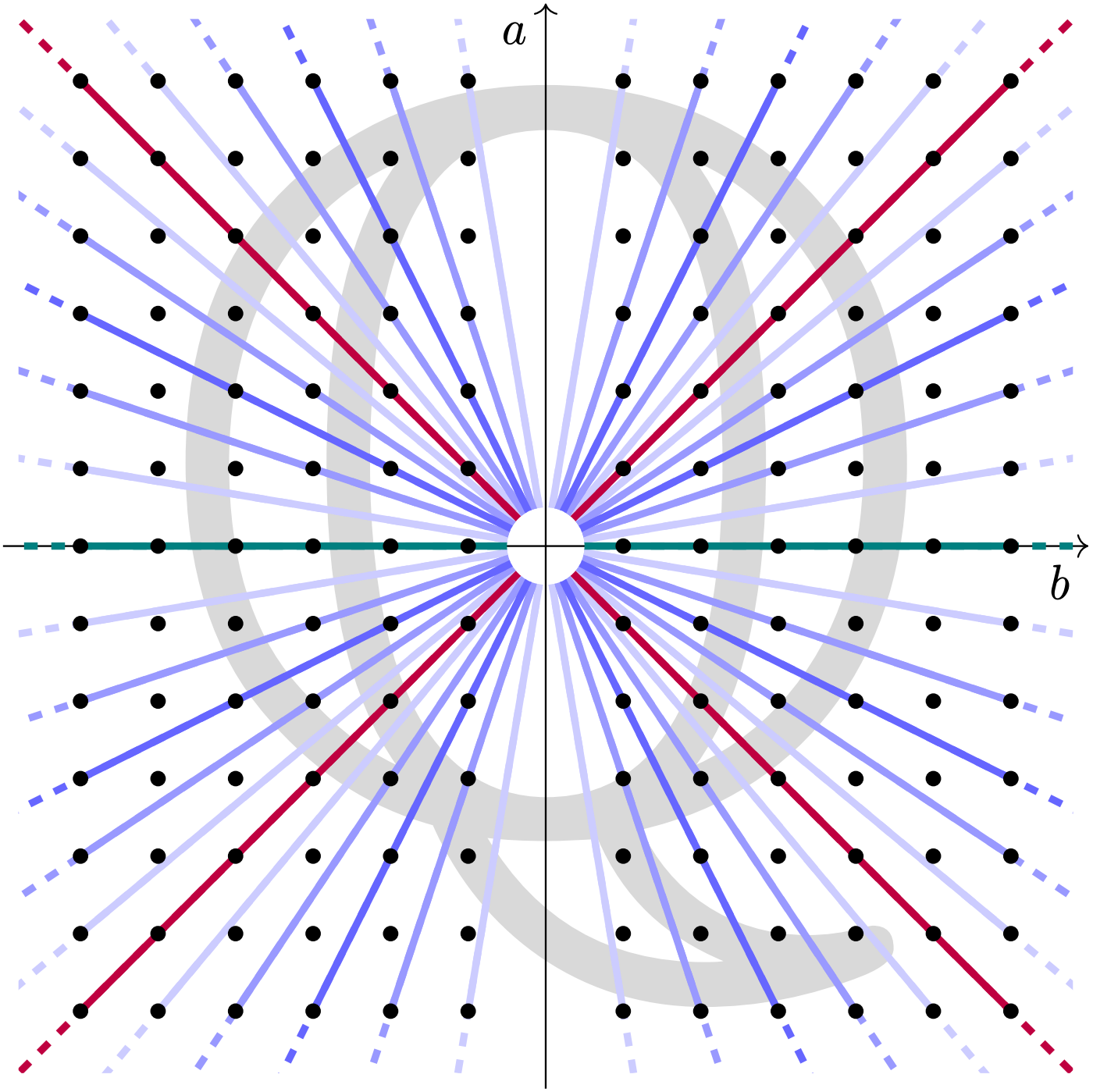
Assoziativität,	**Ass**$(K, \cdot)$:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Neutralität,	**Ntr**$(K, \cdot, 1)$:	$1 \cdot a = a$ und $a \cdot 1 = a$

Wir sagen dazu kurz: $(K, \cdot, 1)$ ist ein **Monoid**. Es ist zudem kommutativ:

Kommutativität,	**Com**$(K, \cdot)$:	$a \cdot b = b \cdot a$

Wir sagen kurz: $(K, +, 0, -, \cdot, 1)$ ist ein **kommutativer Ring** / CRing.

Konstruktion der rationalen Zahlen $[a/b] \in \mathbb{Q}$



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

In $\mathbb{Z}$ können wir Gleichungen wie $3 = 6 \cdot x$ formulieren, aber nicht lösen.
In $\mathbb{Q} \supseteq \mathbb{Z}$ hingegen finden wir $x = [3/6] = [2/4] = \ldots = [1/2] = 2^{-1}$.

Wunsch: Wir erweitern die ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen

$$\mathbb{Q} = \left\{ q = [a/b] \,\middle|\, a, b \in \mathbb{Z},\ b \neq 0 \right\}.$$

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

Ergebnis: Nach diesen Wünschen gelingt die Konstruktion von $\mathbb{Q}$.

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

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Addition erfreut sich folgender Eigenschaften für alle $a, b, c \in K$:

Assoziativität, **Ass**$(K, +)$: $(a + b) + c = a + (b + c)$

Neutralität, **Ntr**$(K, +, 0)$: $0 + a = a$ und $a + 0 = a$

Negatives, **Inv**$(K, +, 0, -)$: $(-a) + a = 0$ und $a + (-a) = 0$

Wir sagen dazu: $(K, +, 0, -)$ ist eine **Gruppe**. Sie ist zudem kommutativ:

Kommutativität, **Com**$(K, +)$: $a + b = b + a$

Die Multiplikation distribuiert über die Addition gemäß **DL** und **DR**.

Die Multiplikation erfreut sich nun folgender Eigenschaften:

Assoziativität, **Ass**$(K, \cdot)$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Neutralität, **Ntr**$(K, \cdot, 1)$: $1 \cdot a = a$ und $a \cdot 1 = a$

Inverses, neu **Inv**$(K^*, \cdot, 1, ^{-1})$: $a \cdot a^{-1} = 1$ und $a^{-1} \cdot a = 1$

Vorsicht, Letzteres gilt nur für $a \neq 0$, also für alle $a \in K^* := K \setminus \{0\}$.

Wir sagen zusammenfassend: $(K^*, \cdot, 1, ^{-1})$ ist eine **Gruppe**. Zudem gilt:

Kommutativität, **Com**$(K, \cdot)$: $a \cdot b = b \cdot a$

Wir sagen dazu zusammenfassend: $(K, +, 0, -, \cdot, 1, ^{-1})$ ist ein **Körper**.

Die vier Grundrechenarten und ihre Rechenregeln

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition B2H: Ringe und Körper

Wir nennen $(K, +, 0, -, \cdot, 1, ^{-1})$ einen **Körper**, falls $0 \neq 1$ gilt sowie alle zehn der obigen Rechenregeln.

Struktur $(K, +, 0, \cdot, 1)$		$(K, +, 0)$				$(K, +, \cdot)$		$(K, \cdot, 1)$			
Name	Beispiele	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	Inv*	Com
Körper	$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DRing	$\mathbb{H} \subseteq \mathbb{C}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	
CRing	$\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}[X]$	✓	✓	✓	✓	✓	✓	✓	✓		✓
Ring	$\mathbb{Z}^{2\times 2}, \mathbb{R}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓		

Die vier Grundrechenarten und ihre Rechenregeln

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Triviales Beispiel: $(\{0\}, +, 0, \cdot, 1)$ ist ein Ring, mit $0 = 1$.

Sei $(K, +, 0, \cdot, 1)$ ein Ring mit $0 \neq 1$. Wir setzen $K^* := K \setminus \{0\}$ und

$$K^\times := \left\{ a \in K \,\middle|\, \exists a' \in K : aa' = a'a = 1 \right\} \subseteq K^*.$$

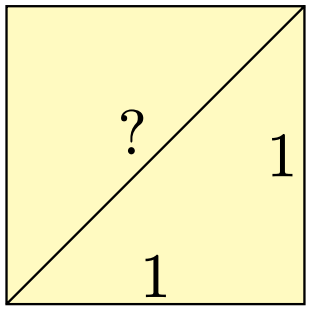
Beispiel: Für jeden Körper K gilt $K^\times = K^*$, hingegen $\mathbb{Z}^\times = \{\pm 1\} \subsetneq \mathbb{Z}^*$.

Zwar ist $K = \mathbb{Z}$ kein Körper, doch nullteilerfrei; für alle $a, b \in K$ gilt:

$$\text{Nullprodukt} \quad ab = 0 \quad \Leftrightarrow \quad a = 0 \lor b = 0$$

Ein **Integritätsring**, kurz IRing, ist ein CRing mit $0 \neq 1$ und nullteilerfrei.

Die rationalen Zahlen haben erhebliche Lücken!



Satz B2L: Irrationalität von $\sqrt{2}$, Euklid ca. 300 v.u.Z.

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 $r = p/q$ mit $p, q \in \mathbb{Z}$ und $q \neq 0$. Zudem sei p/q vollständig gekürzt.

Aus der Gleichung $(p/q)^2 = 2$ folgt $p^2 = 2q^2$.
Daher ist p^2 gerade, also $p = 2\overline{p}$ mit $\overline{p} \in \mathbb{Z}$.

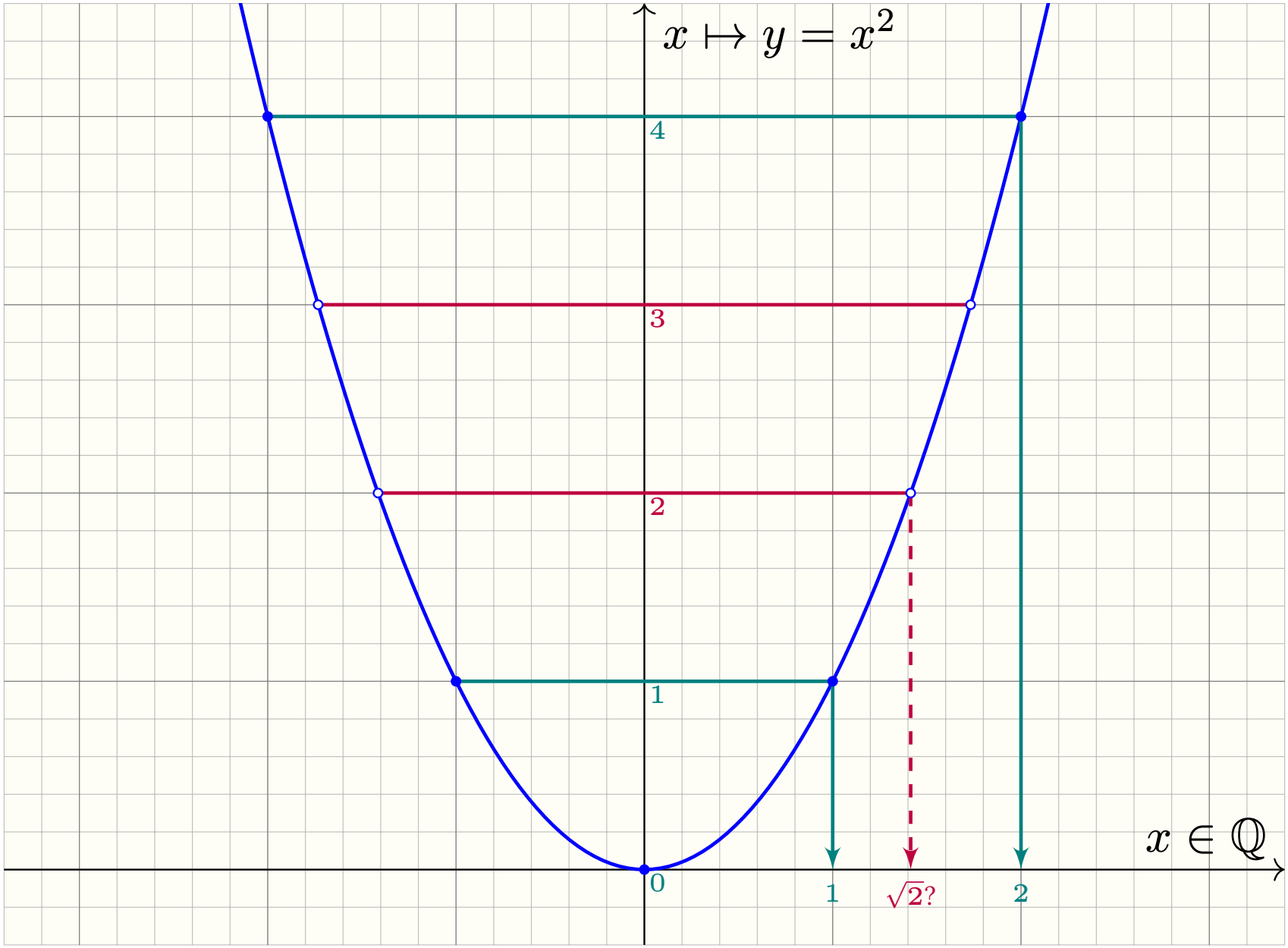
Einsetzen ergibt $4\overline{p}^2 = 2q^2$, also $2\overline{p}^2 = q^2$.
Daher ist q^2 gerade, also $q = 2\overline{q}$ mit $\overline{q} \in \mathbb{Z}$.

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

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die rationalen Zahlen haben erhebliche Lücken!



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wunsch: Wir wollen $\mathbb{K} = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ durch $\sqrt{\alpha}$ erweitern, etwa $\alpha = 2$, zu

$$\mathbb{K}[\sqrt{\alpha}] = \left\{ z = x + y\sqrt{\alpha} \,\middle|\, x, y \in \mathbb{K} \right\}^{!}.$$

$$\begin{aligned}
\text{Addition:} \quad (x + y\sqrt{\alpha}) + (x' + y'\sqrt{\alpha}) &= (x + x') + (y + y')\sqrt{\alpha} \\
\text{Produkt:} \quad (x + y\sqrt{\alpha}) \cdot (x' + y'\sqrt{\alpha}) &= (xx' + \alpha yy') + (xy' + yx')\sqrt{\alpha}
\end{aligned}$$

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

Ergebnis: Nach diesen Wünschen gelingt die Konstruktion von $\mathbb{K}[\sqrt{\alpha}]$.

Kurzschreibweise für Σummen und Πrodukte

$$\sum_{i=k}^{\ell} a_i := \begin{cases} a_k + a_{k+1} + \cdots + a_\ell & \text{falls } k \leq \ell \text{ in } \mathbb{Z}, \\ 0 \quad \text{(leere Summe)} & \text{falls } \ell < k \text{ in } \mathbb{Z}. \end{cases}$$

$$\prod_{i=k}^{\ell} a_i := \begin{cases} a_k \cdot a_{k+1} \cdot \cdots \cdot a_\ell & \text{falls } k \leq \ell \text{ in } \mathbb{Z}, \\ 1 \quad \text{(leeres Produkt)} & \text{falls } \ell < k \text{ in } \mathbb{Z}. \end{cases}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kurzschreibweise für Σummen und Πrodukte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$a \cdot n := \sum_{i=1}^{n} a$$

$$a^n \quad := \prod_{i=1}^{n} a$$

Ist $-a$ das Negative zu a, so definieren wir $a \cdot (-n) := (-a) \cdot n$.
Ist a^{-1} das Inverse zu a, so definieren wir $a^{-n} := (a^{-1})^n$.

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

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

Sei J eine beliebige Menge, $I \subseteq J$ endlich mit $a_j = 0$ für alle $j \in J \setminus I$.
Dann definieren wir $\sum_{j \in J} a_j := \sum_{i \in I} a_i$.

Arithmetik ganzer Zahlen: Division mit Rest

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Teile 372 durch 25, ganzzahlig! $372 = 25 \cdot q + r = 25 \cdot 14 + 22$

Satz B3A: euklidische Division / ganzzahlige Division mit Rest

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

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

Dies definiert $q =: a \operatorname{quo} b$ und $r =: a \operatorname{rem} b$.

Arithmetik ganzer Zahlen: Zifferndarstellung in Basis B

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Dezimal schreiben wir $1729 = 1 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10^1 + 9 \cdot 10^0$.

Satz B3B: Zifferndarstellung in Basis B

Wir fixieren $B \in \mathbb{N}_{\geq 2}$, etwa $B = 2$ (binär) oder $B = 10$ (dezimal).
Jede natürliche Zahl $n \in \mathbb{N}$ schreibt sich eindeutig in Basis B gemäß

$$n = n_{\ell-1} B^{\ell-1} + n_{\ell-2} B^{\ell-2} + \cdots + n_2 B^2 + n_1 B + n_0 = \sum_{k=0}^{\ell-1} n_k B^k$$

mit Länge $\ell \in \mathbb{N}$ und Ziffern $n_i \in \mathbb{Z}_B = \{0, 1, \ldots, B-1\}$, wobei $n_{\ell-1} \neq 0$.

Teilbarkeit in ganzen Zahlen und ggT

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\mathrm{GT}_{\mathbb{Z}}(18,24) = \{\pm 1, \pm 2, \pm 3, \pm 6\},\ \mathrm{GGT}_{\mathbb{Z}}(18,24) = \{\pm 6\},\ \mathrm{ggT}_{\mathbb{Z}}(18,24) = 6.$$

Definition B3c: größter gemeinsamer Teiler im Ring $\mathbb{Z}$

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

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

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

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

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

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

Der euklidische Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Bemerkung: Für alle $a, b, c \in \mathbb{Z}$ gilt $\mathrm{GT}(a, b) = \mathrm{GT}(b, a) \overset{!}{=} \mathrm{GT}(b, a - bc)$.
„$\subseteq$“: Aus $ta' = a$ und $tb' = b$ folgt $t(a' - b'c) = a - bc$. „$\supseteq$“: Ebenso mit $-c$.

$$\mathrm{GT}\begin{bmatrix}102\\78\end{bmatrix} = \mathrm{GT}\begin{bmatrix}78\\24\end{bmatrix} = \mathrm{GT}\begin{bmatrix}24\\6\end{bmatrix} = \mathrm{GT}\begin{bmatrix}6\\0\end{bmatrix} = \left\{\begin{smallmatrix}\pm 6\\ \pm 3\\ \pm 2\\ \pm 1\end{smallmatrix}\right\} \Longrightarrow \mathrm{ggT}\begin{bmatrix}102\\78\end{bmatrix} = 6$$

Algo B3D: euklidischer Algorithmus zur Berechnung des ggT

Eingabe: $a_0, b_0 \in \mathbb{Z}$
Ausgabe: $\mathrm{ggT}(a_0, b_0)$

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

Satz B3D: Euklid im Ring $\mathbb{Z}$

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

Bézout und der erweiterte euklidische Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz B3E: Bézout im Ring $\mathbb{Z}$

(1) Zu je zwei Zahlen $a, b \in \mathbb{Z}$ existieren $u, v \in \mathbb{Z}$ mit $\operatorname{ggT}(a, b) = au + bv$.

Algo B3E: Berechnung des ggT mit Bézout–Koeffizienten

Eingabe: $a_0, b_0 \in \mathbb{Z}$

Ausgabe: $a, u, v \in \mathbb{Z}$ mit $\operatorname{ggT}(a_0, b_0) = a = a_0 u + b_0 v$

1: $\begin{bmatrix} a & u & v \\ b & s & t \end{bmatrix} \leftarrow \begin{bmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \end{bmatrix}$ // Invariante: Es gilt $\left\{ \begin{matrix} a = a_0 u + b_0 v, \\ b = a_0 s + b_0 t. \end{matrix} \right.$

2: while $b \neq 0$ do $q \leftarrow a \operatorname{quo} b$ // euklidische Division $a = qb + r$

3: $\begin{bmatrix} a & u & v \\ b & s & t \end{bmatrix} \leftarrow \begin{bmatrix} b & s & t \\ a-qb & u-qs & v-qt \end{bmatrix}$ // Invariante: Es gilt $\left\{ \begin{matrix} a = a_0 u + b_0 v, \\ b = a_0 s + b_0 t. \end{matrix} \right.$

4: return $(a, u, v) \cdot \operatorname{sign}(a)$ // $\operatorname{ggT}(a_0, b_0) = a = a_0 u + b_0 v$

Bézout und der erweiterte euklidische Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

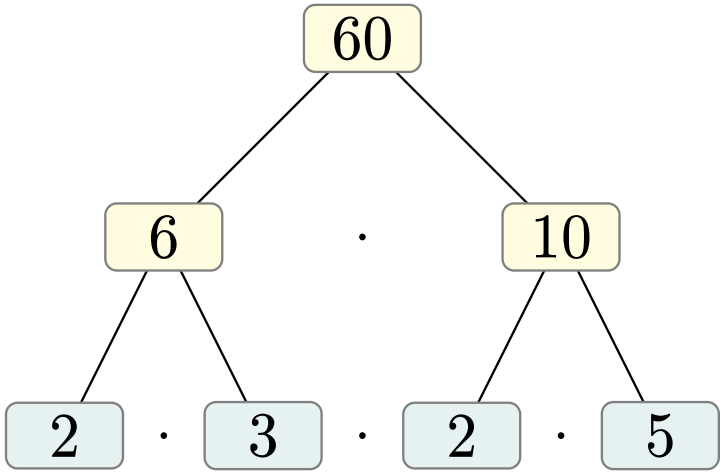
Ausführliche Erläuterungen bietet die Vollversion.

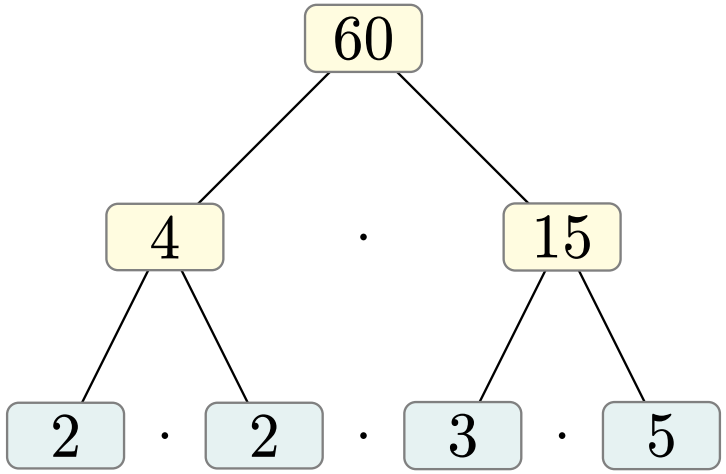
Zahlenbeispiel: Für $a_0 = 102$ und $b_0 = 78$ erhalten wir:

init		102	1	0	Invariante:	$102 = 1\,a_0 + 0\,b_0$
init		78	0	1	Invariante:	$78 = 0\,a_0 + 1\,b_0$
$q = 1$	$\Rightarrow$	24	1	-1	Invariante:	$24 = 1\,a_0 - 1\,b_0$
$q = 3$	$\Rightarrow$	6	-3	4	Invariante:	$6 = -3\,a_0 + 4\,b_0$
$q = 4$	$\Rightarrow$	0	13	-17	Invariante:	$0 = 13\,a_0 - 17\,b_0$

So finden wir $\mathrm{ggT}(a_0, b_0) = 6 = a_0 u + b_0 v$ mit $u = -3$ und $v = 4$.

Was bedeutet Primzerlegung? Existenz? Eindeutigkeit?





Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Prim vs unzerlegbar in $\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition B3F: prim vs unzerlegbar im Ring $(\mathbb{Z}, +, \cdot)$

(1) Wir nennen $a \in \mathbb{Z} \setminus (\{0\} \cup \mathbb{Z}^\times)$ **unzerlegbar**, falls für alle $b, c \in \mathbb{Z}$ gilt:
Aus $a = b \cdot c$ folgt entweder $b \in \mathbb{Z}^\times$ oder $c \in \mathbb{Z}^\times$.

(2) Wir nennen $a \in \mathbb{Z} \setminus (\{0\} \cup \mathbb{Z}^\times)$ **prim**, falls für alle $b, c \in \mathbb{Z}$ gilt:
Aus $a \mid b \cdot c$ folgt $a \mid b$ oder $a \mid c$.

Beispiele: (1) In $\mathbb{Z}$ unzerlegbar sind $\ldots, -3, -2, 2, 3, 5, 7, 11, 13, 17, 19, \ldots$.
In $\mathbb{Z}$ zerlegbar sind $\ldots -6, -4, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, \ldots$.

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

Prim vs unzerlegbar: erste Gegenbeispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel B3G: löchrige Zahlen – unzerlegbar, aber nicht prim

$$\mathbb{N} = \{1, \mathbf{2}, \mathbf{3}, 4, \mathbf{5}, 6, \mathbf{7}, 8, 9, 10, \mathbf{11}, 12, \mathbf{13}, 14, 15, \dots\}$$

$$L = \{1, \mathbf{2}, \cancel{3}, 4, \mathbf{5}, \mathbf{6}, \mathbf{7}, 8, \mathbf{9}, 10, \mathbf{11}, 12, \mathbf{13}, 14, \mathbf{15}, \dots\}$$

Ist 6 in $(L, \cdot)$ immer noch zerlegbar? Nein, in $(L, \cdot)$ ist 6 unzerlegbar!
Ist 6 in $(L, \cdot)$ nun prim? Nein, weiterhin gilt $6 \mid 4 \cdot 9$, aber $6 \nmid 4$ und $6 \nmid 9$.
In $(L, \cdot)$ sind $6 \cdot 6 = 36 = 2 \cdot 2 \cdot 9$ zwei Produkte unzerlegbarer Faktoren, ebenso $2 \cdot 5 \cdot 6 = 60 = 2 \cdot 2 \cdot 15$. Eindeutigkeit gilt hier also nicht mehr!

Das Lemma von Euklid: In $\mathbb{Z}$ gilt prim = unzerlegbar.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma B31: Lemma von Euklid

(1) Seien $a, b, c \in \mathbb{Z}$ mit $a \mid bc$. Aus $\operatorname{ggT}(a, b) = 1$ folgt $a \mid c$.
(2) Im Ring $(\mathbb{Z}, +, \cdot)$ ist „prim“ äquivalent zu „unzerlegbar“.

Beweis: (1) Dank Bézout B3E existieren $u, v \in \mathbb{Z}$ mit $au + bv = 1$.
Die vorausgesetzte Teilbarkeit $a \mid bc$ bedeutet $aa' = bc$ für ein $a' \in \mathbb{Z}$.
Daraus folgt $c = 1c = (au + bv)c = auc + bcv = a(uc + a'v)$, also $a \mid c$.

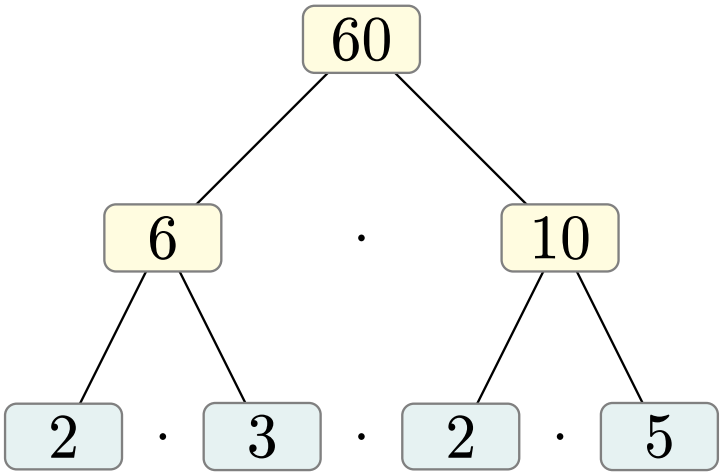
(2) „$\Rightarrow$“: Sei $p \in \mathbb{Z}$ prim und $p = ab$ in $\mathbb{Z}$. Dann folgt $p \mid a$ oder $p \mid b$.
Nehmen wir $p \mid a$ an, also $pp' = a$ für ein $p' \in \mathbb{Z}$. Dann gilt $p = ab = pp'b$,
nach Kürzung $1 = p'b$, also $b \in \mathbb{Z}^\times$. Analog folgt aus $p \mid b$, dass $a \in \mathbb{Z}^\times$.

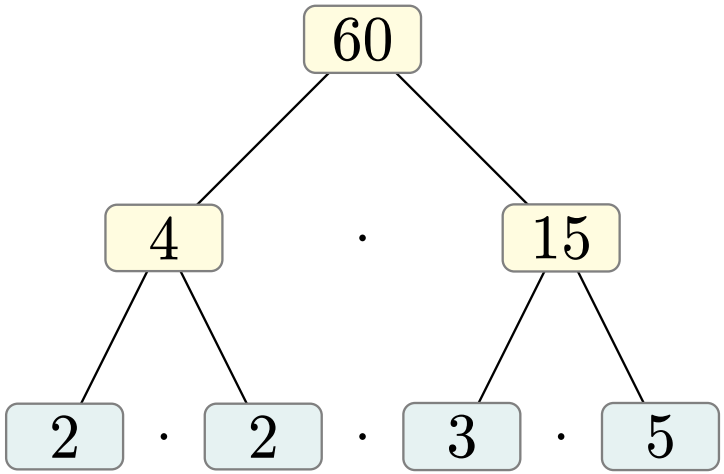
„$\Leftarrow$“: Sei p unzerlegbar und $p \mid ab$. Wir müssen $p \mid a$ oder $p \mid b$ zeigen.
Hierzu sei $d = \operatorname{ggT}(p, a)$. Es gilt $d \mid p$, also entweder $d = 1$ oder $d = |p|$.
(2a) Aus $d = |p|$ folgt sofort $p \mid a$. (2b) Aus $d = 1$ folgt $p \mid b$ dank (1). $\boxed{\text{QED}}$

Der Fundamentalsatz der Arithmetik

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Ein „Produkt unzerlegbarer Faktoren in $\mathbb{N}$“ nenne ich kurz **UProdukt**.

Satz B3J: Fundamentalsatz der Arithmetik, eindeutige Primzerlegung

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

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

(2) Diese Zerlegung ist eindeutig bis auf Umordnung.

Fundamentalsatz: Existenz einer Zerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

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

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 ist a 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 $n + 1 \in E$.

Per Induktion gilt $E = \mathbb{N}_{\geq 1}$: Jede Zahl $a \in \mathbb{N}_{\geq 1}$ ist ein UProdukt. $\boxed{\text{QED}}$

Fundamentalsatz: Eindeutigkeit der Zerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis der Eindeutigkeit (2): In $\mathbb{N}_{\geq 1}$ betrachten wir zwei UProdukte

$$a \;=\; p_1 \cdots p_{\ell-1} p_\ell \;=\; q_1 \cdots q_{k-1} q_k.$$

Wir zeigen, dass $\ell = k$ gilt und nach Umordnung $p_i = q_i$ für alle i.

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

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

Aus $\ell - 1 \in E$ folgt $\ell \in E$: Wir betrachten zwei UProdukte wie oben.
Der Faktor p_ℓ ist unzerlegbar, und somit auch prim dank Euklid B31.
Also gilt $p_\ell \mid q_i$ für ein $i \in \{1, \dots, k\}$. Nach Umordnung gilt $i = k$.
Da q_k unzerlegbar ist, folgt $p_\ell = q_k$. Wir kürzen beide Seiten:

$$a/p_\ell \;= p_1 \cdots p_{\ell-1} \cancel{p_\ell} \;=\; q_1 \cdots q_{k-1} \cancel{q_k}$$

Nach Voraussetzung gilt $\ell - 1 \in E$, für diese gekürzten Produkte also $\ell - 1 = k - 1$ und nach Umordnung $p_i = q_i$ für alle $i \in \{1, \dots, \ell - 1\}$. $\boxed{\text{QED}}$

Anwendung: Welche Wurzeln sind rational?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Ist die Kubikwurzel $\sqrt[3]{864}$ rational? Nein, denn $864 = 2^5 \cdot 3^3$.

Beispiel: Ist $\log_{10}(99)$ rational? Dann wäre $\log_{10}(99) = r/s$ mit $r, s \in \mathbb{Z}_{>0}$, also $99 = 10^{r/s}$, somit $3^{2s} \cdot 11^s = 2^r \cdot 5^r$. Nach Satz B3J ist das unmöglich!

Satz B3K: Fundamentalsatz der Arithmetik als Isomorphismus

Sei $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$ die Menge aller positiven Primzahlen in $(\mathbb{Z}, \cdot)$.

$$e = (e_p)_{p \in \mathbb{P}} = (e_2, e_3, e_5, \dots) \quad \mapsto \quad a = \prod_{p \in \mathbb{P}} p^{e_p} = 2^{e_2}\, 3^{e_3}\, 5^{e_5} \cdots .$$

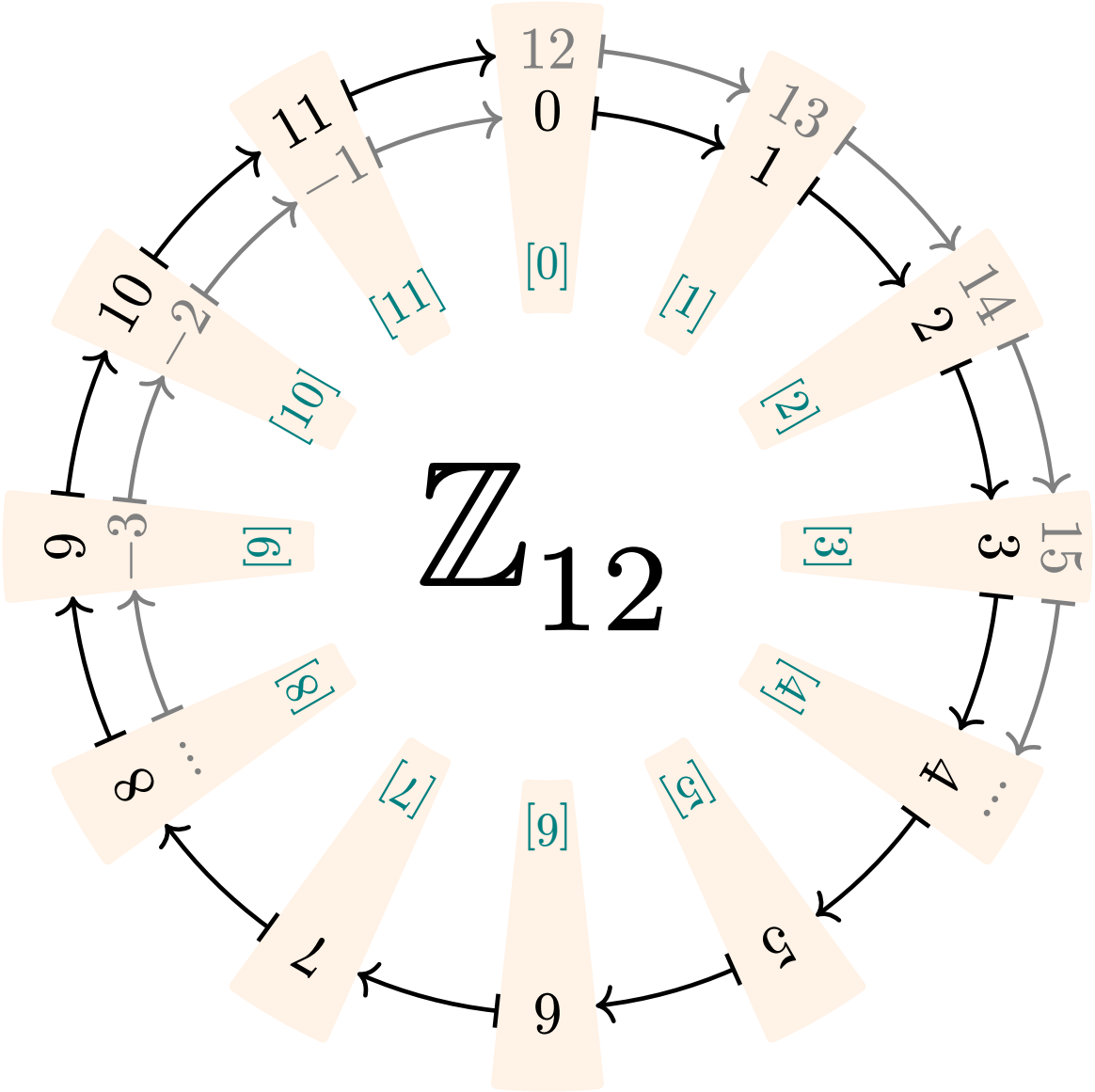
(1) Wir erhalten so die Bijektion

$$\Phi : (\mathbb{N}^{(\mathbb{P})}, +, 0) \xrightarrow{\sim} (\mathbb{Z}_{>0}, \cdot, 1) : e \mapsto \prod_{p \in \mathbb{P}} p^{e_p}.$$

(2) Übergang zu Brüchen in $\mathbb{Q}$ ergibt

$$\Phi : (\mathbb{Z}^{(\mathbb{P})}, +, 0) \xrightarrow{\sim} (\mathbb{Q}_{>0}, \cdot, 1) : e \mapsto \prod_{p \in \mathbb{P}} p^{e_p}.$$

Visualisierung des Restklassenrings $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Rechnen mit Resten: modulare Arithmetik

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

$+_2$	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!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Der Restring $\mathbb{Z}_n$ – informatische Sichtweise

$$\begin{tikzcd}
\mathbb{Z} \times \mathbb{Z} \arrow[r, "+", "(a,b)\mapsto a+b"'] \arrow[d, two heads, "\rho"'] \arrow[dr, phantom, "="] & \mathbb{Z} \arrow[d, two heads, "\rho"'] \\
\mathbb{Z}_n \times \mathbb{Z}_n \arrow[r, "+_n", "(r,s)\mapsto (r+s) \operatorname{rem} n"'] & \mathbb{Z}_n
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{Z} \times \mathbb{Z} \arrow[r, "\cdot", "(a,b)\mapsto a\cdot b"'] \arrow[d, two heads, "\rho"'] \arrow[dr, phantom, "="] & \mathbb{Z} \arrow[d, two heads, "\rho"'] \\
\mathbb{Z}_n \times \mathbb{Z}_n \arrow[r, "\cdot_n", "(r,s)\mapsto (r\cdot s) \operatorname{rem} n"'] & \mathbb{Z}_n
\end{tikzcd}$$

Satz B3M: Konstruktion des Rings $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$ für $n \in \mathbb{N}_{\geq 2}$

(0) Die Reduktion $\rho : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n : a \mapsto a \operatorname{rem} n$ ist ein Homomorphismus: Für alle $a, b \in \mathbb{Z}$ gilt $\rho(a+b) = \rho(a) +_n \rho(b)$ und $\rho(a \cdot b) = \rho(a) \cdot_n \rho(b)$.

(1) Daher ist $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$ ein CRing.

(2) Genau dann ist a in $(\mathbb{Z}_n, \cdot_n, 1)$ invertierbar, wenn $\operatorname{ggT}(a, n) = 1$ gilt. Explizite Inversion dank Bézout: $au + nv = 1$ bedeutet $au \operatorname{rem} n = 1$.

(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*).

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Der Restring $\mathbb{Z}_n$ – informatische Sichtweise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: (0) Euklidische Division ergibt $a = nq_a + r_a$ und $b = nq_b + r_b$.
(0a) Mit der Division $r_a + r_b = nq + r$ folgt $a + b = n(q_a + q_b + q) + r$.
(0b) Mit $r_a \cdot r_b = nq + r$ folgt $a \cdot b = n^2 q_a q_b + n(q_a r_b + r_a q_b + q) + r$.

(1) Wir zeigen Assoziativität von $(\mathbb{Z}_n, +_n)$. Für alle $r_1, r_2, r_3 \in \mathbb{Z}_n$ gilt:

$$(r_1 +_n r_2) +_n r_3 \overset{\text{sur}}{=} (\rho(r_1) +_n \rho(r_2)) +_n \rho(r_3) \overset{(0)}{=} \rho((r_1 + r_2) + r_3)$$
$$r_1 +_n (r_2 +_n r_3) \overset{\text{sur}}{=} \rho(r_1) +_n (\rho(r_2) +_n \rho(r_3)) \overset{(0)}{=} \rho(r_1 + (r_2 + r_3))$$

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

Die Kongruenz $a \equiv b$ modulo n – bequeme Schreibweise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir nennen $a, b \in \mathbb{Z}$ **kongruent** modulo n, wenn sie selben Rest lassen:

$$a \equiv_n b \quad \Longleftrightarrow \quad a \operatorname{rem} n = b \operatorname{rem} n \quad \Longleftrightarrow \quad (b-a) \operatorname{rem} n = 0 \quad \Longleftrightarrow$$
$$n \mid b-a \quad \Longleftrightarrow \quad \exists n' : nn' = b-a \quad \Longleftrightarrow \quad b-a \in n\mathbb{Z}$$

Die Kongruenz $\equiv$ ist eine **Äquivalenzrelation** auf $\mathbb{Z}$:

Reflexivität, **Refl**$(\mathbb{Z}, \equiv)$: $a \equiv a$

Symmetrie, **Sym**$(\mathbb{Z}, \equiv)$: $a \equiv b \Rightarrow b \equiv a$

Transitivität, **Tran**$(\mathbb{Z}, \equiv)$: $a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$

Die Kongruenz $\equiv$ auf $\mathbb{Z}$ ist **verträglich** mit Addition und Multiplikation:

$$a \equiv a', \;\; b \equiv b' \quad \Longrightarrow \quad a+b \equiv a'+b', \;\; a \cdot b \equiv a' \cdot b'$$

Die Kongruenz $a \equiv b$ modulo n – bequeme Schreibweise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Ist $5^8 - 2^4$ durch 23 teilbar? Bonus: $5^{8000} - 2^{4000}$?

Brutale Gewalt: Wir finden $5^8 - 2^4 = 390625 - 16 = 390609 = 23 \cdot 16983$.

Elegante Effizienz: Modulo 23 gilt $5^8 = 25^4 \equiv 2^4$, also $23 \mid 5^8 - 2^4$.

Anwendung: Quersumme und Teilbarkeit

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Ist $a = 2025$ durch 3 teilbar? durch 9? durch 11?

$$\begin{array}{lrl} \text{Quersumme} & q(a) = & 2+0+2+5=9 \\ \text{Wechselsumme} & w(a) = & -2+0-2+5=1 \end{array}$$

Bemerkung B3N: schneller Rest modulo $3, 9, 11$

Jede natürliche Zahl $a \in \mathbb{N}$ schreiben wir wie üblich dezimal

$$a = \sum_{k=0}^{\ell} 10^k a_k \quad \text{mit Ziffern } a_k \in \{0, \dots, 9\}.$$

Daraus erhalten wir die **Quersumme** und die **Wechselquersumme**:

$$q(a) := \sum_{k=0}^{\ell} a_k \quad \text{und} \quad w(a) := \sum_{k=0}^{\ell} (-1)^k a_k$$

Modulo 3 oder 9 gilt $10 \equiv 1$, also $a \equiv q(a)$.
Modulo 11 gilt $10 \equiv -1$, also $a \equiv w(a)$.

Topfrechnen mit Restklassen – mathematische Sichtweise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$[a]_n := \{ b \in \mathbb{Z} \mid a \equiv_n b \} = a + n\mathbb{Z}$$

Modulo 2:

$$[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\} = 0 + 2\mathbb{Z} =: \overline{0} = \overline{2} = \overline{4} = \dots$$
$$[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\} = 1 + 2\mathbb{Z} =: \overline{1} = \overline{3} = \overline{5} = \dots$$

Modulo 3:

$$[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\} = 0 + 3\mathbb{Z} =: \overline{0} = \overline{3} = \overline{6} = \dots$$
$$[1]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\} = 1 + 3\mathbb{Z} =: \overline{1} = \overline{4} = \overline{7} = \dots$$
$$[2]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\} = 2 + 3\mathbb{Z} =: \overline{2} = \overline{5} = \overline{8} = \dots$$

Vorteil: Die Kongruenz $a \equiv_n b$ wird nun zur Gleichheit $[a]_n = [b]_n$.
Modulo 3 gilt $[-4] = [-1] = [2] = [5]$. Modulo 23 gilt $[25] = [2]$.

Vom Restring $\mathbb{Z}_n$ zum Restklassenring $\mathbb{Z}/n\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir rechnen mit **Resten** bezüglich $n \in \mathbb{Z}_{\geq 2}$ und erhalten den **Restring**

$$\begin{array}{ll} (\mathbb{Z}_n, +_n, 0, \cdot_n, 1), & a +_n b = (a+b) \operatorname{rem} n, \\ \mathbb{Z}_n = \{0, 1, \dots, n-1\}^!, & a \cdot_n b = (a \cdot b) \operatorname{rem} n. \end{array}$$

Auf der Menge $\mathbb{Z}/n\mathbb{Z} := \{\, [a] \mid a \in \mathbb{Z} \,\}$ erhalten wir den **Restklassenring**

$$\begin{array}{ll} (\mathbb{Z}/n\mathbb{Z}, \mathbf{+}, [0], \bullet, [1]), & [a] \mathbf{+} [b] = [a+b], \\ \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}^!, & [a] \bullet [b] = [a \cdot b]. \end{array}$$

Wo keine Verwechslung droht, schreiben wir $(\mathbb{Z}_n, +, \cdot) = (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

Homer Simpson vs Pierre de Fermat

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\text{(A)} \quad 1782^{12} + 1841^{12} \overset{?}{=} 1922^{12}$$

$$\text{(B)} \quad 3987^{12} + 4365^{12} \overset{?}{=} 4472^{12}$$

Aufgabe: Welche dieser beiden Behauptungen sind wahr?

Lösung: Auf dem Taschenrechner: beide! In Wirklichkeit: keine!

$$\text{(A) modulo 2} \quad \Longrightarrow \quad 0^{12} + 1^{12} \overset{?}{\equiv} 0^{12} \quad \lightning \text{ falsch!}$$

$$\text{(B) modulo 2} \quad \Longrightarrow \quad 1^{12} + 1^{12} \overset{?}{\equiv} 0^{12} \quad ?$$

$$\text{(B) modulo 4} \quad \Longrightarrow \quad 3^{12} + 1^{12} \overset{?}{\equiv} 0^{12} \quad \lightning \text{ falsch!}$$

Ein quadratisches Gleichungssystem

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel B4A: BWM 2020, Runde 2, Aufgabe 2

Finden Sie alle $(x, y, z) \in \mathbb{Q}^3$ mit $x + y + z = 0$ und $x^2 + y^2 + z^2 = 100$.

Lösung: Angenommen $(x, y, z) \in \mathbb{Q}^3$ ist eine Lösung. (1) Daraus folgt $z = -(x + y)$, also $z^2 = x^2 + 2xy + y^2$. Einsetzen in die zweite Gleichung:

$$2x^2 + 2xy + 2y^2 = 100$$

(2) Für $x, y \in \mathbb{Q}$ gilt $x = a/c$ und $y = b/c$ mit $a, b, c \in \mathbb{Z}$ und gemeinsamem Nenner $c > 0$ sowie (nach Kürzen) $\mathrm{ggT}(a, b, c) = 1$. Einsetzen ergibt:

$$a^2 + ab + b^2 = 2 \cdot (5c)^2$$

(3) Ist a oder b ungerade, so auch die linke Seite. Die rechte ist gerade. Also müssen a und b gerade sein. Wegen $\mathrm{ggT}(a, b, c) = 1$ ist c ungerade. Nun ist die linke Seite durch 4 teilbar, die rechte aber nicht. Widerspruch!

Demnach gibt es keine rationale Lösung $(x, y, z) \in \mathbb{Q}^3$. $\boxed{\text{QED}}$

Rückblick auf dieses Kapitel

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Frage B4B: Aufbau des Zahlensystems

(0) Wie erklären Sie $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ und das Rechnen darin?

(1) Existiert zu $a, b \in \mathbb{Z}$ ein größter gemeinsamer Teiler $d \in \mathbb{Z}$?

(2) Ist jedes $n \in \mathbb{N}_{\geq 1}$ ein Produkt von Primzahlen? eindeutig?

(3) Ist $\sqrt{2}$ rational? irrational? und $\sqrt[3]{864}$? und $\log_{10}(99)$?

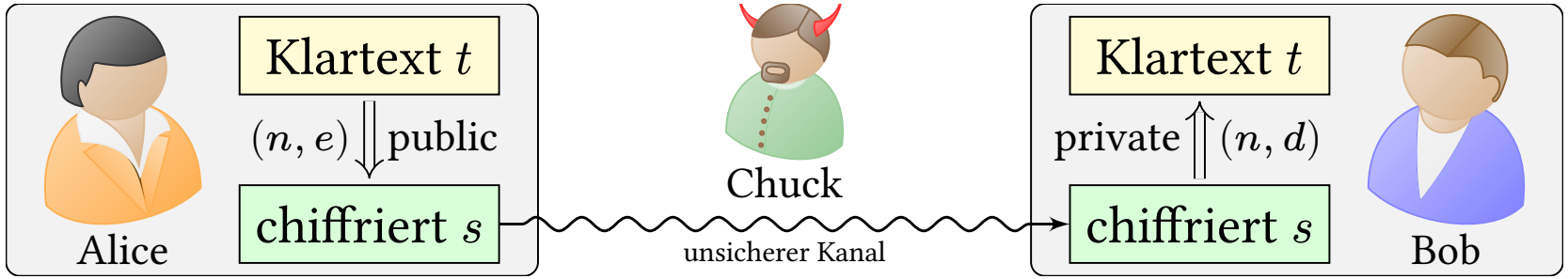
(4) Gibt es rationale Punkte $(x, y, z) \in \mathbb{Q}^3$ in der Ebene $x + y + z = 0$, die zudem auf der Sphäre $x^2 + y^2 + z^2 = 10^2$ von Radius 10 liegen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel B

Bonusmaterial



Also lautet ein Beschluß, // Daß der Mensch was lernen muß.
Nicht allein das ABC // Bringt den Menschen in die Höh';
Nicht allein in Schreiben, Lesen // Übt sich ein vernünftig Wesen;
Gerade auch in Rechnungssachen // Soll der Mensch sich Mühe machen.

frei nach Wilhelm Busch (1832–1908)

Inhalt dieses Kapitels B

5 Rechentricks, legale und illegale

6 Schnelles Rechnen, insbesondere in $\mathbb{Z}$ und $\mathbb{Z}_n$

7 *General abstract nonsense:* Was sind Kategorien?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel C

Polynome und Euklids Algorithmus

$$
\begin{array}{c|cccccc}
 & & & & & & g \\
b_2x^2 & a_0b_2x^2 & a_1b_2x^3 & a_2b_2x^4 & a_3b_2x^5 & a_4b_2x^6 & a_5b_2x^7 \\
+ & & & & & & \\
b_1x^1 & a_0b_1x^1 & a_1b_1x^2 & a_2b_1x^3 & a_3b_1x^4 & a_4b_1x^5 & a_5b_1x^6 \\
+ & & & & & & \\
b_0x^0 & a_0b_0x^0 & a_1b_0x^1 & a_2b_0x^2 & a_3b_0x^3 & a_4b_0x^4 & a_5b_0x^5 \\
\hline
\cdot & a_0x^0 + a_1x^1 + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 & & & & & f
\end{array}
$$

Alles Gescheite ist schon gedacht worden,
man muss nur versuchen, es noch einmal zu denken.

Johann Wolfgang von Goethe (1749–1832)

Inhalt dieses Kapitels C

1 Was sind Polynome, wirklich?

2 Polynomdivision in $\mathbb{K}[X]$ über einem CRing $\mathbb{K}$

3 Der Polynomring $\mathbb{K}[X]$ über einem Körper $\mathbb{K}$

4 Fazit: Polynome und Euklids Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Motivation: Rechnen mit einer Variablen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{aligned}
f &= f_0 + f_1 X + f_2 X^2 + \dots \\
g &= g_0 + g_1 X + g_2 X^2 + \dots
\end{aligned}
$$

$$f = g \iff \forall i \in \mathbb{N} : f_i = g_i \quad \text{Koeffizientenvergleich}$$

$$
\begin{aligned}
f + g &= (f_0 + g_0) + (f_1 + g_1) X + (f_2 + g_2) X^2 + \dots \\
f \cdot g &= (f_0 g_0) + (f_0 g_1 + f_1 g_0) X + (f_0 g_2 + f_1 g_1 + f_2 g_0) X^2 + \dots
\end{aligned}
$$

Vorschau: praktische Beispiele, Fragen, Anwendungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Frage C0A: Was sind und was können Polynome?

Wie funktioniert das Rechnen mit physikalischen Einheiten?

Wie berechnen Sie Wahrscheinlichkeiten von Würfelsummen?

Wie erklären Sie Polynome und das Rechnen damit?

(1) Sind $f, g : \mathbb{F}_2 \to \mathbb{F}_2$ mit $f(x) = x^2 + x$ und $g(x) = 0$ verschieden?

(2) Wie viele Nullstellen hat $P = \sum_{k=0}^{n} p_k X^k$ über $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \ldots$?

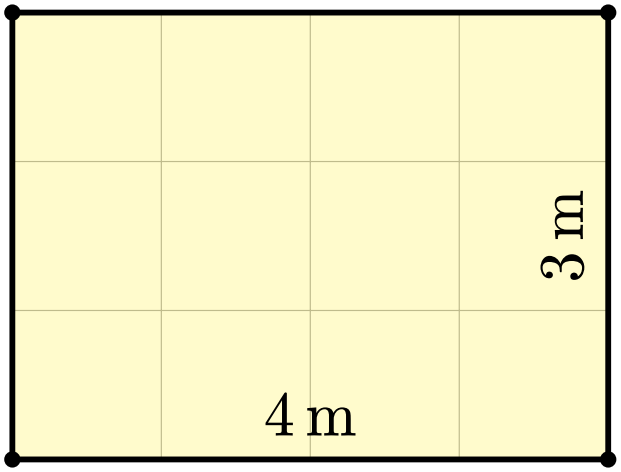
(3) Haben auch Polynome eine eindeutige Primzerlegung?

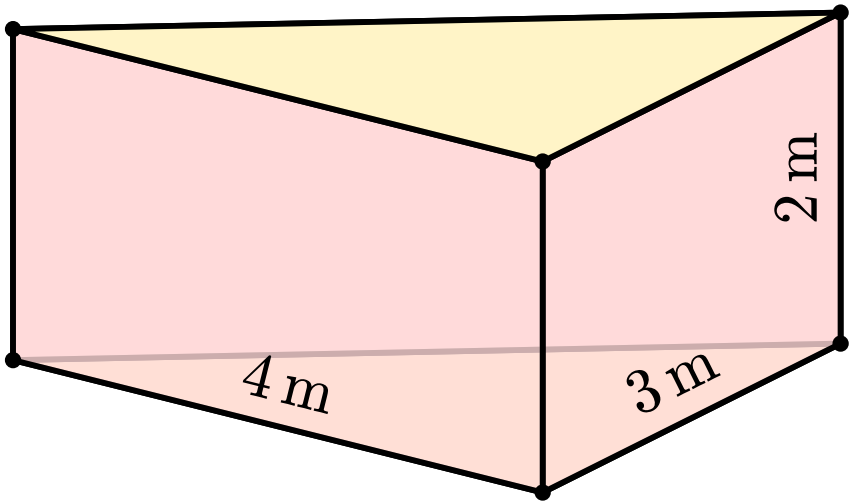
(4) Wie konstruieren Sie einen Körper mit 4 Elementen?

Anwendungsbeispiel: Rechnen mit physikalischen Einheiten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

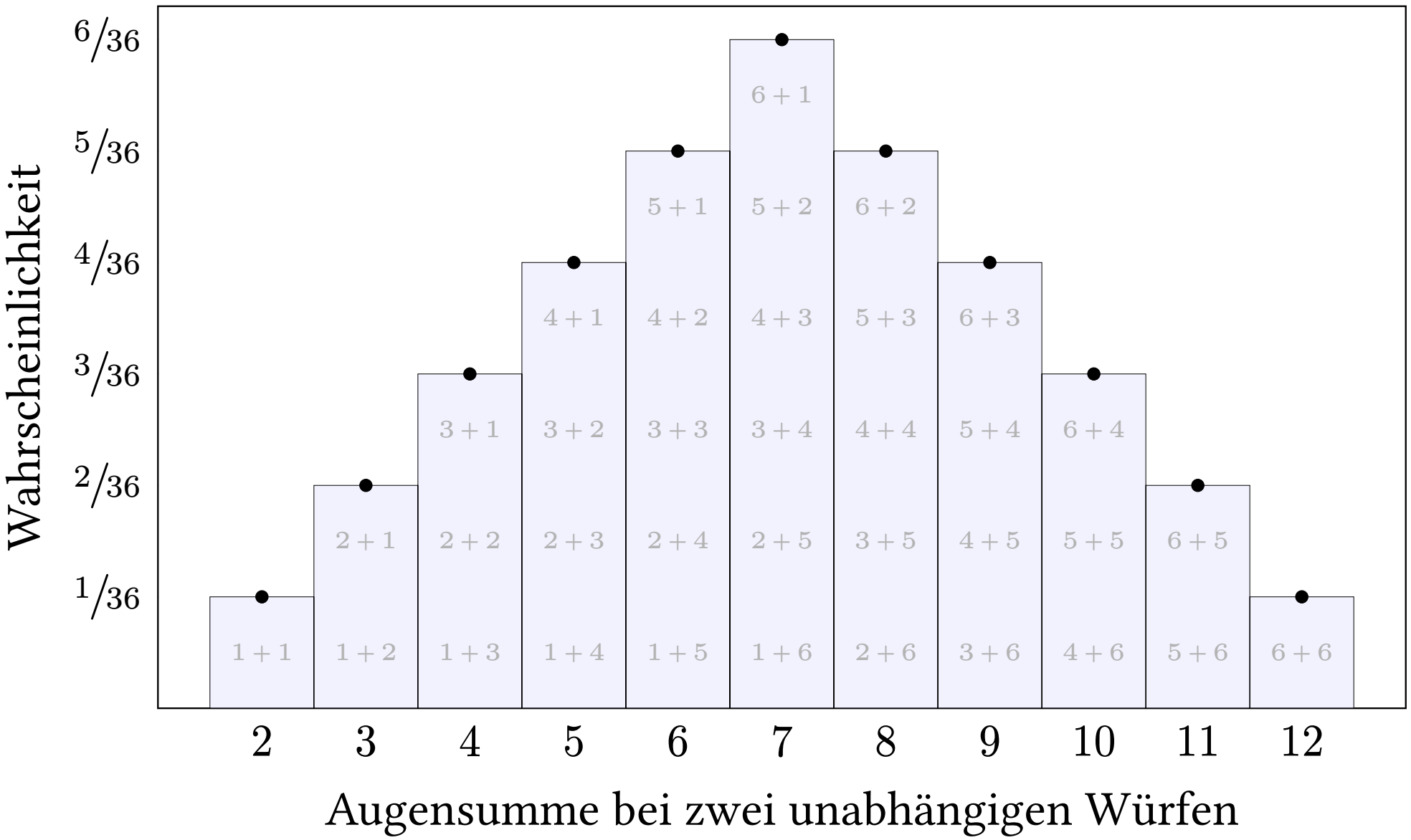




$$\left.\begin{aligned} a &= 4\,\mathrm{m}^1 + 2\,\mathrm{m}^0 \\ b &= 3\,\mathrm{m}^1 + 2\,\mathrm{m}^0 \end{aligned}\right\} \Longrightarrow a \cdot b = 12\,\mathrm{m}^2 + 14\,\mathrm{m}^1 + 4\,\mathrm{m}^0$$

$$\left.\begin{aligned} g &= 6\,\mathrm{m}^2 + 12\,\mathrm{m}^1 + 3\,\mathrm{m}^0 \\ h &= \phantom{6\,\mathrm{m}^2 + {}} 2\,\mathrm{m}^1 + 2\,\mathrm{m}^0 \end{aligned}\right\} \Longrightarrow g \cdot h = 12\,\mathrm{m}^3 + 36\,\mathrm{m}^2 + 30\,\mathrm{m}^1 + 6\,\mathrm{m}^0$$

Anwendungsbeispiel: zweimaliger Wurf eines fairen Würfels



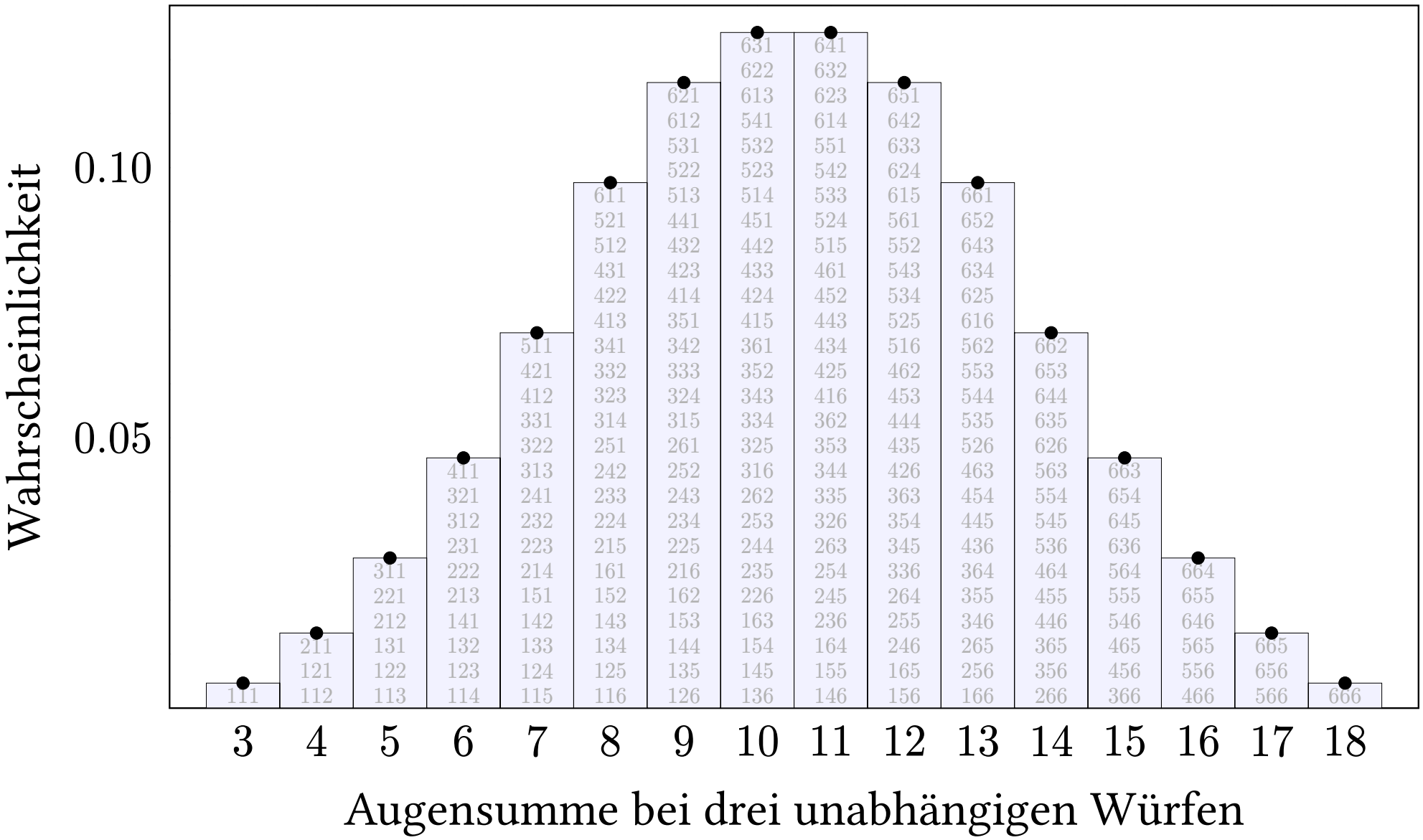
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

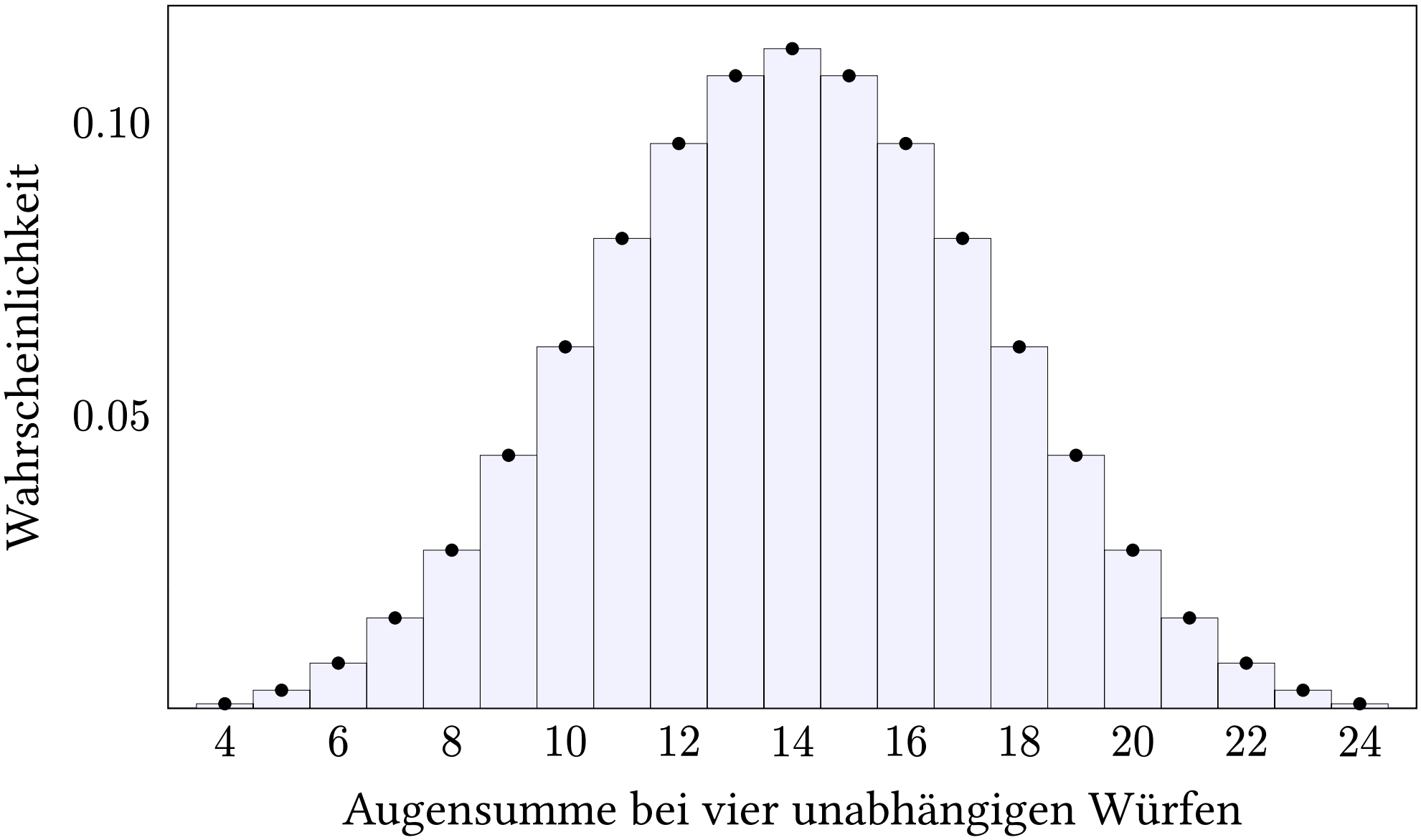
Anwendungsbeispiel: dreimaliger Wurf eines fairen Würfels

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



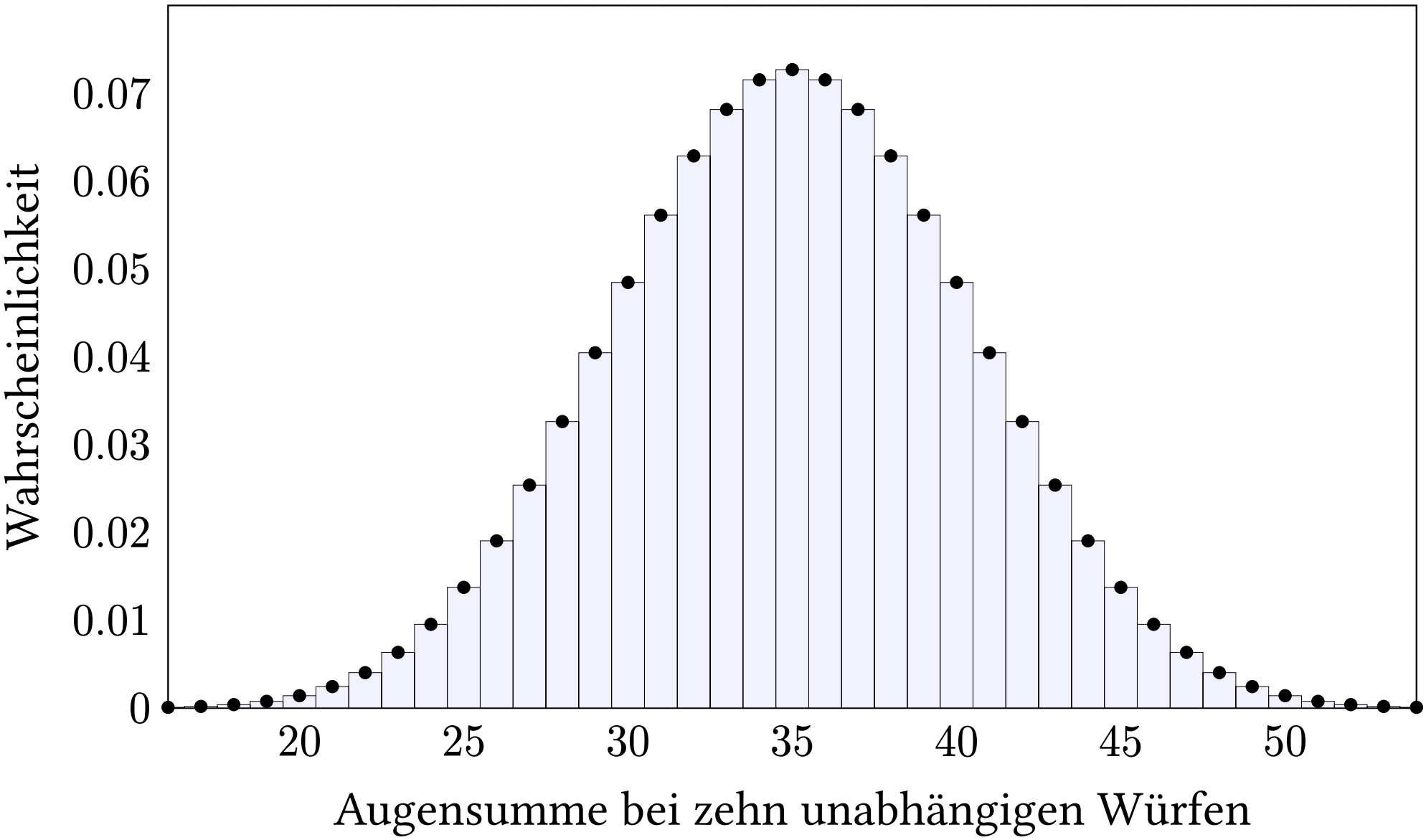
Anwendungsbeispiel: viermaliger Wurf eines fairen Würfels



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Anwendungsbeispiel: zehnmaliger Wurf eines fairen Würfels



Dies ist nur die Saalversion ohne Erläuterungen.
Ausführliche Erläuterungen bietet die Vollversion.

Anwendungsbeispiel: Summe von Zufallsvariablen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Zufallsgröße $X : \Omega \to \mathbb{N}$ nimmt die Werte $i = 0, 1, 2, \ldots$ an mit Wkt

$$(p_0, p_1, p_2, \ldots) = (p_i)_{i \in \mathbb{N}} = p : \mathbb{N} \to \mathbb{R}.$$

Unabhängig davon nimmt $Y : \Omega \to \mathbb{N}$ die Werte $j = 0, 1, 2, \ldots$ an mit Wkt

$$(q_0, q_1, q_2, \ldots) = (q_j)_{j \in \mathbb{N}} = q : \mathbb{N} \to \mathbb{R}.$$

Aufgabe: Ihre Summe $S = X + Y : \Omega \to \mathbb{N}$ hat dann welche Verteilung

$$(r_0, r_1, r_2, \ldots) = (r_k)_{k \in \mathbb{N}} = r : \mathbb{N} \to \mathbb{R}?$$

Lösung: Die gesuchte Wkt r_k finden wir durch

$$\boxed{r_k = \sum_{(i,j):i+j=k} p_i \cdot q_j, \quad \text{kurz} \quad r =: p * q.}$$

Anwendungsbeispiel: Summe von Zufallsvariablen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

q					
q_3	p_0q_3	p_1q_3	p_2q_3	p_3q_3	
q_2	p_0q_2	p_1q_2	p_2q_2	p_3q_2	
q_1	p_0q_1	p_1q_1	p_2q_1	p_3q_1	
q_0	p_0q_0	p_1q_0	p_2q_0	p_3q_0	
$*$	p_0	p_1	p_2	p_3	p

Beispiel: unabhängige Münzwürfe

q					
0	0	0	0	0	
0	0	0	0	0	
$1/2$	$1/4$	$1/4$	0	0	
$1/2$	$1/4$	$1/4$	0	0	
$*$	$1/2$	$1/2$	0	0	p

$$r_0 = p_0q_0 \overset{\text{Bsp}}{=} 1/4$$

$$r_1 = p_0q_1 + p_1q_0 \overset{\text{Bsp}}{=} 1/2$$

$$r_2 = p_0q_2 + p_1q_1 + p_2q_0 \overset{\text{Bsp}}{=} 1/4$$

$$\vdots$$

$$r_k = \sum_{i+j=k} p_iq_j = \sum_{i=0}^{k} p_iq_{k-i} = \sum_{j=0}^{k} p_{k-j}q_j$$

Rechenregeln für Folgen: Addition und Faltung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $(\mathbb{K}, +, 0, \cdot, 1)$ ein Ring, etwa $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots, \mathbb{Z}, \mathbb{Z}_n, \dots$.
Folgen $f, g : \mathbb{N} \to \mathbb{K}$ skalieren / addieren / falten wir wie folgt:

$$\begin{array}{llll}
\lambda \bullet f & : \mathbb{N} \to \mathbb{K}, & (\lambda \bullet f)_k := \lambda \cdot f_k & \text{für } \lambda \in \mathbb{K}, \\
f \bullet \mu & : \mathbb{N} \to \mathbb{K}, & (f \bullet \mu)_k := f_k \cdot \mu & \text{für } \mu \in \mathbb{K}, \\
f \mathbf{+} g & : \mathbb{N} \to \mathbb{K}, & (f \mathbf{+} g)_k := f_k + g_k, & \mathbf{0} := (0, 0, 0, \dots), \\
f * g & : \mathbb{N} \to \mathbb{K}, & (f * g)_k := \sum_{(i,j):i+j=k} f_i \cdot g_j, & \mathbf{1} := (1, 0, 0, \dots).
\end{array}$$

Satz C1A: der Folgenring $\mathbb{K}^{\mathbb{N}} = \{ f : \mathbb{N} \to \mathbb{K} \}$ mit Faltung

(1) Ist $(\mathbb{K}, +, 0, \cdot, 1)$ ein (kommutativer) Ring, so auch $(\mathbb{K}^{\mathbb{N}}, \mathbf{+}, \mathbf{0}, *, \mathbf{1})$.
(2) Darin liegt $\mathbb{K}$ als Teilring vermöge $\mathbb{K} \hookrightarrow \mathbb{K}^{\mathbb{N}} : \lambda \mapsto \lambda \bullet \mathbf{1} = (\lambda, 0, 0, \dots)$.

Rechenregeln für Folgen: Addition und Faltung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: Exemplarisch zeigen wir die Assoziativität der Multiplikation. Gegeben seien drei Folgen $f, g, h : \mathbb{N} \to \mathbb{K}$. Wir zeigen die Gleichheit

$$(f * g) * h = f * (g * h) \ : \mathbb{N} \to \mathbb{K}.$$

Wir prüfen dazu die Gleichheit für jeden Index $n \in \mathbb{N}$:

$$[(f * g) * h]_n \overset{\text{Def}}{=} \sum_{\substack{(s,k)\in\mathbb{N}^2 \\ s+k=n}} (f * g)_s \cdot h_k \overset{\text{Def}}{=} \sum_{\substack{(s,k)\in\mathbb{N}^2 \\ s+k=n}} \left(\sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=s}} f_i \cdot g_j \right) \cdot h_k \overset{\text{Dst}}{=} \sum_{\substack{(i,j,k)\in\mathbb{N}^3 \\ i+j+k=n}} (f_i \cdot g_j) \cdot h_k$$

$$[f * (g * h)]_n \overset{\text{Def}}{=} \sum_{\substack{(i,s)\in\mathbb{N}^2 \\ i+s=n}} f_i \cdot (g * h)_s \overset{\text{Def}}{=} \sum_{\substack{(i,s)\in\mathbb{N}^2 \\ i+s=n}} f_i \cdot \left(\sum_{\substack{(j,k)\in\mathbb{N}^2 \\ j+k=s}} g_j \cdot h_k \right) \overset{\text{Dst}}{=} \sum_{\substack{(i,j,k)\in\mathbb{N}^3 \\ i+j+k=n}} f_i \cdot (g_j \cdot h_k)$$

Rechnen im Folgenring $\mathbb{K}^{\mathbb{N}}$: Monome und Polynome

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Im Folgenring $\mathbb{K}^{\mathbb{N}}$ benennen wir $X := (0, 1, 0, 0, \ldots)$. Für alle $f \in \mathbb{K}^{\mathbb{N}}$ gilt

$$X * f \;=\; f * X \;=\; (0, f_0, f_1, f_2, \ldots).$$

Insbesondere finden wir so alle Potenzen X^k mit $k \in \mathbb{N}$:

$$\begin{aligned} X^0 &= (1, 0, 0, 0, 0, \ldots), \\ X^1 &= (0, 1, 0, 0, 0, \ldots), \\ X^2 &= (0, 0, 1, 0, 0, \ldots), \quad \ldots \end{aligned}$$

Mit den Koeffizienten $f_0, \ldots, f_n \in \mathbb{K}$ erhalten wir daraus das **Polynom**

$$f = \textstyle\sum_{k=0}^{n} f_k \cdot X^k = (f_0, \ldots, f_n, 0, 0, \ldots).$$

Rechnen im Folgenring $\mathbb{K}^{\mathbb{N}}$: der Polynomring $\mathbb{K}[X] = \mathbb{K}^{(\mathbb{N})}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\mathbb{K}^{(\mathbb{N})} := \left\{ f : \mathbb{N} \to \mathbb{K} \,\middle|\, \exists n \in \mathbb{N} \;\; \forall k \in \mathbb{N}_{>n} : f_k = 0 \right\}$$

Satz C1B: der Polynomring $\mathbb{K}^{(\mathbb{N})} = \mathbb{K}[X]$ – kanonische Konstruktion

(1) Ist $(\mathbb{K}, +, 0, \cdot, 1)$ ein (kommutativer) Ring, so auch $(\mathbb{K}^{(\mathbb{N})}, \mathbf{+}, \mathbf{0}, *, \mathbf{1})$.
Wo keine Verwechslung droht, schreiben wir bequem $(\mathbb{K}^{(\mathbb{N})}, +, 0, \cdot, 1)$.

(2) Jedes Element $f \in \mathbb{K}^{(\mathbb{N})} \setminus \{\mathbf{0}\}$ ist eine eindeutige Linearkombination $f = \sum_{k=0}^{n} f_k X^k$ vom Grad $n \in \mathbb{N}$ mit Koeffizienten $f_0, \dots, f_n \in \mathbb{K}$, $f_n \neq 0$.

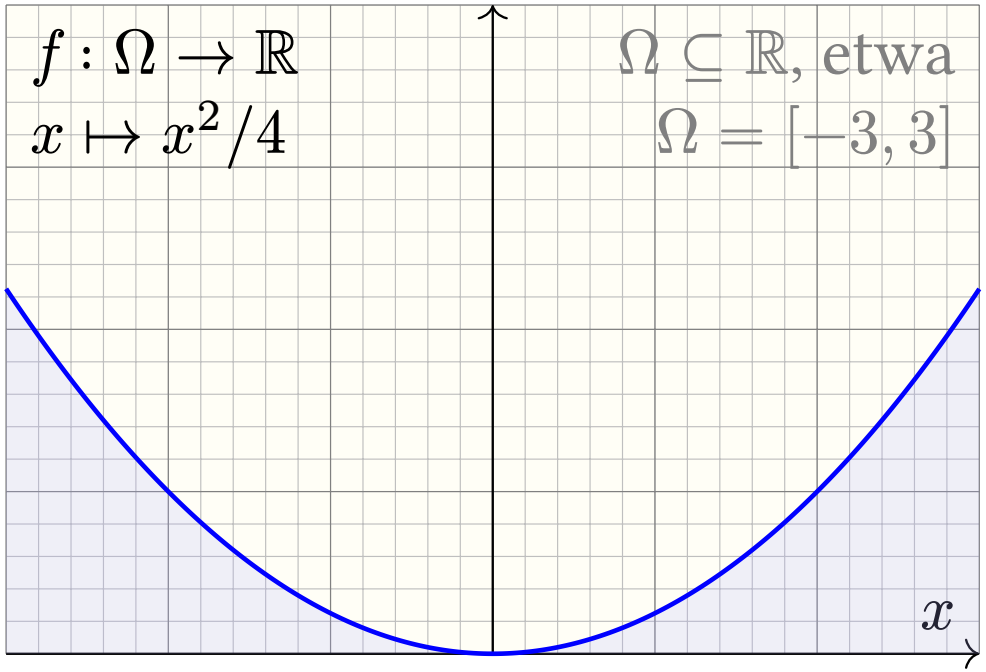
M Polynome sind einfach Koeffizientenfolgen $f \in \mathbb{K}^{(\mathbb{N})}$. ☺

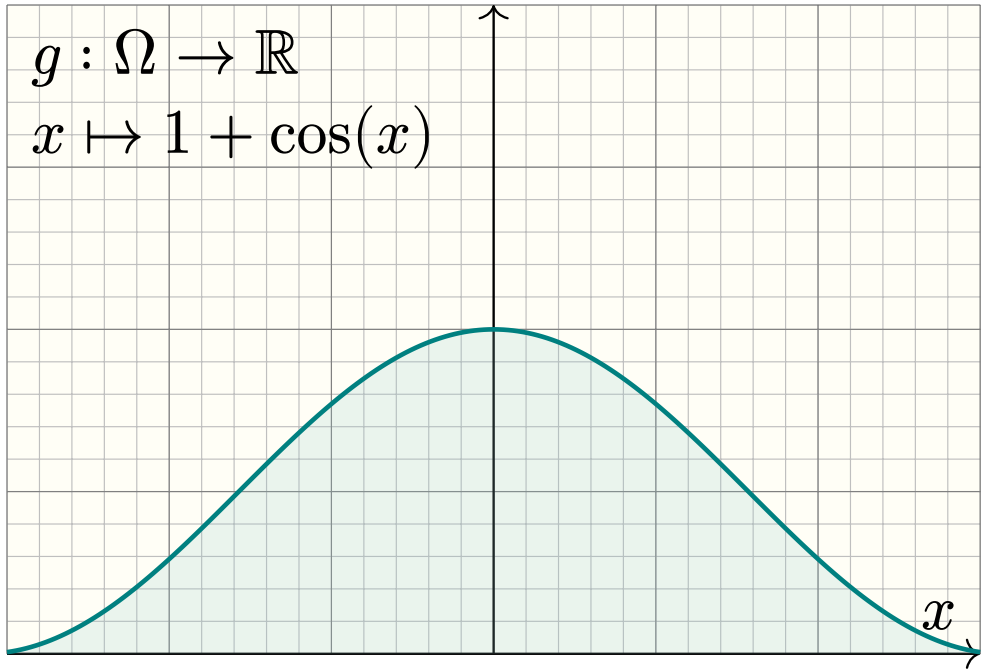
L So nutzen wir Polynome in der Schule, jetzt gut begründet. ☺

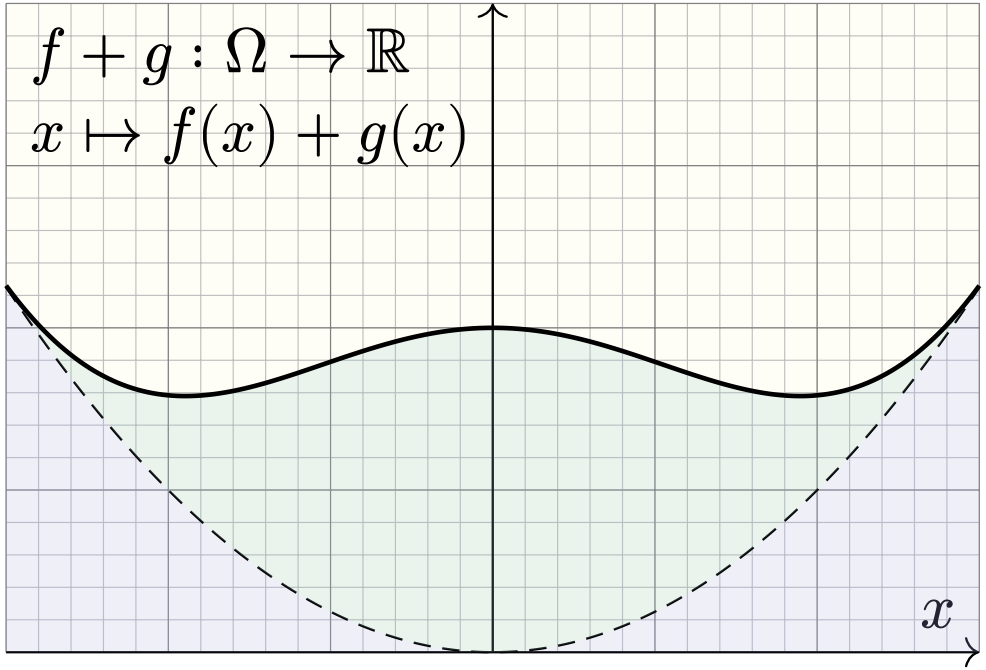
I So implementieren wir Polynome und ihre Operationen. ☺

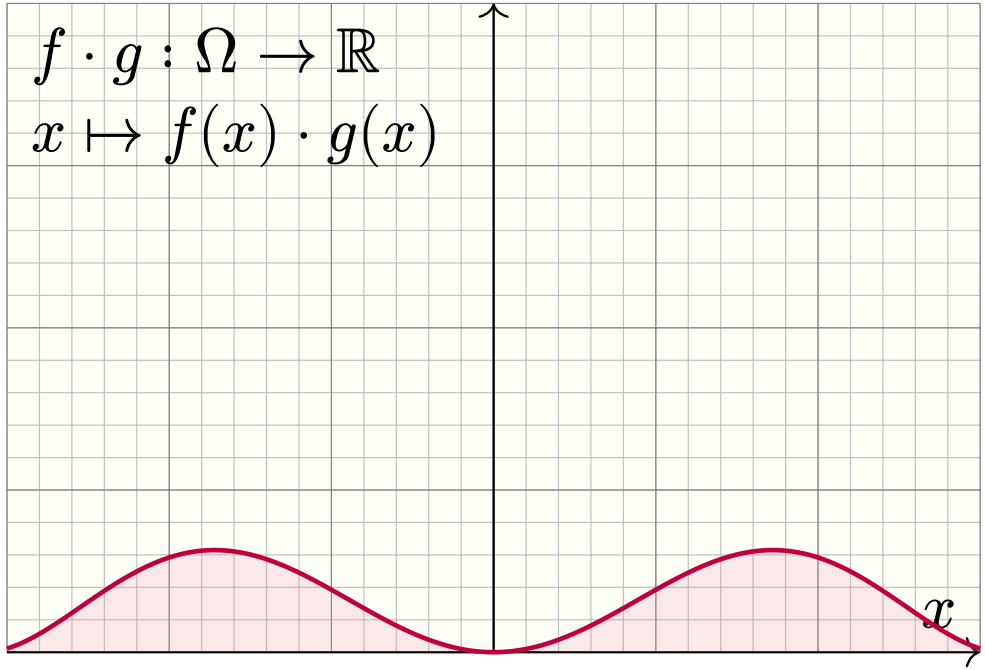
P Physikalische Größe $f_k X^k$ gleich Maßzahl mal Einheit. ☺

Wie rechnen wir mit Funktionen $f, g : \Omega \to \mathbb{K}$?









Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wie rechnen wir mit Funktionen $f, g : \Omega \to \mathbb{K}$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $\Omega \neq \emptyset$ eine beliebige Menge, etwa $\Omega \subseteq \mathbb{K}^n$. Funktionen $f, g : \Omega \to \mathbb{K}$ skalieren / addieren / multiplizieren wir punktweise, in jedem $x \in \Omega$:

$$\begin{aligned}
\lambda \cdot f &: \Omega \to \mathbb{K}, & (\lambda \cdot f)(x) &:= \lambda \cdot f(x) & &\text{für } \lambda \in \mathbb{K},\\
f + g &: \Omega \to \mathbb{K}, & (f + g)(x) &:= f(x) + g(x), & &\mathbf{0}(x) := 0,\\
f \cdot g &: \Omega \to \mathbb{K}, & (f \cdot g)(x) &:= f(x) \cdot g(x), & &\mathbf{1}(x) := 1
\end{aligned}$$

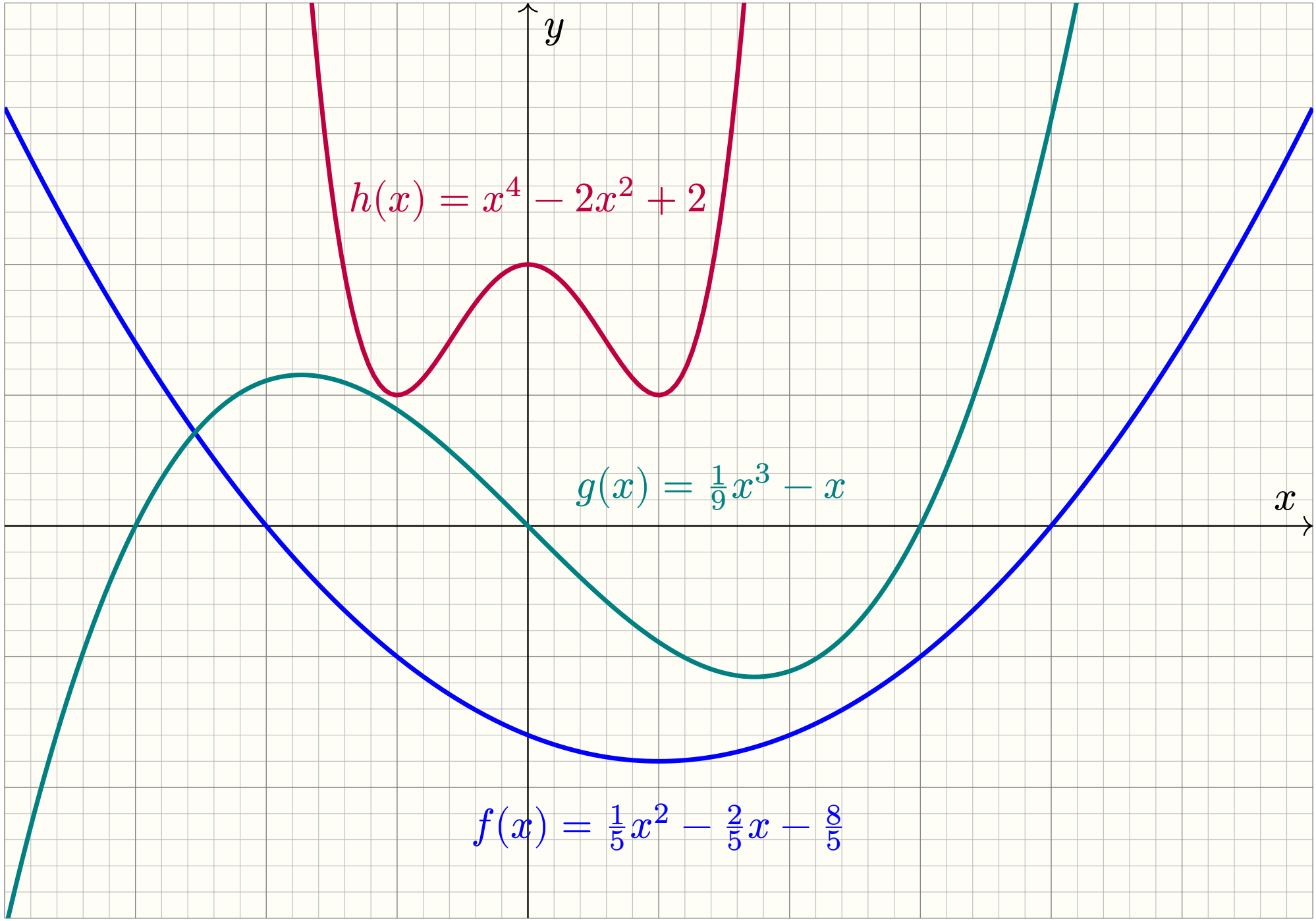
Satz C1c: der Ring $\mathbb{K}^\Omega = \{ f : \Omega \to \mathbb{K} \}$ der Funktionen über $\mathbb{K}$

(1) Ist $(\mathbb{K}, +, 0, \cdot, 1)$ ein (kommutativer) Ring, so auch $(\mathbb{K}^\Omega, \mathbf{+}, \mathbf{0}, \cdot, \mathbf{1})$.
(2) Darin liegt $\mathbb{K}$ als Teilring vermöge $\mathbb{K} \to \mathbb{K}^\Omega : \lambda \mapsto \lambda \cdot \mathbf{1} = \mathrm{const}_\Omega^\lambda$.

Aufgabe: Zeigen Sie $f \cdot g = g \cdot f$. **Lösung:** In jedem Punkt $x \in \Omega$ gilt:

$$(f \cdot g)(x) \overset{\text{Def}}{=} f(x) \cdot g(x) \overset{\text{Com}}{=} g(x) \cdot f(x) \overset{\text{Def}}{=} (g \cdot f)(x)$$

Was sind Polynomfunktionen $f, g : \mathbb{K} \to \mathbb{K}$?



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wie rechnen wir mit Polynomfunktionen $f, g : \mathbb{K} \to \mathbb{K}$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Eine **Polynomfunktion** $f : \mathbb{K} \to \mathbb{K}$ hat die spezielle Form

$$x \mapsto f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n.$$

$$\mathrm{Poly}(\mathbb{K}, \mathbb{K}) := \left\{ f : \mathbb{K} \to \mathbb{K} \,\middle|\, \exists a \in \mathbb{K}^{(\mathbb{N})} \;\; \forall x \in \mathbb{K} : \; f(x) = \sum_i a_i x^i \right\}$$

Für Polynomfunktionen $f(x) = \sum_i a_i x^i$ und $g(x) = \sum_i b_i x^i$ folgt:

$$\begin{aligned}
(\lambda \cdot f)(x) &\overset{\text{Def}}{=} \lambda \cdot \left[\textstyle\sum_i a_i x^i\right] &&\overset{\mathbb{K}}{=} \textstyle\sum_i (\lambda a_i) x^i \\
(f + g)(x) &\overset{\text{Def}}{=} \left[\textstyle\sum_i a_i x^i\right] + \left[\textstyle\sum_i b_i x^i\right] &&\overset{\mathbb{K}}{=} \textstyle\sum_i (a_i + b_i) x^i \\
(f \cdot g)(x) &\overset{\text{Def}}{=} \left[\textstyle\sum_i a_i x^i\right] \cdot \left[\textstyle\sum_j b_j x^j\right] &&\overset{\mathbb{K}}{=} \textstyle\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k
\end{aligned}$$

Wie rechnen wir mit Polynomfunktionen $f, g : \mathbb{K} \to \mathbb{K}$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

g					
b_3x^3	$a_0b_3x^3$	$a_1b_3x^4$	$a_2b_3x^5$	$a_3b_3x^6$	$a_4b_3x^7$
$+$					
b_2x^2	$a_0b_2x^2$	$a_1b_2x^3$	$a_2b_2x^4$	$a_3b_2x^5$	$a_4b_2x^6$
$+$					
b_1x^1	$a_0b_1x^1$	$a_1b_1x^2$	$a_2b_1x^3$	$a_3b_1x^4$	$a_4b_1x^5$
$+$					
b_0x^0	$a_0b_0x^0$	$a_1b_0x^1$	$a_2b_0x^2$	$a_3b_0x^3$	$a_4b_0x^4$
$\cdot$	$a_0x^0 + a_1x^1 + a_2x^2 + a_3x^3 + a_4x^4$				f

$$\left[\sum_i a_i x^i\right] \cdot \left[\sum_j b_j x^j\right]$$
$$= \sum_{(i,j)} a_i x^i \cdot b_j x^j$$
$$= \sum_{(i,j)} a_i b_j x^{i+j} =$$
$$\sum_k \underbrace{\left[\sum_{i+j=k} a_i b_j\right]}_{=:\, c_k} x^k$$

Polynome auswerten durch Einsetzen $X \mapsto x$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz C1D: vom Polynom zur Funktion

Sei $(\mathbb{K}, +, 0, \cdot, 1)$ ein kommutativer Ring, etwa $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots, \mathbb{Z}, \mathbb{Z}_n, \dots$.
Jedes Polynom $P = \sum_{k=0}^{n} p_k X^k \in \mathbb{K}[X]$ definiert seine Polynomfunktion

$$f_P : \mathbb{K} \to \mathbb{K} : x \mapsto P(x) := \sum_{k=0}^{n} p_k x^k.$$

Die Abbildung $\Phi_{\mathbb{K}} : (\mathbb{K}[X], +, 0, \cdot, 1) \to (\mathrm{Poly}(\mathbb{K}, \mathbb{K}), \mathbf{+}, \mathbf{0}, \mathbf{\cdot}, \mathbf{1}) : P \mapsto f_P$
ist surjektiv und ein Ringhomomorphismus: Für alle $P, Q \in \mathbb{K}[X]$ gilt

$$f_{P+Q} = f_P \mathbf{+} f_Q, \qquad f_0 = \mathbf{0} = \mathrm{const}_K^0,$$
$$f_{P \cdot Q} = f_P \mathbf{\cdot} f_Q, \qquad f_1 = \mathbf{1} = \mathrm{const}_K^1.$$

$$f_{P+Q}(x) \overset{\text{Def}}{=} \sum_k (p_k + q_k) x^k \overset{\text{s.o.}}{=} f_P(x) + f_Q(x) \overset{\text{Def}}{=} (f_P \mathbf{+} f_Q)(x)$$
$$f_{P \cdot Q}(x) \overset{\text{Def}}{=} \sum_k \Big(\sum_{i+j=k} (p_i q_j)\Big) x^k \overset{\text{s.o.}}{=} f_P(x) \cdot f_Q(x) \overset{\text{Def}}{=} (f_P \mathbf{\cdot} f_Q)(x)$$

Wo gilt die Methode des Koeffizientenvergleichs, wo nicht?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Für Funktionen $f, g : \mathbb{K} \to \mathbb{K}$ mit $f(x) = \sum_i a_i x^i$ und $g(x) = \sum_i b_i x^i$ gilt:

$$(\forall i \in \mathbb{N} : a_i = b_i) \quad \Longrightarrow \quad f = g$$

Methode des Koeffizientenvergleichs: Gilt umgekehrt auch „$\Longleftarrow$“?

Beispiel C1E: Polynom vs Funktion

Sind $f, g : \mathbb{F}_2 \to \mathbb{F}_2$ mit $f(x) = x^2 + x$ und $g(x) = 0$ verschieden? Nein!
Auf $\mathbb{F}_2 = \{0, 1\}$ gilt $f(0) = 0 = g(0)$ und $f(1) = 0 = g(1)$, also $f = g$.

Polynomring $\mathbb{K}[X]$: intrinsische Definition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition C1G: Polynomring $\mathbb{K}[X]$ in einer Variablen X über $\mathbb{K}$

Sei $(R, +, 0, \cdot, 1)$ ein CRing, $\mathbb{K} \leq R$ ein Teilring und $X \in R$ ein Element. Der Ring $R =: \mathbb{K}[X]$ heißt **Polynomring** in X über $\mathbb{K}$, falls Folgendes gilt:

Jedes Element $P \in R \setminus \{0\}$ schreibt sich eindeutig als Linearkombination $P = p_0 X^0 + p_1 X^1 + \ldots + p_n X^n$ mit $n \in \mathbb{N}$ und $p_0, p_1, \ldots, p_n \in \mathbb{K}$, $p_n \neq 0$.

Dabei ist $\deg(P) := n$ der **Grad** und $\mathrm{lc}(P) := p_n$ der **Leitkoeffizient**.
Für das **Nullpolynom** $P = 0$ setzen wir $\deg(0) := -\infty$ und $\mathrm{lc}(0) := 0$.
Wir schreiben kurz $P = \sum_{i \in \mathbb{N}} p_i X^i$ mit $p_i = 0$ für $i > n$. Damit gilt:

Vergleich:	$\sum_i p_i X^i = \sum_i q_i X^i$ in $\mathbb{K}[X] \iff p_i = q_i$ in $\mathbb{K}$ für alle i
Summe:	$[\sum_i p_i X^i] + [\sum_i q_i X^i] = \sum_i s_i X^i, \quad s_i = p_i + q_i$ in $\mathbb{K}$
Produkt:	$[\sum_i p_i X^i] \cdot [\sum_j q_j X^j] = \sum_k r_k X^k, \; r_k = \sum_{i+j=k} p_i \cdot q_j$

☺ Kurz: $R = \mathbb{K}[X]$ ist eine Kopie des kanonischen Polynomrings $\mathbb{K}^{(\mathbb{N})}$.

Polynomring $\mathbb{K}[X]$: Produkt

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{array}{c|ccccc}
Q & & & & & \\
q_3X^3 & p_0q_3X^3 & p_1q_3X^4 & p_2q_3X^5 & p_3q_3X^6 & p_4q_3X^7 \\
+ & & & & & \\
q_2X^2 & p_0q_2X^2 & p_1q_2X^3 & p_2q_2X^4 & p_3q_2X^5 & p_4q_2X^6 \\
+ & & & & & \\
q_1X^1 & p_0q_1X^1 & p_1q_1X^2 & p_2q_1X^3 & p_3q_1X^4 & p_4q_1X^5 \\
+ & & & & & \\
q_0X^0 & p_0q_0X^0 & p_1q_0X^1 & p_2q_0X^2 & p_3q_0X^3 & p_4q_0X^4 \\
\hline
\cdot & p_0X^0 + p_1X^1 + p_2X^2 + p_3X^3 + p_4X^4 & & & & P
\end{array}
$$

$$
\begin{aligned}
&\left[\textstyle\sum_i p_iX^i\right] \cdot \left[\textstyle\sum_j q_jX^j\right] \\
&= \textstyle\sum_{(i,j)} p_iX^i \cdot q_jX^j \\
&= \textstyle\sum_{(i,j)} p_iq_jX^{i+j} = \\
&\textstyle\sum_k \underbrace{\left[\sum_{i+j=k} p_iq_j\right]}_{=:\, r_k} X^k
\end{aligned}
$$

Rechenregeln für den Polynomgrad

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz C11: Rechenregeln für den Polynomgrad

(1) Bei Addition zweier Polynome P und Q in $\mathbb{K}[X]$ gilt:

$$\deg(P+Q) \leq \max\{\deg P, \deg Q\} \quad \text{in } \mathbb{N} \cup \{-\infty\}$$

Es gilt „<“ nur bei Auslöschung: $\deg P = \deg Q \geq 0$ und $\operatorname{lc} P + \operatorname{lc} Q = 0$.

(2) Bei Multiplikation zweier Polynome P und Q in $\mathbb{K}[X]$ gilt:

$$\deg(P \cdot Q) \leq \deg P + \deg Q \quad \text{in } \mathbb{N} \cup \{-\infty\}$$

Es gilt „<“ nur bei Auslöschung: $\operatorname{lc} P \neq 0 \neq \operatorname{lc} Q$ und $\operatorname{lc} P \cdot \operatorname{lc} Q = 0$.

(3) Ist der Leitkoeffizient $\operatorname{lc} P$ oder $\operatorname{lc} Q$ kürzbar oder null, so gilt:

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

(4) Ist $\mathbb{K}$ ein Integritätsring, so auch $\mathbb{K}[X]$, und (3) gilt allgemein.

Polynomdivision: euklidische Division mit Rest

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{aligned} \mathbb{K}[X]_{<n} &:= \{\, P \in \mathbb{K}[X] \mid \deg P < n \,\} \\ \mathbb{K}[X]_n^\times &:= \{\, P \in \mathbb{K}[X] \mid \deg P = n,\ \operatorname{lc} P \in \mathbb{K}^\times \,\} \end{aligned}$$

Satz C2A: Polynomdivision über jedem kommutativen Ring $\mathbb{K}$

Sei $B \in \mathbb{K}[X]_n^\times$. Jedes Polynom $A \in \mathbb{K}[X]$ schreibt sich eindeutig

$$A = BQ + R \quad \text{mit } Q \in \mathbb{K}[X] \text{ und } R \in \mathbb{K}[X]_{<n}.$$

Dies definiert $Q =: A \operatorname{quo} B$ und $R =: A \operatorname{rem} B$.

Polynomdivision: euklidische Division mit Rest

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Dividiere $A = 2X^4 - 5X^3 + 2X^2 - 9X + 8$ durch $B = X^2 - 3X$.

$$
\begin{array}{rrrrrl}
2X^4 & -5X^3 & +2X^2 & -9X & +8 & = \left(X^2 - 3X\right)\left(2X^2 + X + 5\right) + 6X + 8 \\
-2X^4 & +6X^3 & & & & \\
\hline
 & X^3 & +2X^2 & & & \\
 & -X^3 & +3X^2 & & & \\
\hline
 & & 5X^2 & -9X & & \\
 & & -5X^2 & +15X & & \\
\hline
 & & & 6X & +8 &
\end{array}
$$

Polynomdivision: euklidische Division mit Rest

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Algo C2A: Division mit Rest in $\mathbb{K}[X]$

Eingabe: $A, B \in \mathbb{K}[X]$ mit $\operatorname{lc} B \in \mathbb{K}^\times$

Ausgabe: $Q, R \in \mathbb{K}[X]$ mit $A = BQ + R$ und $\deg R < \deg B$

1: $Q \leftarrow 0;\ R \leftarrow A$ // Invariante: Es gilt $A = BQ + R$

2: **while** $\deg R \geq \deg B$ **do** // Solange noch etwas zu tun ist

3: $\quad T \leftarrow \operatorname{lc}(B)^{-1} \operatorname{lc}(R) \cdot X^{\deg R - \deg B}$ // $\deg(BT) = \deg R$, $\operatorname{lc}(BT) = \operatorname{lc} R$

4: $\quad R \leftarrow R - BT;\ Q \leftarrow Q + T$ // Invariante: Es gilt $A = BQ + R$

5: **return** (Q, R) // $A = BQ + R$ und $\deg R < \deg B$

Beweis: Dieser Algorithmus ist korrekt, erfüllt also seine Spezifikation:

(1) Der Algorithmus terminiert, denn $\deg R$ sinkt in jeder Iteration.

(2) Die Ausgabe (Q, R) erfüllt $A = BQ + R$ und $\deg R < \deg B$. QED

Wie finden wir alle rationalen Nullstellen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Das Polynom $15X - 10$ hat die Nullstelle $x = 2/3$. Der Zähler 2 teilt den Grundkoeffizienten 10, der Nenner 3 den Leitkoeffizienten 15.

Beispiel: Das Polynom $12X^2 - 11X - 5$ hat die Nullstellen $x_1 = -1/3$ und $x_2 = 5/4$. Für beide gilt: Der Zähler teilt -5, der Nenner teilt 12.

Aufgabe: Finden Sie *alle* rationalen Nullstellen von $7X^3 - 4X^2 + 4X + 3$.

Lösung: Wir probieren alle $x = a/b \in \mathbb{Q}$ mit $a \in \{\pm 1, \pm 3\}$ und $b \in \{1, 7\}$. Unter diesen acht Kandidaten finden wir genau eine Nullstelle: $x = -3/7$.

Satz C2B: die rationalen Nullstellen eines ganzzahligen Polynoms

Sei $P = p_0 + p_1 X + \ldots + p_n X^n \in \mathbb{Z}[X]$ und $x = a/b \in \mathbb{Q}$ gekürzt, also $a, b \in \mathbb{Z}$, $b > 0$ und $\mathrm{ggT}(a, b) = 1$. Aus $P(x) = 0$ folgt $a \mid p_0$ und $b \mid p_n$.

Beweis: Sei $c := P(a/b)\, b^n = p_0 a^0 b^n + p_1 a^1 b^{n-1} + \ldots + p_n a^n b^0$.
Aus $c = 0$ folgt $a \mid c$ und $b \mid c$, also $a \mid p_0 b^n$ und $b \mid p_n a^n$.
Dank Lemma von Euklid B3I folgt $a \mid p_0$ und $b \mid p_n$. QED

Nullstellen und Vielfachheiten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz C2c: Nullstelle als Linearfaktor abspalten

Sei $\mathbb{K}$ ein CRing, $a \in \mathbb{K}$ ein Element und $P \in \mathbb{K}[X]^*$ ein Polynom.
(0) Genau dann gilt $P(a) = 0$, wenn $P = (X - a)Q$ für ein $Q \in \mathbb{K}[X]^*$.

Beweis: (0) Die Implikation „$\Leftarrow$“ ist klar. Interessant ist vor allem „$\Rightarrow$“: Polynomdivision C2A ergibt $P = (X - a)Q + R$ mit Quotient $Q \in \mathbb{K}[X]$ und Rest $R \in \mathbb{K}[X]_{<1} = \mathbb{K}$. Folglich verschwindet $P(a) = R$ gdw $R = 0$.

Satz C2c: Vielfachheit $m = \operatorname{ord}(P, a)$ einer Stelle $a \in \mathbb{K}$ zu $P \in \mathbb{K}[X]^*$

(1) Es gilt $P = (X - a)^m Q$ für genau ein $(m, Q) \in \mathbb{N} \times \mathbb{K}[X]$ mit $Q(a) \neq 0$.

Nullstellen und Vielfachheiten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz C2c: Faktorisierung aller Nullstellen

(2) Jedes Polynom $P \in \mathbb{K}[X]_n$ vom Grad $n = \deg(P) \in \mathbb{N}$ faktorisiert zu

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$$

mit $\{a_1, \ldots, a_k\}^! \subseteq \mathbb{K}$ und $m_1, \ldots, m_k \geq 1$ und $Q(a) \neq 0$ für alle $a \in \mathbb{K}$.
Extremfall: Gilt $Q \in \mathbb{K}^*$, so **zerfällt** P über $\mathbb{K}$ in Linearfaktoren.

—

Im Folgenden sei $\mathbb{K}$ ein Integritätsring.

(3) In diesem Falle sind $a_1, \ldots, a_k$ die einzigen Nullstellen von P.

(4) Dank $n \geq m_1 + \ldots + m_k$ hat P höchstens n Nullstellen in $\mathbb{K}$.

(5) Je zwei Polynome $P, Q \in \mathbb{K}[X]_{\leq n}$ sind bereits dann gleich, wenn sie an $n + 1$ Stellen $x_0, x_1, \ldots, x_n \in \mathbb{K}$ übereinstimmen.

Beweis: (5) $P - Q \in \mathbb{K}[X]_{\leq n}$ hat $n + 1$ Nullstellen, also $P - Q = 0$.

Geometrische Anwendung: Nullstellen zählen!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel C2D: Wie viele Nullstellen?

In $\mathbb{Q}$ hat $X^2 - 2$ keine Nullstelle, über $\mathbb{R}$ gilt $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$.
In $\mathbb{Z}$ hat $X^2 - 1 = (X - 1)(X + 1)$ genau zwei Nullstellen, nämlich ± 1.
Warnung: Im Ring $\mathbb{Z}_8$ hat $X^2 - 1$ vier (!) Nullstellen, nämlich $1, 3, 5, 7$.

Korollar C2E: Methode des Koeffizientenvergleichs

Sei $(\mathbb{K}, +, 0, \cdot, 1)$ ein kommutativer Ring. Für je zwei Polynomfunktionen $f, g : \mathbb{K} \to \mathbb{K}$, gegeben durch $f(x) = \sum_{i=0}^{n} f_i x^i$ und $g(x) = \sum_{i=0}^{n} g_i x^i$, gilt

$$(\forall i \in \mathbb{N} : f_i = g_i) \quad \Longrightarrow \quad f = g, \text{ d.h. } f(x) = g(x) \text{ für alle } x \in \mathbb{K}.$$

Die ersehnte Umkehrung „$\Leftarrow$“ gilt für jeden Integritätsring $\mathbb{K}$ mit $\sharp\mathbb{K} > n$, etwa unendliche Körper wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$ oder unendliche IRinge wie $\mathbb{Z}$.

Lagrange–Interpolation: Polynome durch Stützpunkte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

? Wir suchen Polynome $P \in \mathbb{K}[X]_{\leq n}$ mit $P(x_0) = y_0, \ldots, P(x_n) = y_n$.

Hierzu sei $\mathbb{K}$ ein Körper, etwa $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \ldots$, und $n \in \mathbb{N}$. Gegeben sind $n+1$ verschiedene Stützstellen $x_0, \ldots, x_n \in \mathbb{K}$ und Werte $y_0, \ldots, y_n \in \mathbb{K}$.

Aufgabe: Wie viele Lösungen gibt es? Konstruieren Sie alle!

Lösung: Dank Satz C2c(5) gibt es *höchstens* eine Lösung. Konstruktion:

$$L_i(X) := \prod_{k \neq i} \frac{X - x_k}{x_i - x_k} \quad = \quad \frac{X - x_0}{x_i - x_0} \cdots \cancel{\frac{X - x_i}{x_i - x_i}} \cdots \frac{X - x_n}{x_i - x_n} \in \mathbb{K}[X]_n.$$

Diese Basispolynome erfüllen $L_i(x_i) = 1$ und $L_i(x_j) = 0$ für $j \neq i$.

$$L(X) := \textstyle\sum_{i=0}^{n} y_i L_i(X) \quad = \quad y_0 L_0(X) + \ldots + y_n L_n(X) \in \mathbb{K}[X]_{\leq n}.$$

Dieses Polynom L erfüllt $L(x_j) = y_j$ für alle $j = 0, \ldots, n$, wie gewünscht.

Lagrange–Interpolation: Polynome durch Stützpunkte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz C2F: Polynomauswertung und Lagrange–Interpolation

Sei $(\mathbb{K}, +, \cdot)$ ein Körper und $x_0, \dots, x_n \in \mathbb{K}$ paarweise verschieden. Auswertung und Interpolation sind zueinander inverse Bijektionen

$$(\pi, \iota) : \mathbb{K}[X]_{\leq n} \cong \mathbb{K}^{n+1}, \qquad \begin{aligned} \pi &: P \mapsto (P(x_0), \dots, P(x_n)), \\ \iota &: y \mapsto y_0 L_0 + \dots + y_n L_n, \end{aligned}$$

Zusammenfassung: Polynom vs Polynomfunktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz C2G: Polynom vs Polynomfunktion

Sei $\mathbb{K}$ ein Körper. Jedes Polynom $P = \sum_{i=0}^{n} p_i X^i \in \mathbb{K}[X]$ definiert seine zugehörige Polynomfunktion $f_P : \mathbb{K} \to \mathbb{K} : a \mapsto P(x) := \sum_{i=0}^{n} p_i x^i$.

Dies stiftet den Ringhomomorphismus $\Phi_{\mathbb{K}} : \mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}} : P \mapsto f_P$ (C1D).

1. Ist $\mathbb{K}$ unendlich, dann ist $\Phi_{\mathbb{K}}$ injektiv (C2E), aber nicht surjektiv (C230).
2. Ist $\mathbb{K}$ endlich, dann ist $\Phi_{\mathbb{K}}$ surjektiv (C2F), aber nicht injektiv (C1E).

Arithmetik in $\mathbb{Z}$ und in $\mathbb{K}[X]$ – erfreulich ähnlich

Ring $\mathbb{Z}$ der ganzen Zahlen	Polynomring $\mathbb{K}[X]$ über dem Körper $\mathbb{K}$
Stellensystem $n = \pm \sum_{i=0}^{\ell-1} n_i B^i$	Monomdarstellung $P = \sum_{i=0}^{n} p_i X^i$
$a = bq + r$ mit $0 \leq r < \lvert b \rvert$	$A = BQ + R$ mit $\deg R < \deg B$

B3E ←	ggT: Algorithmen von Euklid & Bézout	→ C3E
B3I ←	Lemma von Euklid: unzerlegbar = prim	→ C3I
B3J ←	faktoriell: eindeutige Primfaktorzerlegung	→ C3J

B3M ←	Restring $\mathbb{Z}_n \cong \mathbb{Z}/n$	Restring $\mathbb{K}[X]_P \cong \mathbb{K}[X]/P$	→ C3M
B3M ←	Körper gdw n prim	Körper gdw P prim	→ C3M

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Der Restring $\mathbb{K}[X]_p$ – informatische Sichtweise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: (1) Ist $p = X^2 - 2$ in $\mathbb{Q}[X]$ un/zerlegbar?

Lösung: (1) Wäre p in $\mathbb{Q}[X]$ zerlegbar, dann wäre $p = (X - \lambda)(X + \lambda)$ mit $\lambda \in \mathbb{Q}$. Dann wäre $0 = p(\lambda) = \lambda^2 - 2$. Das ist jedoch für $\lambda \in \mathbb{Q}$ unmöglich.

Aufgabe: (2) Wie rechnen Sie mit Resten modulo $p = X^2 - 2$ in $\mathbb{Q}[X]$?

$$R = \mathbb{Q}[X]_p := \mathbb{Q}[X]_{<2} = \{ u = a + bX \mid a, b \in \mathbb{Q} \}^!$$

Lösung: (2) Für $X \in R$ gilt $X \cdot X = (X^2 - 2) \cdot 1 + 2$, kurz $X \cdot_p X = 2$.

$$\begin{aligned} \text{Summe:} \quad (a + bX) + (a' + b'X) &= (a + a') + (b + b')X \\ \text{Produkt:} \quad (a + bX) \cdot_p (a' + b'X) &= (aa' + 2bb') + (ab' + ba')X \end{aligned}$$

☺ Das sind exakt die Rechenregeln des Körpers $\mathbb{Q}[\sqrt{2}]$!

$$\begin{aligned} \text{Summe:} \quad (a + b\sqrt{2}) + (a' + b'\sqrt{2}) &= (a + a') + (b + b')\sqrt{2} \\ \text{Produkt:} \quad (a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) &= (aa' + 2bb') + (ab' + ba')\sqrt{2} \end{aligned}$$

Der Restring $\mathbb{K}[X]_p$ – informatische Sichtweise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Statt im Polynomring $P = \mathbb{K}[X]$ rechnen wir mit Resten in $R = \mathbb{K}[X]_{<n}$:

$$\begin{tikzcd} P \times P \arrow[r, "+", "(a,b)\mapsto a+b"'] \arrow[d, two heads, "\rho"'] \arrow[dr, phantom, "="] & P \arrow[d, two heads, "\rho"'] \\ R \times R \arrow[r, "+", "(r,s)\mapsto r+s"'] & R \end{tikzcd} \qquad \begin{tikzcd} P \times P \arrow[r, "\cdot", "(a,b)\mapsto a\cdot b"'] \arrow[d, two heads, "\rho"'] \arrow[dr, phantom, "="] & P \arrow[d, two heads, "\rho"'] \\ R \times R \arrow[r, "\cdot_p", "(r,s)\mapsto (r\cdot s) \operatorname{rem} p"'] & R \end{tikzcd}$$

Satz C3M: Konstruktion des Restrings $\mathbb{K}[X]_p := (\mathbb{K}[X]_{<n}, +, 0, \cdot_p, 1)$

Sei $\mathbb{K}$ ein CRing, $p \in \mathbb{K}[X]_n^1$ normiert vom Grad $n \geq 1$ und $\rho(a) = a \operatorname{rem} p$.

(0) Für alle $a, b \in P$ gilt $\rho(a + b) = \rho(a) + \rho(b)$ und $\rho(a \cdot b) = \rho(a) \cdot_p \rho(b)$.

(1) Daher ist auch $\mathbb{K}[X]_p$ ein CRing. Nach Konstruktion gilt $\mathbb{K} \leq \mathbb{K}[X]_p$.

Im Folgenden sei $\mathbb{K}$ ein Körper.

(2) Genau dann ist $a \in \mathbb{K}[X]_p$ invertierbar, wenn $\operatorname{ggT}(a, p) = 1$ gilt.
Explizite Inversion dank Bézout: $au + pv = 1$ bedeutet $au \operatorname{rem} p = 1$.

(3) Genau dann ist $\mathbb{K}[X]_p$ ein Körper, wenn p in $\mathbb{K}[X]$ prim ist.

Ausblick: Wie konstruieren wir endliche Körper?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: (1) Wie konstruieren Sie einen Körper $\mathbb{F}_p$ mit $p \in \mathbb{P}$ Elementen?
(2) Wie konstruieren Sie einen Körper $\mathbb{F}_q$ mit $q = p^d$ Elementen, $d \in \mathbb{N}_{\geq 2}$?
(3) Führen Sie dies explizit aus für $q = 4$, also $p = 2$ und $d = 2$.

Lösung: (1) Der Restring $\mathbb{F}_p := \mathbb{Z}_p$ ist ein Körper (B3M) mit p Elementen.

(2) Wir finden / wählen ein Primpolynom $G \in \mathbb{F}_p[X]_d^1$. Der Restring $\mathbb{F}_q := \mathbb{F}_p[X]_G = \mathbb{F}_p[X]_{<d}$ ist dann ein Körper (C3M) und hat p^d Elemente.

(3) Für $\mathbb{F}_4 = \mathbb{F}_2[X]_G$ suchen wir $G = X^2 + aX + b \in \mathbb{F}_2[X]_2^1$ prim. Das ist äquivalent zu unzerlegbar (Euklid C3I). Von den vier Kandidaten sind drei zerlegbar: $X^2 = X \cdot X$, $X^2 + X = X(X+1)$, $X^2 + 1 = (X+1)(X+1)$.

Unsere letzte Hoffnung $G = X^2 + X + 1$ ist unzerlegbar! Andernfalls wäre $G = (X-a)(X-b)$ mit $a, b \in \mathbb{F}_2$, es gilt jedoch $G(0) = 1$ und $G(1) = 1$.

Beispiel C3N: der Körper $\mathbb{F}_4$

Dank Satz C3M ist $\mathbb{F}_4 := \mathbb{F}_2[X]_{X^2+X+1}$ ein / der Körper mit vier Elementen.

Ausblick: Wie konstruieren wir endliche Körper?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Explizit erhalten wir $\mathbb{F}_4 = \mathbb{F}_2[X]_{<2} = \{\, 0,\ 1,\ X,\ X+1 =: Y \,\}$ mit:

$+$	0	1	X	Y
0	0	1	X	Y
1	1	0	Y	X
X	X	Y	0	1
Y	Y	X	1	0

$\cdot_G$	0	1	X	Y
0	0	0	0	0
1	0	1	X	Y
X	0	X	Y	1
Y	0	Y	1	X

Satz C30: Klassifikation aller endlichen Körper – Ausblick

(1) Jeder endliche Körper $\mathbb{F}$ hat p^d Elemente, wobei $p \in \mathbb{P}$ und $d \in \mathbb{N}_{\geq 1}$.
(2) Zu jedem Paar $(p, d) \in \mathbb{P} \times \mathbb{N}_{\geq 1}$ existieren Körper mit p^d Elementen.
(3) Je zwei endliche Körper mit gleicher Elementezahl p^d sind isomorph.

Rückblick: praktische Beispiele, Fragen, Anwendungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Frage C4A: Was sind und was können Polynome?

Wie berechnen Sie Wahrscheinlichkeiten von Würfelsummen?

Wie gelingt das Rechnen mit physikalischen Einheiten?

Wie erklären Sie Polynome und das Rechnen damit?

(1) Sind $f, g : \mathbb{F}_2 \to \mathbb{F}_2$ mit $f(x) = x^2 + x$ und $g(x) = 0$ verschieden?

(2) Wie viele Nullstellen hat $P = \sum_{k=0}^{n} p_k X^k$ über $\mathbb{Q}, \mathbb{R}, \mathbb{C}$?

(3) Haben auch Polynome eine eindeutige Primzerlegung?

(4) Wie konstruieren Sie einen Körper mit 4 Elementen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel C

Bonusmaterial

Give someone a fish, and you feed them for a day.
Teach them to fish, and they can eat for a lifetime.

Anne Isabella Thackeray Ritchie (1837–1919)

Inhalt dieses Kapitels C

5 Arithmetik: Polynome als Ring mit Gradfunktion

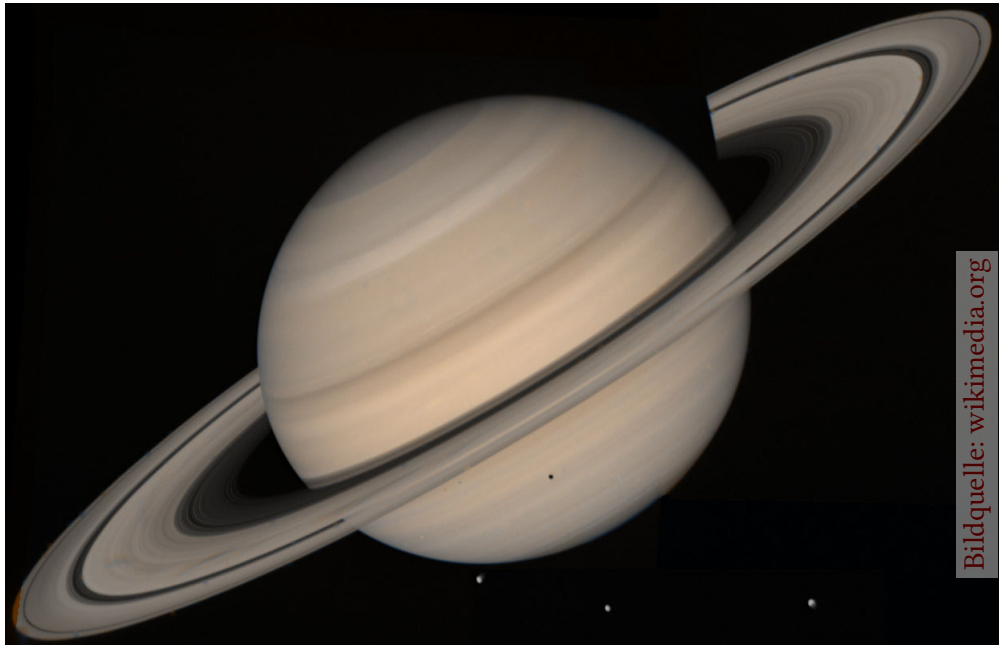
6 Fehlerkorrigierende Codes nach Reed–Solomon

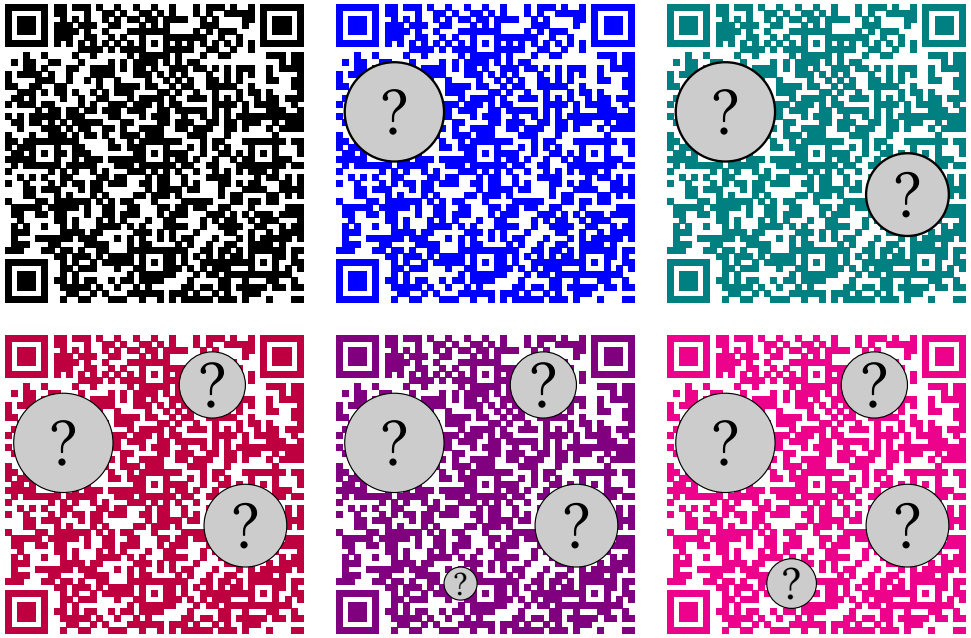
7 Rechnen mit formalen Potenzreihen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Fehlerkorrigierende Codes





Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Fehlererkennende Codes

Alice möchte ein **Wort** $t = (t_0, \dots, t_{k-1}) \in \mathbb{F}_2^k$ an Bob übertragen.
Wir interpretieren t als Polynom $T = t_0 + t_1 X + \dots + t_{k-1} X^{k-1} \in \mathbb{F}_2[X]_{<k}$.

Alice sendet $s \in \mathbb{F}_2^n$, interpretiert als $S = s_0 + s_1 X + \dots + s_{n-1} X^{n-1}$.
Ein gestörtes Bit an der Stelle i führt zum Empfang von $S' = S + X^i$.
Wie kann Bob diesen einzigen Bitfehler erkennen? gar korrigieren?

(1) Alice sendet t zweimal, also $S = T + X^k T$ mit Länge $n = 2k$.
So kann Bob einen Bitfehler *erkennen*, leider noch nicht *korrigieren*.

(2) Sparsamer ist das **Paritätsbit** $T(1) = t_0 + t_1 + \dots + t_{k-1} \in \mathbb{F}_2$.
Alice überträgt $S = T(1) + X^1 T$, also $S(1) = 0$, Länge $n = k + 1$.

Dies ist nur die Saalversion ohne Erläuterungen.
Ausführliche Erläuterungen bietet die Vollversion.

Fehlerkorrigierende Codes nach Reed–Solomon

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Alice möchte ein Wort $t \in \mathbb{F}_2^k$ von $k = 120$ Bits so geschickt übermitteln, dass Bob einen Bitfehler nicht nur *erkennen*, sondern *korrigieren* kann.

(3) Alice sendet t dreimal, also $S = T + X^k T + X^{2k} T$, Länge $n = 3k = 360$.

(4) Besser: Alice sendet zweimal $S = T(1) + X^1 T$, Länge $n = 2k + 2 = 242$.

(5) Einfach-genial: Wir nutzen das Polynom $G = X^7 + X^3 + 1 \in \mathbb{F}_2[X]$.
Alice berechnet $R = X^7 T \operatorname{rem} G$ und sendet $S = R + X^7 T$, Länge $n = 127$.

Es gilt $S \operatorname{rem} G = 0$. Für $i \in \{0, \dots, 126\}$ ist $i \mapsto X^i \operatorname{rem} G$ injektiv und $\neq 0$.
So kann Bob einen Bitfehler $S' = S + X^i$ dank $R' = S' \operatorname{rem} G$ korrigieren!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel D

Matrixkalkül und Gauß–Algorithmus

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 2 & 4 & 3 \\ -4 & 2 & 3 & -4 \\ 2 & -2 & -5 & 1 \end{bmatrix}$$

$$A \cdot B = \begin{bmatrix} -1 & 0 & -5 & -2 \\ -4 & 6 & 1 & -2 \end{bmatrix}$$

Matrix theory is the arithmetic of advanced mathematics.
Richard Bellman (1920–1984), *Eye of the Hurricane*

Inhalt dieses Kapitels D

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

1 Mit Matrizen können wir rechnen.

2 Der Gauß–Algorithmus über einem Divisionsring

3 Fazit: Matrixkalkül und Gauß–Algorithmus

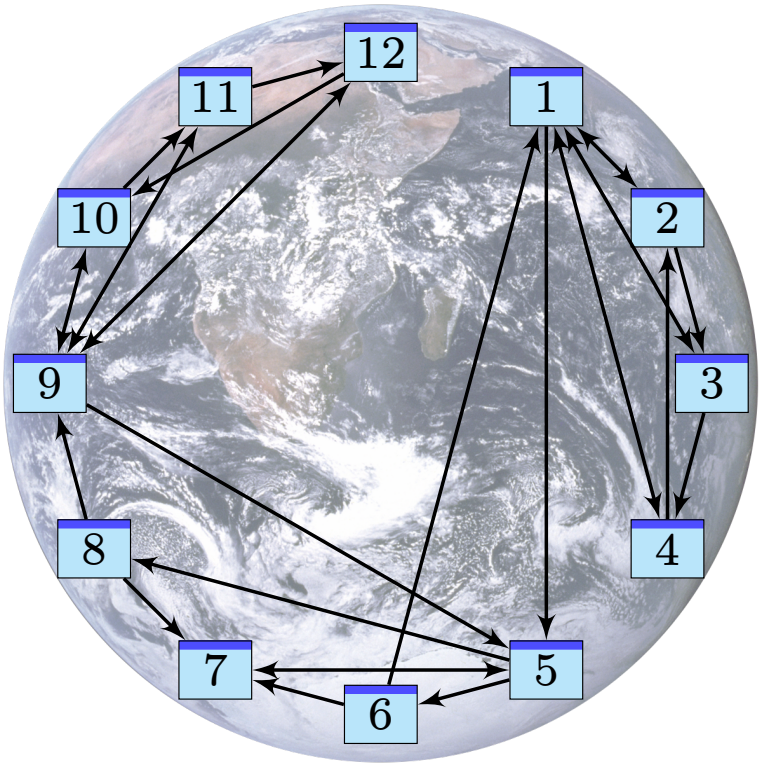
Matrizen und lineare Gleichungssysteme sind überall!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel D0A: die Milliarden-Dollar-Gleichung, Googles PageRank

Wie bewertet Google die „Relevanz“ oder „Popularität“ von Webseiten?



PageRank $\quad p_i = \dfrac{q}{n} + \sum_{j \to i} \dfrac{1-q}{\ell_j} p_j$

Vorschau: praktische Beispiele, Fragen, Anwendungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Frage D0B: segensreicher Matrixkalkül

(0) Wie erklären Sie Matrizen $\mathbb{K}^{m\times n}$ und das Rechnen damit?

(1) Ist jede invertierbare Matrix quadratisch?

(2) Wie bringen Sie jede Matrix A in Zeilenstufenform dank Gauß?

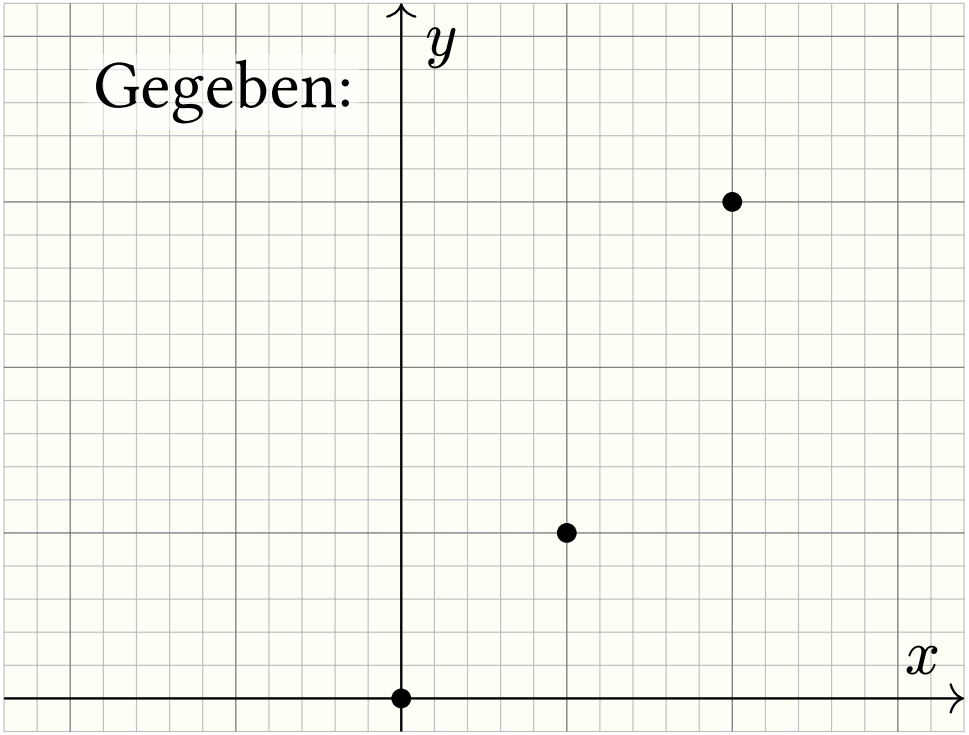
(3) Wie lösen Sie damit jedes lineare Gleichungssystem $Ax = b$?

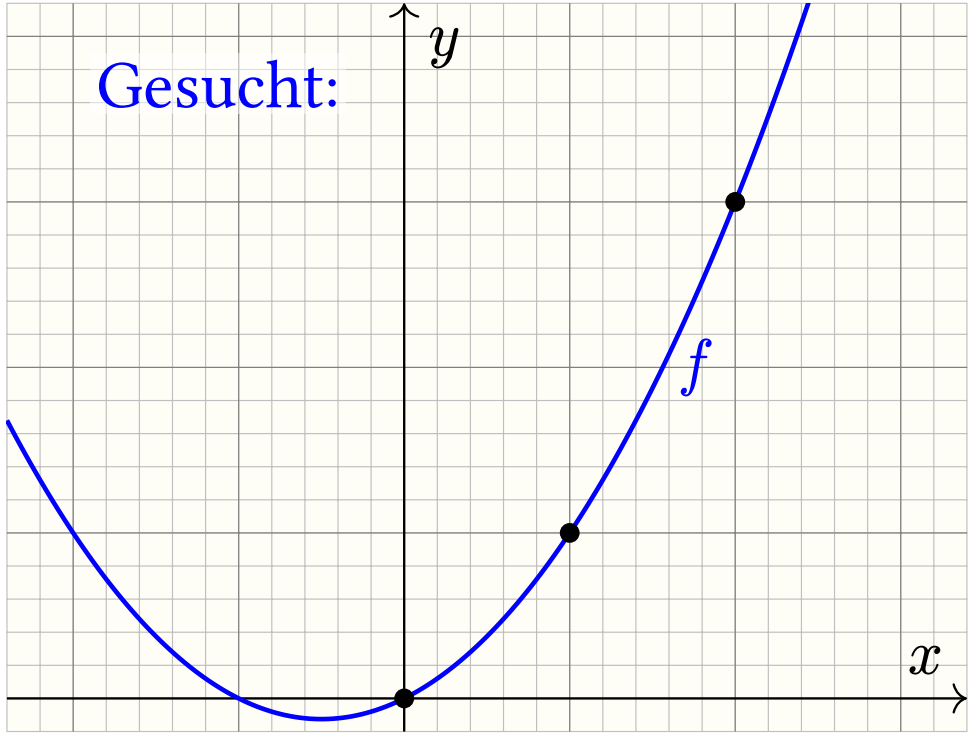
(4) Wie invertieren Sie A zu B mit $AB = 1$ und $BA = 1$?

Geometrisches Beispiel: Kurve durch Datenpunkte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Aufgabe: Finden Sie alle Polynomfunktionen

$$f : \mathbb{R} \to \mathbb{R} : f(x) = ax^2 + bx + c \quad \text{mit } a, b, c \in \mathbb{R},$$

die durch diese Punkte laufen, $f(0) = 0$ und $f(1) = 1$ und $f(2) = 3$.

Zweite Lösung: dank Gauß–Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Ansatz: $f(x) = ax^2 + bx + c$

$$
\begin{array}{lcll}
f(0) = 0 & \Leftrightarrow & R_1: & 0 \cdot a + 0 \cdot b + 1 \cdot c = 0 \\
f(1) = 1 & \Leftrightarrow & R_2: & 1 \cdot a + 1 \cdot b + 1 \cdot c = 1 \\
f(2) = 3 & \Leftrightarrow & R_3: & 4 \cdot a + 2 \cdot b + 1 \cdot c = 3
\end{array}
$$

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.

Dies sind Äquivalenzumformungen!

Zweite Lösung: dank Gauß–Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{array}{ll}
R_1 & \\
R_2 & \\
R_3 &
\end{array}
\quad
\boxed{\begin{array}{rcrcrcr}
 & & & & c & = & 0 \\
a & + & b & + & c & = & 1 \\
4a & + & 2b & + & c & = & 3
\end{array}}
$$

$$
\begin{array}{ll}
R_1 \leftrightarrow R_2 & \\
R_2 \leftrightarrow R_1 & \\
R_3 &
\end{array}
\quad
\boxed{\begin{array}{rcrcrcr}
a & + & b & + & c & = & 1 \\
 & & & & c & = & 0 \\
4a & + & 2b & + & c & = & 3
\end{array}}
$$

$$
\begin{array}{ll}
R_1 & \\
R_2 & \\
R_3 \leftarrow R_3 - 4R_1 &
\end{array}
\quad
\boxed{\begin{array}{rcrcrcr}
a & + & b & + & c & = & 1 \\
 & & & & c & = & 0 \\
 & - & 2b & - & 3c & = & -1
\end{array}}
$$

$$
\begin{array}{ll}
R_1 & \\
R_2 \leftrightarrow R_3 & \\
R_3 \leftrightarrow R_2 &
\end{array}
\quad
\boxed{\begin{array}{rcrcrcr}
a & + & b & + & c & = & 1 \\
 & - & 2b & - & 3c & = & -1 \\
 & & & & c & = & 0
\end{array}}
$$

Zweite Lösung: dank Gauß–Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{array}{ll}
R_1 & \\
R_2 & \\
R_3 &
\end{array}
\quad
\boxed{\begin{array}{rcrcrcr}
a & + & b & + & c & = & 1 \\
 & - & 2b & - & 3c & = & -1 \\
 & & & & c & = & 0
\end{array}}
$$

$$
\begin{array}{ll}
R_1 & \\
R_2 \leftarrow -{}^1\!/_2 R_2 & \\
R_3 &
\end{array}
\quad
\boxed{\begin{array}{rcrcrcr}
a & + & b & + & c & = & 1 \\
 & & b & + & {}^3\!/_2 c & = & {}^1\!/_2 \\
 & & & & c & = & 0
\end{array}}
$$

$$
\begin{array}{ll}
R_1 \leftarrow R_1 - R_2 & \\
R_2 & \\
R_3 &
\end{array}
\quad
\boxed{\begin{array}{rcrcrcr}
a & & & - & {}^1\!/_2 c & = & {}^1\!/_2 \\
 & & b & + & {}^3\!/_2 c & = & {}^1\!/_2 \\
 & & & & c & = & 0
\end{array}}
$$

$$
\begin{array}{ll}
R_1 \leftarrow R_1 + {}^1\!/_2 R_3 & \\
R_2 \leftarrow R_2 - {}^3\!/_2 R_3 & \\
R_3 &
\end{array}
\quad
\boxed{\begin{array}{rcrcrcr}
a & & & & & = & {}^1\!/_2 \\
 & & b & & & = & {}^1\!/_2 \\
 & & & & c & = & 0
\end{array}}
$$

Was ist eine Matrix?

Sei $(\mathbb{K}, +, 0, \cdot, 1)$ ein Ring, etwa $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \dots, \mathbb{Z}, \mathbb{Z}_n, \mathbb{H}, \dots$.

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Definition D1A: die Menge $\mathbb{K}^{m\times n}$ der $m \times n$–Matrizen über $\mathbb{K}$

Als Indexmengen nutzen wir $I = \{1, 2, \dots, m\}$ und $J = \{1, 2, \dots, n\}$.
Eine **Matrix** A der Größe $m \times n$ über $\mathbb{K}$ ist eine Abbildung

$$A : I \times J \to \mathbb{K} : (i, j) \mapsto A(i, j) = A_{i,j} = A_{ij} = a_{i,j} = a_{ij}.$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Matrixkalkül: Transposition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \iff A^\mathsf{T} = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$$

$$\underbrace{S = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}}_{\text{symmetrisch}}, \qquad \underbrace{A = \begin{bmatrix} 0 & 4 & 0 \\ -4 & 0 & -2 \\ 0 & 2 & 0 \end{bmatrix}}_{\text{antisymmetrisch}}, \qquad \underbrace{T = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}}_{\text{weder noch}}$$

Matrixkalkül: Einheitsmatrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

In dieser Schreibweise ist $u \in \mathbb{K}^{1\times n}$ ein **Zeilenvektor** mit n Spalten, und entsprechend ist $v \in \mathbb{K}^{m\times 1}$ ein **Spaltenvektor** mit m Zeilen.

$$A = \begin{bmatrix} — u_1 — \\ \vdots \\ — u_m — \end{bmatrix} = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix}, \quad A^\top = \begin{bmatrix} | & & | \\ u_1^\top & \cdots & u_m^\top \\ | & & | \end{bmatrix} = \begin{bmatrix} — v_1^\top — \\ \vdots \\ — v_n^\top — \end{bmatrix}$$

$$= (u_1; \dots; u_m) = (v_1, \dots, v_n), \qquad = (u_1^\top, \dots, u_m^\top) = (v_1^\top; \dots; v_n^\top)$$

Die **Einheitsmatrix** oder **Identitätsmatrix** der Größe $n \times n$ ist

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} =: 1_{n\times n} = I_n = E_n \quad \text{mit} \quad e_{ij} = \delta_{ij} := \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Sie hat als Spalten die **Spalten-Einheitsvektoren** $e_1, \dots, e_n \in \mathbb{K}^{n\times 1}$, und als Zeilen die **Zeilen-Einheitsvektoren** $e_1^\top, \dots, e_n^\top \in \mathbb{K}^{1\times n}$.

Matrixkalkül: Addition von Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 0 & 2 & 0 \\ 2 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 1+0 & 2+2 & 3+0 \\ 4+2 & 5+0 & 6+3 \end{bmatrix} = \begin{bmatrix} 1 & 4 & 3 \\ 6 & 5 & 9 \end{bmatrix}$$

$$\mathbf{0} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \qquad - \begin{bmatrix} 0 & 1 & -2 \\ 3 & -5 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 2 \\ -3 & 5 & 0 \end{bmatrix}$$

Satz D1B: Die Matrixaddition bildet eine Gruppe.

Wir definieren die **Matrixaddition** koeffizientenweise:

$$+ : \mathbb{K}^{m\times n} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n} : (A, B) \mapsto C = A + B, \quad c_{ij} = a_{ij} + b_{ij}$$

Die Matrizen bilden damit eine kommutative Gruppe $(\mathbb{K}^{m\times n}, +, \mathbf{0}, -)$.

Matrixkalkül: Addition von Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(A0)	$A + B = B + A,$	(A2)	$A + \mathbf{0} = A,$
(A1)	$(A + B) + C = A + (B + C),$	(A3)	$A + (-A) = \mathbf{0}.$

$$(A + B)_{ij} \overset{\text{Def}}{=} a_{ij} + b_{ij}$$
$$(B + A)_{ij} \overset{\text{Def}}{=} b_{ij} + a_{ij}$$

Matrixkalkül: Multiplikation mit Skalaren

$$2 \bullet \begin{bmatrix} 1 & 3 & 4 \\ 3 & 4 & 0 \end{bmatrix} = \begin{bmatrix} 2 \cdot 1 & 2 \cdot 3 & 2 \cdot 4 \\ 2 \cdot 3 & 2 \cdot 4 & 2 \cdot 0 \end{bmatrix} = \begin{bmatrix} 2 & 6 & 8 \\ 6 & 8 & 0 \end{bmatrix}$$

Satz D1c: Skalierung von links

Wir definieren die **Skalierung** / Skalarmultiplikation von links:

$$\bullet : \mathbb{K} \times \mathbb{K}^{m \times n} \to \mathbb{K}^{m \times n} : (\lambda, A) \mapsto B = \lambda \bullet A, \quad b_{ij} = \lambda \cdot a_{ij}$$

Für alle Matrizen $A, B \in \mathbb{K}^{m \times n}$ und Skalare $\lambda, \mu \in \mathbb{K}$ gilt:

(L1)	$1 \bullet A = A,$	(L3)	$(\lambda + \mu) \bullet A = (\lambda \bullet A) \boldsymbol{+} (\mu \bullet A),$
(L2)	$(\lambda \cdot \mu) \bullet A = \lambda \bullet (\mu \bullet A),$	(L4)	$\lambda \bullet (A \boldsymbol{+} B) = (\lambda \bullet A) \boldsymbol{+} (\lambda \bullet B).$

Somit ist $(\mathbb{K}^{m \times n}, \boldsymbol{+}, \bullet)$ ein **linkslinearer Raum** über $(\mathbb{K}, +, \cdot)$.

Dies ist nur die Saalversion ohne Erläuterungen.
Ausführliche Erläuterungen bietet die Vollversion.

Anwendungsbeispiele: Zeilenvektor mal Spaltenvektor

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Im Lostopf $\Omega = \{1, \dots, n\}$ liegen die Lose $i = 1, \dots, n$ mit ihren Wahrscheinlichkeiten $u = (u_1, \dots, u_n)$ und Auszahlungen $v = (v_1; \dots; v_n)$.

Aufgabe: Wie berechnen Sie den erwarteten Gewinn einer Ziehung?

$$\begin{bmatrix} u_1 & \dots & u_n \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = u_1 \cdot v_1 + \dots + u_n \cdot v_n$$

Matrixkalkül: Multiplikation von Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$B = \begin{bmatrix} 1 & 2 & 4 & 3 \\ -4 & 2 & 3 & -4 \\ 2 & -2 & -5 & 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \qquad A \cdot B = \begin{bmatrix} -1 & 0 & -5 & -2 \\ -4 & 6 & 1 & -2 \end{bmatrix}$$

Definition D1D: Matrixmultiplikation

$$\cdot : \mathbb{K}^{p\times q} \times \mathbb{K}^{q\times r} \to \mathbb{K}^{p\times r} : (A, B) \mapsto C = A \cdot B, \quad c_{ik} = \sum_{j=1}^{q} a_{ij} \cdot b_{jk}.$$

Ist die Matrixmultiplikation kommutativ?

$$\boxed{A} \cdot \boxed{B} = \boxed{AB} \quad \text{vs} \quad \boxed{B} \cdot \boxed{A} = \boxed{BA}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{vs} \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Ist die Matrixmultiplikation assoziativ?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Erster Versuch: Wir betrachten das kleinste Beispiel $A, B, C \in \mathbb{K}^{2\times 2}$:

$$(A \cdot B) \cdot C = \left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \right) \cdot \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix} \cdot \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} (a_{11}b_{11}+a_{12}b_{21})c_{11}+(a_{11}b_{12}+a_{12}b_{22})c_{21} & (a_{11}b_{11}+a_{12}b_{21})c_{12}+(a_{11}b_{12}+a_{12}b_{22})c_{22} \\ (a_{21}b_{11}+a_{22}b_{21})c_{11}+(a_{21}b_{12}+a_{22}b_{22})c_{21} & (a_{21}b_{11}+a_{22}b_{21})c_{12}+(a_{21}b_{12}+a_{22}b_{22})c_{22} \end{bmatrix}$$

$$A \cdot (B \cdot C) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \left(\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \cdot \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11}c_{11}+b_{12}c_{21} & b_{11}c_{12}+b_{12}c_{22} \\ b_{21}c_{11}+b_{22}c_{21} & b_{21}c_{12}+b_{22}c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}(b_{11}c_{11}+b_{12}c_{21})+a_{12}(b_{21}c_{11}+b_{22}c_{21}) & a_{11}(b_{11}c_{12}+b_{12}c_{22})+a_{12}(b_{21}c_{12}+b_{22}c_{22}) \\ a_{21}(b_{11}c_{11}+b_{12}c_{21})+a_{22}(b_{21}c_{11}+b_{22}c_{21}) & a_{21}(b_{11}c_{12}+b_{12}c_{22})+a_{22}(b_{21}c_{12}+b_{22}c_{22}) \end{bmatrix}$$

Matrixkalkül: Assoziativität der Multiplikation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Für je drei multiplizierbare Matrizen $A \in \mathbb{K}^{p\times q}$, $B \in \mathbb{K}^{q\times r}$, $C \in \mathbb{K}^{r\times s}$ gilt:

$$\begin{aligned}
[A \bullet (B \bullet C)]_{i\ell} &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot (B \bullet C)_{j\ell} \\
&\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot \left[\sum_{k=1}^{r} b_{jk} \cdot c_{k\ell}\right] \overset{\text{DL}}{=} \sum_{j=1}^{q} \sum_{k=1}^{r} a_{ij} \cdot (b_{jk} \cdot c_{k\ell})
\end{aligned}$$

$$\begin{aligned}
[(A \bullet B) \bullet C]_{i\ell} &\overset{\text{Def}}{=} \textstyle\sum_{k=1}^{r} (A \bullet B)_{ik} \cdot c_{k\ell} \\
&\overset{\text{Def}}{=} \textstyle\sum_{k=1}^{r} \left[\sum_{j=1}^{q} a_{ij} \cdot b_{jk}\right] \cdot c_{k\ell} \overset{\text{DR}}{=} \sum_{k=1}^{r} \sum_{j=1}^{q} (a_{ij} \cdot b_{jk}) \cdot c_{k\ell}
\end{aligned}$$

Matrixkalkül: Rechenregeln der Multiplikation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D1F: Rechenregeln für die Matrixmultiplikation

(1) Die Matrixmultiplikation ist assoziativ, sobald sie definiert ist:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

(2) Zu jeder Matrix $A \in \mathbb{K}^{p \times q}$ ist die passende Einheitsmatrix neutral:

$$1_{p \times p} \cdot A = A \quad \text{und} \quad A \cdot 1_{q \times q} = A$$

(3) Die Matrixmultiplikation distribuiert über die Addition:

DL:	$A \cdot (B + B') = A \cdot B + A \cdot B'$,	L0:	$A \cdot \mathbf{0} = \mathbf{0}$,
DR:	$(A + A') \cdot B = A \cdot B + A' \cdot B$,	R0:	$\mathbf{0} \cdot B = \mathbf{0}$.

Matrixkalkül: Die Transposition ist involutiv.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Transposition erfüllt $(A^\top)^\top = A$. Zudem ist sie **additiv**, das heißt:

$$\boxed{(A+B)^\top = A^\top + B^\top}$$

$$\begin{aligned}
(A+B)^\top{}_{ji} &\overset{\text{Def}}{=} (A+B)_{ij} &&\overset{\text{Def}}{=} a_{ij} + b_{ij} \\
(A^\top + B^\top)_{ji} &\overset{\text{Def}}{=} A^\top{}_{ji} + B^\top{}_{ji} &&\overset{\text{Def}}{=} a_{ij} + b_{ij}
\end{aligned}$$

Ist $\mathbb{K}$ kommutativ, so ist die Transposition **anti-multiplikativ**, das heißt:

$$\boxed{(A \bullet B)^\top = B^\top \bullet A^\top}$$

$$\begin{aligned}
(A \bullet B)^\top{}_{ki} &\overset{\text{Def}}{=} (A \bullet B)_{ik} &&\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} a_{ij} \cdot b_{jk} \\
(B^\top \bullet A^\top)_{ki} &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} B^\top{}_{kj} \cdot A^\top{}_{ji} &&\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{q} b_{jk} \cdot a_{ij}
\end{aligned}$$

Matrixkalkül: die Spur einer quadratischen Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition D1H: die Spur einer quadratischen Matrix

$$\mathrm{tr}_n : \mathbb{K}^{n\times n} \to \mathbb{K} : A \mapsto \sum_{k=1}^{n} a_{kk} = a_{11} + \ldots + a_{nn}.$$

Aufgabe: Gilt $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ für alle $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times p}$?

Lösung: Wir setzen die Definitionen ein und vergleichen:

$$\begin{aligned}
\mathrm{tr}_p(AB) &\overset{\text{Def}}{=} \sum_{i=1}^{p} (AB)_{ii} \overset{\text{Def}}{=} \sum_{i=1}^{p} \sum_{j=1}^{q} a_{ij} b_{ji} \\
\mathrm{tr}_q(BA) &\overset{\text{Def}}{=} \sum_{j=1}^{q} (BA)_{jj} \overset{\text{Def}}{=} \sum_{j=1}^{q} \sum_{i=1}^{p} b_{ji} a_{ij}
\end{aligned}$$

Ist der Ring $\mathbb{K}$ kommutativ, so sind diese Summen termweise gleich. $\boxed{\text{QED}}$

Matrixkalkül: Zusammenfassung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D1ı: Matrixkalkül über einem Ring $(\mathbb{K}, +, 0, \cdot, 1,)$

Matrizen passender Größe können wir addieren und multiplizieren:

$$\mathbf{+} : \mathbb{K}^{p\times q} \times \mathbb{K}^{p\times q} \to \mathbb{K}^{p\times q} : (A, B) \mapsto C = A \mathbf{+} B, \;\; c_{ij} = a_{ij} + b_{ij}$$

$$\bullet : \mathbb{K}^{p\times q} \times \mathbb{K}^{q\times r} \to \mathbb{K}^{p\times r} : (A, B) \mapsto C = A \bullet B, \quad c_{ik} = \textstyle\sum_{j=1}^{q} a_{ij} \cdot b_{jk}$$

Die Matrixaddition bildet eine abelsche Gruppe $(\mathbb{K}^{p\times q}, \mathbf{+}, \mathbf{0}, \mathbf{-})$ und zusammen mit der Skalierung einen linearen Raum über $\mathbb{K}$.

Die Matrixmultiplikation $\bullet$ ist distributiv über $\mathbf{+}$, nicht kommutativ, aber assoziativ. Die passende Einheitsmatrix ist links-/rechtsneutral.

Die quadratischen Matrizen bilden den Ring $(\mathbb{K}^{n\times n}, \mathbf{+}, 0_{n\times n}, \bullet, 1_{n\times n},)$. Für $n \geq 2$ ist dieser Matrixring nicht kommutativ und hat Nullteiler:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{vs} \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Jede Matrix A definiert eine lineare Abbildung $f_A : x \mapsto Ax$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede Matrix $A \in \mathbb{K}^{m\times n}$ definiert ihre zugehörige **lineare Abbildung**

$$f = f_A : \mathbb{K}^{n\times 1} \to \mathbb{K}^{m\times 1} : x \mapsto Ax.$$

Diese Abbildung ist **additiv** für alle Vektoren $x, x' \in \mathbb{K}^n$:

$$f(x+x') \overset{\text{Def}}{=} A(x+x') \underset{\text{D1F}}{\overset{\text{Dst}}{=}} Ax + Ax' \overset{\text{Def}}{=} f(x) + f(x').$$

Sie ist zudem **homogen** bezüglich Skalierung mit $\lambda \in \mathbb{K}$ von rechts:

$$f(x\lambda) \overset{\text{Def}}{=} A(x\lambda) \underset{\text{D1F}}{\overset{\text{Ass}}{=}} (Ax)\lambda \overset{\text{Def}}{=} f(x)\lambda.$$

Definition D1J: lineare Abbildung aka $\mathbb{K}$–Homomorphismus

Sei $f : \mathbb{K}^n \to \mathbb{K}^m$ eine Abbildung. Sie heißt **linear** über $\mathbb{K}$, falls gilt

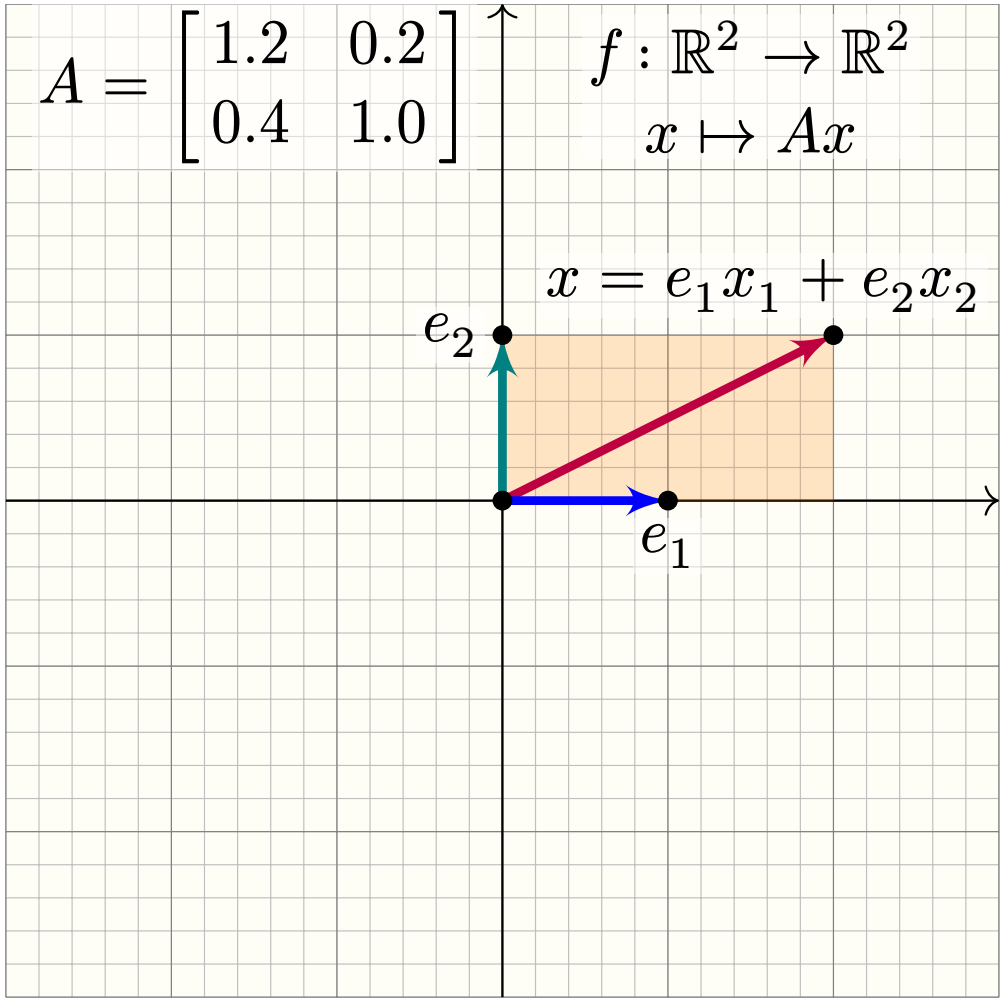
$$f(x+x') = f(x) + f(x') \quad \text{und} \quad f(x\cdot\lambda) = f(x)\cdot\lambda$$

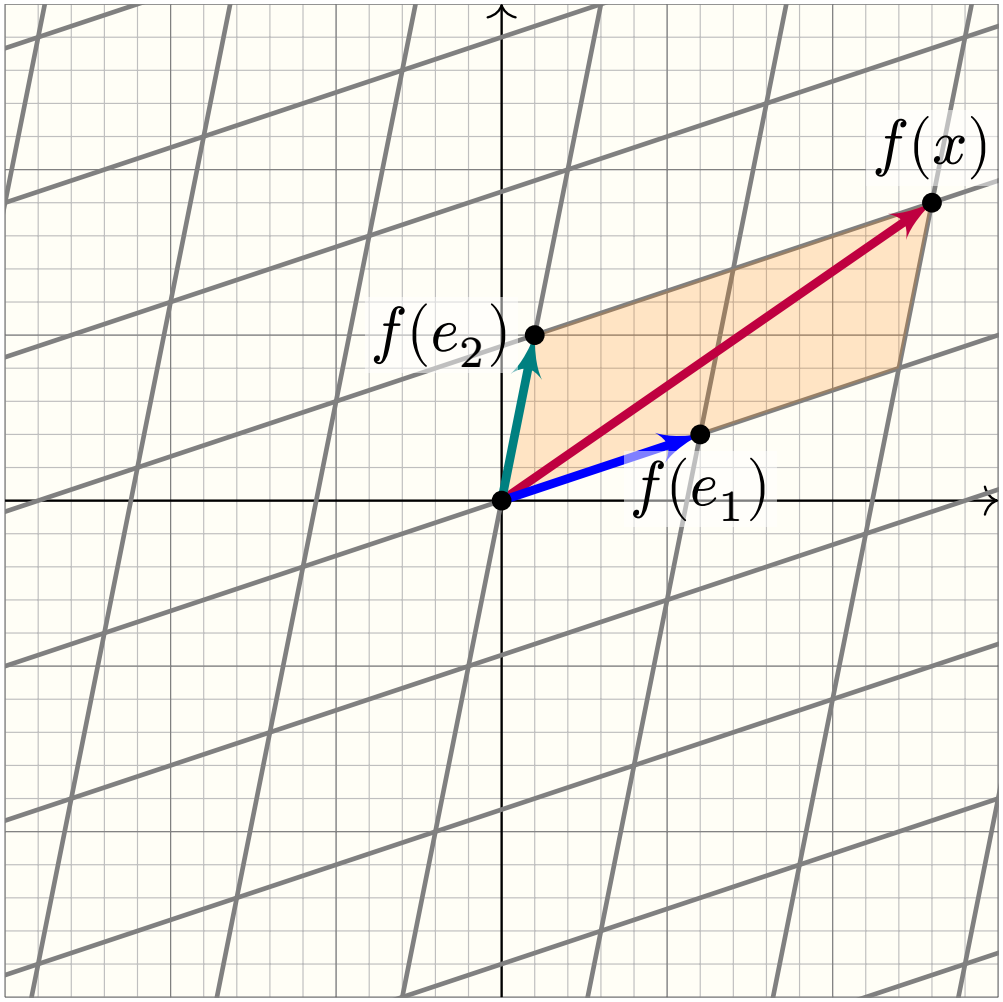
für alle Vektoren $x, x' \in \mathbb{K}^n$ und alle Skalare $\lambda \in \mathbb{K}$.

Geometrische Wirkung einer Matrix A als Abbildung f_A

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Jede lineare Abbildung $f : \mathbb{K}^n \to \mathbb{K}^m$ definiert eine Matrix.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D1J: Jede lineare Abbildung definiert eine Matrix.

(1) Für $f : \mathbb{K}^n \to \mathbb{K}^m$ linear gilt $f = f_A$ mit $A = (f(e_1), \dots, f(e_n)) \in \mathbb{K}^{m \times n}$.

Beweis: (1) Wir müssen $f(x) = Ax$ zeigen für alle $x \in \mathbb{K}^n$. Wir rechnen:

$$f(x) \overset{\text{Def}}{=} f\left(\sum_{j=1}^n e_j x_j\right) \overset{\text{Add}}{=} \sum_{j=1}^n f(e_j x_j) \overset{\text{Hom}}{=} \sum_{j=1}^n f(e_j) x_j \overset{\text{Def}}{=} Ax$$

Inverse Matrizen: links, rechts, beidseitig

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{bmatrix} 1 & -2 & * \\ 0 & 1 & * \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ * & * \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Satz D1κ: Die Inverse ist eindeutig.

Wir nennen $B \in \mathbb{K}^{q\times p}$ **linksinvers** zu $A \in \mathbb{K}^{p\times q}$, falls $B \cdot A = 1_{q\times q}$ gilt.
Wir nennen $C \in \mathbb{K}^{q\times p}$ **rechtsinvers** zu $A \in \mathbb{K}^{p\times q}$, falls $A \cdot C = 1_{p\times p}$ gilt.

(1) Gilt beides, so folgt $B = C$, denn

$$B \overset{\text{rNtr}}{=} B \cdot 1_{p\times p} \overset{\text{rInv}}{=} B \cdot (A \cdot C) \overset{\text{Ass}}{=} (B \cdot A) \cdot C \overset{\text{lInv}}{=} 1_{q\times q} \cdot C \overset{\text{lNtr}}{=} C.$$

(2) Wir nennen B **invers** zu A, falls $B \cdot A = 1_{q\times q}$ und $A \cdot B = 1_{p\times p}$ gilt.
Dank (1) ist B eindeutig durch A bestimmt, und wir schreiben $A^{-1} := B$.

$$\underbrace{\begin{bmatrix} -4 & 9 \\ -3 & 7 \end{bmatrix}}_{=A} \cdot \underbrace{\begin{bmatrix} -7 & 9 \\ -3 & 4 \end{bmatrix}}_{=B} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \underbrace{\begin{bmatrix} -7 & 9 \\ -3 & 4 \end{bmatrix}}_{=B} \cdot \underbrace{\begin{bmatrix} -4 & 9 \\ -3 & 7 \end{bmatrix}}_{=A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Inverse Matrizen: links, rechts, beidseitig

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sind die folgenden Matrizen über $\mathbb{Q}$ invertierbar aka regulär?

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Die Matrix A hat *mehrere* Linksinverse, demnach *kein* Rechtsinverses.
Die Matrix B hat *mehrere* Rechtsinverse, demnach *kein* Linksinverses.

Ist jede invertierbare Matrix quadratisch?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D1L: Jede invertierbare Matrix über $\mathbb{Z}$ ist quadratisch.

Sei $\mathbb{K} \geq \mathbb{Z}$ ein kommutativer Ring, der $\mathbb{Z}$ enthält, etwa $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
Dann ist jede invertierbare Matrix $A \in \mathbb{K}^{p \times q}$ quadratisch, also $p = q$.

Beweis: Seien $A \in \mathbb{K}^{p \times q}$ und $B \in \mathbb{K}^{q \times p}$ zueinander invers.
Aus $AB = 1_{p \times p}$ erhalten wir die Spur $\operatorname{tr}(AB) = p \in \mathbb{Z} \subseteq \mathbb{K}$.
Aus $BA = 1_{q \times q}$ erhalten wir die Spur $\operatorname{tr}(BA) = q \in \mathbb{Z} \subseteq \mathbb{K}$.
Da $\mathbb{K}$ kommutativ ist, gilt $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ dank D1H, also $p = q$. $\boxed{\text{QED}}$

Die allgemeine lineare Gruppe $\mathrm{GL}_n\,\mathbb{K}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition D1M: die allgemeine lineare Gruppe

$$\mathrm{GL}_n(\mathbb{K}) := \left\{ A \in \mathbb{K}^{n\times n} \,\middle|\, \exists B \in \mathbb{K}^{n\times n} : A \bullet B = B \bullet A = 1_{n\times n} \right\}.$$

Der Ring der 2×2–Matrizen

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} + \begin{bmatrix} a' & c' \\ b' & d' \end{bmatrix} = \begin{bmatrix} a+a' & c+c' \\ b+b' & d+d' \end{bmatrix}$$

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \cdot \begin{bmatrix} a' & c' \\ b' & d' \end{bmatrix} = \begin{bmatrix} aa'+cb' & ac'+cd' \\ ba'+db' & bc'+dd' \end{bmatrix}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Determinante und Inversion von 2×2–Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sei $(\mathbb{K}, +, \cdot)$ ein kommutativer Ring. Berechnen Sie:

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \cdot \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \overset{!}{=} (ad - bc) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \overset{!}{=} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

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

$$\det : \mathbb{K}^{2\times 2} \to \mathbb{K} : \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = ad - bc.$$

Anwendungsbeispiel: Lösung linearer Gleichungssysteme

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: (1) Wir wollen folgendes Gleichungssystem über $\mathbb{Z}$ lösen:

$$\left.\begin{aligned} -4x_1 + 9x_2 &= 3 \\ -3x_1 + 7x_2 &= 2 \end{aligned}\right\} \iff Ax = b \text{ mit } A = \begin{bmatrix} -4 & 9 \\ -3 & 7 \end{bmatrix}, x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, b = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$$

(2) Hier gilt $\det A = -1 \in \mathbb{Z}^\times$, also ist A in $\mathbb{Z}^{2\times 2}$ invertierbar vermöge

$$A^{-1} = \frac{1}{-1}\begin{bmatrix} 7 & -9 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} -7 & 9 \\ -3 & 4 \end{bmatrix}, \quad \text{also} \quad x = A^{-1}b = \begin{bmatrix} -3 \\ -1 \end{bmatrix}.$$

Determinante und Inversion von 2×2–Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D1N: Inversion von 2×2–Matrizen

Sei $(\mathbb{K}, +, 0, \cdot, 1)$ ein kommutativer Ring. (1) Dann ist die Determinante $\det : \mathbb{K}^{2\times 2} \to \mathbb{K} : \left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right] \mapsto ad - bc$ multiplikativ, also $\det(1_{2\times 2}) = 1$ und

$$\boxed{\det(A \bullet B) = \det(A) \cdot \det(B).}$$

(2) Genau dann ist eine Matrix A im Matrixring $\mathbb{K}^{2\times 2}$ invertierbar, wenn ihre Determinante $\det(A)$ im Grundring $\mathbb{K}$ invertierbar ist.

$$\boxed{\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.}$$

(3) Wir erhalten die allgemeine und darin die spezielle lineare Gruppe:

$$\begin{aligned} \mathrm{GL}_2(\mathbb{K}) &\overset{(2)}{=} \left\{ A \in \mathbb{K}^{2\times 2} \,\middle|\, \det A \in \mathbb{K}^\times \right\} \\ \mathrm{SL}_2(\mathbb{K}) &:= \left\{ A \in \mathbb{K}^{2\times 2} \,\middle|\, \det A = 1 \right\} \end{aligned}$$

Lineares Gleichungssystem in Matrixschreibweise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zu lösen sei ein **lineares Gleichungssystem** (LGS) über dem Ring $\mathbb{K}$:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = y_1 \\ \vdots \qquad\qquad \vdots \qquad\quad \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = y_m \end{cases}$$

$$\begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$$

$$\boxed{Ax = y}$$

Gesucht ist $\text{Lös}(A, y) := \{x \in \mathbb{K}^n \mid Ax = y\}$, speziell $\text{Ker}(A) := \text{Lös}(A, 0)$.

Lineare Gleichungssysteme lösen: Diagonalform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{bmatrix} a_{11} & 0 & 0 & 0 & 0 \\ 0 & a_{22} & 0 & 0 & 0 \\ 0 & 0 & a_{33} & 0 & 0 \\ 0 & 0 & 0 & a_{44} & 0 \\ 0 & 0 & 0 & 0 & a_{55} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{bmatrix}$$

$$a_{ii} x_i = b_i \quad \Longleftrightarrow \quad x_i = a_{ii}^{-1} b_i$$

Lineare Gleichungssysteme lösen: Dreiecksform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{bmatrix} \blacksquare & * & * & * & * \\ 0 & \blacksquare & * & * & * \\ 0 & 0 & \blacksquare & * & * \\ 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & \blacksquare \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{bmatrix}$$

$$a_{ii}x_i + \sum_{j>i} a_{ij}x_j = b_i \quad \Longleftrightarrow \quad x_i = a_{ii}^{-1}\big(b_i - \sum_{j>i} a_{ij}x_j\big)$$

Zeilenstufenform, allgemein und reduziert

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{bmatrix} \blacksquare & * & * & * & * & * & * & * & * & * \\ 0 & 0 & \blacksquare & * & * & * & * & * & * & * \\ 0 & 0 & 0 & \blacksquare & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 0 & * & 0 & * & * & 0 & * & * \\ 0 & 0 & 1 & * & 0 & * & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 1 & * & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Zu jeder **Pivotspalte** $j = s_n, \dots, s_2, s_1$ folgt die Koordinate x_j wie oben.
Zu jeder **freien Spalte** k können wir die Koordinate $x_k \in \mathbb{K}$ frei wählen.

Zeilenstufenform, allgemein und reduziert

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition D2E: Zeilenstufenform, allgemein und reduziert

Sei $A \in \mathbb{K}^{m \times n}$. Für jede Zeile $i = 1, \dots, m$ definieren wir die **Pivotspalte**

$$s_i := \min\{\, \infty,\ j \mid a_{ij} \neq 0 \,\}$$

Die Matrix A hat **Zeilenstufenform** (ZSF, engl. *row echelon form*, REF) falls $s_1 < \dots < s_r < \infty = s_{r+1} = \dots = s_m$.

Die Matrix A hat **reduzierte Zeilenstufenform** (RZSF, engl. RREF), falls zudem gilt: Jeder Pivot ist Eins, und darüber stehen nur Nullen.

Beispiel: Die Diagonalmatrix $\operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0)$ mit $d_1, \dots, d_r \neq 0$ ist in Zeilenstufenform vom Rang r, und reduziert gdw $d_1 = \dots = d_r = 1$.

Lineare Gleichungssysteme: erweiterte Koeffizientenmatrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir betrachten ein lineares Gleichungssystem $Ax = b$, ausgeschrieben:

$$\begin{cases} a_{11}x_1 & + a_{12}x_2 & + \ldots + a_{1n}x_n & = b_1 \\ a_{21}x_1 & + a_{22}x_2 & + \ldots + a_{2n}x_n & = b_2 \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}x_1 & + a_{m2}x_2 & + \ldots + a_{mn}x_n & = b_m \end{cases}$$

Dies bündeln wir übersichtlich zur **erweiterten Koeffizientenmatrix**:

$$(A, b) = \left[\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_n \end{array}\right]$$

Lineare Gleichungssysteme lösen in Zeilenstufenform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\left[\begin{array}{cccc|c} \blacksquare & * & * & * & * \\ 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & \blacksquare \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

nicht lösbar
für dieses b

$$\left[\begin{array}{cccc|c} \blacksquare & * & * & * & * \\ 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

lösbar für dieses b,
aber nicht eindeutig

$$\left[\begin{array}{ccc|c} \blacksquare & * & * & * \\ 0 & \blacksquare & * & * \\ 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

lösbar für dieses b
und zudem eindeutig

$$\left[\begin{array}{ccccc|c} \blacksquare & * & * & * & * & * \\ 0 & \blacksquare & * & * & * & * \\ 0 & 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & \blacksquare & * & * \\ 0 & 0 & 0 & 0 & \blacksquare & * \end{array}\right]$$

eindeutig lösbar
für jedes b

Lineare Gleichungssysteme lösen in Zeilenstufenform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\left[\begin{array}{rrrrr|r} 1 & -2 & 1 & -6 & 5 & -6 \\ 0 & 1 & -1 & 2 & -6 & -3 \\ 0 & 0 & 1 & -2 & 3 & 7 \\ 0 & 0 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right] \xrightarrow[\text{(optional)}]{\text{reduzieren}} \left[\begin{array}{rrrrr|r} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 9 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

$$\text{Lös}(A, b) = \left\{ \begin{bmatrix} -1 \\ 4 \\ 9 \\ 1 \\ 0 \end{bmatrix} \right\}$$

Lineare Gleichungssysteme lösen in Zeilenstufenform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\left[\begin{array}{rrrrr|r} 1 & -2 & -1 & -4 & 1 & 4 \\ 0 & 0 & -1 & -7 & 1 & 5 \\ 0 & 0 & 0 & 0 & 1 & 9 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \xrightarrow[\text{(optional)}]{\text{reduzieren}} \left[\begin{array}{rrrrr|r} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 9 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

$$\text{Lös}(A, b) = \emptyset = \{\,\}$$

Lineare Gleichungssysteme lösen in Zeilenstufenform

Struktur des Lösungsraums

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\underbrace{\left[\begin{array}{rrrrr|r} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]}_{A \qquad\qquad b} \xrightarrow[\text{Merkregel}]{\text{graphische}} \begin{array}{c} \left[\begin{array}{rrrrrr} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 9 \end{array}\right] \begin{array}{l} \\ \lambda_1 \\ \\ \lambda_2 \\ \\ \end{array} \\ \begin{array}{rrr} v_1 & v_2 & v_0 \end{array} \end{array}$$

Lösung: Freie Variablen sind $\lambda_1 = -x_2$, $\lambda_2 = -x_4$. Rückwärtseinsetzen ergibt $x_5 = 9$, $x_4 = -\lambda_2$, $x_3 = 4 + 7\lambda_2$, $x_2 = -\lambda_1$, $x_1 = -1 - 2\lambda_1 + 3\lambda_2$.

$$L = \left\{ \begin{bmatrix} -1 \\ 0 \\ 4 \\ 0 \\ 9 \end{bmatrix} + \begin{bmatrix} -2 \\ -1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \lambda_1 + \begin{bmatrix} 3 \\ 0 \\ 7 \\ -1 \\ 0 \end{bmatrix} \lambda_2 \right\} = \left\{ v_0 + v_1\lambda_1 + v_2\lambda_2 \,\middle|\, \lambda \in \mathbb{R}^2 \right\}^!$$

Lineare Gleichungssysteme lösen in Zeilenstufenform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D2F: Lösung in Zeilenstufenform

Gegeben seien $A \in \mathbb{K}^{m \times n}$ und $b \in \mathbb{K}^m$. Wir setzen voraus, dass (A, b) schon in Zeilenstufenform vorliegt mit Stufen $s = (s_1, \dots, s_r)$.

(1) Das Gleichungssystem $Ax = b$ ist

1. unlösbar genau dann, wenn $s_r = n + 1$,
2. lösbar genau dann, wenn $s_r \leq n$ gilt, sowie
3. eindeutig lösbar genau dann, wenn $s = (1, \dots, n)$.

$$\left(\begin{array}{cccc|c} \blacksquare & * & * & * & * \\ 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & \blacksquare \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \quad \left(\begin{array}{cccc|c} \blacksquare & * & * & * & * \\ 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \quad \left(\begin{array}{cccc|c} \blacksquare & * & * & * & * \\ 0 & \blacksquare & * & * & * \\ 0 & 0 & \blacksquare & * & * \\ 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

(2) Lösungen $x \in \mathbb{K}^n$: Zu jeder freien Spalte $k \in \{1, \dots, n\} \setminus \{s_1, \dots, s_r\}$ können wir $x_k \in \mathbb{K}$ frei wählen. Zu jeder Pivotspalte $j \in \{s_r, \dots, s_1\}$ folgt $x_j \in \mathbb{K}$ eindeutig durch Rückwärtseinsetzen. Wir erhalten:

$$\boxed{\{x \in \mathbb{K}^n \mid Ax = b\} \;=\; \{v_0 + v_1\lambda_1 + \dots + v_d\lambda_d \mid \lambda \in \mathbb{K}^d\}^!}$$

Wir nennen $r \in \{0, \dots, \min\{m, n\}\}$ den **Rang** und $d = n - r$ den **Defekt**. Die Lösungsmenge ist ein **affin-linearer Unterraum** der Dimension d.

Gauß–Algorithmus zur reduzierten Zeilenstufenform

$$
\begin{array}{c|ccccccc}
 & & & & & \ell & & \\
 & 0 & 1 & 0 & * & 0 & * & * & * \\
 & 0 & 0 & 1 & * & 0 & * & * & * \\
 & 0 & 0 & 0 & 0 & 1 & * & * & * \\
k & 0 & 0 & 0 & 0 & 0 & \boxed{*} & * & * \\
 & 0 & 0 & 0 & 0 & 0 & * & * & *
\end{array}
\longrightarrow
\begin{array}{c|ccccccc}
 & & & & & \ell & & \\
 & 0 & 1 & 0 & * & 0 & * & * & * \\
 & 0 & 0 & 1 & * & 0 & * & * & * \\
 & 0 & 0 & 0 & 0 & 1 & * & * & * \\
k & 0 & 0 & 0 & 0 & 0 & 0 & * & * \\
 & 0 & 0 & 0 & 0 & 0 & 0 & * & *
\end{array}
\quad \text{oder} \quad
\begin{array}{c|ccccccc}
 & & & & & \ell & & \\
 & 0 & 1 & 0 & * & 0 & 0 & * & * \\
 & 0 & 0 & 1 & * & 0 & 0 & * & * \\
 & 0 & 0 & 0 & 0 & 1 & 0 & * & * \\
k & 0 & 0 & 0 & 0 & 0 & 1 & * & * \\
 & 0 & 0 & 0 & 0 & 0 & 0 & * & *
\end{array}
$$

Algo D2G: Gauß–Algorithmus für die Spalten $\ell = 1, \dots, n$

Eingabe: $A \in \mathbb{K}^{m \times n}$ mit Stufen $s = (s_1, \dots, s_r)$ vor Spalte $\ell \in \{1, \dots, n\}$
Ausgabe: $A' \in \mathbb{K}^{m \times n}$ zeilenumgeformt aus A mit Stufen $s' = (s'_1, \dots, s'_{r'})$

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 ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zeitaufwand des Gauß–Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D2H: Gauß–Algorithmus zur reduzierten Zeilenstufenform / RZSF

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$; es genügt ein Divisionsring, wie $\mathbb{H}$.

(1) Jede Matrix $A \in \mathbb{K}^{m \times n}$ können wir allein durch Zeilenoperationen umformen in ihre reduzierte Zeilenstufenform A'.

(2) 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 $r \le \min\{m, n\}$ der Rang ist,
- somit höchstens mnr arithmetische Operationen im Grundring $\mathbb{K}$.

Speziell für jede quadratische Matrix, mit $m = n$, genügen demnach $\le n^2$ Zeilenoperationen, somit $\le n^3$ arithmetische Operationen in $\mathbb{K}$.

Zeitaufwand des Gauß–Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

	Größe n	Operationen in $\mathbb{K}$ (feste Kosten)	Zeit bei 10^{12} op/s (GPU/CPU)	Zeit bei 10^{18} op/s (Supercomputer)
„klein“	10^1	$\lesssim 10^3$	$\lesssim$ 1ns	
	10^2	$\lesssim 10^6$	$\lesssim$ 1µs	
	10^3	$\lesssim 10^9$	$\lesssim$ 1ms	
„mittel“	10^4	$\lesssim 10^{12}$	$\lesssim$ 1 s	$\lesssim$ 1µs
	10^5	$\lesssim 10^{15}$	$\lesssim$ 30 min	$\lesssim$ 1ms
	10^6	$\lesssim 10^{18}$	$\lesssim$ 12 Tage	$\lesssim$ 1 s
„groß“	10^7	$\lesssim 10^{21}$	$\lesssim$ 32 Jahre	$\lesssim$ 30 min
	10^8	$\lesssim 10^{24}$	$\lesssim$ 32000 Jahre	$\lesssim$ 12 Tage
	10^9	$\lesssim 10^{27}$		$\lesssim$ 32 Jahre

Zeilenoperation = Linksmultiplikation mit Elementarmatrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_{i1} & \dots & a_{in} \\ a_{j1} & \dots & a_{jn} \end{bmatrix} = \begin{bmatrix} a_{j1} & \dots & a_{jn} \\ a_{i1} & \dots & a_{in} \end{bmatrix}$$

$$\begin{bmatrix} \mu & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{i1} & \dots & a_{in} \\ a_{j1} & \dots & a_{jn} \end{bmatrix} = \begin{bmatrix} \mu a_{i1} & \dots & \mu a_{in} \\ a_{j1} & \dots & a_{jn} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{i1} & \dots & a_{in} \\ a_{j1} & \dots & a_{jn} \end{bmatrix} = \begin{bmatrix} a_{i1} & \dots & a_{in} \\ \lambda a_{i1} + a_{j1} & \dots & \lambda a_{in} + a_{jn} \end{bmatrix}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zeilenoperation = Linksmultiplikation mit Elementarmatrix

$$P_{ij} = \begin{array}{c} \begin{array}{ccccc} & i & & j & \end{array} \\ \begin{bmatrix} 1 & . & . & . & . \\ . & 0 & . & 1 & . \\ . & . & 1 & . & . \\ . & 1 & . & 0 & . \\ . & . & . & . & 1 \end{bmatrix} \end{array} \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array}$$

$$S_i(\mu) = \begin{bmatrix} 1 & . & . & . & . \\ . & \mu & . & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array}$$

$$T_{ij}(\lambda) = \begin{bmatrix} 1 & . & . & . & . \\ . & 1 & . & 0 & . \\ . & . & 1 & . & . \\ . & \lambda & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zeilenoperationen = Matrixmultiplikation von links

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zeilenoperationen $B_1, \dots, B_\ell \in \{P_{ij}, S_i(\mu), T_{ij}(\lambda)\} \subset \mathrm{GL}_m \mathbb{K}$ ergeben:

$$A \mapsto B_1 A \mapsto \dots \mapsto B_\ell(\cdots(B_1 A)\cdots) \overset{\text{Ass}}{=} \underbrace{(B_\ell \cdots B_1)}_{= B \in \mathrm{GL}_m \mathbb{K}} A = A'$$

Jede der Operationen $B_1, \dots, B_\ell$ können wir umkehren:

$$A' \mapsto B_\ell^{-1} A' \mapsto \dots \mapsto B_1^{-1}(\cdots(B_\ell^{-1} A')\cdots) \overset{\text{Ass}}{=} \underbrace{(B_1^{-1} \cdots B_\ell^{-1})}_{= B^{-1} \in \mathrm{GL}_m \mathbb{K}} A' = A$$

Invertierbarkeitskriterien für Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D2M: Invertierbarkeitskriterien für Matrizen

Sei $\mathbb{K}$ ein Körper, wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$; es genügt ein Divisionsring, wie $\mathbb{H}$. Die Matrix $A \in \mathbb{K}^{m\times n}$ bringen wir in eine Zeilenstufenform $A' = SA$, vom Rang $r \le \min\{m, n\}$, vermöge $S \in \mathrm{GL}_m \mathbb{K}$.

(1) Surjektivität. Äquivalent sind:
(1a) Zu jedem $y \in \mathbb{K}^m$ existiert mindestens ein $x \in \mathbb{K}^n$ mit $Ax = y$.
(1b) Die Matrix A ist rechtsinvertierbar, $\exists C \in \mathbb{K}^{n\times m} : AC = 1_{m\times m}$.
(1c) Es gilt $r = m \le n$, also Rang gleich Zeilenzahl.

(2) Injektivität. Äquivalent sind:
(2a) Zu jedem $y \in \mathbb{K}^m$ existiert höchstens ein $x \in \mathbb{K}^n$ mit $Ax = y$.
(2b) Die Matrix A ist linksinvertierbar, $\exists B \in \mathbb{K}^{n\times m} : BA = 1_{n\times n}$.
(2c) Es gilt $r = n \le m$, also Rang gleich Spaltenzahl.

(3) Bijektivität. Äquivalent sind:
(3a) Zu jedem $y \in \mathbb{K}^m$ existiert genau eine Lösung $x \in \mathbb{K}^n$ mit $Ax = y$.
(3b) Die Matrix A ist invertierbar, $\exists B \in \mathbb{K}^{n\times m} : BA = 1_{n\times n},\ AB = 1_{m\times m}$.
(3c) Es gilt $r = m = n$, unsere Matrix A ist quadratisch mit vollem Rang.

Surjektivitätskriterium für Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: „(1a) $\Rightarrow$ (1b)“: Wir lösen $Ac_i = e_i$. Für $C = (c_1, \dots, c_m)$ gilt

$$AC \overset{\text{Def}}{=} (Ac_1, \dots Ac_m) \overset{\text{Vor}}{=} (e_1, \dots, e_m) \overset{\text{Def}}{=} 1_{m\times m}.$$

„(1b) $\Rightarrow$ (1a)“: Zu $y \in \mathbb{K}^m$ erfüllt $x = Cy \in \mathbb{K}^n$ die gewünschte Gleichung

$$Ax \overset{\text{Def}}{=} A(Cy) \overset{\text{Ass}}{=} (AC)y \overset{\text{Vor}}{=} 1_{m\times m}\, y \overset{\text{Def}}{=} y.$$

„(1c) $\Leftrightarrow$ (1a)“: Gilt $r = m$, so ist $Ax = y$ für jedes $y \in \mathbb{K}^m$ lösbar (D2F). Umgekehrt, gilt $r < m$, so ist $Ax = y$ unlösbar für $y = S^{-1}e_m \in \mathbb{K}^m$.

Injektivitätskriterium für Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: „(2c) $\Leftrightarrow$ (2a)“: Wir nutzen Satz D2F. Gilt $r = n$, so hat $Ax = y$ für jedes $y \in \mathbb{K}^m$ 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 $x \in \mathbb{K}^n$.

„(2b) $\Rightarrow$ (2a)“: Aus $BA = 1_{n\times n}$ folgt Eindeutigkeit: Gilt $Ax = Ax' = y$, so liefert Linksmultiplikation mit B die Gleichung $x = x' = By$.

„(2c) $\Rightarrow$ (2b)“: Wir überführen A in *reduzierte* Zeilenstufenform $A' = SA$ mit $S \in \mathrm{GL}_m\,\mathbb{K}$. Wegen $r = n$ beginnt A' mit den Zeilen $e_1^\top, \dots, e_n^\top$.
Seien $b_1^\top, \dots, b_n^\top \in \mathbb{K}^m$ die ersten Zeilen von S, also $b_i^\top A = e_i^\top$.
Die Matrix $B = (b_1^\top; \dots; b_n^\top) \in \mathbb{K}^{n\times m}$ erfüllt $BA = 1_{n\times n}$. $\boxed{\text{QED}}$

Invarianz der Dimension

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar D2N: Invarianz der Dimension

Über jedem Divisionsring $\mathbb{K}$ gilt: invertierbare Matrizen sind quadratisch!

Invertierbarkeit quadratischer Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar D2o: Invertierbarkeit quadratischer Matrizen

Sei $\mathbb{K}$ ein Divisionsring. Für jede quadratische Matrix $A \in \mathbb{K}^{n \times n}$ gilt:
Jede Linksinverse zu A ist eine Rechtsinverse zu A und umgekehrt.

Invertierbarkeit quadratischer Matrizen

Ausprobieren mit Gaël!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar D2P: Inversion quadratischer Matrizen

Sei $\mathbb{K}$ ein Divisionsring und $A \in \mathbb{K}^{n\times n}$ eine quadratische Matrix.

(1) Bringe A in reduzierte Zeilenstufenform $A' = SA$, mit $S \in \mathrm{GL}_n\,\mathbb{K}$. Dabei entsteht $A' = 1_{n\times n}$ gdw A invertierbar ist, somit $A^{-1} = S$.

(2) Bringe die erweiterte Matrix $X = (A, 1_{n\times n})$ in reduzierte ZSF X'. Dabei entsteht $X' = (1_{n\times n}, S)$ gdw A invertierbar ist, somit $A^{-1} = S$.

Rückblick: praktische Beispiele, Fragen, Anwendungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Frage D3A: segensreicher Matrixkalkül

(0) Wie erklären Sie Matrizen $\mathbb{K}^{m\times n}$ und das Rechnen damit?

(1) Ist jede invertierbare Matrix quadratisch?

(2) Wie bringen Sie jede Matrix A in Zeilenstufenform dank Gauß?

(3) Wie lösen Sie damit jedes lineare Gleichungssystem $Ax = b$?

(4) Wie invertieren Sie A zu B mit $AB = 1$ und $BA = 1$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel D

Bonusmaterial

0	1	2	3	4	5	6	7	8	9	10
0	9	16	21	24	25	24	21	16	9	0

Erwartete Reisezeit bis zum Rand bei zufälliger Irrfahrt auf diesem linearen Spielfeld

If you can reduce a mathematical problem to a problem in linear algebra, you can most likely solve it, provided that you know enough linear algebra. Therefore, a thorough grounding in linear algebra is highly desirable. A sound undergraduate education should offer a second course on the subject, at the senior level. [...] I conclude with a plea to include the simplest aspects of linear algebra in high-school teaching.

Peter Lax (1926–2025), *Linear Algebra and Applications* (2013)

Inhalt dieses Kapitels D

5 Schöne Beispiele und spektakuläre Anwendungen

6 Matrizen in der Wahrscheinlichkeitsrechnung

7 Effizient Rechnen mit Matrizen

8 Schnelle Matrixmultiplikation nach Strassen

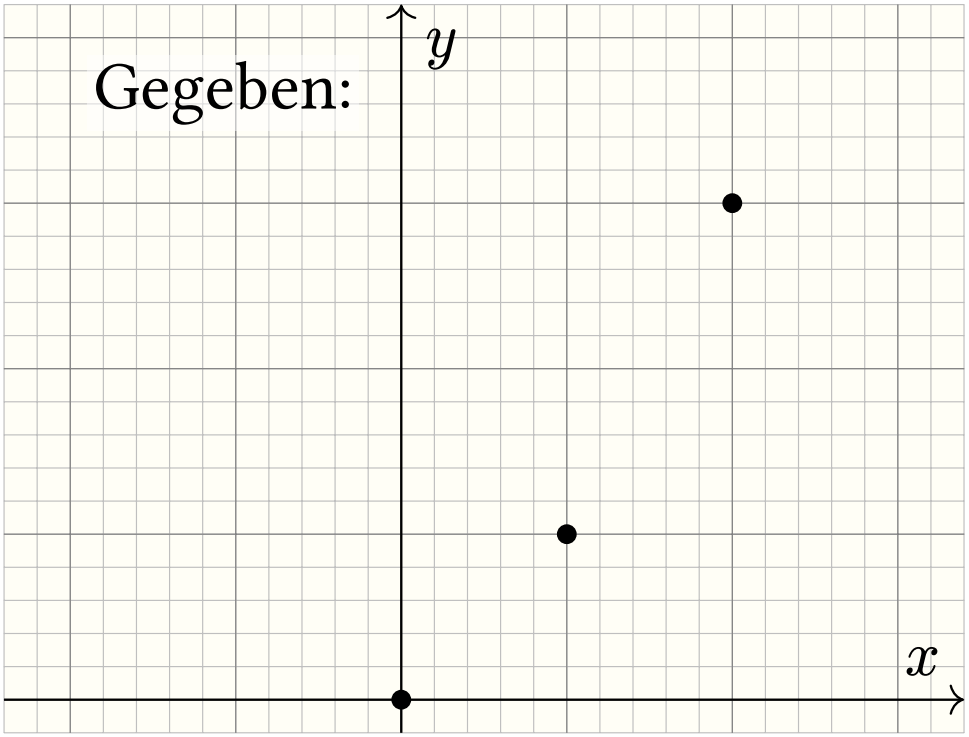
Dies ist nur die Saalversion ohne Erläuterungen.

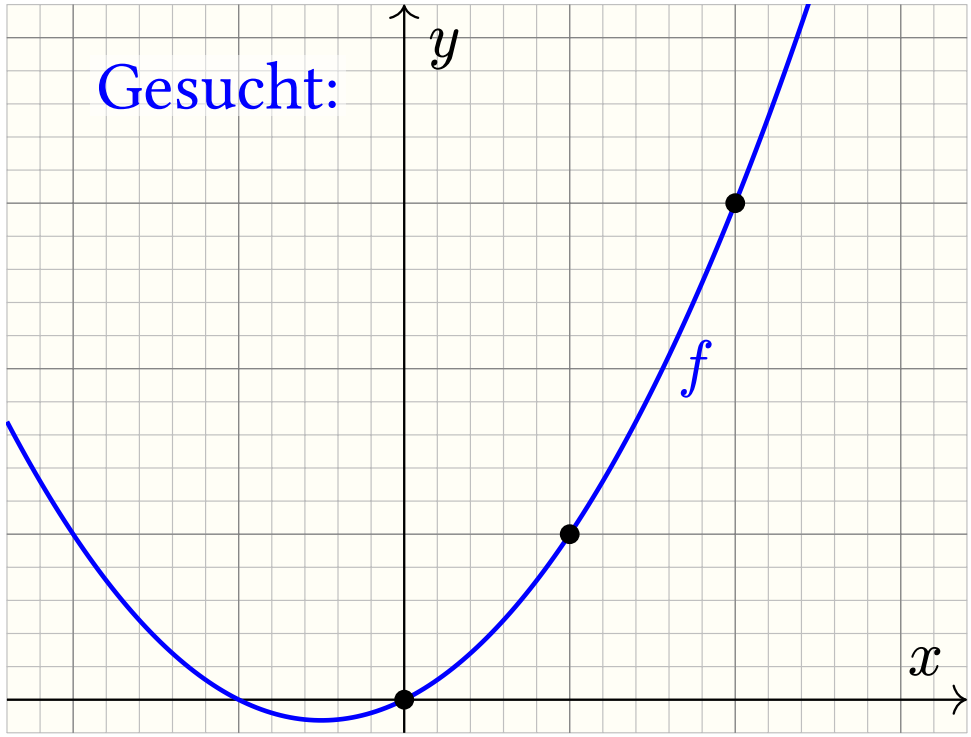
Ausführliche Erläuterungen bietet die Vollversion.

Anwendungsbeispiel: Polynominterpolation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Beispiel D5A: Polynominterpolation

Sei $\mathbb{K}$ ein Körper, etwa $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$. Vorgegeben seien die Datenpunkte $(x_0, y_0), \dots, (x_n, y_n) \in \mathbb{K}^2$ 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.

Anwendungsbeispiel: Polynominterpolation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe:

(0) Schreiben Sie das Problem als lineares Gleichungssystem.

(1) Gibt es immer *mindestens* eine Lösung $P \in \mathbb{K}[X]_{\leq n}$?

(2) Gibt es immer *genau* eine Lösung $P \in \mathbb{K}[X]_{\leq n}$?

Lösung: (0) Wir lösen $Vc = y$ mit der Vandermonde–Matrix

$$V = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ 1 & x_2 & x_2^2 & \dots & x_2^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix} \quad \text{sowie} \quad c = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \quad \text{und} \quad y = \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}.$$

(1) Ja, zu jeder Problemstellung y existiert die Lagrange–Interpolation:

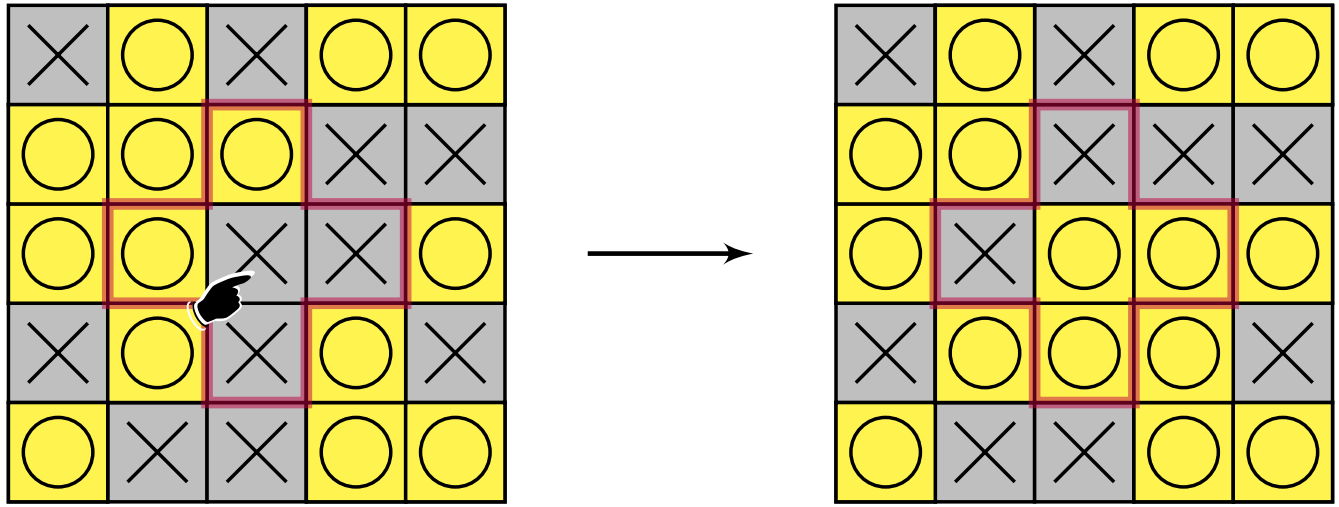
$$L(X) := \sum_{i=0}^{n} y_i L_i(X) \in \mathbb{K}[X]_{\leq n} \quad \text{mit} \quad L_i(X) := \prod_{k \neq i} \frac{X - x_k}{x_i - x_k} \in \mathbb{K}[X]_n$$

(2) Ja, dank Satz D2M ist V ist invertierbar, also $c = V^{-1}y$ einzige Lösung.

Es werde Licht! ... dank Linearer Algebra

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Spielregel: Wenn Sie eine Lampe umschalten, dann auch alle Nachbarn.

Aufgabe: Alle Lampen sind aus. Können Sie alle anschalten? Wie?

Es werde Licht! ... dank Linearer Algebra

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

1	2	3
4	5	6
7	8	9

Welche Knöpfe wurden gedrückt? Dies codieren wir durch $x \in \mathbb{Z}_2^n$.
Welche Lampen brennen am Ende? Dies codieren wir durch $y \in \mathbb{Z}_2^n$.
Die Zuordnung $x \mapsto y$ ist $\mathbb{Z}_2$–linear, also gilt $y = Ax$ mit $A \in \mathbb{Z}_2^{n \times n}$:

$$A = \left[\begin{array}{ccc|ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right], \quad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{bmatrix}, \quad y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \end{bmatrix}.$$

Es werde Licht! ... dank Linearer Algebra

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$X = \left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc}
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right]$$

$$X' = \left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
\hline
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1
\end{array}\right]$$

Es werde Licht! … dank Linearer Algebra

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Mit welcher Umschaltung x gelangen wir von „alle aus“ zu „alle an“?

$$A^{-1} = \left[\begin{array}{ccc|ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}\right], \quad y = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad x = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Zufällige Irrfahrt und harmonische Gewinnerwartung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

0	1	2	3	4	5	6	7	8
7€								23€

(0) Welche Gewinnerwartung $u(x)$ hat jedes Feld $x \in X = \{0, \dots, 8\}$?
(1) Variante: Jeder Zug kostet $c(x) = -1$€. Ab wo würden Sie spielen?

Lösung: Für jedes innere Feld $x \in X^\circ = \{1, \dots, 7\}$ gilt

$$u(x) = \tfrac{1}{2}u(x-1) + \tfrac{1}{2}u(x+1) + c(x).$$

Mögliche Lösungen:

7	9	11	13	15	17	19	21	23
7	2	-1	-2	-1	2	7	14	23

Zufällige Irrfahrt und harmonische Gewinnerwartung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

0	1	2	3	4	5	6	7	8
7	9	11	13	15	17	19	21	23

Lösung: (0) Für $x \in X = \{0, \dots, 8\}$ suchen wir $u_x = u(x)$. Wir haben:

$$
\begin{aligned}
u_0 &= 7 \\
-\tfrac{1}{2}u_0 + u_1 - \tfrac{1}{2}u_2 &= 0 \\
-\tfrac{1}{2}u_1 + u_2 - \tfrac{1}{2}u_3 &= 0 \\
-\tfrac{1}{2}u_2 + u_3 - \tfrac{1}{2}u_4 &= 0 \\
-\tfrac{1}{2}u_3 + u_4 - \tfrac{1}{2}u_5 &= 0 \\
-\tfrac{1}{2}u_4 + u_5 - \tfrac{1}{2}u_6 &= 0 \\
-\tfrac{1}{2}u_5 + u_6 - \tfrac{1}{2}u_7 &= 0 \\
-\tfrac{1}{2}u_6 + u_7 - \tfrac{1}{2}u_8 &= 0 \\
u_8 &= 23
\end{aligned}
$$

Zufällige Irrfahrt und harmonische Gewinnerwartung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

0	1	2	3	4	5	6	7	8
7	2	-1	-2	-1	2	7	14	23

Lösung: (1) Für $x \in X = \{0, \dots, 8\}$ suchen wir $u_x = u(x)$. Wir haben:

$$
\begin{aligned}
u_0 &= 7 \\
-\tfrac{1}{2}u_0 + u_1 - \tfrac{1}{2}u_2 &= c_1 \\
-\tfrac{1}{2}u_1 + u_2 - \tfrac{1}{2}u_3 &= c_2 \\
-\tfrac{1}{2}u_2 + u_3 - \tfrac{1}{2}u_4 &= c_3 \\
-\tfrac{1}{2}u_3 + u_4 - \tfrac{1}{2}u_5 &= c_4 \\
-\tfrac{1}{2}u_4 + u_5 - \tfrac{1}{2}u_6 &= c_5 \\
-\tfrac{1}{2}u_5 + u_6 - \tfrac{1}{2}u_7 &= c_6 \\
-\tfrac{1}{2}u_6 + u_7 - \tfrac{1}{2}u_8 &= c_7 \\
u_8 &= 23
\end{aligned}
$$

Erwartete Reisezeit bis zum Rand

0	1	0								
0	2	2	0							
0	3	4	3	0						
0	4	6	6	4	0					
0	5	8	9	8	5	0				
0	6	10	12	12	10	6	0			
0	7	12	15	16	15	12	7	0		
0	8	14	18	20	20	18	14	8	0	
0	9	16	21	24	25	24	21	16	9	0

Übung: Auf $X = \{0, \dots, n\}$ gilt $u(x) = x(n - x)$.

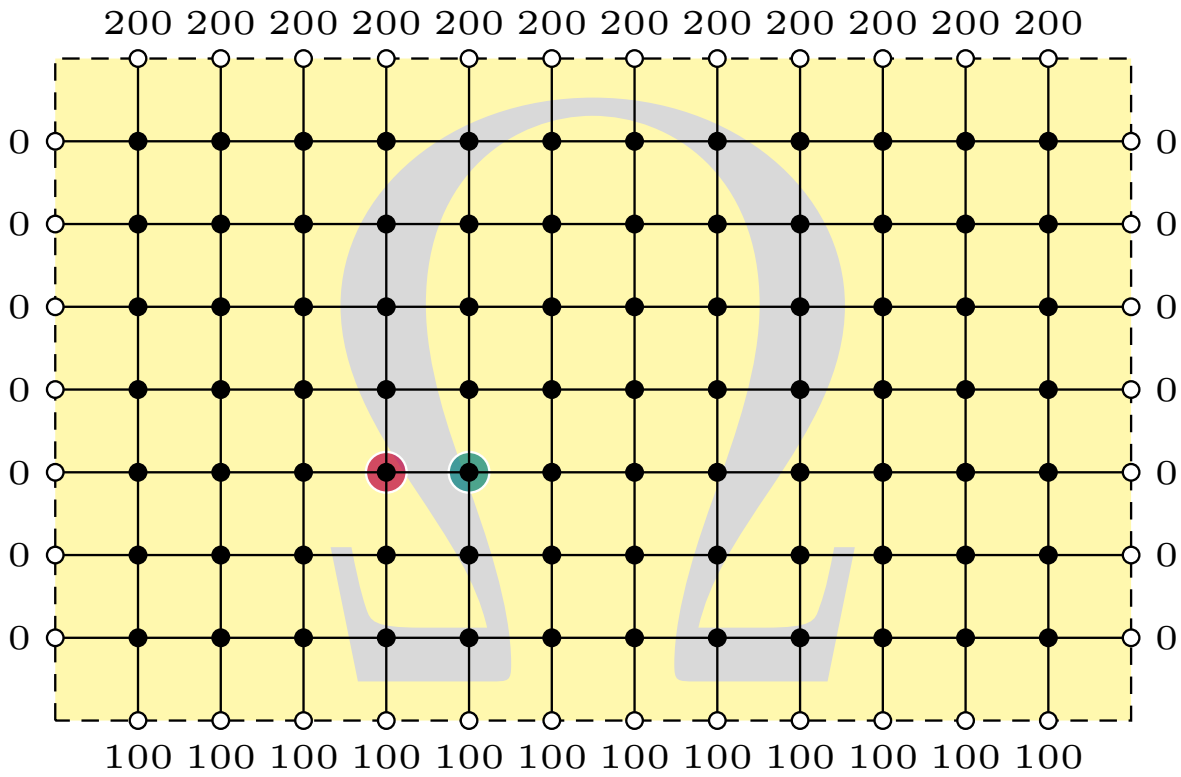
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Irrfahrten und Potentiale: das Dirichlet–Problem

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



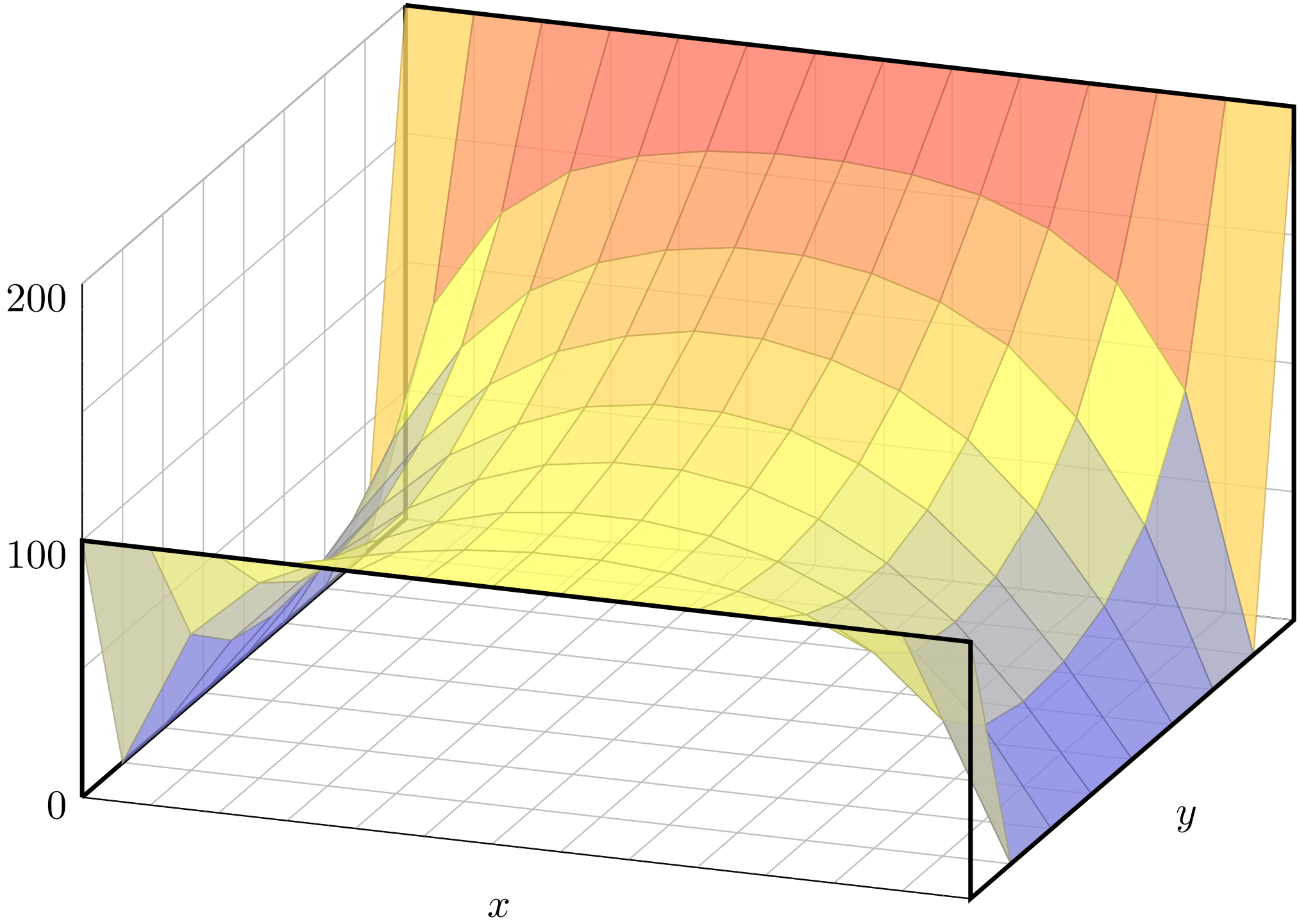
Sie ziehen mit Wkt $\frac{1}{4}$ nach links / rechts / oben / unten.

Das Spiel endet am Rand mit dem gezeigten Gewinn.

Für welche Startpunkte würden Sie 100 zahlen?

Aufgabe: (1) Wie groß ist die Gewinnerwartung $u(x, y)$ auf jedem Feld?

Irrfahrten und Potentiale: das Dirichlet–Problem



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Irrfahrten und Potentiale: das Dirichlet–Problem

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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 Funktion $u : \mathbb{Z}^2 \supset \Omega \to \mathbb{R}$ nennen wir (diskret) **harmonisch**.
Übung: Lösen Sie diese Gleichungen, etwa mit einer Tabellenkalkulation!

	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: Minimum-Maximum-Prinzip

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz D6A: Minimum-Maximum-Prinzip, Eindeutigkeit und 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 $\max_\Omega u = \max_{\partial\Omega} u$.

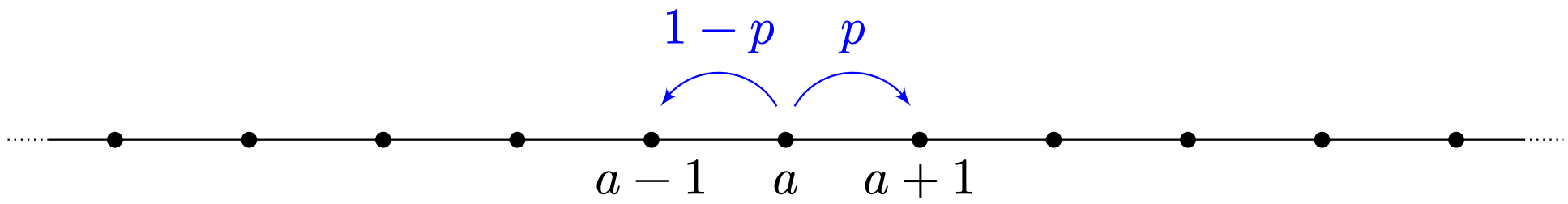
(2) Für je zwei harmonische Funktionen $u, \tilde{u} : \Omega \to \mathbb{R}$ folgt:
Monotonie: Aus $u \geq \tilde{u}$ auf dem Rand $\partial\Omega$ folgt $u \geq \tilde{u}$ auf ganz Ω.
Eindeutigkeit: Aus $u = \tilde{u}$ auf dem Rand $\partial\Omega$ folgt $u = \tilde{u}$ auf ganz Ω.

(3) Existenz: Zu jeder beliebig vorgegebenen Randfunktion $v : \partial\Omega \to \mathbb{R}$ existiert genau eine harmonische Funktion $u : \Omega \to \mathbb{R}$ mit $u|_{\partial\Omega} = v$.

Skizze: (1) Sei $z \in \Omega$ eine Minimalstelle. Im Fall $z \in \partial\Omega$ 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.

(2) Auch $v = u - \tilde{u}$ ist harmonisch. Aus $v \geq 0$ auf $\partial\Omega$ folgt $v \geq 0$ auf Ω.
(3) Wir haben so viele Unbekannte wie Gleichungen. Für jede rechte Seite existiert nach (2) höchstens eine Lösung, also genau eine. (Satz D2M) $\boxed{\text{QED}}$

Markov–Ketten: Konstruktion dank Pfadregel



Wahrscheinlichkeit dank Pfadregel:

$$\mathbf{P}(\, X_0{=}a_0,\, X_1{=}a_1,\, \ldots,\, X_n{=}a_n\,) = q_0(a_0)\, p_0(a_0, a_1) \cdots p_{n-1}(a_{n-1}, a_n)$$

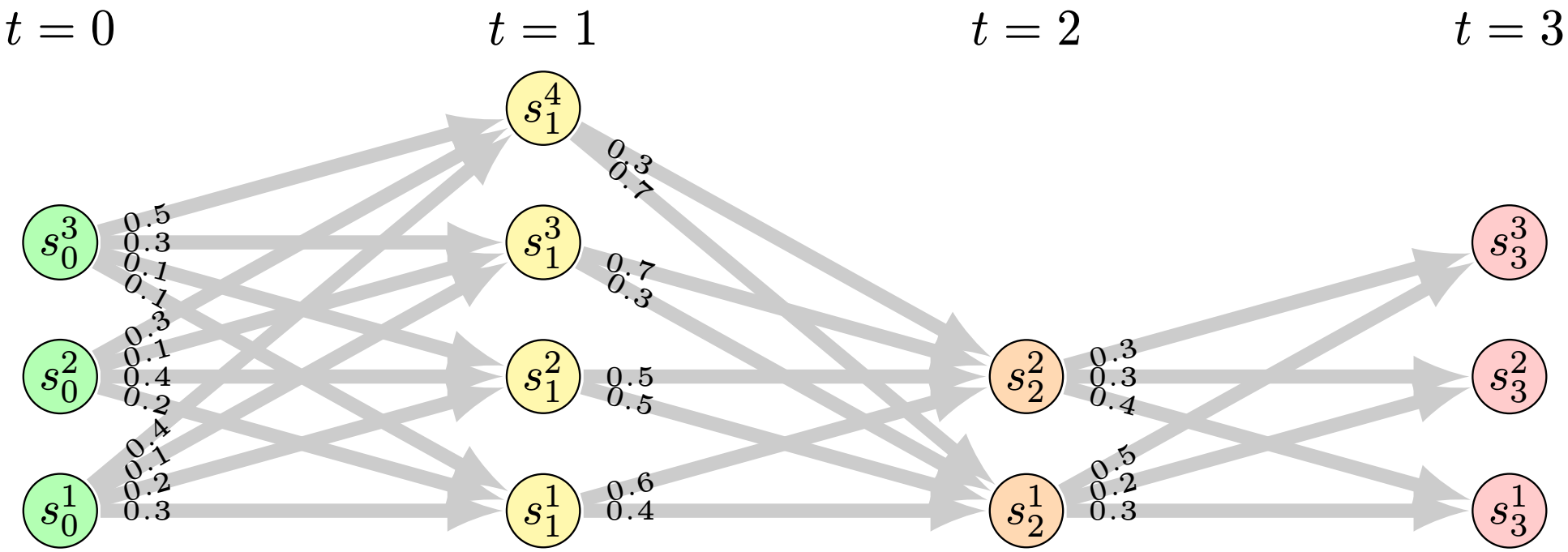
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Markov–Ketten: Pfadregel & Summenregel = Matrixprodukt

Dies ist nur die Saalversion ohne Erläuterungen.

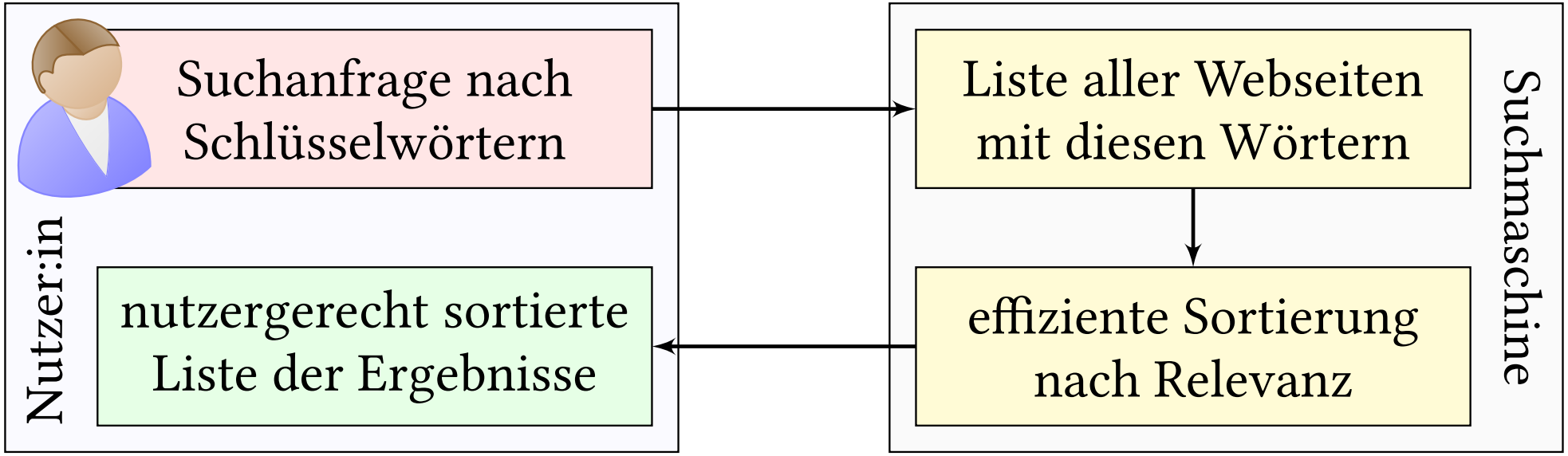
Ausführliche Erläuterungen bietet die Vollversion.



$$[S_0] \xrightarrow{P_0} [S_1] \xrightarrow{P_1} [S_2] \xrightarrow{P_2} [S_3]$$

$$\begin{bmatrix} 0.3 & 0.2 & 0.1 & 0.4 \\ 0.2 & 0.4 & 0.1 & 0.3 \\ 0.1 & 0.1 & 0.3 & 0.5 \end{bmatrix} \qquad \begin{bmatrix} 0.4 & 0.6 \\ 0.5 & 0.5 \\ 0.3 & 0.7 \\ 0.7 & 0.3 \end{bmatrix} \qquad \begin{bmatrix} 0.3 & 0.2 & 0.5 \\ 0.4 & 0.3 & 0.3 \end{bmatrix}$$

Die Mathematik hinter Google



Mathematik: Wie misst man Relevanz von Informationen?

Informatik: Wie verarbeitet man enorm große Datenmengen?

Finanzstrategie: Wie verdient man Geld mit einem Gratisprodukt?

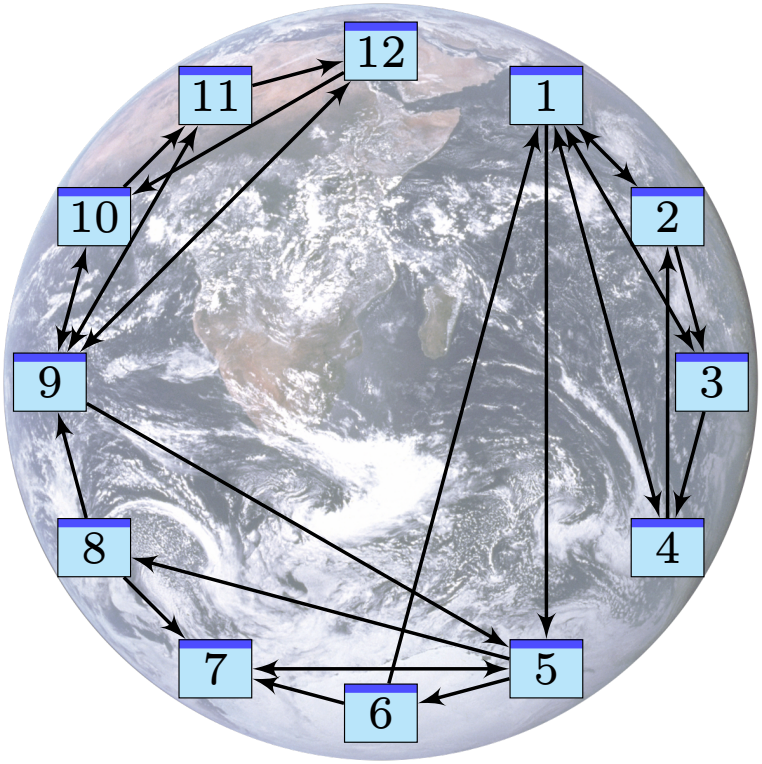
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

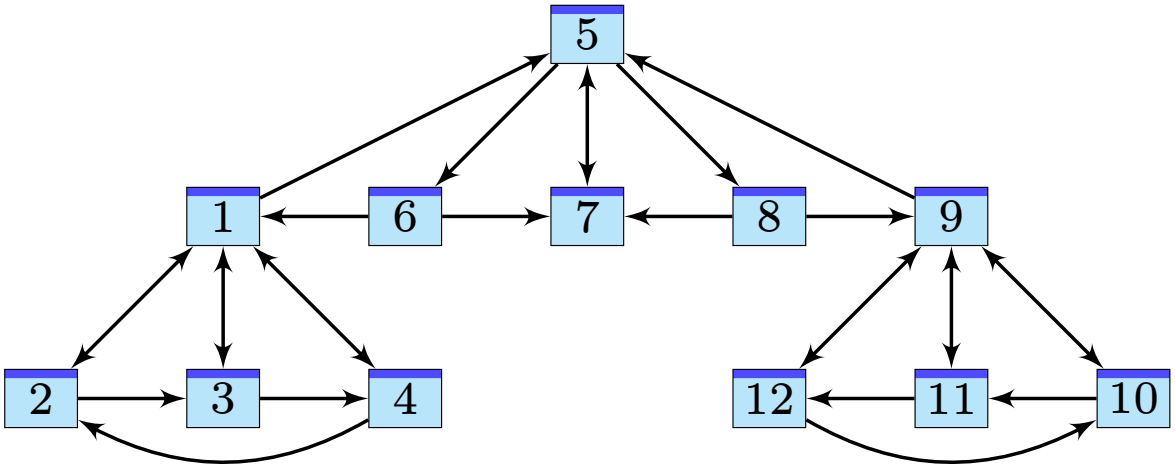
Chaos und Struktur im Web

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Versuch einer hierarchischen Anordnung:



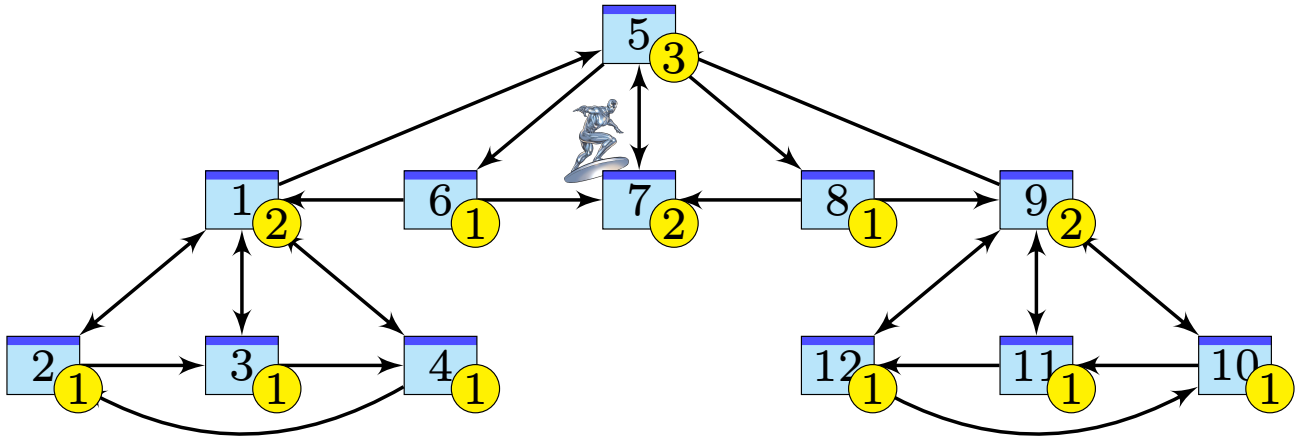
Eine Seite ist populär, wenn viele Seiten auf sie verweisen? Zu naiv! ☹

Eine Seite ist populär, wenn viele populäre Seiten auf sie verweisen. ☺

Irrfahrt eines zufälligen Surfers

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Googles Heuristik: Aufenthaltswkt ∼ Popularität ∼ Relevanz

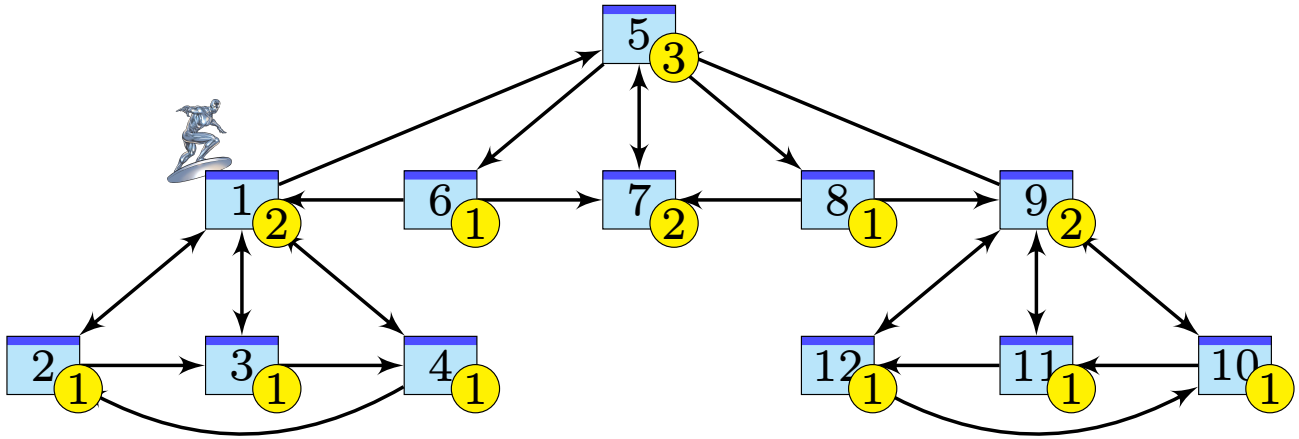
Aufgabe: Berechnen Sie die Aufenthaltswkten bei Start auf Seite 7.

	1	2	3	4	5	6	7	8	9	10	11	12
$t = 0$	.000	.000	.000	.000	.000	.000	1.00	.000	.000	.000	.000	.000
$t = 1$	.000	.000	.000	.000	1.00	.000	.000	.000	.000	.000	.000	.000
$t = 2$	.000	.000	.000	.000	.000	.333	.333	.333	.000	.000	.000	.000
$t = 3$	.167	.000	.000	.000	.333	.000	.333	.000	.167	.000	.000	.000
$t = 4$	.000	.042	.042	.042	.417	.111	.111	.111	.000	.042	.042	.042
$t = 5$	.118	.021	.021	.021	.111	.139	.250	.139	.118	.021	.021	.021
...												
$t = 29$	.117	.059	.059	.059	.177	.059	.117	.059	.117	.059	.059	.059
$t = 30$	.117	.059	.059	.059	.177	.059	.117	.059	.117	.059	.059	.059

Irrfahrt eines zufälligen Surfers

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Googles Heuristik: Aufenthaltswkt $\sim$ Popularität $\sim$ Relevanz

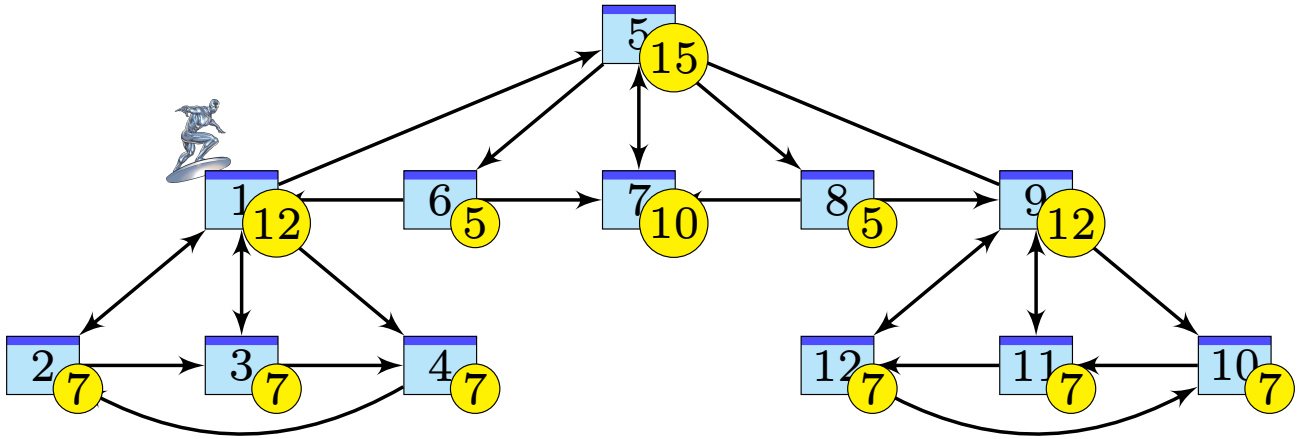
Aufgabe: Berechnen Sie die Aufenthaltswkten bei Start auf Seite 1.

	1	2	3	4	5	6	7	8	9	10	11	12
$t = 0$	1.00	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
$t = 1$	.000	.250	.250	.250	.250	.000	.000	.000	.000	.000	.000	.000
$t = 2$	.375	.125	.125	.125	.000	.083	.083	.083	.000	.000	.000	.000
$t = 3$	.229	.156	.156	.156	.177	.000	.083	.000	.042	.000	.000	.000
$t = 4$	.234	.135	.135	.135	.151	.059	.059	.059	.000	.010	.010	.010
$t = 5$	.233	.126	.126	.126	.118	.050	.109	.050	.045	.005	.005	.005
...												
$t = 69$	.117	.059	.059	.059	.177	.059	.117	.059	.117	.059	.059	.059
$t = 70$	.117	.059	.059	.059	.177	.059	.117	.059	.117	.059	.059	.059

Zufall und Notwendigkeit: Googles PageRank

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Googles Heuristik: Aufenthaltswkt $\sim$ Popularität $\sim$ Relevanz

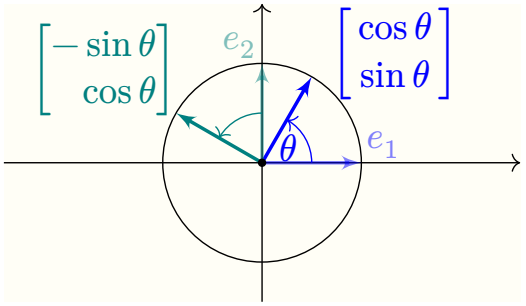
Aufgabe: Wie verläuft die Diffusion bei Sprunghaftigkeit $q = 0.15$?

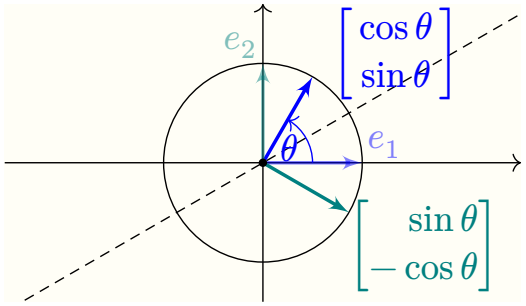
	1	2	3	4	5	6	7	8	9	10	11	12
$t = 0$	1.00	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
$t = 1$	.013	.225	.225	.225	.225	.013	.013	.013	.013	.013	.013	.013
$t = 2$	.305	.111	.111	.111	.028	.076	.087	.076	.034	.020	.020	.020
$t = 3$	.186	.124	.124	.124	.158	.021	.085	.021	.071	.028	.028	.028
$t = 4$	.180	.105	.105	.105	.140	.057	.075	.057	.057	.040	.040	.040
$t = 5$	.171	.095	.095	.095	.126	.052	.101	.052	.087	.042	.042	.042
...												
$t = 29$	.120	.066	.066	.066	.150	.055	.102	.055	.120	.066	.066	.066
$t = 30$	.120	.066	.066	.066	.150	.055	.102	.055	.120	.066	.066	.066

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel E

Aufbau des Zahlensystems II: reelle und komplexe Zahlen





There are exactly four normed division algebras: [...] The real numbers are the dependable breadwinner of the family, the complete ordered field we all rely on. The complex numbers are a slightly flashier but still respectable younger brother: not ordered, but algebraically complete. The quaternions, being noncommutative, are the eccentric cousin who is shunned at important family gatherings. But the octonions are the crazy old uncle nobody lets out of the attic.

John Baez, *The Octonions* (2002)

Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels E

1 Was sind die reellen Zahlen?

2 Analytische Geometrie

3 Von reellen zu komplexen Zahlen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vorschau: praktische Beispiele, Fragen, Anwendungen

$$\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \mathbb{H}$$

Frage E0A: Aufbau des Zahlensystems – Vollständigkeit & Abschluss

(0) Wie konstruieren Sie den Körper $(\mathbb{R}, +, \cdot, \leq)$ der reellen Zahlen?

(1) Lässt sich jede reelle Zahl $x \in \mathbb{R}$ dezimal darstellen?
Was ist $x := 0.99999\ldots$? Gilt $x = 1$?

(2) Wie messen Sie im Raum $\mathbb{R}^n$ Längen und Winkel?
Wie beschreiben Sie Drehungen und Spiegelungen?

(3) Wie konstruieren Sie den Körper $\mathbb{C} = \mathbb{R}[\mathrm{i}]$ mit $\mathrm{i}^2 = -1$?
Wie berechnen Sie Potenzen $z \mapsto z^n$ und Wurzeln w mit $w^n = z$?

(4) Was besagt der Fundamentalsatz der Algebra?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Geordnete Ringe und Körper

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition E1A: geordneter Ring, positive Elemente

Eine **Ordnung** auf dem Ring $(R, +, \cdot)$ ist eine Teilmenge $R_{\geq 0} = P \subseteq R$ mit $P \cap (-P) = \{0\}$ und $P \cup (-P) = R$ sowie $P + P \subseteq P$ und $P \cdot P \subseteq P$.

Beispiele: $(\mathbb{Z}, +, \cdot, \mathbb{N})$ und $(\mathbb{Q}, +, \cdot, \mathbb{Q}_{\geq 0})$ mit $\mathbb{Q}_{\geq 0} = \{\, z/n \mid z \in \mathbb{N},\ n \in \mathbb{N}^* \,\}$.

Für Ringelemente $a, b \in R$ definieren wir $a \leq b$ durch $b - a \in P$. Damit gilt **Refl**: $a \leq a$, **ASym**: $a \leq b \wedge b \leq a \Rightarrow a = b$, **Trans**: $a \leq b \wedge b \leq c \Rightarrow a \leq c$.

Wir definieren die strikte Kleiner-Relation $a < b$ durch $a \leq b \wedge a \neq b$. Symmetrisch hierzu schreiben wir $a \geq b$ für $b \leq a$ und $a > b$ für $b < a$.

Untere und obere Schranken

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $M \subseteq R$ eine Teilmenge. Ein Element $s \in R$ heißt **obere Schranke** der Menge M, geschrieben $M \leq s$, falls $x \leq s$ für alle $x \in M$ gilt.

$$\mathrm{ObSch}_{(R,\leq)}(M) := \{\, s \in R \mid M \leq s \,\}$$
$$\mathrm{UnSch}_{(R,\leq)}(M) := \{\, s \in R \mid s \leq M \,\}$$

Beispiel: Für $I =]0,1[_{\mathbb{Q}}$ gilt $\mathrm{ObSch}_{\mathbb{Q}}(I) = [1,+\infty[_{\mathbb{Q}}$.
Für $J = \{\, x \in \mathbb{Q} \mid x^2 \leq 2 \,\}$ gilt $\mathrm{ObSch}_{\mathbb{Q}}(J) =]\sqrt{2},+\infty[_{\mathbb{Q}}$.

Kleinste und größte Elemente

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir nennen s ein **größtes Element** von M, falls $s \in M$ und $M \leq s$ gilt.
Wir nennen s ein **kleinstes Element** von M, falls $s \in M$ und $s \leq M$ gilt.

$$\mathrm{Gr}_{(R,\leq)}(M) := \{\, s \in M \mid M \leq s \,\}$$
$$\mathrm{Kl}_{(R,\leq)}(M) := \{\, s \in M \mid s \leq M \,\}$$

Beispiel: In $(\mathbb{Q}, \leq)$ gilt $\mathrm{Gr}([0,1]_{\mathbb{Q}}) = \{1\}$, aber $\mathrm{Gr}(]0,1[_{\mathbb{Q}}) = \emptyset$.

Infimum und Supremum

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Ein **Supremum** von M ist eine kleinste obere Schranke.
Ein **Infimum** von M ist eine größte untere Schranke.

$$\begin{aligned} \operatorname{Sup}(M) &:= \operatorname{Kl}\operatorname{ObSch}(M) \\ \operatorname{Inf}(M) &:= \operatorname{Gr}\operatorname{UnSch}(M) \end{aligned}$$

Beispiel: In $(\mathbb{Q}, \leq)$ gilt $\operatorname{Sup}(]0,1[_{\mathbb{Q}}) = \{1\}$ und $\operatorname{Sup}(\{\, x \in \mathbb{Q} \mid x^2 \leq 2 \,\}) = \emptyset$.

Definition E1D: Supremumseigenschaft

Eine geordnete Menge $(R, \leq)$ heißt **vollständig**, falls jede nicht-leere nach oben beschränkte Teilmenge $M \subseteq R$ ein Supremum in R besitzt.

Der Körper der reellen Zahlen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir wünschen uns $(\mathbb{R}, +, \cdot, \leq)$ als vollständig geordneten Körper.
Existiert solch ein Körper? Mögliche Konstruktionen gelingen durch...

0. Ziffernfolgen
1. Dedekind–Schnitte
2. Cauchy–Folgen
3. Intervallschachtelung

```
from Analysis import Reals
```

Satz E1E: der Körper der reellen Zahlen → Analysis ♥

(1) Es existiert ein vollständig geordneter Körper $(\mathbb{R}, +, \cdot, \leq)$.
(2) Zwischen je zwei existiert ein eindeutiger Isomorphismus.

Dezimaldarstellung

$$
\begin{aligned}
1/3 &= 0.\,33333\,33333\,33333\,33333\,33333\,33333\,33333\,33333\,33333\,33333\ldots \in \mathbb{Q}\\
2/3 &= 0.\,66666\,66666\,66666\,66666\,66666\,66666\,66666\,66666\,66666\,66666\ldots \in \mathbb{Q}\\
1 &= 0.\,99999\,99999\,99999\,99999\,99999\,99999\,99999\,99999\,99999\,99999\ldots \in \mathbb{Q}\\
\sqrt{2} &= 1.\,41421\,35623\,73095\,04880\,16887\,24209\,69807\,85696\,71875\,37694\ldots \notin \mathbb{Q}\\
\mathrm{e} &= 2.\,71828\,18284\,59045\,23536\,02874\,71352\,66249\,77572\,47093\,69995\ldots \notin \mathbb{Q}\\
\pi &= 3.\,14159\,26535\,89793\,23846\,26433\,83279\,50288\,41971\,69399\,37510\ldots \notin \mathbb{Q}
\end{aligned}
$$

Satz E1F: Darstellung in Basis $B \in \mathbb{N}_{\geq 2}$ → Analysis ♥

(0) Jede Ziffernfolge $a \in \mathbb{Z}_B^{\mathbb{Z}}$ mit $a_k = 0$ für $k \ll 0$ definiert eine reelle Zahl

$$[a]_B \quad := \quad \sum_{k\in\mathbb{Z}} a_k B^{-k} \quad := \sup_{n\in\mathbb{N}} \sum_{k=\ell}^{n} a_k B^{-k} \quad \in \mathbb{R}_{\geq 0}.$$

(1) Jede reelle Zahl $x \in \mathbb{R}_{\geq 0}$ lässt sich so darstellen, (2) manche doppelt:

$$\left.\begin{aligned} a &= (\ldots, \quad a_n, B-1, B-1, B-1, \ldots)\\ a' &= (\ldots, a_n+1, \quad 0, \quad 0, \quad 0, \ldots)\end{aligned}\right\} \implies [a] = [a']$$

(3) Außerhalb dieses Sonderfalls (2) ist die Darstellung eindeutig.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Reelle Wurzelfunktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $n \in \mathbb{N}_{\geq 1}$. Die Potenzfunktion $p_n : \mathbb{Q}_{\geq 0} \to \mathbb{Q}_{\geq 0} : x \mapsto x^n$ ist injektiv (da streng monoton), aber für $n \geq 2$ nicht surjektiv (da $2, 3, 5, \ldots \notin \operatorname{Im} p_n$).

Satz E11: die reelle Wurzelfunktion $x \mapsto \sqrt[n]{x}$ für $x \geq 0$ → Analysis ♥

(1) Sei $n \in \mathbb{N}_{\geq 1}$. Die Potenzfunktion $p_n : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto x^n$ ist injektiv (da streng monoton) und zudem surjektiv (dank Zwischenwertsatz).

(2) Zu jeder Zahl $x \in \mathbb{R}_{\geq 0}$ existiert genau eine n-te Wurzel $w \in \mathbb{R}_{\geq 0}$, es gilt also $w^n = x$, geschrieben $\sqrt[n]{x} := w = \sup\{\, a \in \mathbb{Q}_{\geq 0} \mid a^n \leq x \,\}$.

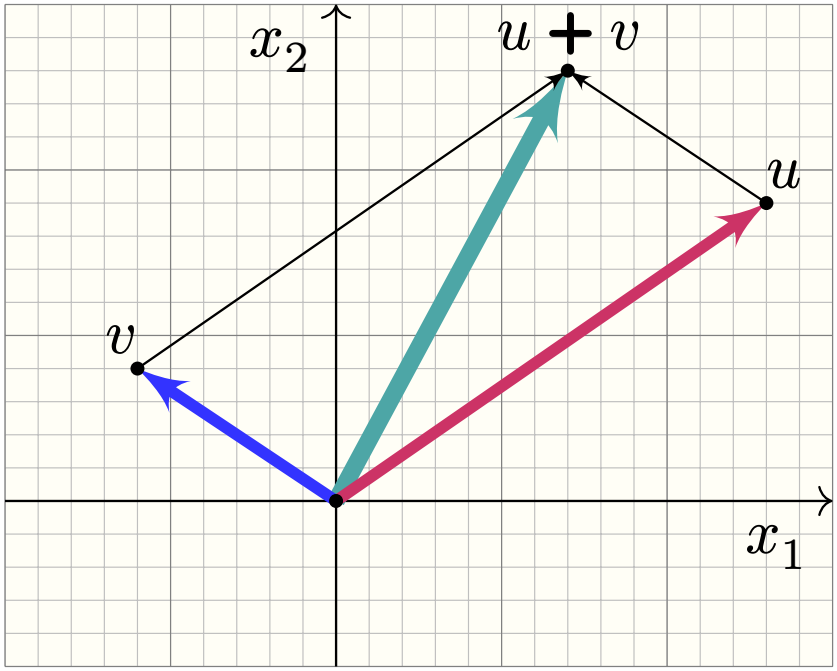
Beispiel: Wir betrachten die Menge $U := \{\, a \in \mathbb{Q}_{\geq 0} \mid a^2 \leq 2 \,\}$.
Sie ist nicht-leer, denn $U \supset \{\, 1 < 1.4 < 1.41 < 1.414 < \ldots \,\}$.
Obere Schranken sind $U \leq \ldots \leq 1.415 \leq 1.42 \leq 1.5 \leq 2$.

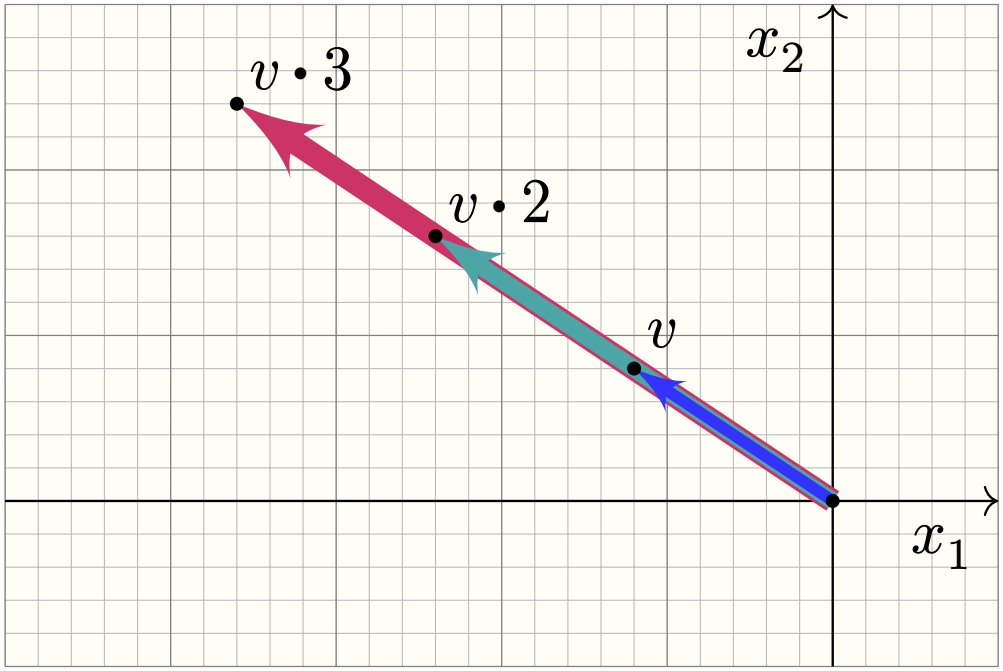
☹ In $(\mathbb{Q}, \leq)$ hat U keine *kleinste* obere Schranke, also kein Supremum!
☺ In $(\mathbb{R}, \leq)$ hingegen existiert $w := \sup U \in \mathbb{R}$ und erfüllt $w^2 = 2$.

Addition und Skalierung von Vektoren im $\mathbb{R}^n$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





$$+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n : (u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n)$$

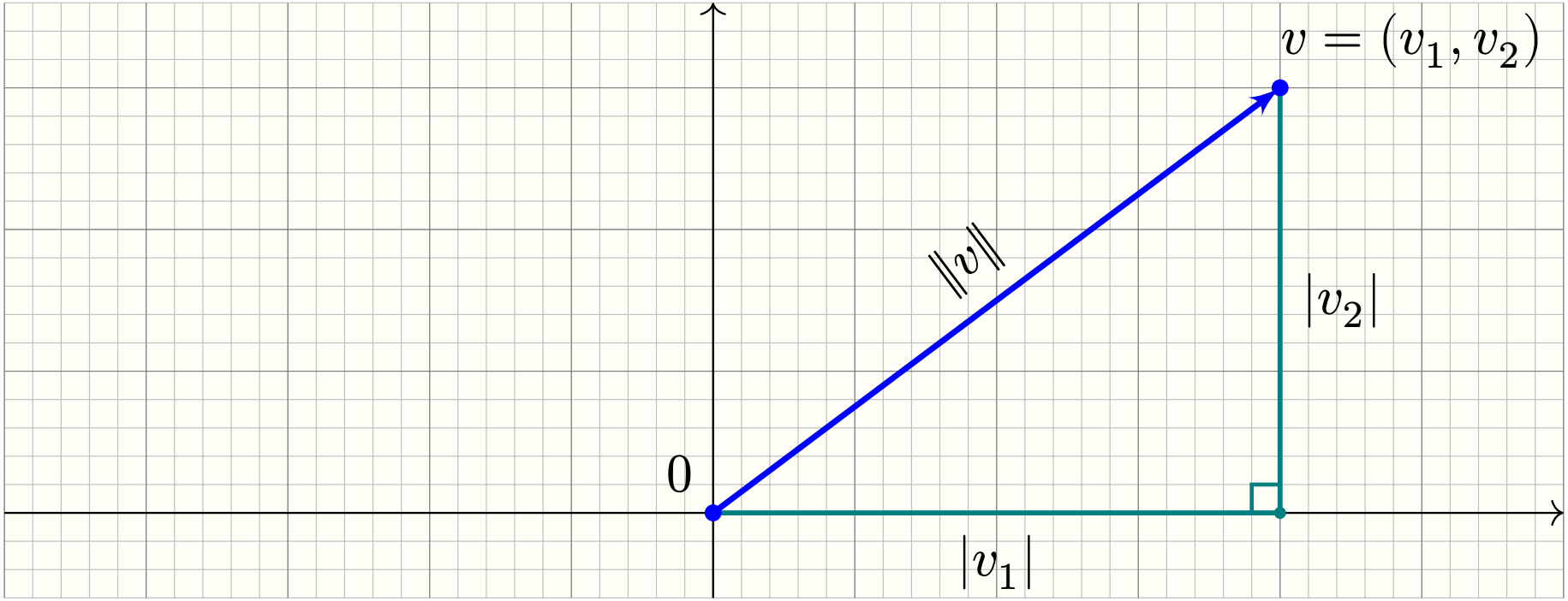
$$\bullet : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n : \quad (v_1, \dots, v_n) \bullet \lambda = (v_1 \cdot \lambda, \dots, v_n \cdot \lambda)$$

$$\circ : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n : \quad \lambda \circ (v_1, \dots, v_n) = (\lambda \cdot v_1, \dots, \lambda \cdot v_n)$$

Euklidische Norm: Länge eines Vektors im $\mathbb{R}^n$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



$$\boxed{|v| = \|v\| = \sqrt{|v_1|^2 + \cdots + |v_n|^2}}$$

Das euklidische Standardskalarprodukt auf $\mathbb{R}^n$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Das **euklidische Skalarprodukt** von zwei Vektoren $u, v \in \mathbb{R}^n$ ist

$$\boxed{\langle u \mid v \rangle = u_1 v_1 + \cdots + u_n v_n.}$$

Die **euklidische Norm** des Vektors $v \in \mathbb{R}^n$ ist definiert durch

$$\boxed{|v| = \|v\| := \sqrt{\langle v \mid v \rangle} = \sqrt{v_1^2 + \cdots + v_n^2}.}$$

Der **euklidische Abstand** zwischen zwei Punkten $u, v \in \mathbb{R}^n$ ist

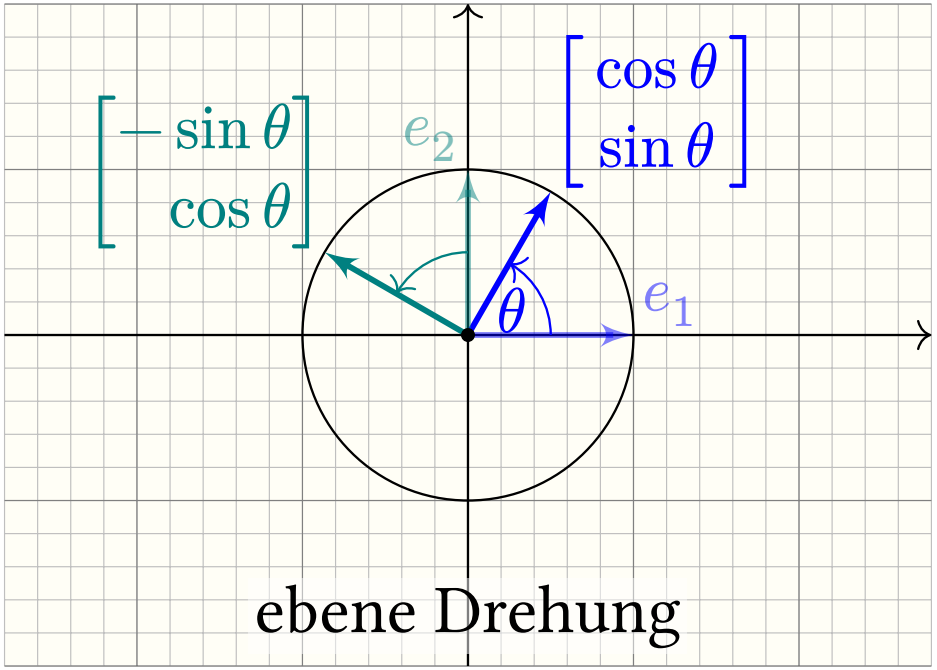
$$\boxed{d(u, v) := |u - v| = \sqrt{(u_1 - v_1)^2 + \cdots + (u_n - v_n)^2}.}$$

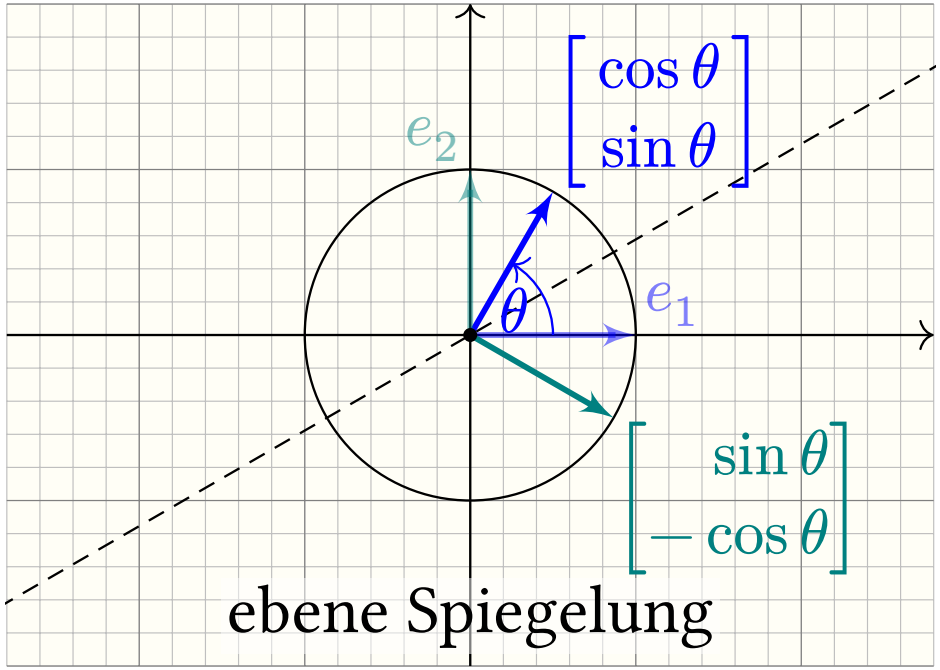
Ebene Drehungen und Spiegelungen als Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sei $\rho_\theta, \sigma_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ die Drehung um den Winkel $\theta \in \mathbb{R}$ bzw. die Spiegelung an der Achse im Winkel $\theta/2$. Schreiben Sie dies als Matrizen!





$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

$$S_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

Die orthogonale Gruppe, generell und speziell

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Berechnen Sie $AA^\top$, $A^\top A$ sowie A^{-1} und $\det A$ für $A = R_\theta, S_\theta$.

$$R_\theta R_\theta^\top = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \det R_\theta = +1$$

$$S_\theta S_\theta^\top = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \det S_\theta = -1$$

Definition E2A: orthogonale Gruppe, generell und speziell

Sei $\mathbb{K}$ ein Körper, etwa $\mathbb{K} = \mathbb{R}$. Die **orthogonale Gruppe** ist

$$\mathrm{GO}_n\,\mathbb{K} := \{\, A \in \mathbb{K}^{n\times n} \mid A^\top A = 1 = AA^\top \,\}.$$

Darin liegt die **spezielle orthogonale Gruppe**

$$\mathrm{SO}_n\,\mathbb{K} = \{\, A \in \mathrm{GO}_n\,\mathbb{K} \mid \det A = 1 \,\}.$$

Die orthogonale Gruppe, generell und speziell

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz E2B: explizite Parametrisierung der Gruppen $\mathrm{SO}_2\,\mathbb{R}$ und $\mathrm{GO}_2\,\mathbb{R}$

$$\begin{aligned} \mathrm{SO}_2\,\mathbb{R} &= \{\, R_\theta \mid \theta \in [0, 2\pi[\,\}^! && \text{alle Drehungen...} \\ \mathrm{GO}_2\,\mathbb{R} &= \mathrm{SO}_2\,\mathbb{R} \sqcup \{\, S_\theta \mid \theta \in [0, 2\pi[\,\}^! && \text{und Spiegelungen} \end{aligned}$$

Die komplexen Zahlen: Motivation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

Wir wünschen uns einen Körper $\mathbb{C} = \mathbb{R}[\mathrm{i}] = \{\, z = x + \mathrm{i}y \mid x, y \in \mathbb{R} \,\}^!$ mit $\mathbb{C} \supset \mathbb{R}$ und $\mathrm{i}^2 = -1$. Falls solch ein Körper $(\mathbb{C}, +, \cdot)$ existiert, so gilt:

$$\begin{aligned} \text{Addition:} \quad (x + \mathrm{i}y) + (x' + \mathrm{i}y') &= (x + x') + \mathrm{i}(y + y') \\ \text{Produkt:} \quad (x + \mathrm{i}y) \cdot (x' + \mathrm{i}y') &= (xx' - yy') + \mathrm{i}(xy' + yx') \end{aligned}$$

Zu jedem Element $z = x + y\mathrm{i}$ haben wir das Negative $-z = -x - y\mathrm{i}$ und das Konjugierte $\overline{z} = x - y\mathrm{i}$. Es gilt $z\overline{z} = x^2 + y^2 \in \mathbb{R}_{\geq 0}$, für $z \neq 0$ also

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

Die komplexen Zahlen: Konstruktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz E3A: Konstruktion des Körpers $\mathbb{C}$ der komplexen Zahlen

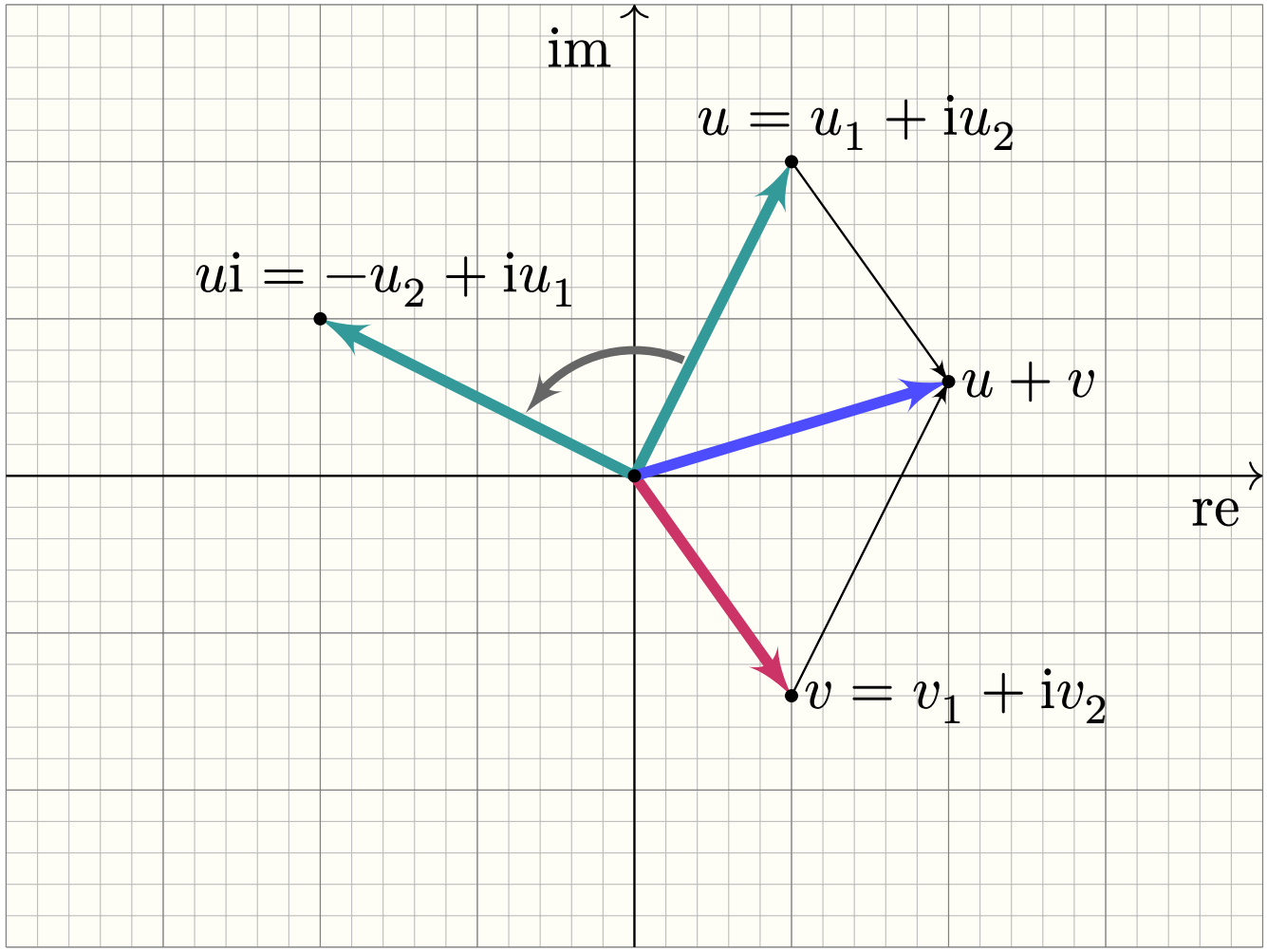
Auf der Menge $\mathbb{C} = \mathbb{R}^2$ definieren wir Addition und Multiplikation durch

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : (x, y) + (x', y') := (\, x + x',\, y + y' \,),$$
$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : (x, y) \cdot (x', y') := (\, xx' - yy',\, xy' + yx' \,).$$

(1) 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 $\mathbb{R} \subseteq \mathbb{C}$. Im Körper $\mathbb{C}$ erfüllt das Element $\mathrm{i} = (0, 1)$ die Eigenschaft $\mathrm{i}^2 = -1$.

Beweis: (1) Im Polynomring $\mathbb{R}[I]$ ist $P = I^2 + 1$ unzerlegbar, also prim. Dank C3M ist $\mathbb{R}[I]_P = \{\, x + yI \mid x, y \in \mathbb{R} \,\}$ ein Körper mit $I^2 = -1$. QED

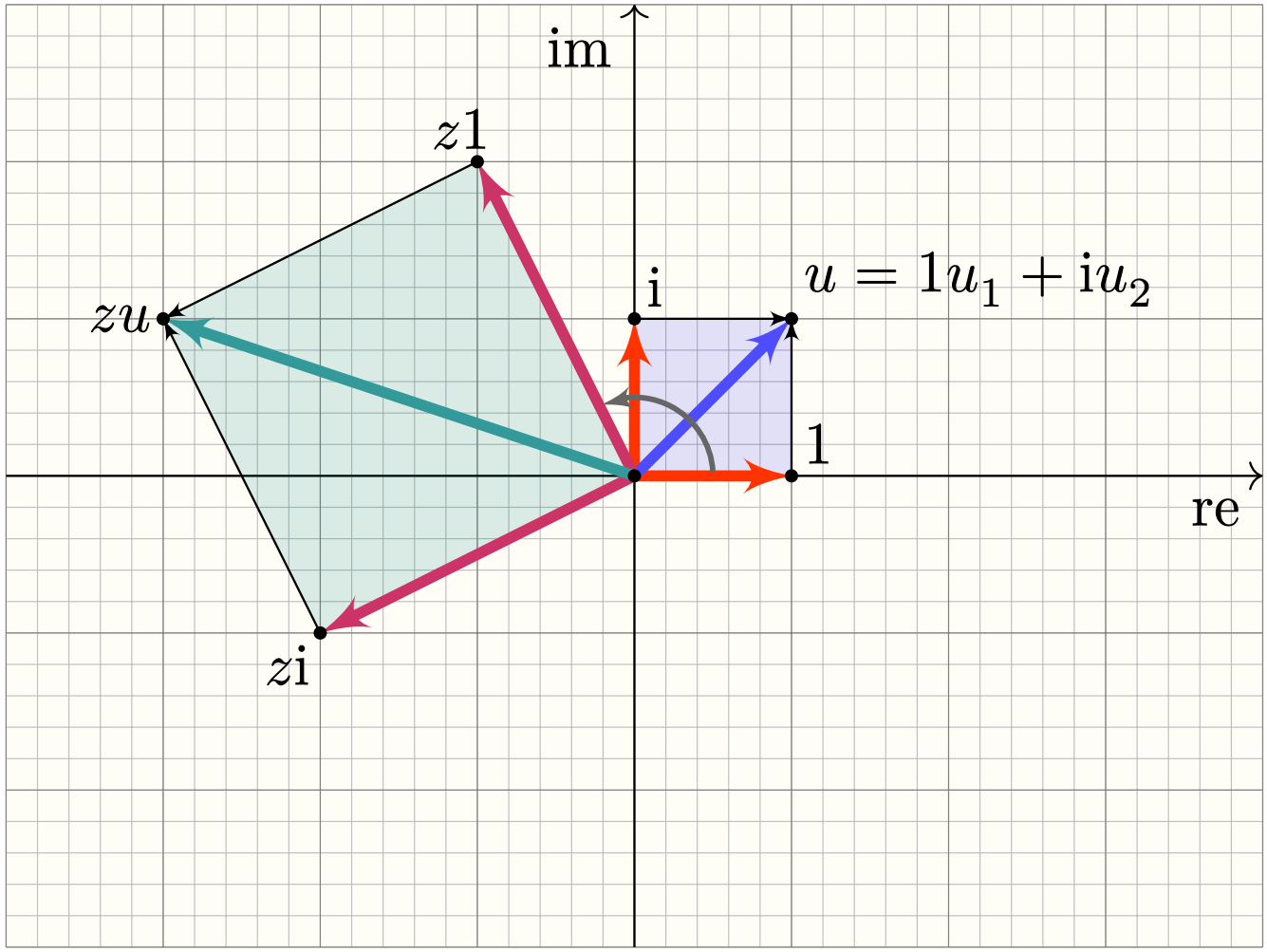
Die komplexe Zahlenebene nach Gauß und Argand



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Multiplikation mit $z \in \mathbb{C}$ ist eine Drehstreckung.



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Matrixkalkül: komplexe Zahlen als reelle 2×2–Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz E3B: die komplexen Zahlen $\mathbb{C}$ als Matrizen über $\mathbb{R}$

$$C := \left\{ z = \left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right] \,\middle|\, x, y \in \mathbb{R} \right\} \leq \mathbb{R}^{2\times 2}$$

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix} \cdot \begin{bmatrix} u & -v \\ v & u \end{bmatrix} = \begin{bmatrix} xu-yv & -(yu+xv) \\ yu+xv & xu-yv \end{bmatrix}$$

In $(C, \cdot)$ ist jedes Element $z \neq 0$ invertierbar, da $\det(z) = x^2 + y^2 > 0$:

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix}^{-1} = \frac{1}{x^2+y^2} \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

Somit ist $(C, +, \cdot)$ ein Divisionsring. Er ist zudem sogar kommutativ:

$$\begin{bmatrix} u & -v \\ v & u \end{bmatrix} \cdot \begin{bmatrix} x & -y \\ y & x \end{bmatrix} = \begin{bmatrix} ux-vy & -(uy+vx) \\ uy+vx & ux-vy \end{bmatrix}$$

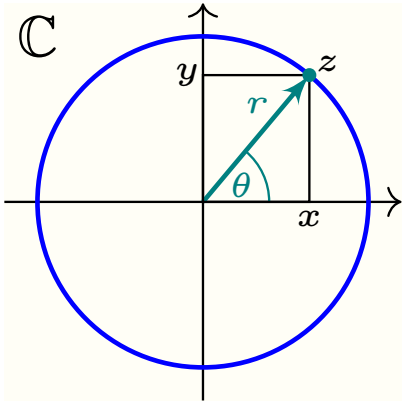
Somit ist C ein Körper. Er ist isomorph zu den komplexen Zahlen:

$$(\mathbb{C}, +, \cdot) \cong (C, +, \cdot) \,:\, x + \mathrm{i}y \;\rightleftarrows\; \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

Komplexe Zahlen: Polarkoordinaten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



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

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

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

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

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

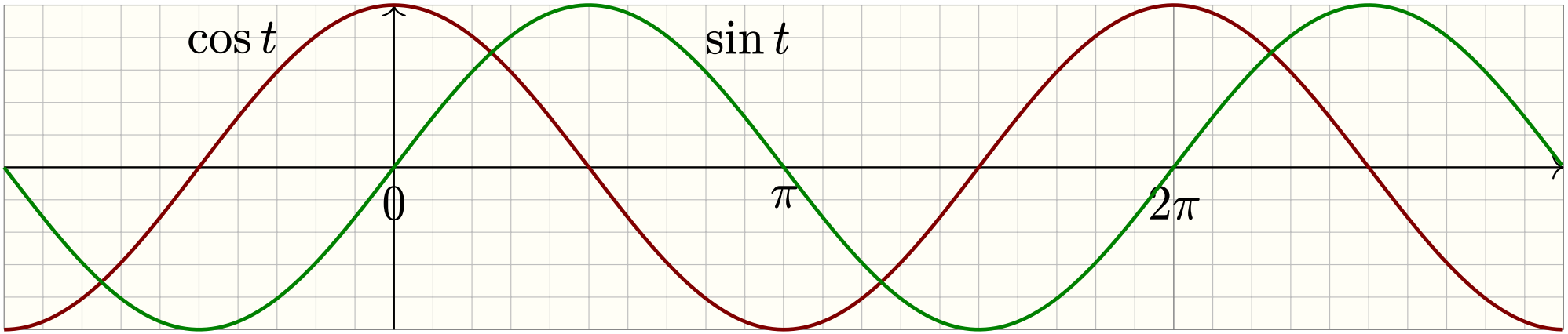
Lösung: Wir lösen die Gleichung $w^n = z$ für $z = r\,\mathrm{e}^{\mathrm{i}\theta}$ und $n \in \mathbb{N}_{\geq 2}$ durch

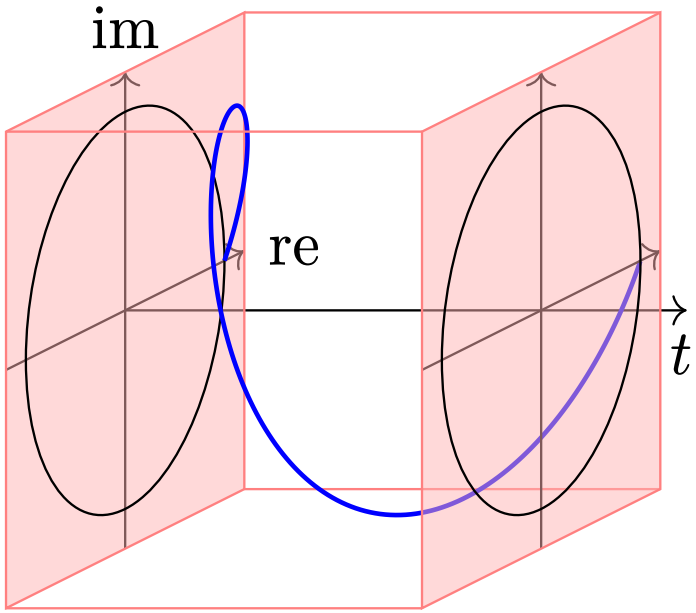
$$w_k = \sqrt[n]{r} \cdot \mathrm{e}^{\mathrm{i}(\theta+2\pi k)/n} \qquad \text{mit} \qquad k = 0, 1, \dots, n-1.$$

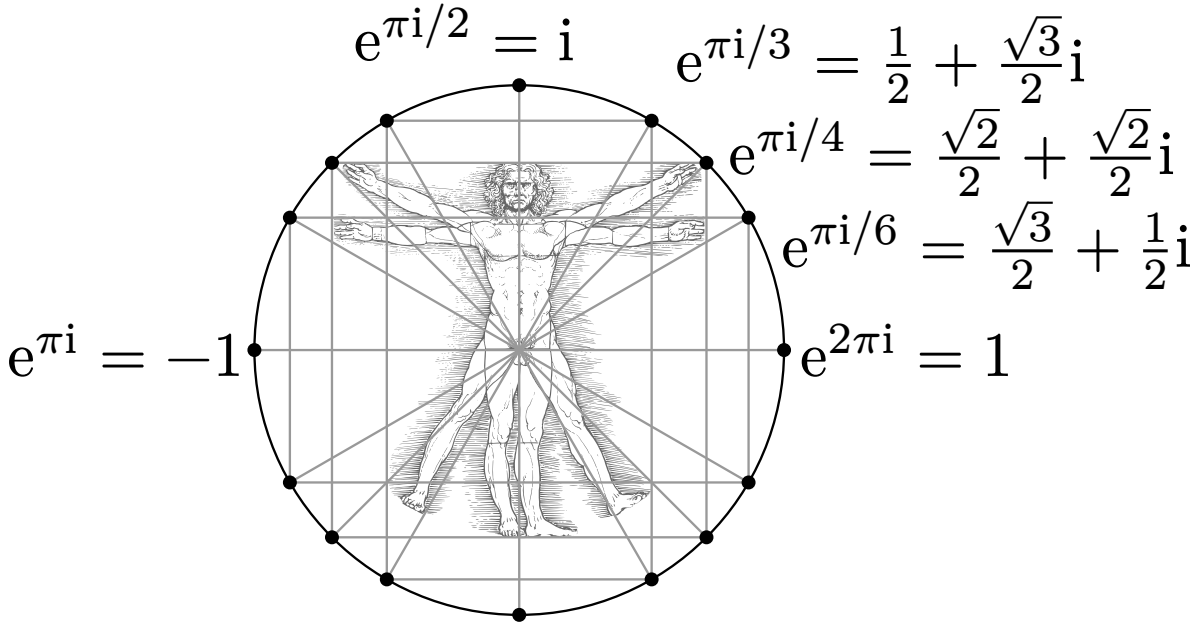
Komplexe Zahlen: Polarkoordinaten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.







Komplexe Zahlen: Fundamentalsatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Über $\mathbb{R} \supset \mathbb{Q}$ zerfällt $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$.
Über $\mathbb{C} \supset \mathbb{R}$ zerfällt $X^2 + 1 = (X - \mathrm{i})(X + \mathrm{i})$. Allgemein:

Satz E3c: Fundamentalsatz der Algebra der komplexen Zahlen, FTA

Zu jedem Polynom $P(X) = X^n + c_1 X^{n-1} + \cdots + c_n$ mit $c_1, \dots, c_n \in \mathbb{C}$ existieren Nullstellen $z_1, \dots, z_n \in \mathbb{C}$ so, dass $P(X) = (X - z_1) \cdots (X - z_n)$.

Für $n = 1$ ist das trivial, für $n = 2$ leicht dank Mitternachtsformel:

$$\begin{aligned} z^2 - 2pz + q = 0 \quad &\overset{(1)}{\iff} \quad z^2 - 2pz + p^2 = p^2 - q \\ &\overset{(2)}{\iff} \quad (z - p)^2 = p^2 - q \\ &\overset{(3)}{\iff} \quad z \in \{p \pm \sqrt{p^2 - q}\} \end{aligned}$$

Für $n \geq 3$ ist der Beweis raffinierter, siehe Umlaufzahl in der Topologie.

Hamiltons Quaternionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition E3D: Quaternionen erweitern die komplexen Zahlen.

Die **Quaternionen** $(\mathbb{H}, +, 0, \cdot, 1)$ sind ein Schiefkörper mit $\mathbb{H} \supseteq \mathbb{C} \supseteq \mathbb{R}$; dabei gilt $\mathbb{H} = \mathbb{R}[\mathrm{i}, \mathrm{j}, \mathrm{k}] = \{\, q = \alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k} \mid \alpha, \beta, \gamma, \delta \in \mathbb{R} \,\}^!$ mit

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-\mathrm{j}$
j	j	$-\mathrm{k}$	-1	i
k	k	j	$-\mathrm{i}$	-1

Jede reelle Zahl $\alpha \in \mathbb{R} \subseteq \mathbb{H}$ kommutiert dabei mit $\mathrm{i}, \mathrm{j}, \mathrm{k}$, also mit jeder Quaternion q.

Damit folgt die Tabelle bereits aus $-1 = \mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk}$.

Matrixkalkül: Quaternionen als komplexe 2×2–Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz E3E: die Quaternionen $\mathbb{H}$ als Matrizen über $\mathbb{C}$

$$H := \left\{ q = \left[\begin{smallmatrix} z & -w \\ \overline{w} & \overline{z} \end{smallmatrix}\right] \,\middle|\, z, w \in \mathbb{C} \right\} \leq \mathbb{C}^{2\times 2}$$

$$\begin{bmatrix} z_1 & -w_1 \\ \overline{w_1} & \overline{z_1} \end{bmatrix} \cdot \begin{bmatrix} z_2 & -w_2 \\ \overline{w_2} & \overline{z_2} \end{bmatrix} = \begin{bmatrix} z_1 z_2 - w_1 \overline{w_2} & -z_1 w_2 - w_1 \overline{z_2} \\ \overline{w_1} z_2 + \overline{z_1} w_2 & -\overline{w_1} w_2 + \overline{z_1} \overline{z_2} \end{bmatrix}$$

In $(H, \cdot)$ ist jedes Element $q \neq 0$ invertierbar, da $\det(q) = |z|^2 + |w|^2 > 0$:

$$\begin{bmatrix} z & -w \\ \overline{w} & \overline{z} \end{bmatrix}^{-1} = \frac{1}{z\overline{z} + w\overline{w}} \begin{bmatrix} \overline{z} & w \\ -\overline{w} & z \end{bmatrix}$$

Somit ist $(H, +, \cdot)$ ein Divisionsring. Er ist jedoch nicht kommutativ:

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ I = \begin{bmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix},\ J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ K = \begin{bmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{bmatrix} \implies$$

$\cdot$	I	J	K
I	$-E$	K	$-J$
J	$-K$	$-E$	I
K	J	$-I$	$-E$

Dieser Divisionsring ist demnach isomorph zu Hamiltons Quaternionen:

$$(\mathbb{H}, +, \cdot) \cong (H, +, \cdot) : \alpha + \beta \mathrm{i} + \gamma \mathrm{j} + \delta \mathrm{k} \leftrightarrows \alpha E + \beta I + \gamma J + \delta K.$$

Zusammenfassung: Aufbau des Zahlensystems

$$\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \mathbb{H}$$

♦ Frage E0A: Aufbau des Zahlensystems – Vollständigkeit & Abschluss

(0) Wie konstruieren Sie den Körper $(\mathbb{R}, +, \cdot, \leq)$ der reellen Zahlen?

(1) Lässt sich jede reelle Zahl $x \in \mathbb{R}$ dezimal darstellen?
Was ist $x := 0.99999\ldots$? Gilt $x = 1$?

(2) Wie messen Sie im Raum $\mathbb{R}^n$ Längen und Winkel?
Wie beschreiben Sie Drehungen und Spiegelungen?

(3) Wie konstruieren Sie den Körper $\mathbb{C} = \mathbb{R}[\mathrm{i}]$ mit $\mathrm{i}^2 = -1$?
Wie berechnen Sie Potenzen $z \mapsto z^n$ und Wurzeln w mit $w^n = z$?

(4) Was besagt der Fundamentalsatz der Algebra?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel E

Bonusmaterial

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

Celui qui ne sait pas la géométrie peut l'apprendre:
osez penser par vous-même.
Voltaire (1694–1778), *Dictionnaire philosophique*

Inhalt dieses Kapitels E

5 Erweiterung von Ringen und Körpern durch Matrizen

6 Computer können keine reellen Zahlen, aber fast.

7 Die sagenhaft schnelle Fourier–Transformation

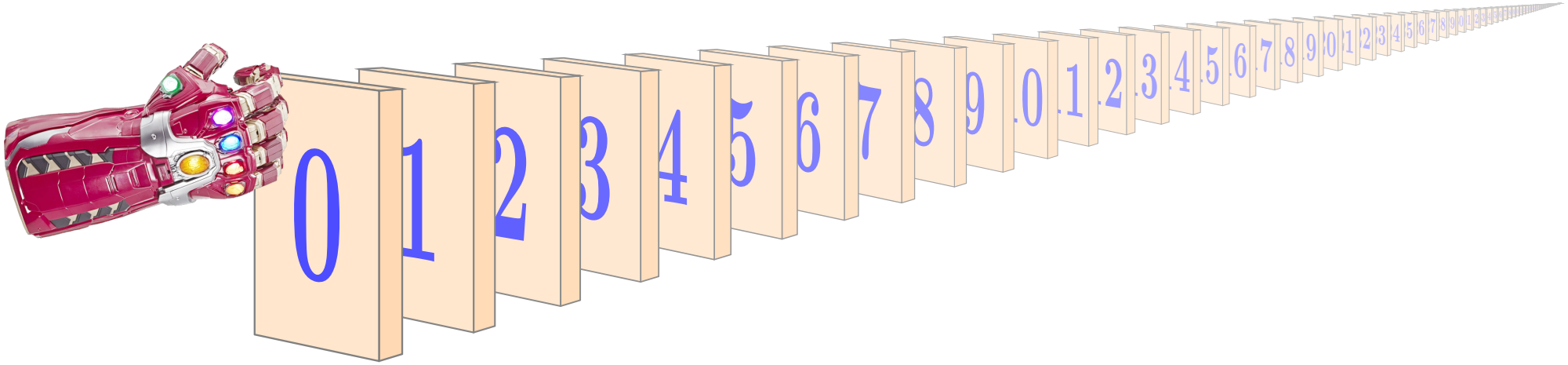
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel F

Mathematische Logik und Beweistechniken



The aim of theory really is, to a great extent, that of systematically organizing past experience in such a way that the next generation [...] will be able to absorb the essential aspects in as painless a way as possible.

Michael F. Atiyah (1929–2019), *How research is carried out*

Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels F

1 Aussagen und Wahrheitswerte

2 Schlussregeln und Beweisverfahren

3 Prädikate und Quantoren

4 Induktion: highway to infinity!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aussagen und Wahrheitswerte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition F1A: Aussage und Wahrheitswert

Eine **Aussage** A ist ein sprachlicher Ausdruck, dem ein eindeutiger Wahrheitswert $[A]$ zugeordnet ist: entweder $0 =$ falsch oder $1 =$ wahr.

Aussagen und Wahrheitswerte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel F1B: Aussage oder nicht? wahr oder falsch?

$A =$ (Alle Primzahlen sind ungerade.)
$\neg A =$ (Es gibt eine gerade Primzahl.)

$B =$ (Dieses Beispiel F1B ist nicht leicht, aber hilfreich.)
$\neg B =$ (Dieses Beispiel F1B 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 mein Verein die Meisterschaft.)

Verknüpfung von Aussagen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition F1c: logische Verknüpfungen, boolesche Logik

Sind A und B Aussagen, so auch folgende **verknüpfte 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 genau dann wenn B	Äquivalenz (Bijunktion)
$(A \Rightarrow B)$	wenn A gilt, dann gilt B	Implikation (Subjunktion)

$[A]$	$[B]$	$[\neg A]$	$[A \wedge B]$	$[A \vee B]$	$[A \dot{\vee} B]$	$[A \Leftrightarrow B]$	$[A \Rightarrow B]$
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

Hinreichend vs notwendig: Wenn Spinat, dann Nachtisch?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

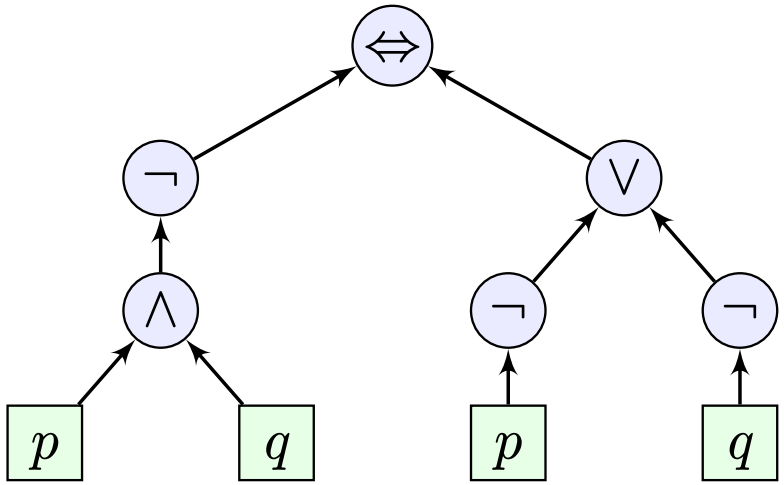
(1) Die strengen Eltern mahnen ihre Kinder: „Wenn ihr euren Spinat nicht aufesst, dann bekommt ihr heute keinen Nachtisch.“ Die Kinder essen tapfer ihren Spinat, bekommen aber dennoch keinen Nachtisch.

ALF: Aussagenlogische Formeln

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\neg(p \wedge q) \;\Leftrightarrow\; (\neg p \vee \neg q)$$



Als Bausteine haben wir

- die Konstanten $\bot$ (falsum, falsch) und $\top$ (verum, wahr),
- die Variablen $p, q, r, \ldots$ als freie Symbole (noch nicht belegt),
- die Verknüpfungen $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ mit den Klammern (und).

Definition F1D: Erzeugung aller aussagenlogischen Formeln

(0) Konstanten und Variablen sind Formeln.
(1) Sind a und b Formeln, so auch $\neg a$ und $(a \wedge b), (a \vee b), (a \Rightarrow b), (a \Leftrightarrow b)$.

Verknüpfung von Wahrheitswerten

a	b	$\neg a$	$a \wedge b$	$a \vee b$	$a \dot{\vee} b$	$a \Rightarrow b$	$a \Leftrightarrow b$
1	1	0	1	1	0	1	1
1	0	0	0	1	1	0	0
0	1	1	0	1	1	1	0
0	0	1	0	0	0	1	1

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Auswertungen und Tautologien

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition F1E: Auswertungen und Tautologien

Eine **Belegung** der Variablen ist eine Abbildung $\beta : \{p, q, r, \dots\} \to \{0, 1\}$.
(0) Die Konstanten $\bot$ und $\top$ werten wir aus zu $\beta(\bot) := 0$ und $\beta(\top) := 1$.
(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.
Ist $a \Leftrightarrow b$ eine Tautologie, so nennen wir a und b **äquivalent**, kurz $a \equiv b$.

Doppelte Verneinung und das ausgeschlossene Dritte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

p	$\neg p$	$\neg\neg p$	$p \vee \neg p$	$p \wedge \neg p$	$p \dot{\vee} \neg p$
1	0	1	1	0	1
0	1	0	1	0	1

Satz F1F: doppelte Verneinung und das ausgeschlossene Dritte

Folgende Ausdrücke sind Tautologien, also allgemeingültig:

$\neg\neg p \Leftrightarrow p$	doppelte Verneinung bejaht, *duplex negatio affirmat*
$p \vee \neg p$	das ausgeschlossene Dritte, *Tertium non datur*
$\neg(p \wedge \neg p)$	der ausgeschlossene Widerspruch
$p \dot{\vee} \neg p$	beides zusammengefasst

Tautologien als nützliche Rechenregeln

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz F1G: elementare Äquivalenzen

Folgende Ausdrücke sind Tautologien, also allgemeingültig:

(1) De Morgan	$\neg(p \wedge q)$	$\Leftrightarrow$	$(\neg p \vee \neg q)$
	$\neg(p \vee q)$	$\Leftrightarrow$	$(\neg p \wedge \neg q)$
(2) Kommutativität	$(p \wedge q)$	$\Leftrightarrow$	$(q \wedge p)$
	$(p \vee q)$	$\Leftrightarrow$	$(q \vee p)$
(3) Assoziativität	$((p \wedge q) \wedge r)$	$\Leftrightarrow$	$(p \wedge (q \wedge r))$
	$((p \vee q) \vee r)$	$\Leftrightarrow$	$(p \vee (q \vee r))$
(4) Distributivität	$(p \vee (q \wedge r))$	$\Leftrightarrow$	$((p \vee q) \wedge (p \vee r))$
	$(p \wedge (q \vee r))$	$\Leftrightarrow$	$((p \wedge q) \vee (p \wedge r))$

Tautologien als nützliche Rechenregeln

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Beweisen Sie, dass dies Tautologien sind! Was ist zu tun?

Lösung: Wir prüfen dies als Wahrheitstabelle, hier exemplarisch für (1):

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

Mehrfache Verknüpfungen

$$\bigwedge_{i=1}^{n} p_i \quad := \quad p_1 \wedge p_2 \wedge \cdots \wedge p_n \quad := \quad (\cdots(p_1 \wedge p_2) \wedge \cdots) \wedge p_n$$

$$\bigvee_{i=1}^{n} p_i \quad := \quad p_1 \vee p_2 \vee \cdots \vee p_n \quad := \quad (\cdots(p_1 \vee p_2) \vee \cdots) \vee p_n$$

$$p_1 \Rightarrow p_2 \Rightarrow \cdots \Rightarrow p_n \quad := \quad (p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \ldots \wedge (p_{n-1} \Rightarrow p_n),$$

$$p_1 \Leftrightarrow p_2 \Leftrightarrow \cdots \Leftrightarrow p_n \quad := \quad (p_1 \Leftrightarrow p_2) \wedge (p_2 \Leftrightarrow p_3) \wedge \ldots \wedge (p_{n-1} \Leftrightarrow p_n).$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Junktoren aka logische Verknüpfungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir kennen die logischen Verknüpfungen $\wedge, \vee, \Rightarrow, \Leftrightarrow$: $\{0,1\}^2 \to \{0,1\}$.
Ein n–stelliger **Junktor** ist eine Funktion $J : \{0,1\}^n \to \{0,1\} : a \mapsto J(a)$.

Aufgabe: Wie viele n–Junktoren gibt es für $n = 0, 1, 2, \dots, 8$? **Lösung:**
Es gibt 2^n Tupel $a \in \{0,1\}^n$, also 2^{2^n} Junktoren $J : \{0,1\}^n \to \{0,1\}$.

n	Anzahl der n–Tupel	Anzahl der n–Junktoren
0	$2^0 = 1$ leeres Tupel	$2^1 = 2$; $\bot, \top$
1	$2^1 = 2$ Elemente	$2^2 = 4$; $c_0, c_1, \mathrm{id}, \neg$
2	$2^2 = 4$ Paare	$2^4 = 16$; siehe Tabelle
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 aka logische Verknüpfungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

$<, \overline{\Leftarrow}$	0	1
0	0	1
1	0	0

$\overline{\mathrm{pr}}_1$	0	1
0	1	1
1	0	0

$>, \overline{\Rightarrow}$	0	1
0	0	0
1	1	0

$\overline{\mathrm{pr}}_2$	0	1
0	1	0
1	1	0

$\neq, \dot{\vee}$	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

$=, \Leftrightarrow$	0	1
0	1	0
1	0	1

pr_2	0	1
0	0	1
1	0	1

$\leq, \Rightarrow$	0	1
0	1	1
1	0	1

pr_1	0	1
0	0	0
1	1	1

$\geq, \Leftarrow$	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

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vorgelegt sei $f \in \mathrm{ALF}_n = \mathcal{F}(\{\bot, \top, \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}, \{x_1, \dots, x_n\})$.
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

Aussagenlogische Formeln als logische Polynome

CRing $(\mathbb{K}, +, 0, -, \cdot, 1)$	Logik $(\mathbb{B} = \{0, 1\}, \vee, 0, \neg, \wedge, 1)$
$(\mathbb{K}, +, 0)$ ist eine abelsche Gruppe	$(\mathbb{B}, \vee, 0)$ ist ein abelsches Monoid
$(\mathbb{K}, \cdot, 1)$ ist ein abelsches Monoid	$(\mathbb{B}, \wedge, 1)$ ist ein abelsches Monoid
$\cdot$ distribuiert über $+$	$\wedge$ distribuiert über $\vee$
$-$	$\vee$ distribuiert über $\wedge$
$-$	$\neg : (\mathbb{B}, \vee, 0, \wedge, 1) \cong (\mathbb{B}, \wedge, 1, \vee, 0)$
Polynome $P, Q \in \mathbb{K}[X_1, \dots, X_n]$	$f, g \in \mathrm{ALF}(x_1, \dots, x_n)$
Koeffizientenvergleich $P = Q$	(syntaktische) Gleichheit $f = g$
Auswertung $P(x_1, \dots, x_n)$	Belegung β und Auswertung $\beta(f)$
Polynomfunktion $f_P = f_Q$	Junktor $J_f = J_g$, Äquivalenz $f \equiv g$
Summe von Produkten C1B/C1G $P = p_0 X^0 + p_1 X^1 + \dots + p_n X^n$	disjunktive Normalform / DNF $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} a_{ij}$
Produkt von Summen C3P/E3C $P = p_n (X - \lambda_1) \cdots (X - \lambda_n)$	konjunktive Normalform / CNF $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Eines der sieben Millennium-Probleme: P vs NP

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition F1L: Erfüllbarkeitsproblem (*satisfiability*, SAT)

Erfüllbarkeitsproblem, SAT: Eingabe $f \in \mathrm{ALF}$. Ist f erfüllbar?

Problem F1M: Gilt $\mathrm{P} = \mathrm{NP}$?

Erlaubt das Erfüllbarkeitsproblem eine Lösung in polynomieller Zeit?

Schlussregeln: neue wahre Aussagen aus alten!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$\wedge$–Beseitigung

$p \wedge q$	Wir beweisen $p \wedge q$.
q	Wir schließen q.

$\vee$–Einführung

p	Wir beweisen p.
$p \vee q$	Wir schließen $p \vee q$.

$\wedge$–Einführung

p	Wir beweisen p.
q	Wir beweisen q.
$p \wedge q$	Wir schließen $p \wedge q$.

$\vee$–Beseitigung

$p \vee q$	Wir beweisen $p \vee q$.
$\neg p$	Wir beweisen $\neg p$.
q	Wir schließen q.

Die Schnittregel: Modus Ponens

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die folgende Implikation ist eine Tautologie, also allgemeingültig:

$$\big(p \wedge (p \Rightarrow q)\big) \quad \Rightarrow \quad q$$

Wir vereinbaren die **Schnittregel**, lat. **Modus Ponens**, kurz MP:

$$\text{Modus Ponens}\quad \begin{array}{|l} p \Rightarrow q \\ p \\ \hline q \end{array}$$

Beispiel: Wenn es regnet, dann ist die Straße nass.
Jetzt regnet es. Daraus folgt: Die Straße ist nass.

Definition F2A: Schlussregeln der Aussagenlogik

Jede Tautologie der Form $p_1 \wedge \ldots \wedge p_n \Rightarrow q$
definiert eine Schlussregel wie rechts gezeigt,
und jede Schlussregel entsteht auf diese Weise.

p_1	Prämisse p_1
$\vdots$	
p_n	Prämisse p_n
q	Konklusion

Beweis durch Kettenschluss

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die folgende Implikation ist eine Tautologie, genannt **Transitivität**:

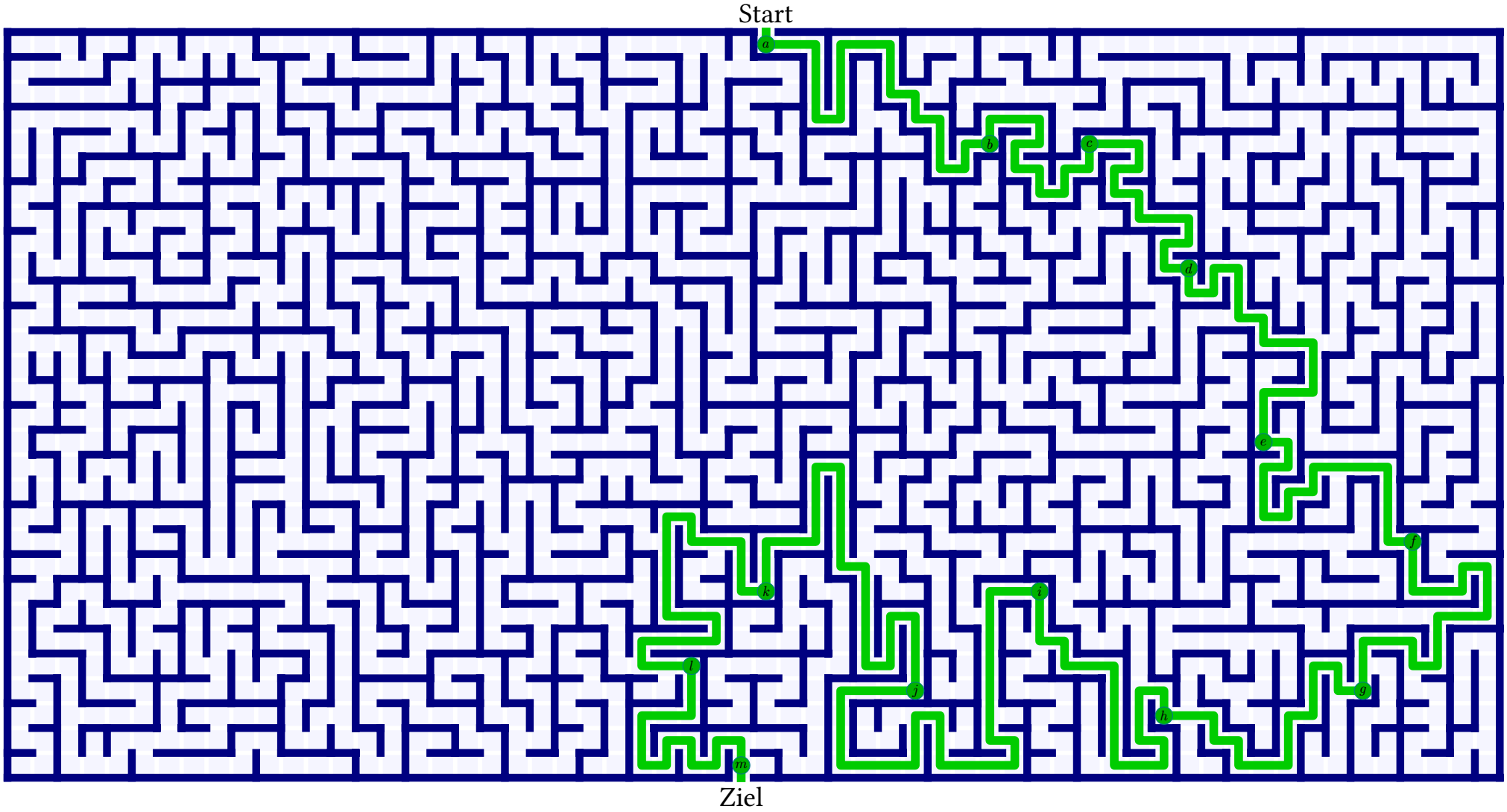
$$\big((p \Rightarrow q) \wedge (q \Rightarrow r)\big) \quad \Rightarrow \quad (p \Rightarrow r)$$

Die zugehörige Schlussregel ist der **Kettenschluss:**

$$\text{Kettenschluss}\ \frac{\begin{array}{l} p \Rightarrow q \\ q \Rightarrow r \end{array}}{p \Rightarrow r}$$

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.

Beweis durch Kettenschluss



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis durch Fallunterscheidung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$\vee$–Beseitigung / Fallunterscheidung

$$\frac{\begin{array}{l} p \Rightarrow p_1 \vee \ldots \vee p_n \\ p_1 \Rightarrow q \\ \ldots \\ p_n \Rightarrow q \end{array}}{p \Rightarrow q}$$

Beispiel: Beweisen Sie die Aussage $q =$ (Es gibt $x, y \in \mathbb{R} \setminus \mathbb{Q}$ mit $x^y \in \mathbb{Q}$.)

Beweis: Wir setzen $a := \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ und $b := a^a \in \mathbb{R}$. Wir unterscheiden:

1. Falls $b \in \mathbb{Q}$ gilt, so beweist $(x, y) = (a, a)$ die Behauptung q.
2. Falls $b \notin \mathbb{Q}$ gilt, so beweist $(x, y) = (b, a)$ die Behauptung q, denn $b^a = (a^a)^a = a^{(a^2)} = a^2 = 2 \in \mathbb{Q}$.

QED

Äquivalenz als gegenseitige Implikation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Folgende Äquivalenz ist eine Tautologie, also allgemeingültig:

$$(p \Leftrightarrow q) \quad \Leftrightarrow \quad ((p \Rightarrow q) \wedge (q \Rightarrow p))$$

Als Schlussregel können wir **Äquivalenz zur Implikation abschwächen**:

$$\Leftrightarrow\text{–Beseitigung} \left| \begin{array}{l} p \Leftrightarrow q \\ \hline p \Rightarrow q \end{array} \right. \qquad \Leftrightarrow\text{–Beseitigung} \left| \begin{array}{l} p \Leftrightarrow q \\ \hline q \Rightarrow p \end{array} \right.$$

Umgekehrt folgt die **Äquivalenz durch gegenseitige Implikation**:

$$\Leftrightarrow\text{–Einführung} \left| \begin{array}{l} p \Rightarrow q \\ q \Rightarrow p \\ \hline p \Leftrightarrow q \end{array} \right.$$

Implikation und Kontraposition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Schnittregel **Modus Ponens** besagt:

Modus Ponens

$$\begin{array}{|l}
p \Rightarrow q \\
p \\
\hline
q
\end{array}$$

„Wenn's regnet, ist die Straße nass."
„Es regnet."
„Die Straße ist nass."

Die gültige Umkehrung dieser Regel heißt **Modus Tollens**:

Modus Tollens

$$\begin{array}{|l}
p \Rightarrow q \\
\neg q \\
\hline
\neg p
\end{array}$$

„Wenn's regnet, ist die Straße nass."
„Die Straße ist nicht nass."
„Es regnet nicht."

Dies entspricht der **Kontraposition**:

Kontraposition

$$\begin{array}{|l}
p \Rightarrow q \\
\hline
\neg q \Rightarrow \neg p
\end{array}$$

Warnung vor Trugschlüssen!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{array}{|l} p \Rightarrow q \\ q \\ \hline p \end{array}$$

„Am Ende der Vorlesung trinke ich immer Wasser.“
„Ich trinke jetzt einen Schluck Wasser.“
„Also ist die Vorlesung zu Ende.“

$$\begin{array}{|l} p \Rightarrow q \\ \neg p \\ \hline \neg q \end{array}$$

„Wenn Sie alles wissen, dann bestehen Sie mit Eins.“
„Sie wissen aber leider noch nicht alles.“
„Also bestehen Sie nicht mit Eins.“

$$\begin{array}{|l} p \Rightarrow q \\ \hline q \Rightarrow p \end{array}$$

„Wenn ich Logik verstehe, dann bin ich glücklich.“
„Also, wenn ich glücklich bin, verstehe ich Logik.“

$$\begin{array}{|l} p \Rightarrow q \\ \hline \neg p \Rightarrow \neg q \end{array}$$

„Wenn Freitag ist, dann tanze ich.“
„Also, wenn nicht Freitag ist, dann tanze ich nicht.“

Negation und Widerspruch: *reductio ad absurdum*

$$\text{Negation}\ \frac{q \Rightarrow \bot}{\neg q}$$

$$\text{Absurdum}\ \frac{\neg\neg r}{r}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

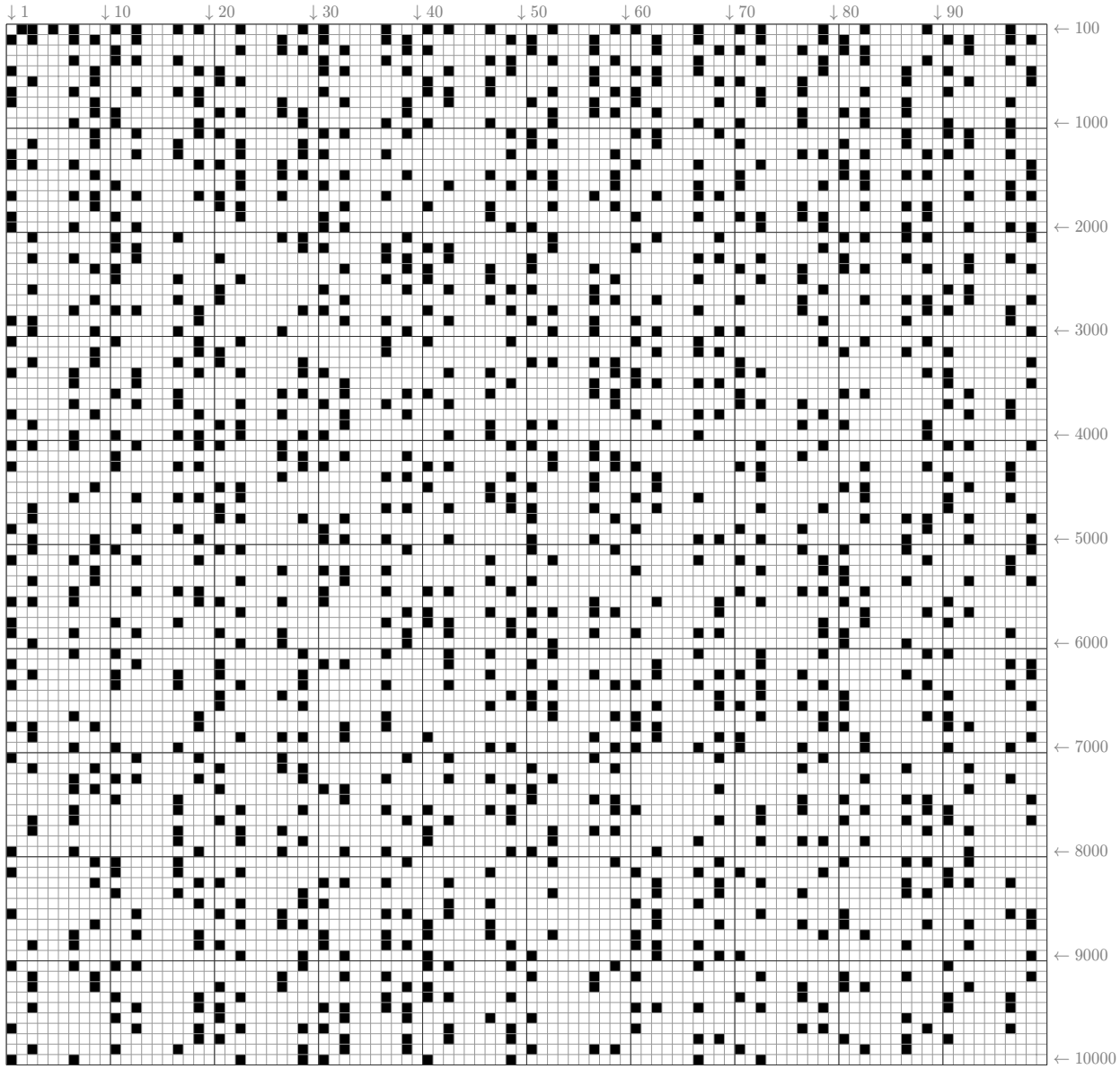
Wie viele Primzahlen gibt es?

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	...

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wie viele Primzahlen gibt es?



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Es gibt unendlich viele Primzahlen: durch Widerspruch?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz F2c: Es gibt unendlich viele Primzahlen.

In den natürlichen Zahlen gibt es unendlich viele Primzahlen.

Beweis durch Widerspruch, vorgeblich „nach Euklid“: Angenommen, es gäbe nur endlich viele Primzahlen $p_1 < \ldots < p_n$. Sei $q = 1 + p_1 \cdots p_n$. Keine der Primzahlen p_i teilt q, also ist q prim. Widerspruch! $\boxed{\text{QED}}$

? „Ich finde $1 + 2 = 3$ prim, $1 + 2 \cdot 3 = 7$ prim, $1 + 2 \cdot 3 \cdot 5 = 31$ prim, ... aber $1 + 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30031 = 59 \cdot 509$. Ist der Beweis / Satz falsch?“

Es gibt unendlich viele Primzahlen: durch Konstruktion!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz F2D: Es gibt unendlich viele Primzahlen. (Euklid, ca. 300 v.u.Z.)

In den natürlichen Zahlen gibt es unendlich viele Primzahlen:
Zu Primzahlen $p_1, \dots, p_k$ ist $p_{k+1} = \operatorname{lpf}(1 + p_1 \cdots p_k)$ eine weitere Primzahl.

Beweis: Wir berechnen $q := 1 + p_1 \cdots p_k \geq 2$ und davon den kleinsten echten Faktor $p := \operatorname{lpf}(q) \geq 2$. Dann ist p unzerlegbar, also prim. Zudem gilt $p \notin \{p_1, \dots, p_k\}$, denn $p_1, \dots, p_k$ teilen nicht q. QED

Aussageformen aka Prädikate

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Über $(\mathbb{N}, +, 0, \cdot, 1, \leq)$ betrachten wir folgende Aussageformen:

$$\begin{aligned} p(x) &:= (5 \leq x) \wedge (x \leq 9), \\ q(x, y) &:= (x \cdot x = y). \end{aligned}$$

Definition F3A: 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 Objekten $\alpha, \beta, \dots$ unseres Diskursuniversums Ω.

Existenz- und Allquantor: Schreibweise

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition F3B: Existenz- und Allquantor

Zu jedem Prädikat $p(x)$ erhalten wir quantifizierte 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

Existenz- und Allquantor: Bedeutung

Sprechen wir nur über endlich viele Objekte $\Omega = \{a_1, a_2, \dots, a_n\}$, so gilt:

$$(\forall x \in \Omega : p(x)) \quad \Longleftrightarrow \quad (p(a_1) \wedge p(a_2) \wedge \dots \wedge p(a_n))$$
$$(\exists x \in \Omega : p(x)) \quad \Longleftrightarrow \quad (p(a_1) \vee p(a_2) \vee \dots \vee p(a_n))$$

Daher schreibt man Quantoren $\forall, \exists$ auch als verallgemeinertes $\wedge, \vee$:

$$\bigwedge_{i=1}^{n} p(a_i) \quad \text{oder allgemein} \quad \bigwedge_{x \in \Omega} p(x) \quad \text{für} \quad \forall x \in \Omega : p(x)$$
$$\bigvee_{i=1}^{n} p(a_i) \quad \text{oder allgemein} \quad \bigvee_{x \in \Omega} p(x) \quad \text{für} \quad \exists x \in \Omega : p(x)$$

Definition F3B: Existenz- und Allquantor

Den Wahrheitswert einer quantifizierten Aussage erklären wir durch

$$[\forall x : p(x)] := \min_{x \in \Omega} [p(x)] \in \{0, 1\},$$
$$[\exists x : p(x)] := \max_{x \in \Omega} [p(x)] \in \{0, 1\}.$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Existenz- und Allquantor: Anwendungsbeispiel

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Formulieren Sie im Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ mit Quantoren „teilbar“, „invertierbar“, „unzerlegbar“ und „prim“ sowie Euklids Lemma. **Lösung:**

$$
\begin{aligned}
a \mid b \quad &:\Leftrightarrow (\exists a' \, (a \cdot a' = b)) \quad \Leftrightarrow \quad \exists a' : a \cdot a' = b \\
\mathrm{invbar}(a) \quad &:\Leftrightarrow \exists a' : a \cdot a' = 1 \quad \Leftrightarrow \quad a \mid 1 \\
\mathrm{irred}(a) \quad &:\Leftrightarrow (\forall b \, (\forall c \, ((a = b \cdot c) \Rightarrow ((b \mid 1) \mathbin{\dot\vee} (c \mid 1))))) \\
&\Leftrightarrow \forall b, c : a = b \cdot c \Rightarrow b \mid 1 \mathbin{\dot\vee} c \mid 1 \\
\mathrm{prim}(a) \quad &:\Leftrightarrow (a \neq 0) \wedge (a \nmid 1) \wedge (\forall b \, (\forall c \, ((a \mid b \cdot c) \Rightarrow ((a \mid b) \vee (a \mid c))))) \\
&\Leftrightarrow a \neq 0 \wedge a \nmid 1 \wedge \forall b, c : (a \mid b \cdot c \Rightarrow a \mid b \vee a \mid c)
\end{aligned}
$$

Euklids Lemma B31 über $\mathbb{Z}$ schließlich besagt $\forall a : \mathrm{prim}(a) \Leftrightarrow \mathrm{irred}(a)$.

Beweisverfahren für Existenz- und Allquantor

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition F3c: Schlussregeln für Quantoren

Für den Allquantor $\forall$ nutzen wir **Spezialisieren** und **Verallgemeinern**:

$\forall$–Beseitigung
$$\frac{\forall x : p(x)}{p(\alpha) \text{ für jedes } \alpha \text{ (beliebig gewählt)}}$$

$\forall$–Einführung
$$\frac{p(\alpha) \text{ für jedes } \alpha}{\forall x : p(x)}$$

Für den Existenzquantor $\exists$ nutzen wir **Auswählen** und **Konstruieren**:

$\exists$–Beseitigung
$$\frac{\exists x : p(x)}{p(\alpha) \text{ für ein } \alpha \text{ (geeignet gewählt)}}$$

$\exists$–Einführung
$$\frac{p(\alpha) \text{ für ein } \alpha}{\exists x : p(x)}$$

Die Reihenfolge der Quantoren ist wesentlich!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Allquantoren vertauschen untereinander, ebenso Existenzquantoren:

$$\forall x : \forall y : p(x,y) \quad \Longleftrightarrow \quad \forall y : \forall x : p(x,y)$$
$$\exists x : \exists y : p(x,y) \quad \Longleftrightarrow \quad \exists y : \exists x : p(x,y)$$

⚠ Existenz- und Allquantor vertauschen jedoch nicht:

$$\exists x : \forall y : p(x,y) \quad \underset{\not\Leftarrow}{\Longrightarrow} \quad \forall y : \exists x : p(x,y)$$

Gegenbeispiel: Über $(\mathbb{Z}, <)$ betrachten wir $p(x,y) = (x < y)$:

$$\forall y : \exists x : x < y \quad \text{also} \quad \forall y \overbrace{(\exists x\,(x < y))}^{q(y)}$$
$$\exists x : \forall y : x < y \quad \text{also} \quad \exists x \underbrace{(\forall y\,(x < y))}_{r(x)}$$

Rechenregeln für Existenz- und Allquantor

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir kennen die Regeln von **De Morgan** aus Satz F1G (endlicher Fall):

$$\neg(p_1 \land p_2 \land \ldots \land p_n) \iff (\neg p_1) \lor (\neg p_2) \lor \ldots \lor (\neg p_n)$$
$$\neg(p_1 \lor p_2 \lor \ldots \lor p_n) \iff (\neg p_1) \land (\neg p_2) \land \ldots \land (\neg p_n)$$

Allgemein gelten die Regeln von **De Morgan für Quantoren**:

$$\neg(\forall x : p(x)) \iff \exists x : (\neg p(x))$$
$$\neg(\exists x : p(x)) \iff \forall x : (\neg p(x))$$

Existenz und Eindeutigkeit: Definition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition F3E: Existenz und Eindeutigkeit als Quantor – ∃&E

(1) Für $\exists x$ sagen wir zur Betonung auch „Es existiert *mindestens* ein x“.

$$\exists^{\geq 1}\, x : p(x) \quad :\Leftrightarrow \quad \exists x : p(x)$$

(2) Wir definieren den Quantor „Es existiert *höchstens* ein x“ wie folgt:

$$\exists^{\leq 1}\, x : p(x) \quad :\Leftrightarrow \quad \forall x, y : \big(p(x) \wedge p(y)\big) \Rightarrow (x = y)$$

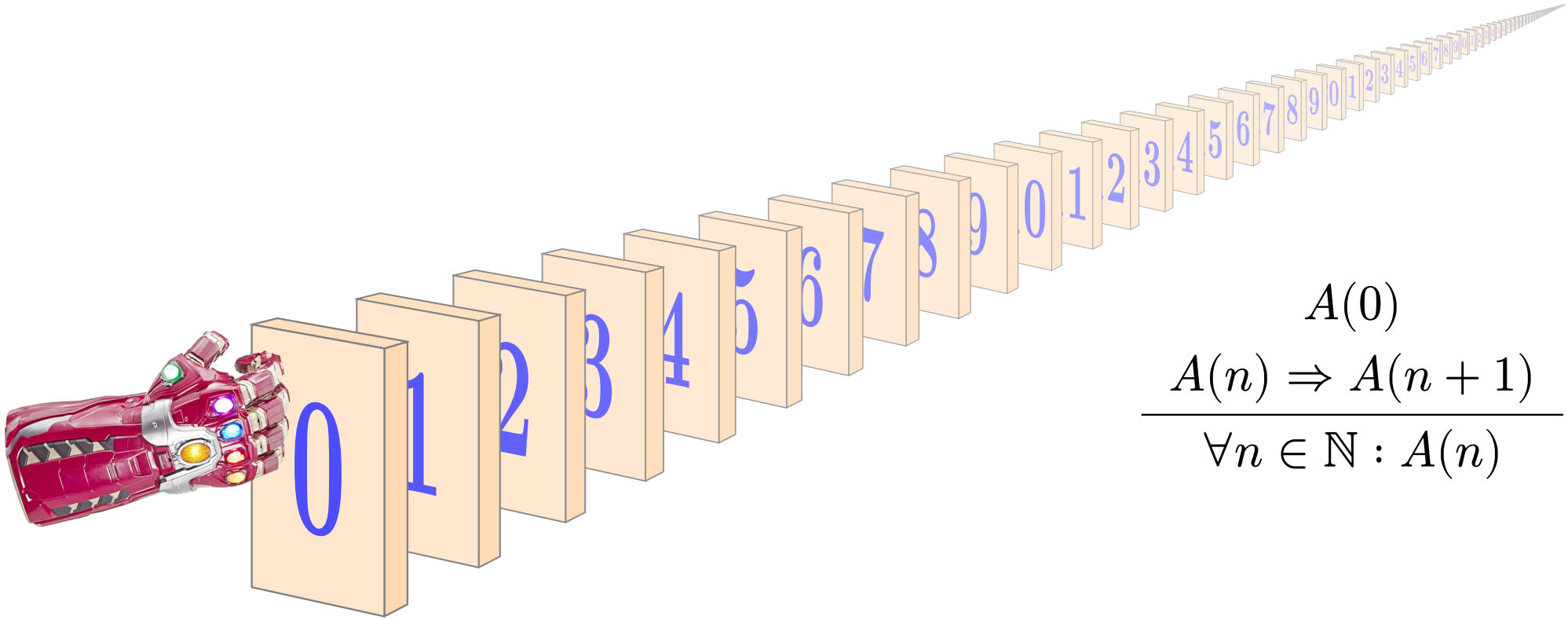
(3) Beides zusammen bedeutet „Es existiert *genau* ein x“:

$$\exists^{=1} \text{ oder } \exists!\, x : p(x) \quad :\Leftrightarrow \quad \exists x\ \forall y : p(y) \Leftrightarrow y = x$$

Beispiele:

Aussage	über $\mathbb{Q}$	über $\mathbb{R}$	über $\mathbb{R}_{\geq 0}$
$\exists^{\geq 1}\, x : x^2 = 2$	falsch	wahr	wahr
$\exists^{\leq 1}\, x : x^2 = 2$	wahr	falsch	wahr
$\exists^{=1}\, x : x^2 = 2$	falsch	falsch	wahr

Vollständige Induktion: highway to infinity!



$$\frac{A(0) \qquad A(n) \Rightarrow A(n+1)}{\forall n \in \mathbb{N} : A(n)}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vollständige Induktion: highway to infinity!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir nutzen die natürlichen Zahlen $(\mathbb{N}, 0, s) = \{\, 0 \mapsto 1 \mapsto 2 \mapsto 3 \mapsto \ldots \}$.

Satz F4A: Prinzip der vollständigen Induktion

Sei $(A(n))_{n\in\mathbb{N}}$ eine Familie von Aussagen $A(n)$. Äquivalent sind:

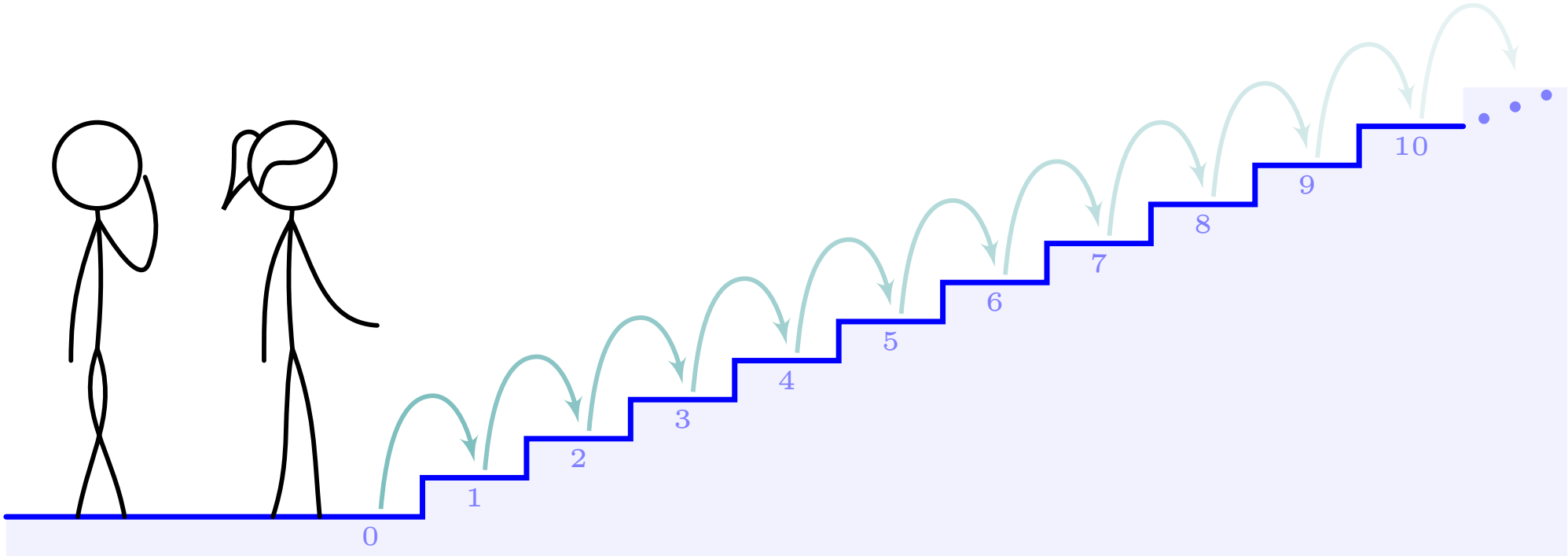
(1) Für jede natürliche Zahl $n \in \mathbb{N}$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in \mathbb{N} : A(n)$$

(2) Der *Induktionsanfang* $A(0)$ ist wahr, und für jede natürliche Zahl $n \in \mathbb{N}$ gilt der *Induktionsschritt* $A(n) \Rightarrow A(n+1)$, kurz:

$$A(0) \;\wedge\; \forall n \in \mathbb{N} : [\, A(n) \Rightarrow A(n+1) \,]$$

Vollständige Induktion: Schritt für Schritt



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

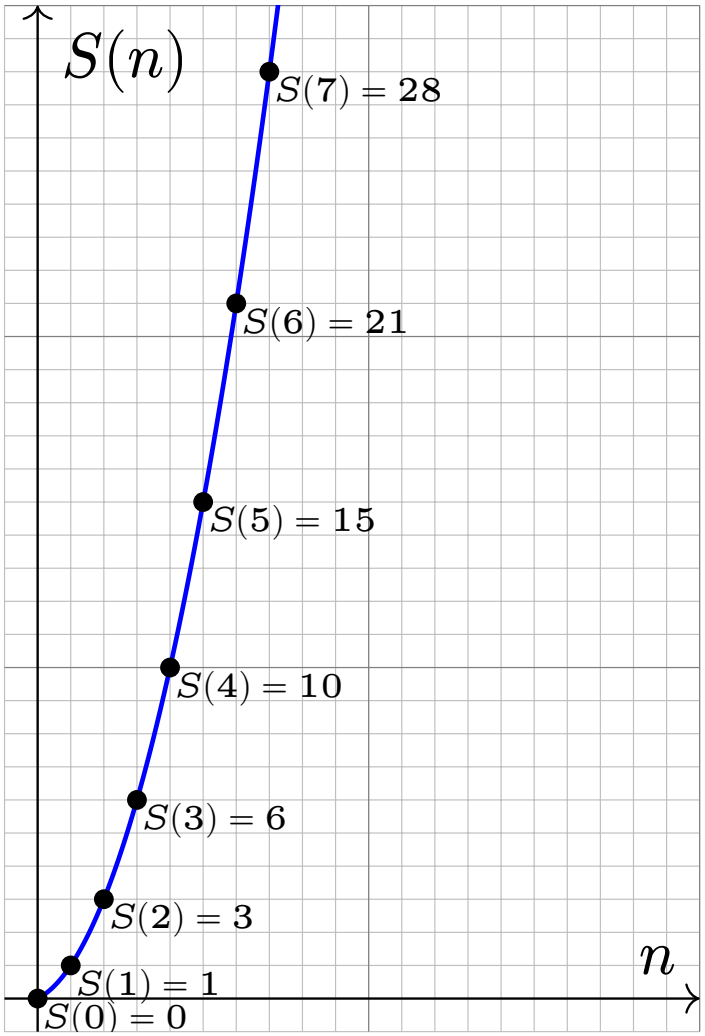
Ein klassisches Beispiel: der kleine Gauß

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Acht Partygäste stoßen an, wie oft erklingen die Gläser?
Größer: Berechnen Sie $1 + 2 + \ldots + 100$, besser gleich allgemein

$$S(n) \quad = \quad 1 + 2 + \ldots + n.$$



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!
Aus D101 wissen wir: Durch die ersten drei Datenpunkte verläuft $F(x) = x(x + 1)/2$.

Ein klassisches Beispiel: der kleine Gauß

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir summieren die Terme $f(k) = k$ für $k = 1, 2, 3, \ldots$ und vergleichen

die Summe $\quad S(n) := \sum_{k=1}^{n} f(k) \quad$ mit der Formel $\quad F(n) := \frac{n(n+1)}{2}$.

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 $A(0)$: Die Werte $S(0) = 0$ und $F(0) = 0$ sind gleich.

Induktionsschritt $A(n) \Rightarrow A(n+1)$:

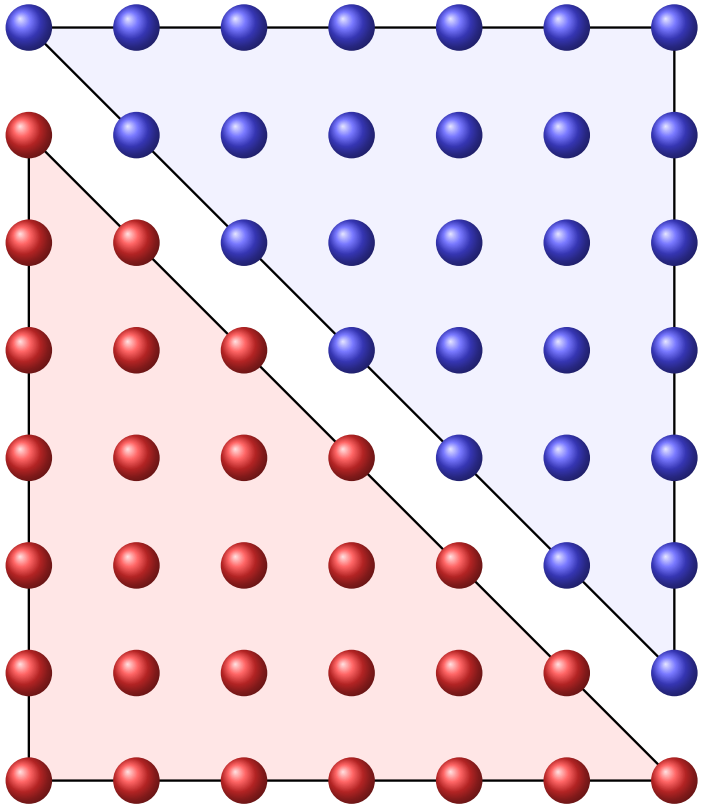
$$\begin{aligned} S(n+1) &\overset{\text{Def}}{=} S(n) + f(n+1) \overset{A(n)}{=} F(n) + (n+1) \\ &\overset{\text{Def}}{=} \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \overset{\mathbb{Q}}{=} \frac{(n+2)(n+1)}{2} \overset{\text{Def}}{=} F(n+1) \end{aligned}$$

Per Induktion schließen wir $A(n) : S(n) = F(n)$ für alle $n \in \mathbb{N}$. $\boxed{\text{QED}}$

Der kleine Gauß: ein geometrischer Beweis

$$1 + 2 + 3 + \quad \ldots \quad + n \;=:\; S(n) \;=\; n(n+1)/2$$

$$S(100) = 5050$$



Carl Friedrich Gauß (1777–1855)

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Nikomachus: Summe der Kuben = Quadrat der Summe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Für welche $n \in \mathbb{N}$ gilt die folgende phantastische Gleichung?

$$\boxed{A_n : \quad 1^3 + \cdots + n^3 = (1 + \ldots + n)^2}$$

Lösung: Wir testen einige kleine Beispiele $n = 0, 1, 2, 3, 4, \ldots$:

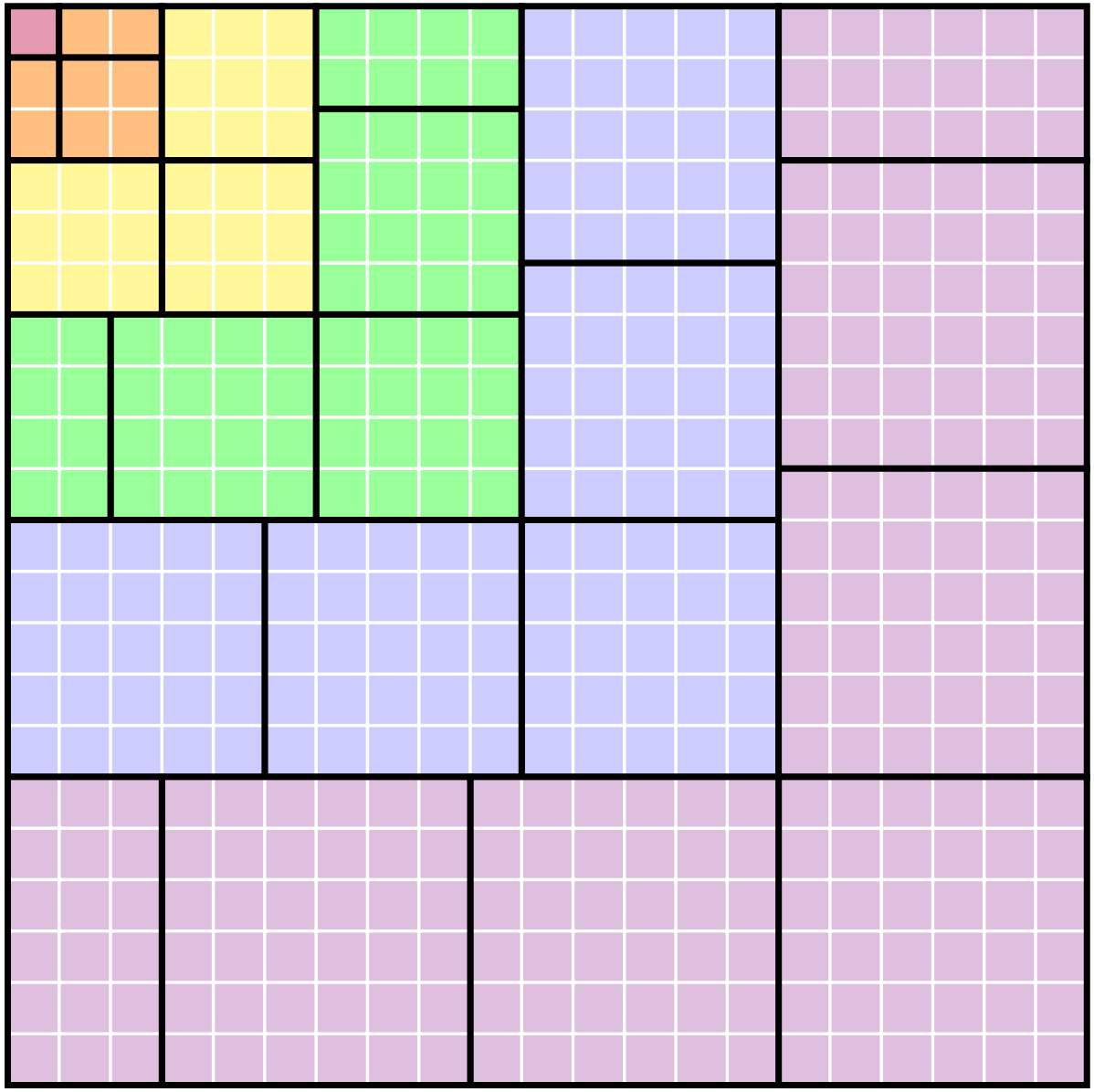
$$\begin{aligned}
A_1 : \quad & 1^3 = 1 = 1^2 \\
A_2 : \quad & 1^3 + 2^3 = 9 = (1+2)^2 \\
A_3 : \quad & 1^3 + 2^3 + 3^3 = 36 = (1+2+3)^2 \\
A_4 : \quad & 1^3 + 2^3 + 3^3 + 4^3 = 100 = (1+2+3+4)^2
\end{aligned}$$

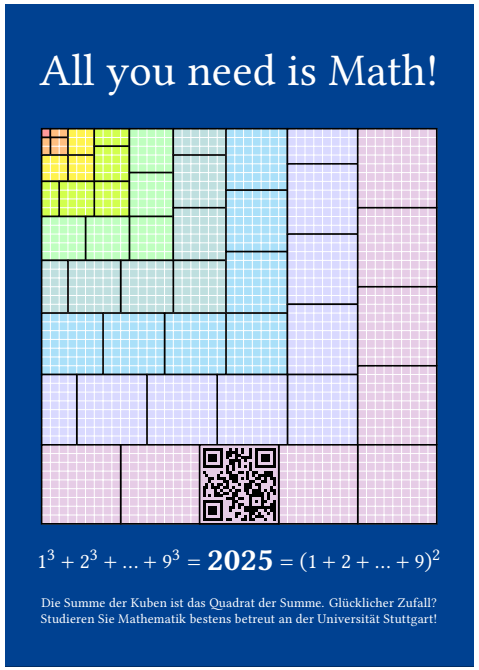
Wir fassen Mut und versuchen den Induktionsschritt $A_n \Rightarrow A_{n+1}$:

$$\begin{aligned}
& [(1 + \ldots + n) + (n{+}1)]^2 \\
\overset{\text{Bin}}{=} \quad & (1 + \ldots + n)^2 + 2(1 + \ldots + n)(n{+}1) + (n{+}1)^2 \\
\overset{\text{Gauß}}{=} \quad & (1 + \ldots + n)^2 + n(n{+}1)(n{+}1) + (n{+}1)^2 \\
\overset{A_n}{=} \quad & 1^3 + \ldots + n^3 + (n{+}1)^3
\end{aligned}$$

Nikomachus: Summe der Kuben = Quadrat der Summe

$$1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$$





Nikomachus von Gerasa
(1./2. Jh. n.u.Z)

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Induktion: Mehr ist leichter. Weniger ist schwer.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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) Zeigen Sie

$$A(n): \quad s_n = 1 - 1/(n+1).$$

Beweis: (2) Induktionsanfang $A(0)$: Wir finden $s_0 = 0 = 1 - 1/(0+1)$.
Induktionsschritt $A(n) \Rightarrow A(n+1)$:

$$s_{n+1} \overset{\text{Def}}{=} s_n + \frac{1}{(n+1)(n+2)} \overset{A(n)}{=} 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)}$$

$$\overset{\mathbb{Q}}{=} 1 - \frac{n+2}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} \overset{\mathbb{Q}}{=} 1 - \frac{(n+1)}{(n+1)(n+2)}$$

Induktion: Teleskopsummen sind genial-einfach.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(1) Wie finden wir eine geschlossene Formel? Hier dank Teleskopsumme:

$$\frac{1}{k(k+1)} = \frac{k+1}{k(k+1)} - \frac{k}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$$

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \ldots + \frac{1}{n} - \frac{1}{n+1} = 1 - \frac{1}{n+1}$$

Induktion mit Start in $m \in \mathbb{N}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz F4B: Prinzip der vollständigen Induktion, zweite Fassung

Sei $A(n)_{n \geq m}$ eine Familie von Aussagen $A(n)$. Äquivalent sind:

(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:

$$A(m) \ \wedge \ \forall n \in \mathbb{N}_{\geq m} : [\, A(n) \Rightarrow A(n+1) \,]$$

Indexverschiebung: Die zweite Fassung ist äquivalent zur ersten für

$$B(n) = A(m+n).$$

Induktion: Mehr ist leichter. Weniger ist schwer.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: (1) Beweisen Sie für alle $n \in \mathbb{N}$ die Schranke

$$s_n := \sum_{k=1}^{n} \frac{1}{k^2} \quad = \quad \frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \quad < \quad 2.$$

(2) Zeigen Sie genauer

$$A(n) \ : \quad s_n \leq 2 - {}^1\!/_n \qquad \text{für alle } n \in \mathbb{N}_{\geq 1}.$$

Beweis: (2) Anfang: Für $n = 1$ gilt $s_1 = 1 \leq 2 - {}^1\!/_1$. Schritt: Für $n \geq 2$ gilt

$$\begin{aligned} s_n \overset{\text{Def}}{=} s_{n-1} + \frac{1}{n^2} &\overset{A(n)}{\leq} 2 - \frac{1}{n-1} + \frac{1}{n^2} \\ &\overset{\mathbb{Q}}{<} 2 - \frac{n}{n(n-1)} + \frac{1}{n(n-1)} \overset{\mathbb{Q}}{=} 2 - \frac{(n-1)}{n(n-1)}. \end{aligned}$$

Induktion: starke Fassung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz F4c: Prinzip der vollständigen Induktion, starke Fassung

Sei $A(n)_{n \geq m}$ eine Familie von Aussagen $A(n)$. Äquivalent sind:

(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 $A(m) \wedge \ldots \wedge A(n) \Rightarrow A(n+1)$ für jedes $n \in \mathbb{N}_{\geq m}$:

$$A(m) \;\wedge\; \forall n \in \mathbb{N}_{\geq m} : \big[\, A(m) \wedge \ldots \wedge A(n) \Rightarrow A(n+1) \,\big]$$

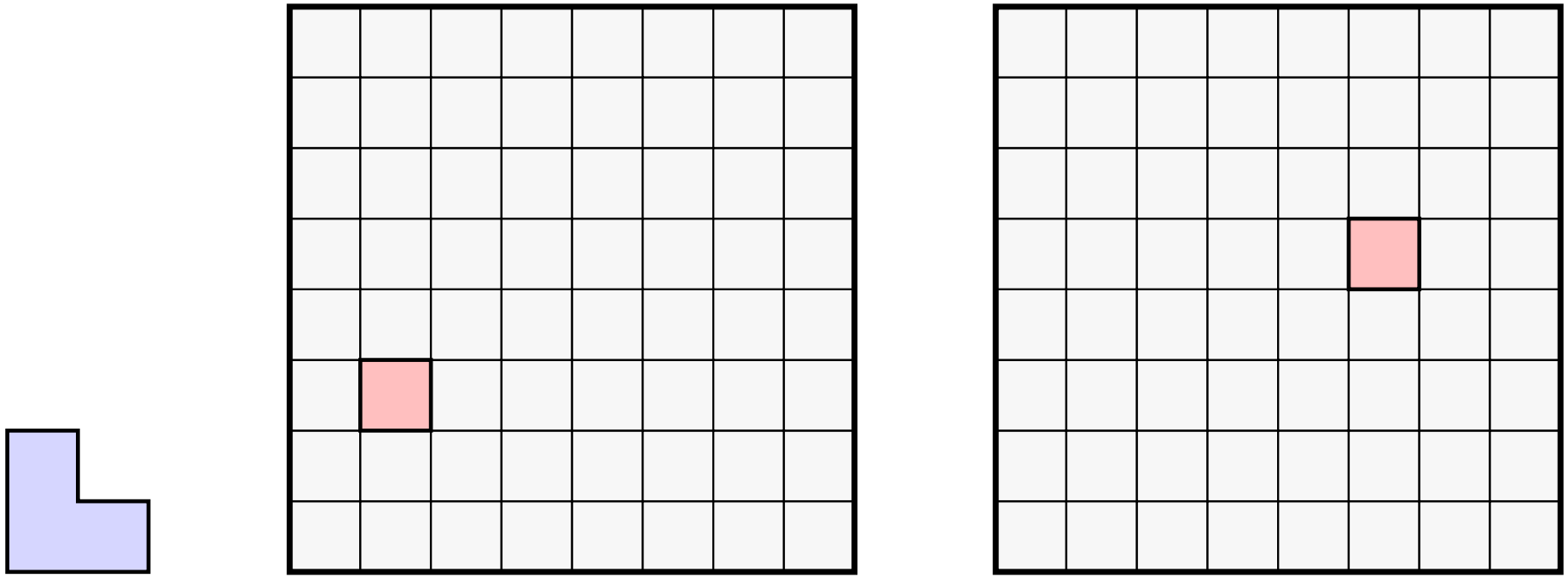
Das ist äquivalent zur einfachen Induktion F4B für die starke Aussage

$$B(n) = A(m) \wedge \ldots \wedge A(n).$$

Versteckte Induktion: Mehr ist leichter. Weniger ist schwer.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



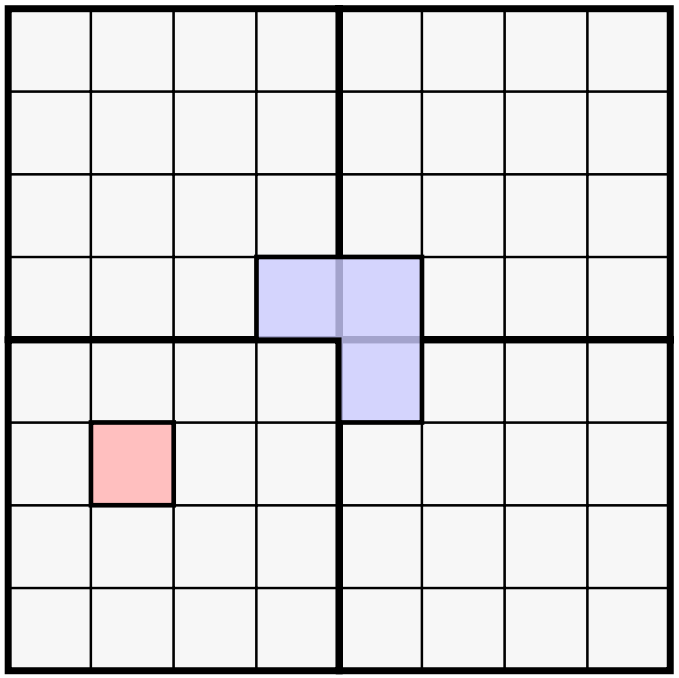
Aufgabe: (1) Wir betrachten ein Schachbrett, mit 8×8 Quadraten. Ein beliebiges dieser 64 Quadrate wird rot markiert. Wie / Können Sie die übrigen 63 Quadrate mit L-Steinen zu je 3 Quadraten bedecken?

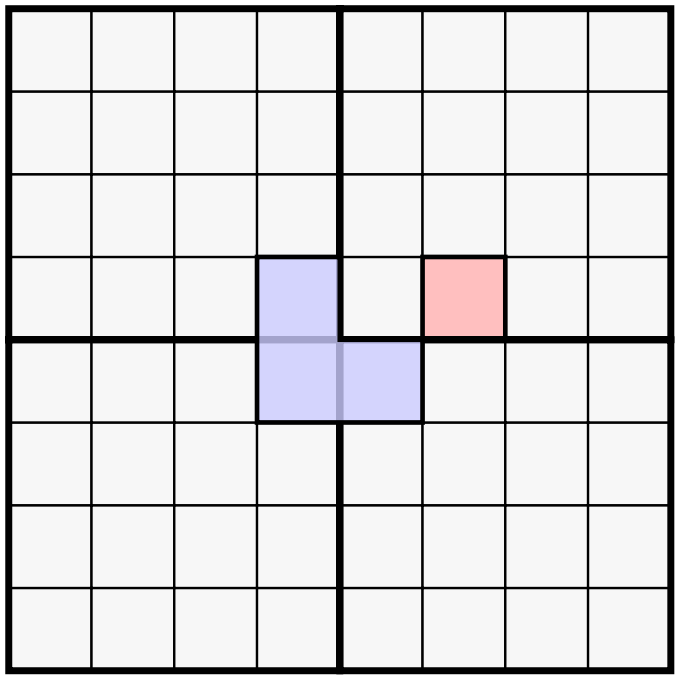
Versteckte Induktion: Mehr ist leichter. Weniger ist schwer.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(2) Lösen Sie das Problem für alle Spielbretter mit $2^n \times 2^n$ Quadraten.



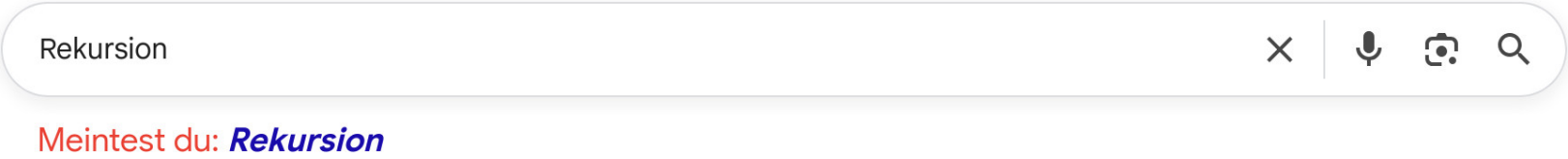


Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel F

Bonusmaterial



Re·kur·sion *gilt als schwierig, doch zu Unrecht!*
So lernen Sie Rekursion in zwei einfachen Schritten:
Prüfen Sie zunächst, ob Sie Rekursion bereits verstehen.
Falls noch nicht, dann lernen Sie als nächstes Rekursion.
— Rekursion, einfach erklärt! —

Inhalt dieses Kapitels F

5 Logik als Spiel

6 Komplexe Spiele, rekursive Lösungen

7 Sie weiß, dass er weiß, dass ich weiß, ...

8 Rekursion und das Master-Theorem

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Individuelles vs geteiltes Wissen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Individuelles vs geteiltes Wissen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Alice gibt verdeckt ihre Zahl $a \in \mathbb{N}$ an die Spielleitung, ebenso Bob seine Zahl $b \in \mathbb{N}$. Die Spielleitung verkündet p und q mit $a + b \in \{p < q\} \subseteq \mathbb{N}$.

Die Spielleitung fragt Alice, ob sie den Wert b zweifelsfrei herleiten kann. Falls ja, so gewinnt Alice. Falls nicht, so fragt die Spielleitung Bob, ob er den Wert a zweifelsfrei herleiten kann. Falls ja, so gewinnt Bob.

Aufgabe: Zeigen Sie, dass das Spiel nach endlich vielen Runden endet.

Individuelles vs geteiltes Wissen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Gemeinsames Wissen ist zunächst $0 \leq a \leq q$ und $0 \leq b \leq q$.

Achtsamkeit: Alice kennt a, weiß also $b \in \{p-a, q-a\}$ sowie $u \leq b \leq v$.
(1a) Gilt $p - a < u$, so kann Alice $b = q - a$ herleiten und antwortet „Ja“.
(1b) Gilt $q - a > v$, so kann Alice $b = p - a$ herleiten und antwortet „Ja“.
Bei „Nein“ gilt somit $p - a \geq u$ und $q - a \leq v$, also $q - v \leq a \leq p - u$.

Zahlenbeispiel: Wir betrachten $a = 5$ und $b = 8$ sowie $p = 13$ und $q = 17$.
1. Alice weiß $a = 5$, also $b \in \{8, 12\}$, sowie $0 \leq b \leq 17$, antwortet „Nein“.
2. Bob weiß $b = 8$, also $a \in \{5, 9\}$, sowie $0 \leq a \leq 13$, antwortet „Nein“.
3. Alice weiß $a = 5$, also $b \in \{8, 12\}$, sowie $4 \leq b \leq 13$, antwortet „Nein“.
4. Bob weiß $b = 8$, also $a \in \{5, 9\}$, sowie $4 \leq a \leq 9$, antwortet „Nein“.
5. Alice weiß $a = 5$, also $b \in \{8, 12\}$, sowie $8 \leq b \leq 9$, antwortet „Ja“.

Quantorenspiele: ∃va gegen ∀dam

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede Aussage mit Existenz- und Allquantoren ist ein Spiel!

∃va spielt die **E**xistenzquantoren und möchte die Behauptung **e**rfüllen.
∀dam spielt die **A**llquantoren und möchte die Behauptung **a**nfechten.

Nulltes Beispiel: Zum Aufwärmen betrachten wir

$$(1) \quad \forall q \in \mathbb{Q}_{>0} \; \exists z \in \mathbb{Z} \; : \; 2^z \geq q$$

$$(2) \quad \forall q \in \mathbb{Q}_{>0} \; \exists z \in \mathbb{Z} \; : \; 2^{z-1} < q \leq 2^z$$

Sei $\mathbb{P} = \{p_0 < p_1 < p_2 < \ldots\}$ die Menge der Primzahlen und $p_{-1} = 0$.

$$(3) \quad \forall n \in \mathbb{N} \; \exists p \in \mathbb{P} \; : \; p > n$$

$$(4) \quad \forall n \in \mathbb{N} \; \exists k \in \mathbb{N} \; : \; p_{k-1} \leq n < p_k$$

Quantorenspiele: ∃va gegen ∀dam

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede Aussage mit Existenz- und Allquantoren ist ein Spiel!

∃va spielt die **E**xistenzquantoren und möchte die Behauptung **e**rfüllen.
∀dam spielt die **A**llquantoren und möchte die Behauptung **a**nfechten.

Erstes Beispiel: Als Spieldaten betrachten wir die Folge

$$(1) \quad x_n := \sum_{k=0}^{n} 2^{-k}.$$

Zwei mögliche Spielregeln sind:

$$\text{(K)} \quad \exists a \in \mathbb{Q} \;\; \forall \varepsilon \in \mathbb{Q}_{>0} \;\; \exists m \in \mathbb{N} \;\; \forall n \in \mathbb{N}_{\geq m} \;:\; |x_n - a| < \varepsilon$$

$$\text{(C)} \quad \forall \varepsilon \in \mathbb{Q}_{>0} \;\; \exists a \in \mathbb{Q} \;\; \exists m \in \mathbb{N} \;\; \forall n \in \mathbb{N}_{\geq m} \;:\; |x_n - a| < \varepsilon$$

Weitere Spieldaten, für noch mehr Spielspaß:

$$(2) \quad x_n := \sum_{k=0}^{n} (-2)^k$$

$$(3) \quad x_n := \sum_{k=0}^{n} 1/k!$$

Quantorenspiele: ∃va gegen ∀dam

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede Aussage mit Existenz- und Allquantoren ist ein Spiel!

∃va spielt die **E**xistenzquantoren und möchte die Behauptung **e**rfüllen.
∀dam spielt die **A**llquantoren und möchte die Behauptung **a**nfechten.

Zweites Beispiel: Als Spieldaten betrachten wir die Funktion

$$f : \mathbb{Q} \to \mathbb{Q} : x \mapsto \operatorname{sign}(x^2 - 2) \qquad \text{auf } X = \mathbb{Q}.$$

Zwei mögliche Spielregeln sind:

$$\forall a \in X \;\; \forall \varepsilon \in \mathbb{Q}_{>0} \;\; \exists \delta \in \mathbb{Q}_{>0} \;\; \forall x \in X \;:\; |a - x| < \delta \Rightarrow |f(a) - f(x)| < \varepsilon$$

$$\forall \varepsilon \in \mathbb{Q}_{>0} \;\; \exists \delta \in \mathbb{Q}_{>0} \;\; \forall a \in X \;\; \forall x \in X \;:\; |a - x| < \delta \Rightarrow |f(a) - f(x)| < \varepsilon$$

Weitere Spieldaten, für noch mehr Spielspaß:

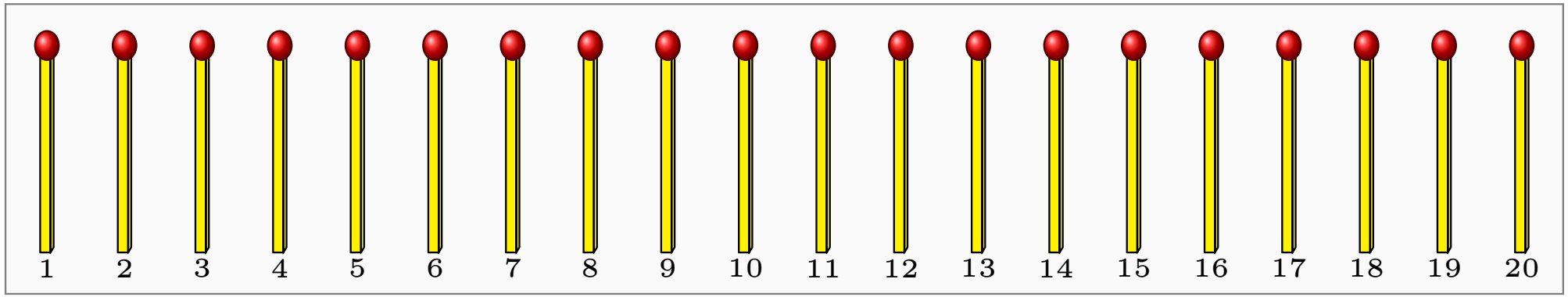
$$g : \mathbb{R} \to \mathbb{R} : x \mapsto \operatorname{sign}(x^2 - 2) \qquad \text{auf } X = \mathbb{R},$$

$$h : \mathbb{R} \to \mathbb{R} : x \mapsto \textstyle\sum_{k=1}^{\infty} \operatorname{dist}(x, \frac{1}{k!}\mathbb{Z}) \qquad \text{auf } X = \mathbb{R}.$$

Nimm eins oder zwei: Rekursion vs Induktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Beide Spieler ziehen abwechselnd, jeder entfernt ein oder zwei Hölzer.
Normalspiel / Misèrespiel: Wer nicht mehr ziehen kann, verliert / gewinnt.

Nimm eins oder zwei: Rekursion vs Induktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

(2) Wie lautet die allgemeine Regel?

Satz F6A: einzeiliges Nim mit Zugoptionen $S = \{1, 2, \dots, n-1\}$

Misèrespiel: Genau dann ist x eine Verlustposition, wenn $x \bmod n = 1$.
Normalspiel: Genau dann ist x eine Verlustposition, wenn $x \bmod n = 0$.

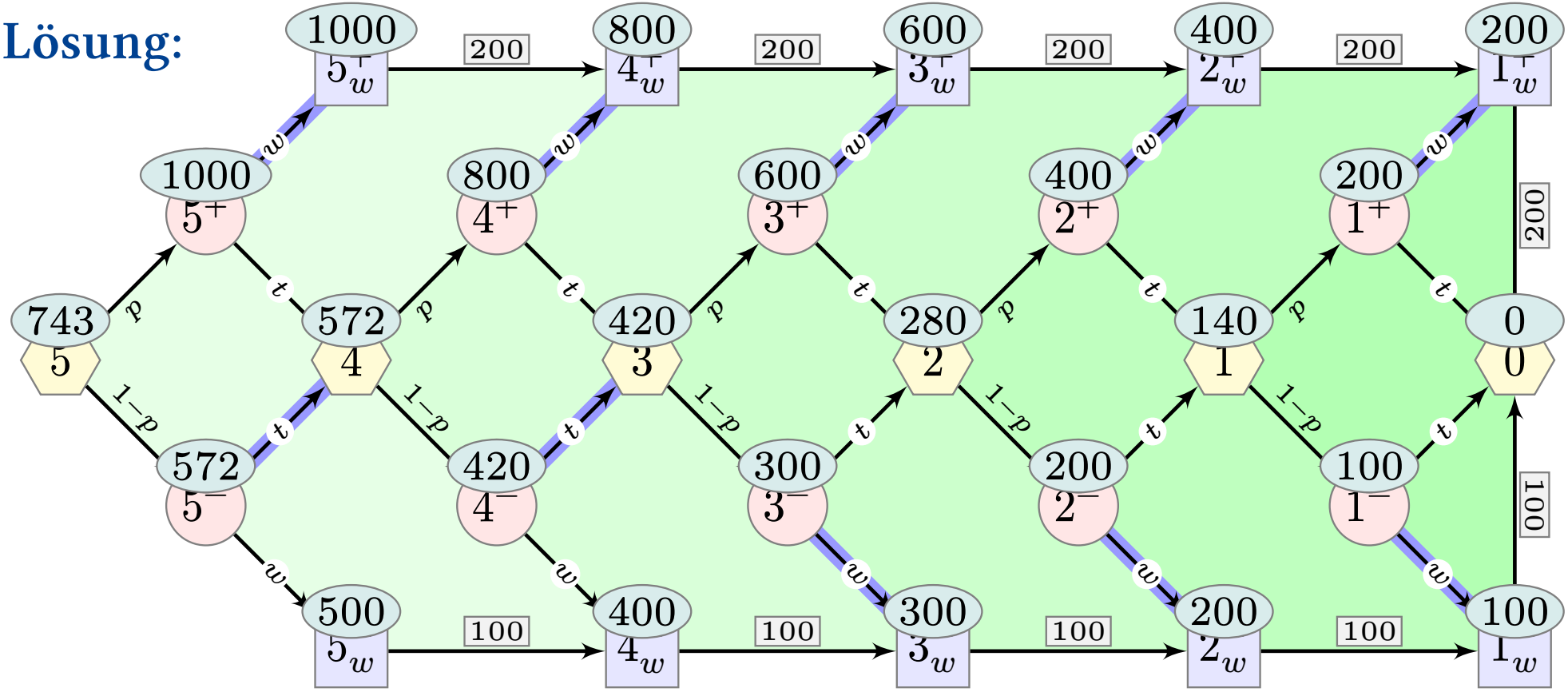
Optimal entscheiden: work or travel?

Dies ist nur die Saalversion ohne Erläuterungen.

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.

Formulieren Sie dies als Graph. Wie viele Strategien gibt es? Welche davon sind optimal profitabel? Welches Einkommen erwarten Sie?

Lösung:



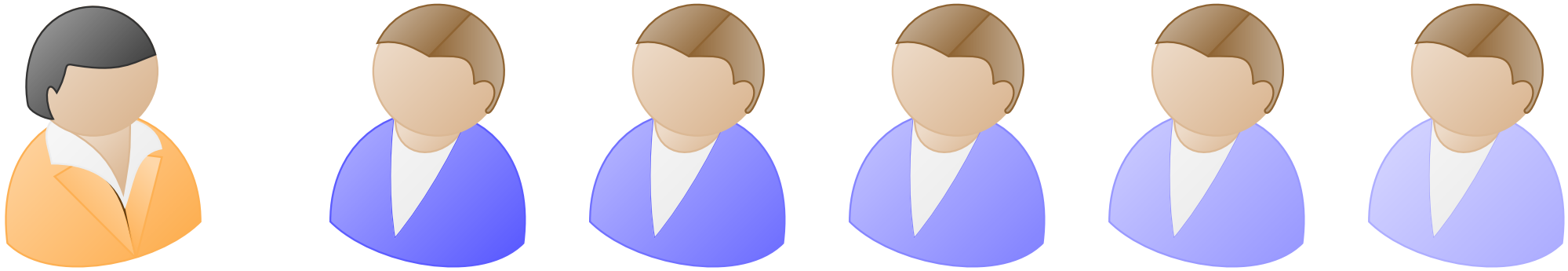
Ausführliche Erläuterungen bietet die Vollversion.

Optimale Partnerwahl: Looking for Mr. Right... or Mr. Almost

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Marriage problem: When to stop dating and start getting married?



Alice 1 2 3 ... n

Alice begegnet im Laufe ihres Lebens n potentiellen Ehemännern.
Bei Kandidat $k = 1, 2, 3, \dots, n$ 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.

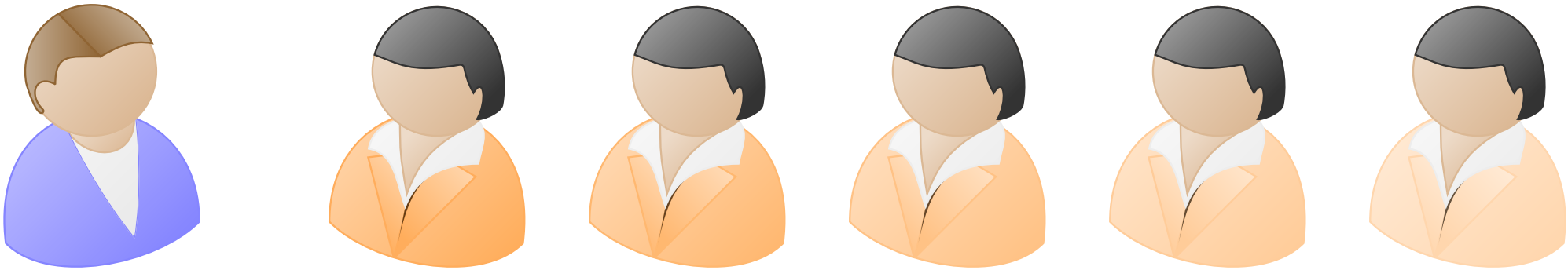
Aufgabe: Wie anspruchsvoll soll Alice sein? Was ist optimal?
Welche Eignung ihres Ehepartners kann Alice maximal erwarten?

Optimales Stoppen: das Sekretärinnen-Problem

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Secretary problem: When to stop interviewing and start hiring?



Bob 1 2 3 ... n

Bob stellt eine Sekretärin (w/m/d) ein. Dazu sind n Bewerber:innen eingeladen, in zufälliger Reihenfolge. Bob sucht die *beste* Kandidatin. Im Interview mit Kandidatin k kann er nur feststellen, ob sie besser ist als alle vorigen. Er kann sie sofort einstellen oder ihr definitiv absagen.

Aufgabe: Wie soll Bob vorgehen? Wie maximiert er seine Trefferwkt?

Die 37%–Regel: Interviewe zunächst $\lceil n/\mathrm{e} \rceil$ Kandidatinnen mit Absage; dann wähle die nächste Kandidatin, die besser ist als alle vorigen.

Optimales Stoppen: das Sekretärinnen-Problem

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Problemstellung: Sie bekommen n Angebote zu Zeiten $t = 1, 2, \dots, n$. Setze $X_t = 1$, falls Angebot t besser ist als alle vorigen, sonst $X_t = 0$.

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.

(a) Die Zufallsvariablen $X_1, X_2, \dots, X_n : \Omega \to \{0, 1\}$ seien unabhängig mit den Wkten $\mathbf{P}(X_t{=}1) = p_t \in [0, 1]$ 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 $p_t = 1/t$.

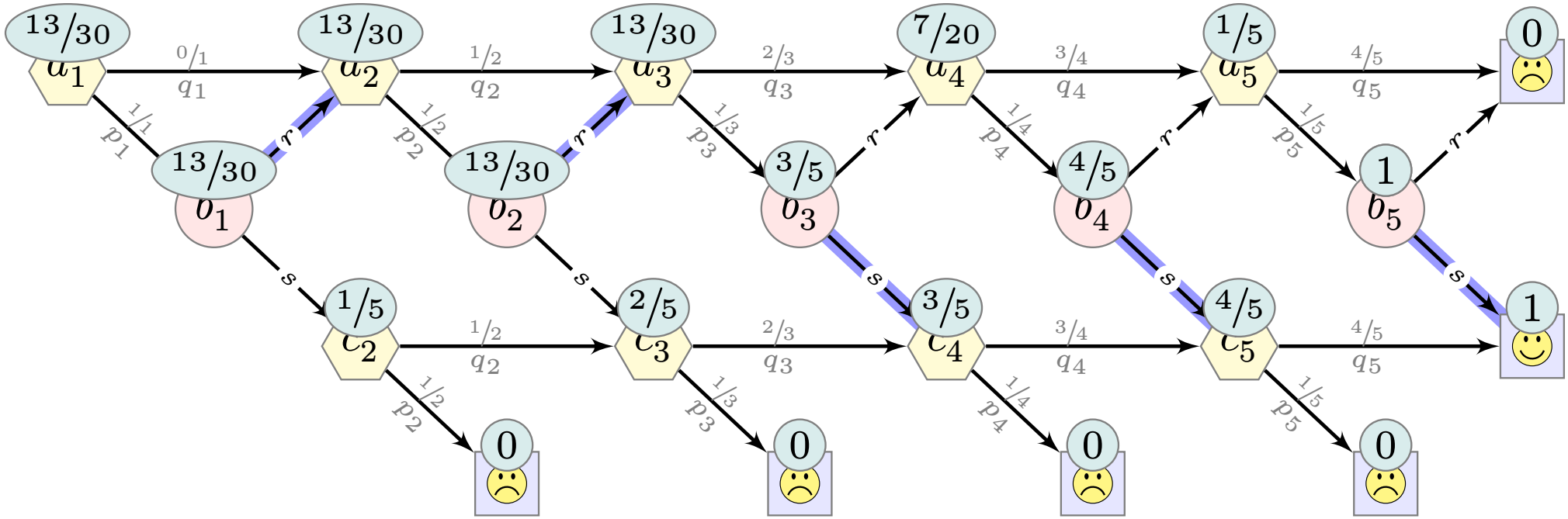
Aufgabe: (1) Formulieren Sie dieses Spiel als einen Markov–Graphen. (2) Was ist die beste Strategie? (3) Was ist die optimale Erfolgswkt?

Optimales Stoppen: der Bruss–Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Untersuchen Sie den Fall $n = 5$ mit $p_k = 1/k$ und $q_k = 1 - p_k$.



Aufgabe: Wie gelingt dies allgemein? Beweisen Sie folgenden Satz:

Satz F6c: *Sum the odds to one and stop*, Bruss 2000

Sei $s \in \{1, \dots, n\}$ 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 $Q_s = q_s \cdots q_n$.

Die 37%–Regel: Für $p_k = 1/k$ gilt $s \gtrapprox n/\mathrm{e}$ und $R_s Q_s \gtrapprox 1/\mathrm{e} \gtrapprox 0.367$.

Meuterei auf der Bounty (1935)

Dies ist nur die Saalversion ohne Erläuterungen.

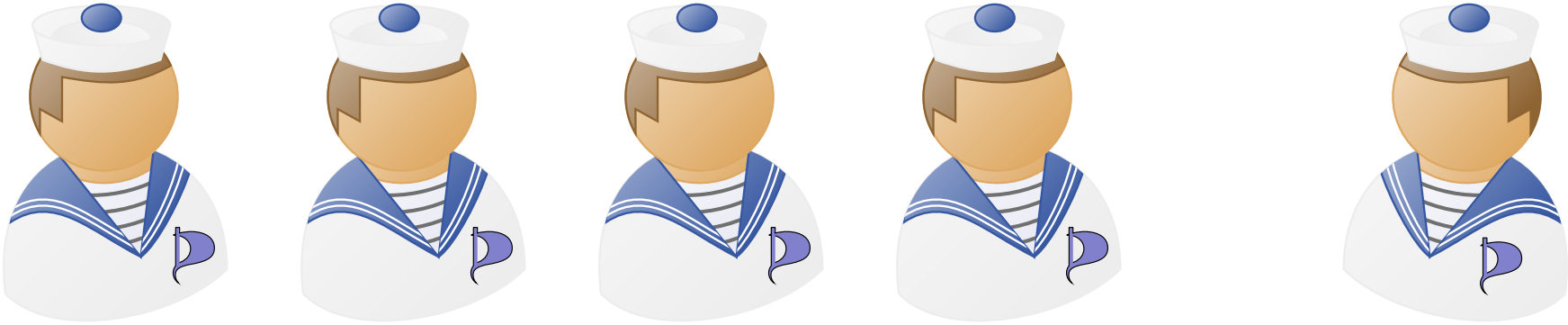
Ausführliche Erläuterungen bietet die Vollversion.

Fünf gierige Piraten / *the pirate game*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Fünf basisdemokratische Piraten $1, 2, 3, 4, 5$ teilen sich 100 Dukaten.



1 2 3 4 5

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.

Fünf gierige Piraten / *the pirate game*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Lösen Sie das Piratenrätsel für $n = 5$, sowie für alle $n \in \mathbb{N}$.

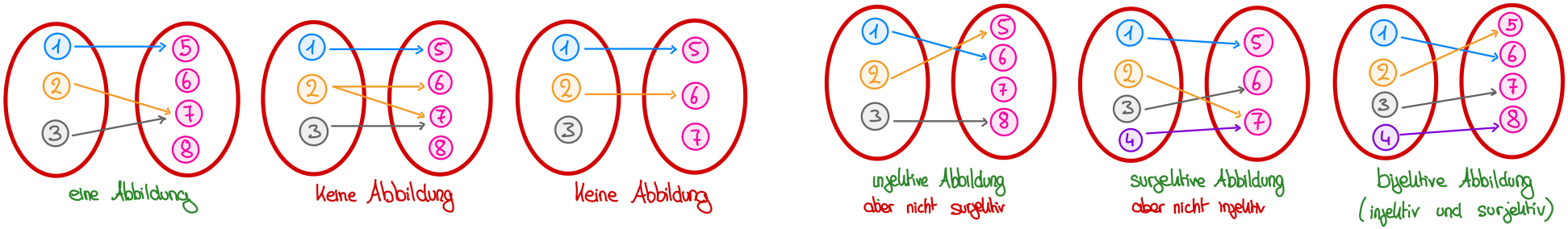
Lösung: Wir nutzen Induktion über $n = 1, 2, 3, 4, 5, \ldots$ und finden:

	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	…	☠	☠	☠	☠	☠	☠
$\vdots$												
$\mathscr{R}_{197}$	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

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel G

Mengen, Relationen und Abbildungen: Set Theory for the Working Mathematician



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*

Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels G

1 Mengenlehre nach Zermelo–Fraenkel

2 Relationen und Abbildungen

3 Abbildungen invertieren

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Mengen und Funktionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Frage G0A: Rechenregeln für Mengen und Funktionen

(0) Wie viele Elemente haben die folgenden Mengen?

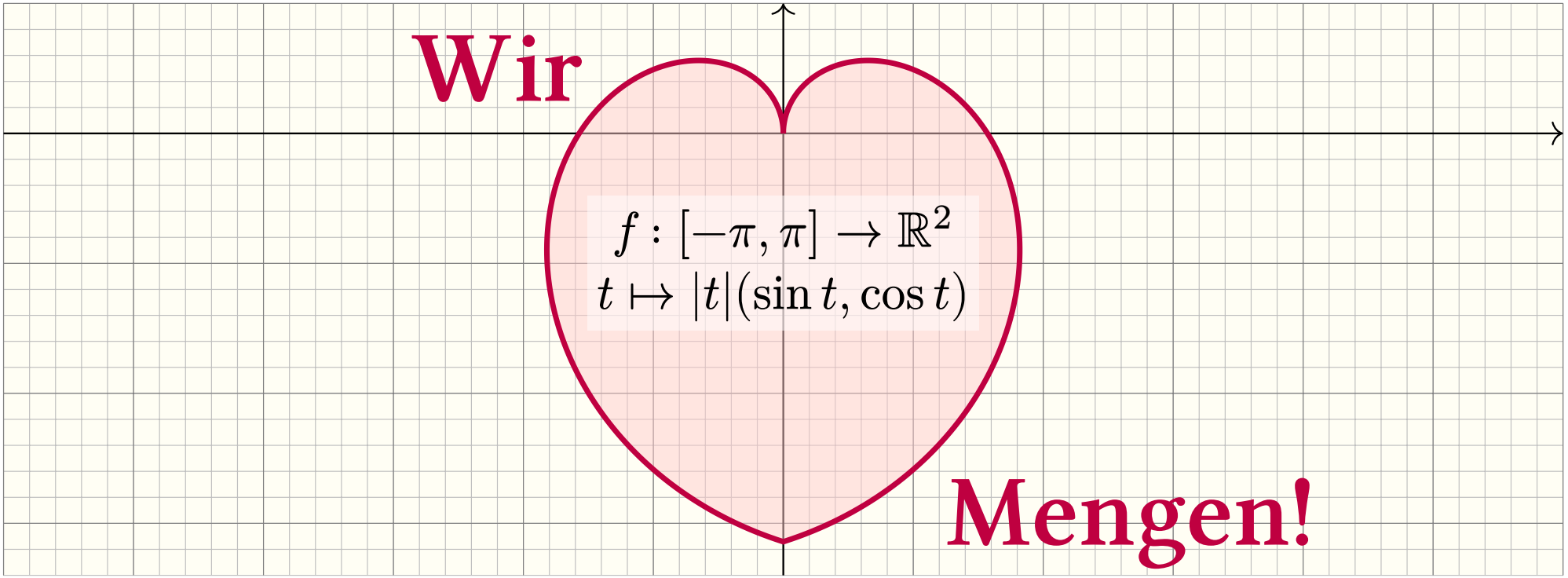
$$\emptyset = \{\}, \quad X = \{\emptyset\}, \quad Y = \{\,\emptyset, \{\}, \{\emptyset\}, X\,\},$$
$$Z = \{\,\emptyset, \emptyset, \{\}, X, \{\emptyset\}, \{\{\}\}, \{0,1\}, \{1,0\}, \{1,0,1\}\,\}$$

(1) Wie viele Elemente hat die Potenzmenge $\mathfrak{P}(Z) = \{\,A \subseteq Z\}$?

(2) Wie bestimmen Sie $L = \left\{\, x \in \mathbb{K}^n \;\middle|\; Ax = b \right\}$ zu $A \in \mathbb{K}^{m\times n}$, $b \in \mathbb{K}^m$?

(3) Wie skizzieren Sie die Kurve $K = \{\,|t|(\sin t, \cos t) : t \in [-\pi, \pi]\,\} \subseteq \mathbb{R}^2$?

Mengen und Funktionen



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Auch Mengen brauchen Regeln.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Georg Cantor (1895): „Mengen sind beliebige Zusammenfassungen.“

Bertrand Russel (1903): „Was ist dann mit der Menge $\mathscr{R} = \{\, x \mid x \notin x \,\}$?“

Ernst Zermelo (1908), Abraham Fraenkel (1921): „Wir brauchen Regeln!“

LAST: die formale Sprache der Mengenlehre

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition G1A: die formale Sprache der Mengenlehre

Wir definieren die **formale Sprache** LAST der Mengenlehre,

$$\mathscr{F}(\underbrace{\{\bot, \top, \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \forall, \exists\}}_{\text{Junktoren (0,1,2–stellig) und Quantoren}}, \underbrace{\{v_0, v_1, v_2, \dots\}}_{\text{Variablen für Mengen}}, \underbrace{\{\emptyset, \dots\}}_{\text{Konstanten}}, \underbrace{\{=, \in, \dots\}}_{\text{Relationen}}).$$

Atomare Formeln: Falsch $\bot$ und Wahr $\top$ sind Formeln und ebenso $(x = y)$ und $(x \in y)$ für je zwei Mengenvariablen bzw. Konstanten x, y.

Zusammensetzung: Sind φ und ψ Formeln, so auch $(\neg\varphi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$ sowie $(\forall x : \varphi)$ und $(\exists x : \varphi)$ für jede Mengenvariable x.

Extensionalität: Wann sind zwei Mengen gleich?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Teilmenge: Inklusion $a \subseteq b$ bedeutet, für jedes Element $x \in a$ gilt $x \in b$.

$$a \subseteq b \quad :\Longleftrightarrow \quad \forall x : (x \in a) \Rightarrow (x \in b)$$

Extensionalität: Gleichheit $a = b$ ist äquivalent zu $a \subseteq b$ und $b \subseteq a$.

$$a = b \quad \Longleftrightarrow \quad \forall x : (x \in a) \Leftrightarrow (x \in b)$$

Klassen von Mengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir arbeiten in einem Universum $\mathcal{U}$, genannt die **Klasse aller Mengen**.
Jedes Prädikat $\varphi(x)$ definiert die zugehörige Klasse $\mathcal{K} := \{\, x \mid \varphi(x) \,\} \subseteq \mathcal{U}$.

$$\emptyset = \{\, x \mid \bot \,\}$$
$$\mathcal{U} = \{\, x \mid \top \,\}$$

Grundlagenkrise: Russels Antinomie (1903)

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel G1B: Russels Antinomie

Wir untersuchen die Klasse

$$\mathscr{R} = \{\, x \mid x \notin x \,\}.$$

Für jede Menge x gilt $x \in \mathscr{R} \Leftrightarrow x \notin x$. Ist $\mathscr{R}$ eine Menge? Falls ja, so folgt $\mathscr{R} \in \mathscr{R} \Leftrightarrow \mathscr{R} \notin \mathscr{R}$. Logische Katastrophe: Wahr und Falsch sind äquivalent!

☺ Ausweg: Wir müssen die Konstruktion von Mengen reglementieren!

Aufzählung $\{\} : \mathcal{U}^n \to \mathcal{U} : (a_1, \dots, a_n) \mapsto \{a_1, \dots, a_n\}$

$$\{a_1, \dots, a_n\} := \{\, x \mid x = a_1 \vee \dots \vee x = a_n \,\} \in \mathcal{U}.$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Potenz $\mathfrak{P} : \mathcal{U} \to \mathcal{U} : a \mapsto \mathfrak{P}(a) := \{\, x \mid x \subseteq a \,\}$

$$\begin{aligned}
\mathfrak{P}(\emptyset) &= \{\, \emptyset \,\} \\
\mathfrak{P}(\{1\}) &= \{\ \emptyset,\ \{1\}\ \} \\
\mathfrak{P}(\{1,2\}) &= \{\ \emptyset,\ \{1\}, \{2\},\ \{1,2\}\ \} \\
\mathfrak{P}(\{1,2,3\}) &= \{\ \emptyset,\ \{1\}, \{2\}, \{3\},\ \{1,2\}, \{1,3\}, \{2,3\},\ \{1,2,3\}\ \}
\end{aligned}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aussonderung $\mathfrak{A}_\varphi : \mathcal{U} \to \mathcal{U} : b \mapsto a := \{\, x \in b \mid \varphi(x) \,\}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Es gilt $\{\, x \in \mathbb{N} \mid \mathrm{prim}(x) \,\} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$.

Ersetzung $\mathfrak{B}_f : \mathcal{U} \to \mathcal{U} : a \mapsto b := \{\, f(x) \mid x \in a \,\}$

Dies ist nur die Saalversion ohne Erläuterungen.

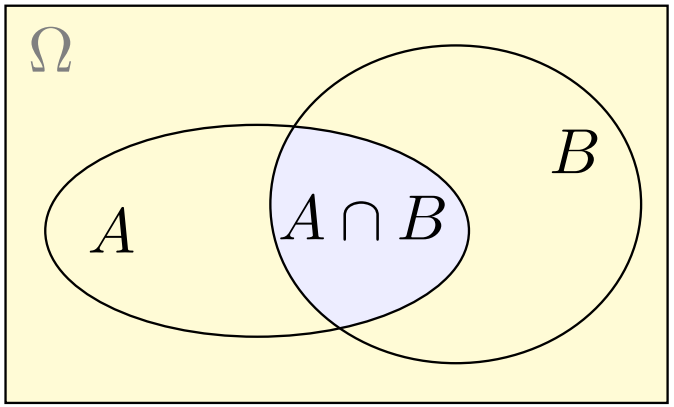
Ausführliche Erläuterungen bietet die Vollversion.

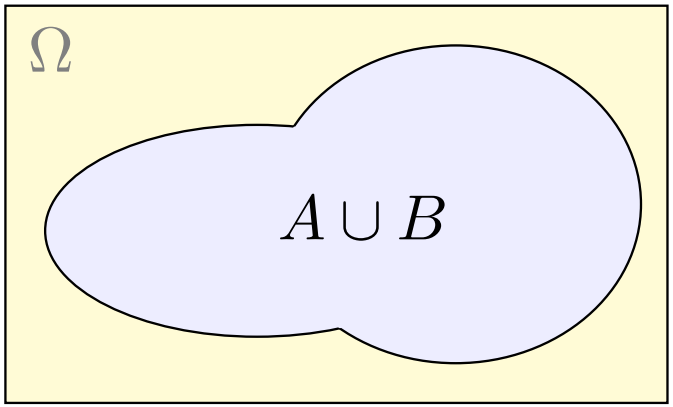
Beispiel: Es gilt $\{\, x^2 \mid x \in \mathbb{Z} \,\} = \{\, 0, 1, 4, 9, 16, 25, 36, 49, \ldots \,\}$.

Schnittmenge und Vereinigung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Die **Schnittmenge** ist

$$A \cap B = \{x \in \Omega \mid x \in A \wedge x \in B\} \in \mathcal{U}.$$

Die **Vereinigungsmenge** ist

$$A \cup B = \{x \in \Omega \mid x \in A \vee x \in B\} \in \mathcal{U}.$$

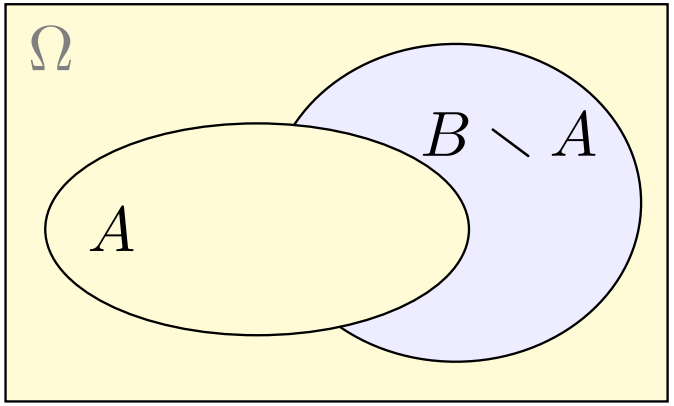
Disjunkte Vereinigung:

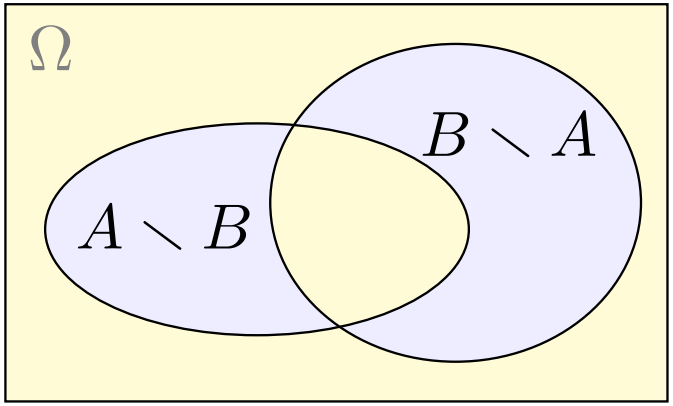
$$V = A \sqcup B \text{ bedeutet } V = A \cup B \text{ und } A \cap B = \emptyset.$$

Restmenge und symmetrische Differenz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Die **Restmenge** oder **Differenzmenge** „B ohne A“ ist

$$B \setminus A := \{ x \in B \mid x \notin A \} \in \mathcal{U}.$$

Die **symmetrische Differenz** „entweder A oder B“ ist

$$A \triangle B := \{ x \in \Omega \mid x \in A \mathbin{\dot{\vee}} x \in B \} \in \mathcal{U}.$$

Rechenregeln für Vereinigung $\cup$ und Schnitt $\cap$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz G1c: Rechenregeln für Mengen

(1) Kommutativität:

$$A \cup B = B \cup A,$$
$$A \cap B = B \cap A$$

(2) Assoziativität:

$$A \cup (B \cup C) = (A \cup B) \cup C,$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$

(3) Distributivität:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Rechenregeln für Komplement und Restmenge

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz G1c: Rechenregeln für Mengen

(4) Für je drei Mengen A, B, C gilt

$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B),$$
$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B).$$

Rechenregeln für Komplement und Restmenge

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(4) De Morgan:

$$
\begin{aligned}
x \in C \setminus (A \cap B) &\overset{\text{Def}}{\Longleftrightarrow} x \in C \wedge \neg(x \in A \wedge x \in B) \\
&\underset{\text{F1G}}{\overset{\text{DeM}}{\Longleftrightarrow}} x \in C \wedge (x \notin A \vee x \notin B) \\
&\underset{\text{F1G}}{\overset{\text{Dst}}{\Longleftrightarrow}} (x \in C \wedge x \notin A) \vee (x \in C \wedge x \notin B) \\
&\overset{\text{Def}}{\Longleftrightarrow} x \in (C \setminus A) \cup (C \setminus B)
\end{aligned}
$$

Vereinigung und Schnitt einer Mengenfamilie

$$\bigcup_{i=1}^{n} A_i := A_1 \cup \cdots \cup A_n \quad \text{und} \quad \bigcap_{i=1}^{n} A_i := A_1 \cap \cdots \cap A_n$$

$$\bigcup_{i \in I} A_i := \{\, x \mid \exists i \in I : x \in A_i \,\} \quad \text{und} \quad \bigcap_{i \in I} A_i := \{\, x \mid \forall i \in I : x \in A_i \,\}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vereinigung $\bigcup : \mathcal{U} \to \mathcal{U}$ und Schnitt $\bigcap : \mathcal{U}^* \to \mathcal{U}$

$$\bigcup S = \bigcup_{A \in S} A := \{\, x \mid \exists A \in S : x \in A \,\}$$
$$\bigcap S = \bigcap_{A \in S} A := \{\, x \mid \forall A \in S : x \in A \,\}$$

Beispiel: Für jede Menge $M \in \mathcal{U}$ gilt $\bigcup \mathfrak{P}(M) = M$ und $\bigcap \mathfrak{P}(M) = \emptyset$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

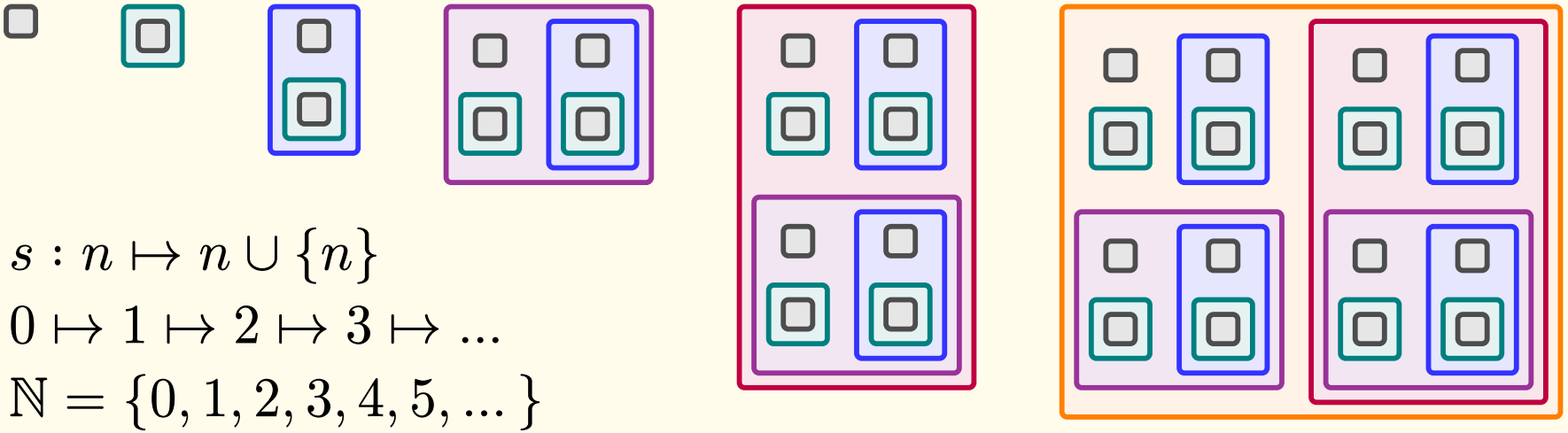
Wie codieren wir natürliche Zahlen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

John von Neumanns Konstruktion

0	1	2	3	4	5
$\ddot{=}$	$\ddot{=}$	$\ddot{=}$	$\ddot{=}$	$\ddot{=}$	$\ddot{=}$
$\emptyset$	$\{0\}$	$\{0,1\}$	$\{0,1,2\}$	$\{0,1,2,3\}$	$\{0,1,2,3,4\}$



$s : n \mapsto n \cup \{n\}$

$0 \mapsto 1 \mapsto 2 \mapsto 3 \mapsto \ldots$

$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$

der natürlichen Zahlen $(\mathbb{N}, 0, s)$

Designed 2024 by Michael Eisermann, University of Stuttgart

Transfinite Ordinalzahlen: *beyond infinity*

$$
\begin{aligned}
0 &:= \emptyset \\
1 &:= \{0\} \\
2 &:= \{0,1\} \\
3 &:= \{0,1,2\} \\
&\vdots \\
\omega &:= \{0,1,2,\ldots\} \\
\omega+1 &:= \{0,1,2,\ldots,\omega\} \\
\omega+2 &:= \{0,1,2,\ldots,\omega,\omega+1\} \\
&\vdots \\
\omega 2 &:= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots\} \\
\omega 2+1 &:= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,\omega 2\} \\
\omega 2+2 &:= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,\omega 2,\omega 2+1\} \\
&\vdots
\end{aligned}
$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Überdeckungen $M = \bigcup U$ und Zerlegungen $M = \bigsqcup Z$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Die Familie $U = \{\emptyset, \{1,2\}, \{2,3\}\}$ überdeckt $M = \{1,2,3\}$.
Die Familie $Z = \{\{1,4\}, \{2,3,6,7\}, \{5\}\}$ zerlegt $M = \{1,2,3,4,5,6,7\}$.

Eine **Überdeckung** von M ist eine Menge $U \subseteq \mathfrak{P}(M)$ mit $\bigcup U = M$:

$$\forall x \in M \;\; \exists A \in U : x \in A$$

Eine **Zerlegung** $M = \bigsqcup Z$ ist eine disjunkte Überdeckung $Z \subseteq \mathfrak{P}(M)^*$:

$$\bigcup Z = M \;\; \wedge \;\; \forall A, B \in Z : A = B \;\dot{\vee}\; A \cap B = \emptyset$$

Auswahlmenge aka Repräsentantensystem

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Zur Zerlegung $Z = \{\{1,4\},\{2,3,6,7\},\{5\}\}$ ist $R = \{1,2,5\}$ eine Auswahl, ebenso $\{4,3,5\}$ oder $\{1,6,5\}$ etc. Wie viele Auswahlen gibt es?

Allgemein sei $Z \subseteq \mathfrak{P}(M)^*$ eine Zerlegung von $M = \bigsqcup Z$. Eine Teilmenge $R \subseteq M$ heißt **Auswahlmenge** oder **Repräsentantensystem** zu Z, falls gilt:

$$\forall A \in Z \;\; \exists! x \in R : x \in A$$

Beispiel: Die Menge $M = \bigsqcup\{A_1, \dots, A_n\}$ der Schüler:innen teilt sich in Klassen auf, $R = \{a_1, \dots, a_n\}$ enthält die Klassensprecher:innen $a_i \in A_i$.

Auswahlaxiom (AC): Zu jeder Zerlegung existiert eine Auswahlmenge.

Globale Auswahl $\mathfrak{C} : \mathcal{U}^* \to \mathcal{U} : a \mapsto x$ mit $x \in a$

Die Wahl $\mathfrak{C} : \mathcal{U}^* \to \mathcal{U}$ bestimmt zu jeder Menge $a \neq \emptyset$ ein $x \in a$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Zermelo–Fraenkel–Axiome: ZF+AC = ZFC

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir arbeiten in einem Mengenuniversum $(\mathcal{U}, \in, =, \{\}, \bigcup, \mathfrak{P}, \mathfrak{A}_\bullet, \mathfrak{B}_\bullet, \omega, \mathfrak{C})$.

(ZF0) **Fundierung:** In $(\mathcal{U}, \in)$ ist jede Kette $M_0 \ni M_1 \ni M_2 \ni \dots$ endlich.

(ZF1) **Extensionalität:** Für $A, B \in \mathcal{U}$ gilt $A = B$ gdw $\forall x : x \in A \Leftrightarrow x \in B$.

(ZF2) **Aufzählung:** Zu $a_1, \dots, a_n \in \mathcal{U}$ existiert $\{a_1, \dots, a_n\} \in \mathcal{U}$.

(ZF3) **Vereinigung:** Zu jeder Menge $S \in \mathcal{U}$ existiert $\bigcup S \in \mathcal{U}$.

(ZF4) **Potenz:** Zu jeder Menge $A \in \mathcal{U}$ existiert $\mathfrak{P}(A) \in \mathcal{U}$.

(ZF5) **Aussonderung:** Zu (B, φ) existiert $A = \{\, x \in B \mid \varphi(x) \,\} \in \mathcal{U}$.

(ZF6) **Ersetzung:** Zu (A, f) existiert $B = \{\, f(x) \mid x \in A \,\} \in \mathcal{U}$.

(ZF7) **Unendlichkeit:** $\mathcal{U} \ni \omega := \bigcap \{\, a \mid \emptyset \in a \wedge \forall n \in a : (n \cup \{n\}) \in a \,\}$

(ZF8) **Globale Auswahl:** Wir haben $\mathfrak{C} : \mathcal{U}^* \to \mathcal{U} : a \mapsto x$ mit $x \in a$.

Paare und kartesische Produktmenge

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aus Elementen $x \in A$ und $y \in B$ bilden wir das geordnete **Paar** (x, y).
Gleichheit $(x, y) = (x', y')$ soll äquivalent sein zu $(x = x') \wedge (y = y')$.

⚠ Die Paarmenge $\{x, y\}$ ist dazu ungeeignet, denn $\{x, y\} = \{y, x\}$.

☺ Es gelingt jedoch mit Kuratowskis Kniff $(x, y) := \{\{x\}, \{x, y\}\}$.

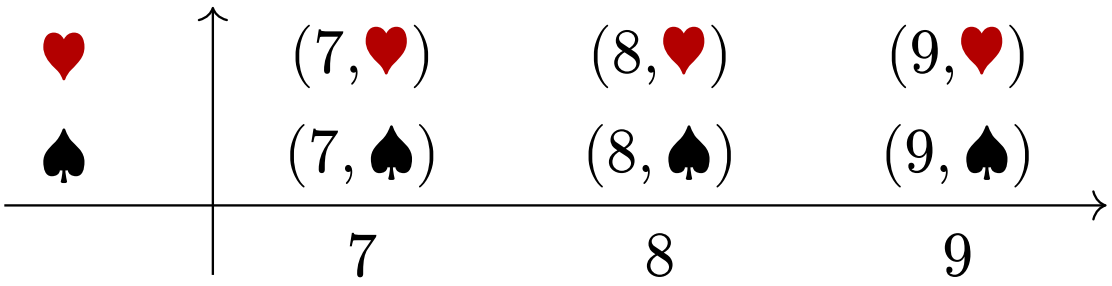
Das kartesische **Produkt** von A und B ist die Menge aller Paare:

$$A \times B := \{\, (x, y) \mid x \in A \wedge y \in B \,\}$$

Beispiel:

$$\{7, 8, 9\} \times \{\spadesuit, \heartsuit\} = \{(7, \spadesuit), (7, \heartsuit), (8, \spadesuit), (8, \heartsuit), (9, \spadesuit), (9, \heartsuit)\}$$

Graphisch:



Relationen, Umkehrung und Komposition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition G2B: Relation zwischen zwei Mengen X und Y

Eine **Relation zwischen X und Y** ist eine Teilmenge $F \subseteq X \times Y$.
Infix-Notation: Für $(x, y) \in F$ schreiben wir auch $x\, F\, y$ (wie „$x \leq y$“).

(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 **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**

$$K =: F \bullet G = G \circ F \subseteq X \times Z \quad (\text{„}F \text{ dann } G\text{“ bzw. „}G \text{ nach } F\text{“}),$$
$$K = \{\, (x, z) \in X \times Z \mid \exists y \in Y : (x, y) \in F \wedge (y, z) \in G \,\}.$$

Wir kürzen $(x, y) \in F \wedge (y, z) \in G$ ab zu $x\, F\, y\, G\, z$ (wie „$x \leq y \leq z$“).
Die Komposition $x\, (F \bullet G)\, z$ ist somit definiert durch $\exists y \in Y : x\, F\, y\, G\, z$.

Diagonale und Umkehrrelation

Δ	♣	♠	♥	♦
♣	1	0	0	0
♠	0	1	0	0
♥	0	0	1	0
♦	0	0	0	1

F	5	6	7
♣	1	0	1
♠	1	1	0
♥	0	1	0
♦	0	0	0

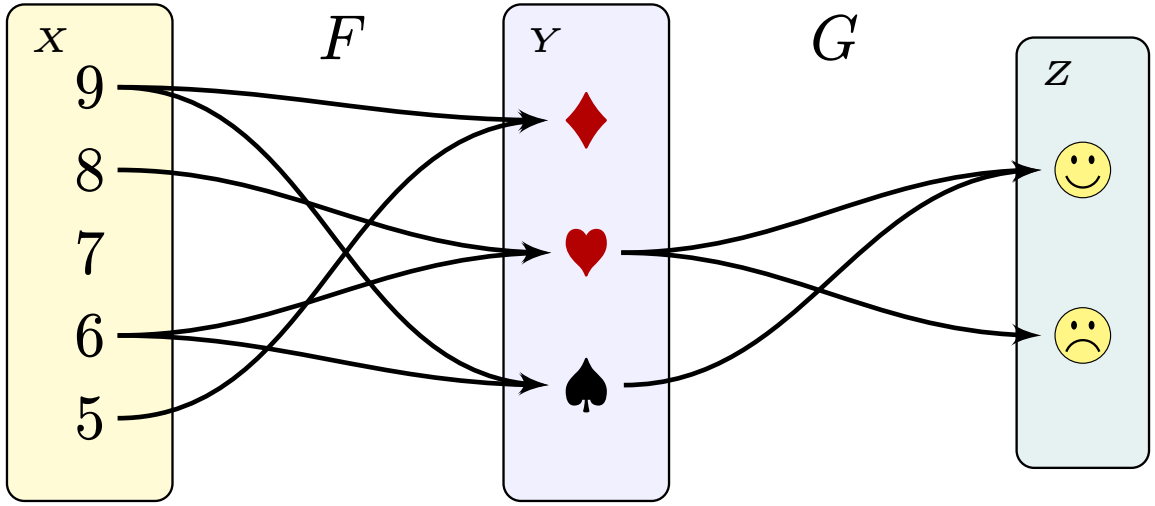
$\longleftrightarrow$

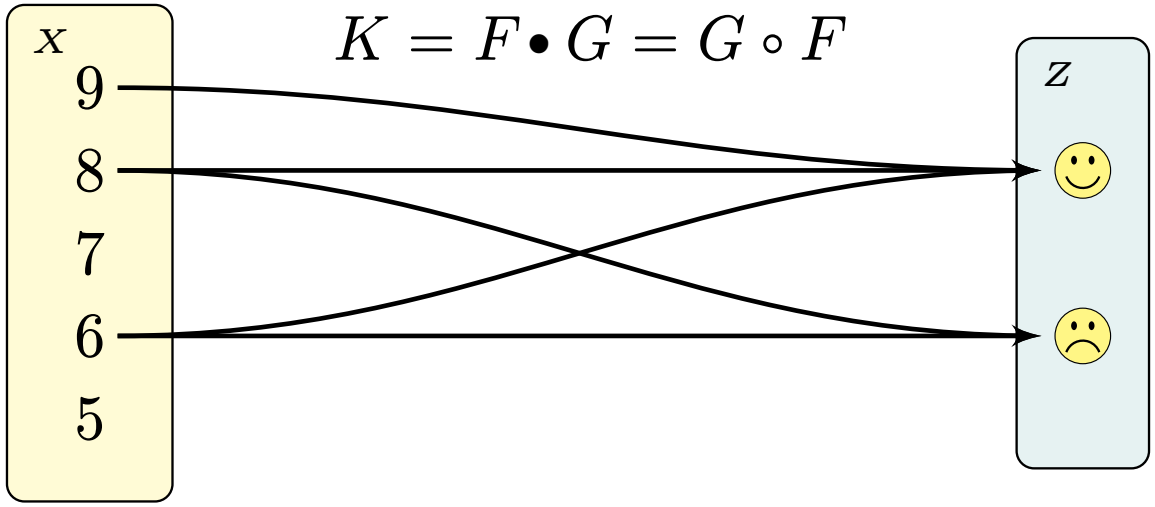
$F^\top$	♣	♠	♥	♦
5	1	1	0	0
6	0	1	1	0
7	1	0	0	0

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Relationen und ihre Komposition





Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Relationen und ihre Komposition

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

$=$

K	☺	☹
5	0	0
6	1	1
7	0	0
8	1	1
9	1	0

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Relationen mit Start und Ziel

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition G2c: Relation mit Start und Ziel

Eine **Relation** $f = (X, F, Y)$ besteht aus ihrer **Startmenge** X und ihrer **Zielmenge** Y sowie ihrem **Relationsgraphen** $F \subseteq X \times Y$.

(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 **Umkehrrelation**

$$f^{-1} = f^{\mathsf{T}} = (Y, F^{\mathsf{T}}, X) \quad \text{mit} \quad F^{\mathsf{T}} = \{\, (y, x) \mid (x, y) \in F \,\}.$$

(3) Zu $f = (X, F, Y)$ und $g = (Y, G, Z)$ definieren wir ihre **Komposition**

$$k = (X, K, Z) =: f \bullet g = g \circ f \quad (\text{„}f \text{ dann } g\text{“ bzw. „}g \text{ nach } f\text{“}),$$

$$K = \{\, (x, z) \in X \times Z \mid \exists y \in Y : (x, y) \in F \wedge (y, z) \in G \,\}.$$

Rechenregeln für die Komposition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz G2D: Neutralität, Umkehrung, Assoziativität (aka *Kategorie)

Für $f = (X, F, Y)$ und $g = (Y, G, Z)$ und $h = (Z, H, W)$ gilt:

(1) Neutralität $\quad \mathrm{id}_X \bullet f = f = f \bullet \mathrm{id}_Y \quad$ bzw. $\quad f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f.$

(2) Umkehrung $\quad (f \bullet g)^\top = g^\top \bullet f^\top \quad$ bzw. $\quad (g \circ f)^\top = f^\top \circ g^\top.$

(3) Assoziativität $\quad (f \bullet g) \bullet h = f \bullet (g \bullet h) \quad$ bzw. $\quad (h \circ g) \circ f = h \circ (g \circ f).$

Rechenregeln für die Komposition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(3) Wir setzen die Definition ein und rechnen es nach!

$$
\begin{aligned}
(x,w) \in F \bullet (G \bullet H) &\overset{\text{Def}}{\iff} \exists y \in Y : x\,F\,y \wedge y\,(G \bullet H)\,w \\
&\overset{\text{Def}}{\iff} \exists y \in Y : x\,F\,y \wedge \big[\exists z \in Z : y\,G\,z \wedge z\,H\,w\big] \\
&\overset{\text{Dst}}{\iff} \exists y \in Y\ \exists z \in Z : x\,F\,y \wedge y\,G\,z \wedge z\,H\,w \\
(x,w) \in (F \bullet G) \bullet H &\overset{\text{Def}}{\iff} \exists z \in Z : x\,(F \bullet G)\,z \wedge z\,H\,w \\
&\overset{\text{Def}}{\iff} \exists z \in Z : \big[\exists y \in Y : x\,F\,y \wedge y\,G\,z\big] \wedge z\,H\,w \\
&\overset{\text{Dst}}{\iff} \exists z \in Z\ \exists y \in Y : x\,F\,y \wedge y\,G\,z \wedge z\,H\,w
\end{aligned}
$$

Von Relationen zu Funktionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition G2E: von Relation zu Funktion

(0) Die Relation $f = (X, F, Y)$ mit Graph $F \subseteq X \times Y$ nennen wir

linkstotal, falls: $\forall x \in X \ \exists y \in Y : (x, y) \in F$,
rechtstotal, falls: $\forall y \in Y \ \exists x \in X : (x, y) \in F$,
rechtseindeutig: $\forall x \in X \ \forall y, y' \in Y : (x, y) \in F \wedge (x, y') \in F \Rightarrow y = y'$,
linkseindeutig: $\forall y \in Y \ \forall x, x' \in X : (x, y) \in F \wedge (x', y) \in F \Rightarrow x = x'$.

(1) Die Relation $f = (X, F, Y)$ heißt **Funktion** / **Abbildung** / **Zuordnung**, falls sie linkstotal und rechtseindeutig ist.

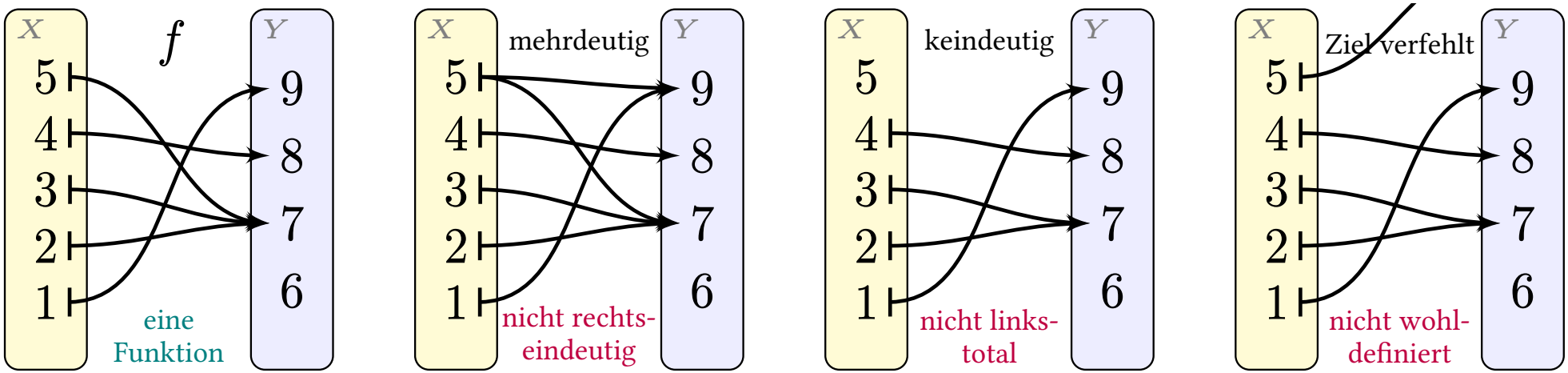
$$\textbf{Fun}(f), \ \text{kurz} \ f : X \to Y \quad :\Longleftrightarrow \quad \forall x \in X \ \exists! y \in Y : (x, y) \in F$$

Zu jedem Paar $(x, y) \in F$ sagen wir dann, f ordnet dem Startelement $x \in X$ das Zielelement $y \in Y$ zu, geschrieben $f : x \mapsto y$, kurz $f(x) = y$.

(2) Die Abbildung $f : X \to Y$ heißt **injektiv**, falls sie linkseindeutig ist, **surjektiv**, falls sie rechtstotal ist, und **bijektiv**, falls sie beides erfüllt:

$$f : X \to Y \text{ bijektiv} \quad :\Longleftrightarrow \quad \forall y \in Y \ \exists! x \in X : f(x) = y$$

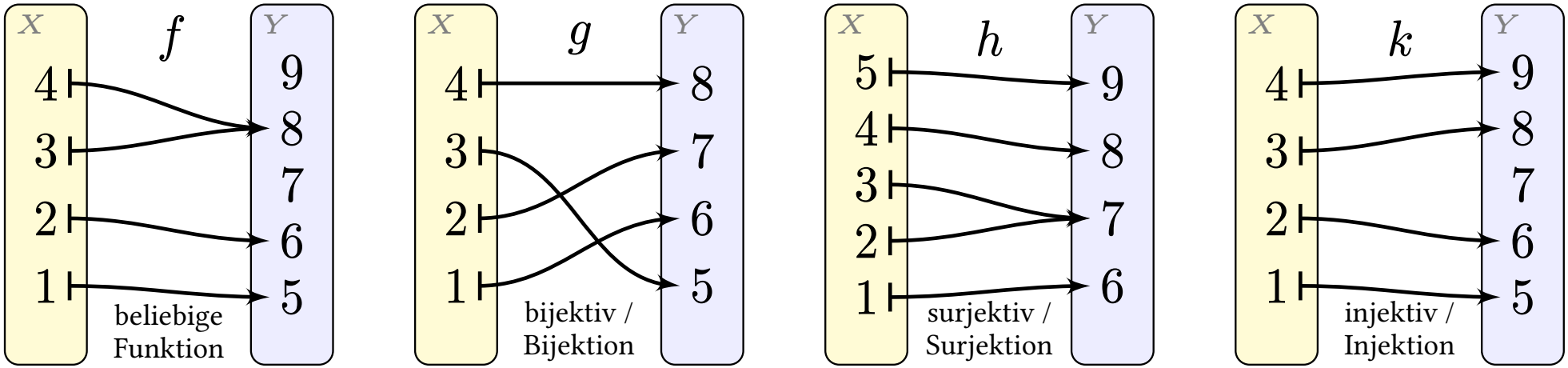
Welche Relationen sind Funktionen, welche nicht?



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Eigenschaften von Funktionen: injektiv, surjektiv, bijektiv



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Funktionen: Komposition und Umkehrung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz G2F: Komposition und Umkehrung von Funktionen

(1) Seien $f = (X, F, Y)$ und $g = (Y, G, Z)$ Funktionen, kurz $f : X \to Y$ und $g : Y \to Z$. Dann ist auch ihre Komposition $k = (X, K, Z)$ eine Funktion, kurz $k : X \to Z$, mit $k(x) = g(f(x))$ für jedes $x \in X$.

(2) Die Umkehrrelation f^{T} ist eine Funktion gdw f bijektiv ist.

Was bedeutet das Signalwort „wohldefiniert“?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(1) Wir definieren die Funktion $\sqrt{} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto y$ durch $y^2 = x$. Dies ist wohldefiniert, also tatsächlich eine Funktion wie behauptet, denn zu jedem $x \in \mathbb{R}_{\geq 0}$ existiert genau ein $y \in \mathbb{R}_{\geq 0}$ mit $y^2 = x$. ☺

(0) Die Quadratfunktion $q : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto x^2$ ist injektiv (da streng monoton) und surjektiv (dank Zwischenwertsatz), also ist q bijektiv. Ihre Umkehrfunktion nennen wir $\sqrt{} := q^{\top} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto \sqrt{x}$. ☺

Das Gegenteil von „wohldefiniert“ ist „übeldefiniert“.

- „Wir definieren die Funktion $\sqrt{} : \mathbb{R} \to \mathbb{R} : x \mapsto y$ durch $y^2 = x$.“
- „Wir definieren $\sqrt{} : \mathbb{Q}_{\geq 0} \to \mathbb{Q}_{\geq 0} : x \mapsto y$ durch $y^2 = x$.“
- „Wir definieren $\sqrt{} : \mathbb{C} \to \mathbb{C} : x \mapsto y$ durch $y^2 = x$.“

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Bildmenge unter einer Abbildung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition G2H: Bildmenge einer Funktion $f : X \to Y$

Zu jeder Teilmenge $A \subseteq X$ definieren wir ihre **Bildmenge unter f** durch

$$f(A) = f_*(A) := \{\, f(x) \mid x \in A \,\}.$$

Die **Bildmenge** der Funktion f ist $\operatorname{Im}(f) := f_*(X) \subseteq Y$.

Beispiele:

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 $g_*(\mathbb{R}) = \mathbb{R}$.

Urbildmenge unter einer Abbildung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition G21: Urbildmenge einer Funktion $f : X \to Y$

Zu jeder Teilmenge $B \subseteq Y$ definieren wir ihre **Urbildmenge unter f** durch

$$f^{-1}(B) = f^*(B) := \{x \in X \mid f(x) \in B\}.$$

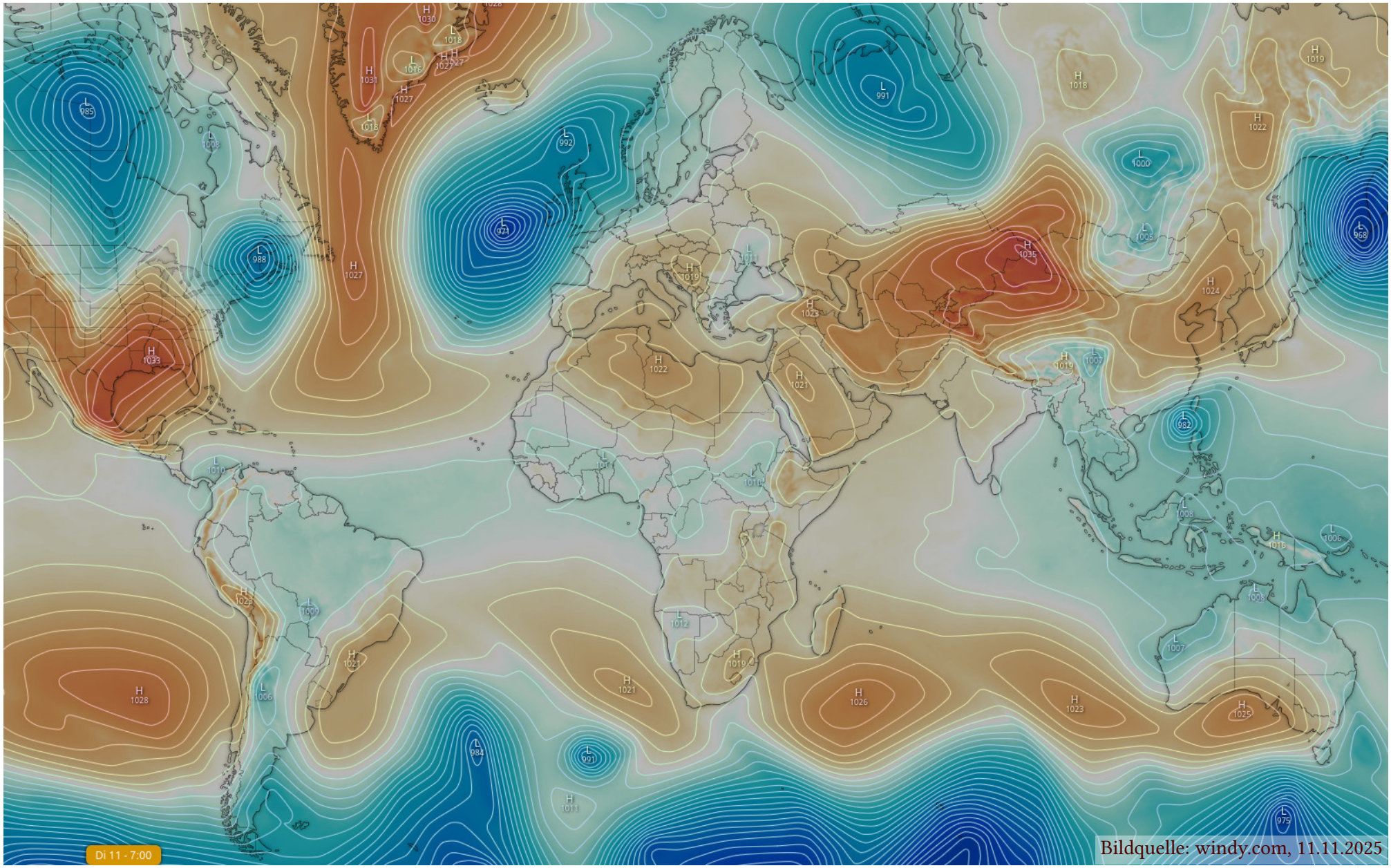
Die **Faser** über dem Zielpunkt $y \in Y$ ist die Urbildmenge $f^{-1}(\{y\})$.

Beispiele:

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 $g^{-1}(\{2\}) = \{\sqrt[3]{2}\}$.

Beispiel zu Urbildmengen: Isobaren, Tiefdruck, Hochdruck



Bildquelle: windy.com, 11.11.2025

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 $f^{-1}(\mathbb{R}_{\geq b})$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel zu Urbildmengen: Lösung linearer Gleichungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\boxed{Ax = y}$$

$$\text{Lös}(A, y) \;:=\; \{\, x \in \mathbb{K}^n \mid Ax = y \,\} \;=\; f_A^{-1}(\{y\}) \qquad \text{Urbild!}$$

$$\text{Lös}(A, y) \;\overset{\text{D2F}}{=}\; \{\, v_0 + v_1\lambda_1 + \ldots + v_d\lambda_d \mid \lambda \in \mathbb{K}^d \,\}^{!} \qquad \text{Bild!}$$

Abbildungen und Mengenoperationen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz G2J: Ur/Bilder und Mengenoperationen

Sei $f : X \to Y$. Für alle $A, A', A_i \subseteq X$ und $B, B', B_i \subseteq Y$ mit $i \in I \neq \emptyset$ gilt:

$f^* : \mathfrak{P}(Y) \to \mathfrak{P}(X)$ Urbild	$f_* : \mathfrak{P}(X) \to \mathfrak{P}(Y)$ Bild
$B \mapsto f^{-1}(B) := \{x \in X \mid f(x) \in B\}$,	$A \mapsto f(A) := \{f(x) \mid x \in A\}$,
$B \subseteq B' \implies f^{-1}(B) \subseteq f^{-1}(B')$,	$A \subseteq A' \implies f(A) \subseteq f(A')$,
$f^{-1}(\emptyset) = \emptyset$, $f^{-1}(Y) = X$,	$f(\emptyset) = \emptyset$, $f(X) \ddot{\subseteq} Y$,
$f^{-1}(\bigcup_{i\in I} B_i) = \bigcup_{i\in I} f^{-1}(B_i)$,	$f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$,
$f^{-1}(\bigcap_{i\in I} B_i) = \bigcap_{i\in I} f^{-1}(B_i)$,	$f(\bigcap_{i\in I} A_i) \dot{\subseteq} \bigcap_{i\in I} f(A_i)$,

Für jede injektive / surjektive Abbildung f gilt statt „$\dot{\subseteq}$“ / „$\ddot{\subseteq}$“ stärker „$=$“.

Abbildungen und Mengenoperationen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: Ich führe dies für Schnittmengen exemplarisch aus.

$$\boxed{f^{-1}\left(\bigcap_{i\in I} B_i\right) \;=\; \bigcap_{i\in I} f^{-1}(B_i)}$$

$$x \in f^{-1}\left(\bigcap_{i\in I} B_i\right) \underset{\text{G259}}{\overset{\text{Def}}{\Longleftrightarrow}} f(x) \in \bigcap_{i\in I} B_i \underset{\text{G141}}{\overset{\text{Def}}{\Longleftrightarrow}} \bigwedge_{i\in I} f(x) \in B_i$$

$$\underset{\text{G259}}{\overset{\text{Def}}{\Longleftrightarrow}} \bigwedge_{i\in I} x \in f^{-1}(B_i) \underset{\text{G141}}{\overset{\text{Def}}{\Longleftrightarrow}} x \in \bigcap_{i\in I} f^{-1}(B_i)$$

$$\boxed{f\left(\bigcap_{i\in I} A_i\right) \;\dot{\subseteq}\; \bigcap_{i\in I} f(A_i)}$$

„$\subseteq$“: Sei $y \in f(\bigcap_{i\in I} A_i)$. 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 irgendein $x_i \in A_i$. Da f injektiv ist, sind alle x_i gleich. Da $I \neq \emptyset$, können wir ein $j \in I$ wählen und $x := x_j$ setzen. Für alle $i \in I$ gilt $x = x_i \in A_i$, also $x \in \bigcap_{i\in I} A_i$ und somit $y = f(x) \in f(\bigcap_{i\in I} A_i)$.

Die Menge $\mathrm{Fun}(X, Y)$ aller Funktionen von X nach Y

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die **Menge aller Abbildungen von X nach Y** bezeichnen wir mit

$$\{\, f = (X, F, Y) \mid F \subseteq X \times Y \text{ linkstotal und rechtseindeutig} \,\}$$
$$= \{\, f : X \to Y \} =: Y^X = \mathrm{Fun}(X, Y) = \mathrm{Abb}(X, Y) = \mathrm{Map}(X, Y)$$

Einschränkung von Relationen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $f = (X, F, Y)$ eine Relation sowie $A \subseteq X$ und $B \subseteq Y$ Teilmengen.
Dies definiert die **Einschränkung in Startmenge und Zielmenge**

$$f|_A^B := (A, E, B) \qquad \text{mit} \qquad E := F \cap (A \times B)$$

Einschränkung von Abbildungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $f : X \to Y$ eine Funktion sowie $A \subseteq X$ und $B \subseteq Y$ Teilmengen.

$$\begin{tikzcd}
X \arrow[r, "f", "x \mapsto f(x)"'] & Y \\
A \arrow[u, hook, "\iota_A^X"] \arrow[r, dashed, "f|_A^B"] & B \arrow[u, hook, "\iota_B^Y"']
\end{tikzcd}$$

Satz G3F: Einschränkung $f|_A^B$ einer Funktion $f : X \to Y$

Genau dann ist $f|_A^B$ eine Funktion, wenn $f(A) \subseteq B$ gilt. Dann erhalten wir

$$f|_A^B : A \to B : x \mapsto f(x).$$

Beispiel zur Einschränkung von Abbildungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Wir betrachten die reelle Quadratfunktion

$$f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2.$$

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:

☹ $\cancel{f|^{[0,5]} : \mathbb{R} \to [0, 5] : x \mapsto x^2}$ ☹

Die Relation $f|^{[0,5]}$ ist nicht mehr linkstotal! Hingegen gilt

$$f([0, 2]) = [0, 4] \subseteq [0, 5],$$

☺ $h = f|^{[0,5]}_{[0,2]} : [0, 2] \to [0, 5] : x \mapsto x^2.$ ☺

Beispiel zur Einschränkung von Verknüpfungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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:

☹ $$\cancel{\mu|^{\mathbb{Z}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Z} : (x, y) \mapsto x \cdot y}$$ ☹

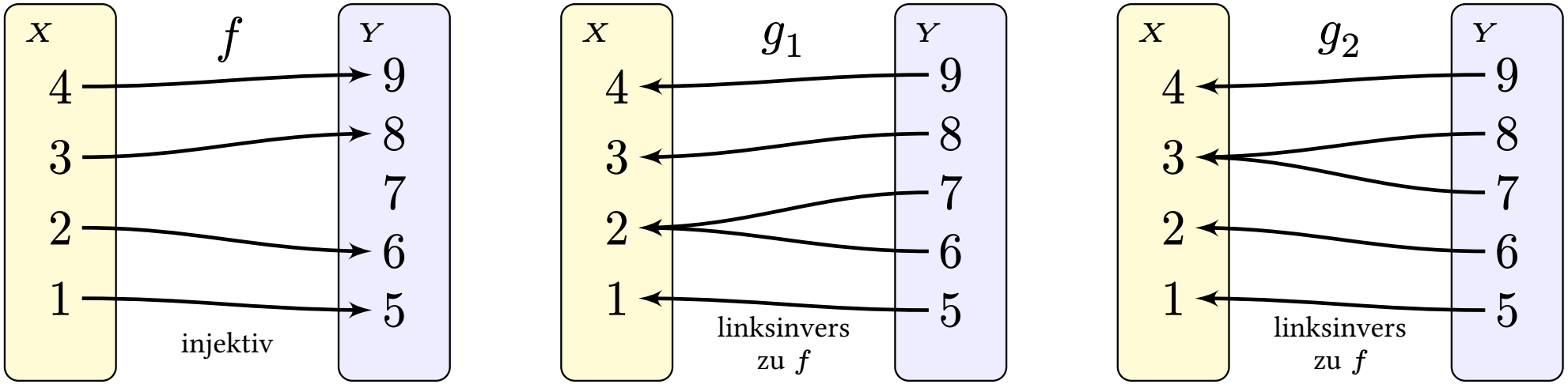
Die Relation $\mu|^{\mathbb{Z}}$ ist nicht mehr linkstotal! Hingegen gilt

$$\mu(\mathbb{Z} \times \mathbb{Z}) \subseteq \mathbb{Z},$$

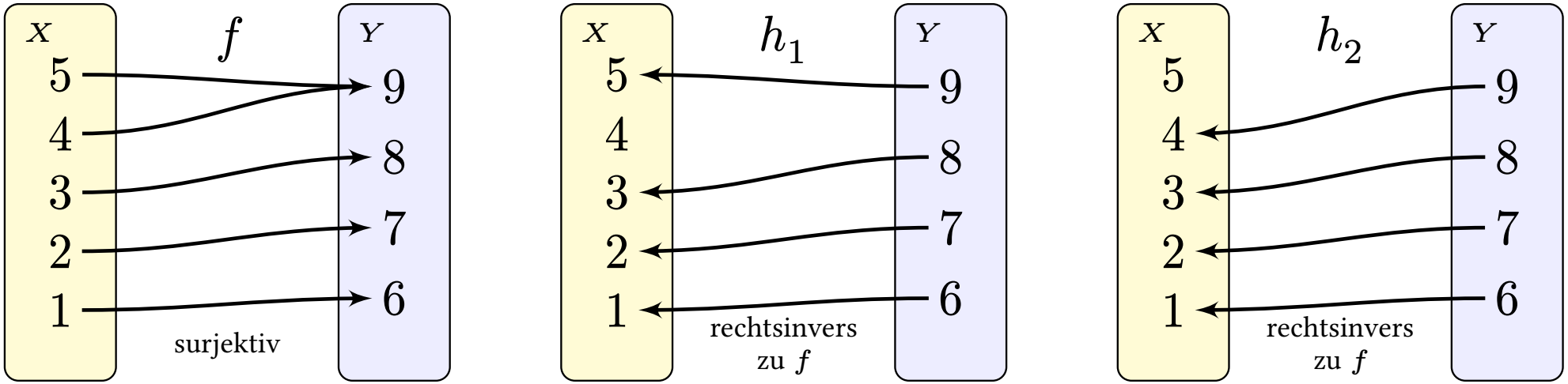
☺ $$\mu|^{\mathbb{Z}}_{\mathbb{Z}\times\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (x, y) \mapsto x \cdot y.$$ ☺

Einseitige Inverse

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 $f \circ h = \mathrm{id}_Y$:



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Invertierbarkeitskriterien für Abbildungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz G3G: Invertierbarkeitskriterien für $f : X \to Y$

(1) **Bijektivität**. Äquivalent sind:

(1a) $f : X \to Y$ ist **bbb**ijektiv: $\forall y \in Y\ \exists! x \in X : f(x) = y$.

(1b) f ist (**bbb**...) invertierbar: $\exists (g : Y \to X) : g \circ f = \mathrm{id}_X \wedge f \circ g = \mathrm{id}_Y$.

(2) **Injektivität**. Mit $X \neq \emptyset$ sind äquivalent:

(2a) $f : X \to Y$ ist **iii**njektiv: $\forall x, x' \in X : f(x) = f(x') \Rightarrow x = x'$

(2b) f ist **lii**inksinvertierbar: $\exists (g : Y \to X) : g \circ f = \mathrm{id}_X$.

(3) **Surjektivität**. Mit AC sind äquivalent:

(3a) $f : X \to Y$ ist **surrr**jektiv: $\forall y \in Y\ \exists x \in X : f(x) = y$.

(3b) f ist **rrr**echtsinvertierbar: $\exists (g : Y \to X) : f \circ g = \mathrm{id}_Y$.

Injektiv $\Leftrightarrow$ linksinvertierbar

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(2) f injektiv $\Leftrightarrow$ f linksinvertierbar.

„$\Leftarrow$“: Sei $g \circ f = \mathrm{id}_X$. Für alle $x, x' \in X$ folgt die Implikation

$$f(x) = f(x') \implies g(f(x)) = g(f(x')) \implies x = x'.$$

„$\Rightarrow$“: Wir wählen $x_0 \in X$ und konstruieren $g : Y \to X$:

0 Für $y \in Y \setminus \mathrm{Im}(f)$ setzen wir $g(y) = x_0$.

1 Für $y \in \mathrm{Im}(f)$ gilt $f^{-1}(\{y\}) = \{x\}$ für ein $x \in X$. Wir setzen $g(y) = x$. Für jedes Element $x \in X$ gilt dann $g(f(x)) = g(y) = x$, also $g \circ f = \mathrm{id}_X$.

Surjektiv $\Leftrightarrow$ rechtsinvertierbar

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(3) f surjektiv $\Leftrightarrow$ f rechtsinvertierbar.

„$\Leftarrow$“: Sei $f \circ g = \mathrm{id}_Y$. Zu jedem $y \in Y$ und $x = g(y)$ gilt dann:

$$f(x) = f(g(y)) = y$$

„$\Rightarrow$“: Wir konstruieren eine Rechtsinverse $g : Y \to X$ wie folgt.
Zu jedem $y \in Y$ gilt $f^{-1}(\{y\}) \neq \emptyset$. Wir wählen irgendein $x \in f^{-1}(\{y\})$ und setzen $g(y) = x$. Damit gilt $f(g(y)) = f(x) = y$, also $f \circ g = \mathrm{id}_Y$.

Bijektiv $\Leftrightarrow$ invertierbar

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(1) f bijektiv $\Leftrightarrow$ f invertierbar.

„$\Leftarrow$“: Dies folgt aus „(2a) $\Leftarrow$ (2b)“ und „(3a) $\Leftarrow$ (3b)“.

„$\Rightarrow$“: Ist f bijektiv, so ist $g = f^{\top}$ eine Funktion und invers zu f. $\boxed{\text{QED}}$

Bijektionen und Retrakte als Abbildungspaare

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition G3H: Retrakt und Bijektion als Abbildungspaar

(1) Ein **Retrakt** $(i, r) : X \leftrightarrows Y$, genauer ein **Retraktionspaar**, besteht aus Abbildungen $i : X \to Y$ und $r : Y \to X$ mit $r \circ i = \mathrm{id}_X$.

(2) 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 $f \circ g = \mathrm{id}_Y$.

(3) 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

$$(\exp, \ln) : \mathbb{R} \cong \mathbb{R}_{>0} \qquad \text{dank} \quad \ln(\mathrm{e}^x) = x, \quad \mathrm{e}^{\ln y} = y$$

$$(f, g) : \mathbb{R} \rightleftarrows \mathbb{R}_{\geq 0} \qquad \text{mit} \quad f(x) = x^2, \quad g(y) = \sqrt{y}$$

$$(h, k) : \mathbb{R}_{\geq 0} \cong \mathbb{R}_{\geq 0} \qquad \text{mit} \quad h(x) = x^2, \quad k(y) = \sqrt{y}$$

$$(\mathrm{id}_{\mathbb{R}}, \mathrm{id}_{\mathbb{R}}) : \mathbb{R} \cong \mathbb{R} \qquad \text{mit} \quad \mathrm{id}_{\mathbb{R}}(x) = x$$

$$(n, n) : \mathbb{R} \cong \mathbb{R} \qquad \text{mit} \quad n(x) = -x$$

$$({}^{\mathsf{T}}, {}^{\mathsf{T}}) : \mathbb{K}^{m \times n} \cong \mathbb{K}^{n \times m} \qquad \text{mit} \quad A \leftrightarrow A^{\mathsf{T}}$$

$$({}^{\mathsf{T}}, {}^{\mathsf{T}}) : \mathrm{Rel}(X, Y) \cong \mathrm{Rel}(Y, X) \qquad \text{mit} \quad f \leftrightarrow f^{\mathsf{T}}$$

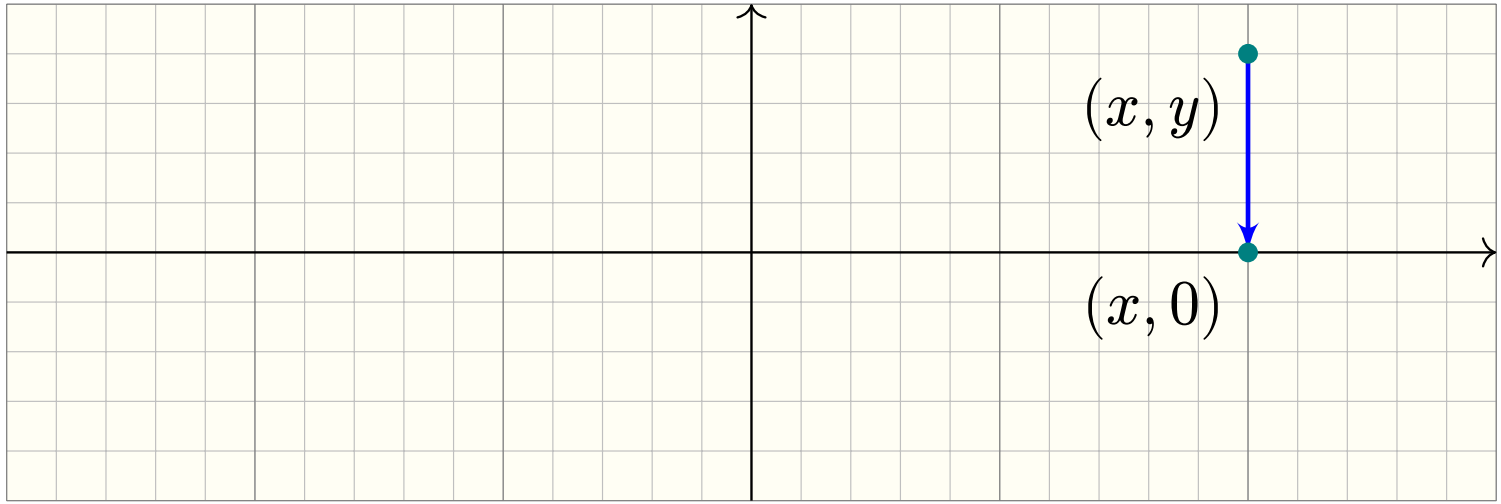
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Anwendung: Einbettung und Projektion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



$$\iota = \iota_1 \,:\, \mathbb{R} \hookrightarrow \mathbb{R}^2 \,:\, x \mapsto (x, 0)$$

$$\pi = \mathrm{pr}_1 \,:\, \mathbb{R}^2 \twoheadrightarrow \mathbb{R} \,:\, (x, y) \mapsto x$$

$$(\iota, \pi) \,:\, \mathbb{R} \leftrightarrows \mathbb{R}^2.$$

Anwendung: Bijektion zwischen $\mathfrak{P}(X)$ und 2^X

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Konstruieren Sie eine Bijektion $\mathfrak{P}(X) \cong 2^X = \mathrm{Fun}(X, \{0,1\})$.

Die **Indikatorfunktion** einer Teilmenge $A \subseteq X$ zeigt die Elemente an:

$$\mathbf{1}_A : X \to \{0,1\} : x \mapsto [x \in A] := \begin{cases} 1 & \text{falls } x \in A, \\ 0 & \text{falls } x \notin A. \end{cases}$$

Die **Trägermenge** von $f : X \to Y \ni 0$ zeigt, wo f nicht verschwindet:

$$\mathrm{supp}(f) := \{ x \in X \mid f(x) \neq 0 \}$$

Für jede Teilmenge $A \subseteq X$ finden wir $A \mapsto \mathbf{1}_A \mapsto \mathrm{supp}(\mathbf{1}_A) = A$.
Für jede Funktion $f : X \to \{0,1\}$ gilt $f \mapsto A = \mathrm{supp}(f) \mapsto \mathbf{1}_A \overset{!}{=} f$.

Satz G31: Bijektion zwischen Teilmengen und Indikatorfunktionen

$$(\mathbf{1}, \mathrm{supp}) : \mathfrak{P}(X) \cong 2^X = \mathrm{Fun}(X, \{0,1\})$$

Kartesische Produkte: allgemeine Konstruktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\mathrm{Fun}(I, X) = \{ x : I \to X : i \mapsto x_i \} = X^I =: \prod_{i \in I} X$$

Definition G3κ: kartesisches Produkt, allgemein

Gegeben sei eine Familie $(X_i)_{i \in I}$ von Mengen X_i.
Wir definieren ihr **kartesisches Produkt** als die Menge

$$\begin{aligned} P = \prod_{i \in I} X_i \;&:=\; \{ x = (x_i)_{i \in I} \mid \forall i \in I : x_i \in X_i \} \\ &= \{ x : I \to \bigcup_{i \in I} X_i : i \mapsto x_i \mid \forall i \in I : x_i \in X_i \}. \end{aligned}$$

Dazu gehören die **kanonischen Projektionen** $p_i = \mathrm{pr}_i : P \to X_i : x \mapsto x_i$.
Jede Funktion $f : Y \to P$ definiert somit $f_i = p_i \circ f : Y \to X_i$ für $i \in I$.

Kartesische Produkte: universelle Eigenschaft

$$\begin{tikzcd} Y \arrow[r, dashed, "\exists! f"] \arrow[dr, "f_i"'] & P \arrow[d, "p_i"] \\ & X_i \end{tikzcd}$$

Satz G3L: UAE, universelle Abbildungseigenschaft des Produkts

Zu jeder Familie $(f_i : Y \to X_i)_{i \in I}$ von Funktionen existiert genau eine Funktion $f : Y \to P$ mit $p_i \circ f = f_i$ für alle $i \in I$, nämlich $f(y) = (f_i(y))_{i \in I}$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Disjunkte Summen: allgemeine Konstruktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$X = \bigsqcup_{i\in I} X_i \quad \text{bedeutet} \quad X = \bigcup_{i\in I} X_i \text{ und } X_i \cap X_j = \emptyset \text{ für alle } i \neq j.$$

Definition G3M: 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** als die Menge

$$S = \coprod_{i\in I} X_i \;:=\; \bigsqcup_{i\in I} \{i\} \times X_i.$$

Dazu gehören die **kanonischen Injektionen** $\iota_i : X_i \hookrightarrow S : x \mapsto (i, x)$.
Jede Funktion $f : S \to Y$ definiert $f_i = f \circ \iota_i : X_i \to Y$ für $i \in I$.

Disjunkte Summen: universelle Eigenschaft

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd} X_i \arrow[d, hook, "\iota_i"'] \arrow[dr, "f_i"] & \\ S \arrow[r, dashed, "\exists! f"'] & Y \end{tikzcd}$$

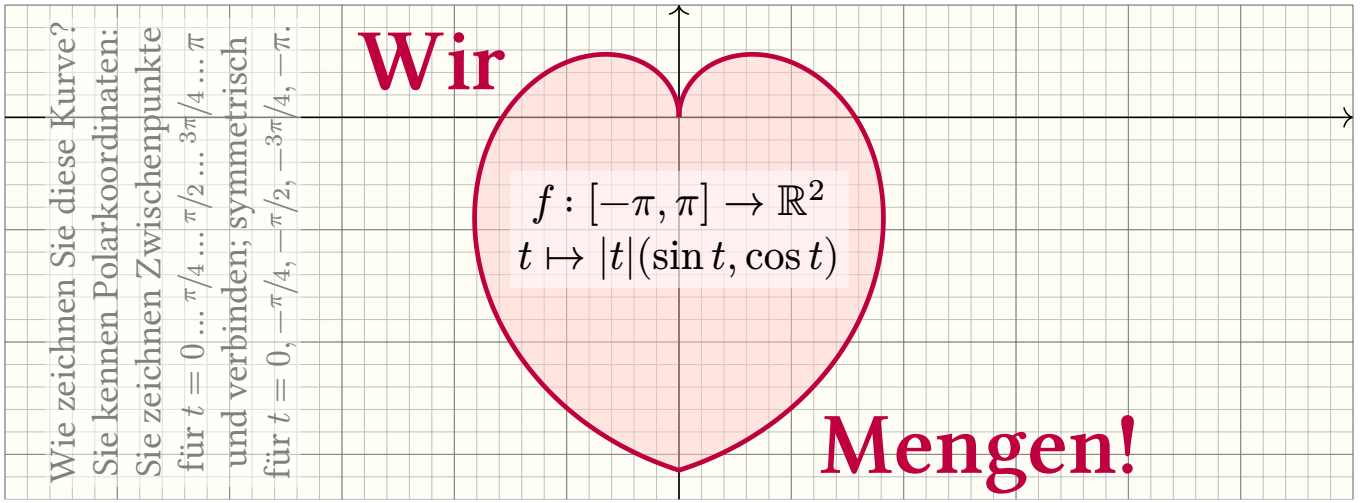
Satz G3N: UAE, universelle Abbildungseigenschaft der Summe

Zu jeder Familie $(f_i : X_i \to Y)_{i \in I}$ von Funktionen existiert genau eine Funktion $f : S \to Y$ mit $f \circ \iota_i = f_i$ für alle $i \in I$, nämlich $f(i, x_i) = f_i(x_i)$.

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel G

Bonusmaterial



Everything is going to be fine in the end.
If it's not fine it's not the end.

Oscar Wilde (1854–1900) fälschlich zugeschrieben

Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels G

5 Spickzettel: Logik und Mengenlehre

6 Zermelo–Fraenkel–Axiome und Modelle

7 Auswahlaxiom (AC) und das ausgeschlossene Dritte (LEM)

Dies ist nur die Saalversion ohne Erläuterungen.

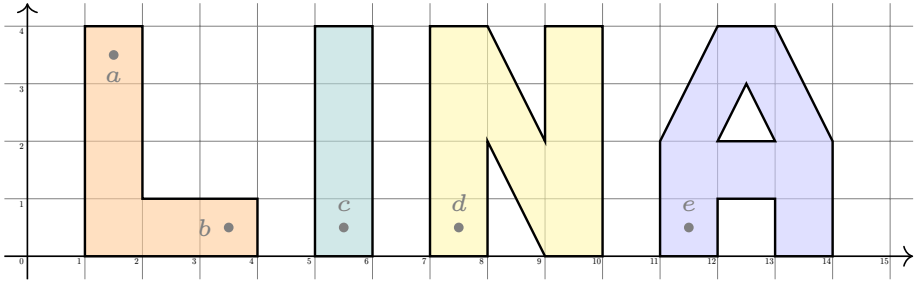
Ausführliche Erläuterungen bietet die Vollversion.

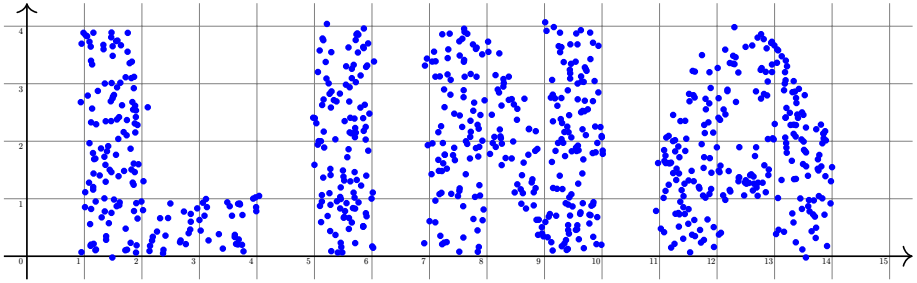
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel H

Zählen und Kombinatorik, Äquivalenzrelationen und Quotienten





Wer hohe Türme bauen will, muss lange beim Fundament verweilen.
Anton Bruckner (1824–1896)

Inhalt dieses Kapitels H

1 Endliche Mengen und ihre Elementezahl

2 Strukturiertes Abzählen

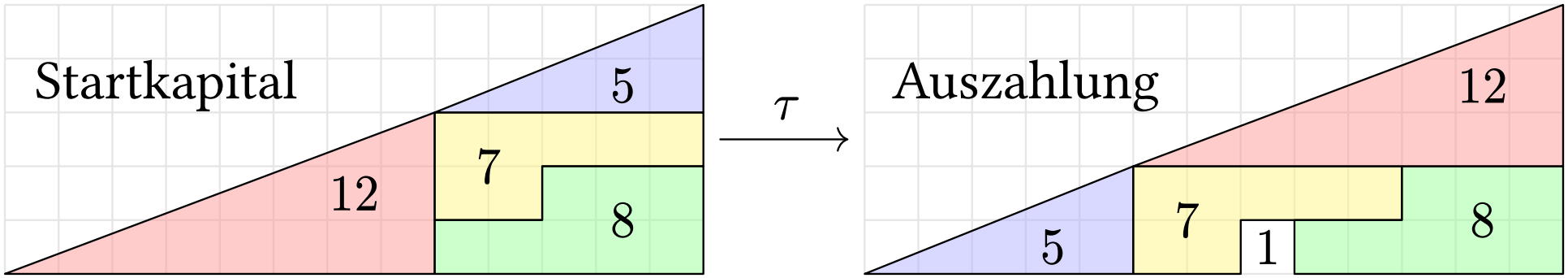
3 Äquivalenzrelationen und Quotienten

4 Übungsaufgaben und Anwendungsbeispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Genie oder Betrug: Geld aus dem Nichts?



Beispiel H0A: Geld aus dem Nichts?

„Jeder Investor gewinnt, garantiert.“ Gelingt folgender Businessplan?

Einzahlen	$X_1 \sqcup \cdots \sqcup X_n = X$	„Investieren Sie jetzt!“
Transformieren	$\tau : X \xrightarrow{\sim} Y$	„Geheime Bijektion!“
Auszahlen	$Y = Y_1 \sqcup \cdots \sqcup Y_n$	„Jeder wird gewinnen!“

„Für jeden Investor $i = 1, \dots, n$ garantieren wir $\sharp Y_i > \sharp X_i$.“ Das ist Betrug!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Transformationen / Selbstabbildungen einer Menge X

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition H1A: das Transformationsmonoid

$$\mathrm{T}_X := \{\, f : X \to X \,\}$$

Die Komposition definiert das Monoid $(\mathrm{T}_X, \bullet, \mathrm{id}_X)$ bzw. $(\mathrm{T}_X, \circ, \mathrm{id}_X)$.

$$f = \begin{bmatrix} x_1 & \dots & x_n \\ y_1 & \dots & y_n \end{bmatrix} \quad \text{bedeutet} \quad \begin{cases} X = \{x_1, \dots, x_n\}^! \text{ und} \\ f : X \to X : x_k \mapsto y_k. \end{cases}$$

$$g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 3 & 4 \end{bmatrix} \bullet \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 3 & 2 & 4 \end{bmatrix}$$

$$h = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 3 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 2 & 4 \end{bmatrix}$$

Transformationen / Selbstabbildungen einer Menge X

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$e = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 3 & 4 \end{bmatrix}, \qquad f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

Aufgabe: (1) Wie erkennt man, ob $f : X \to X$ eine Bijektion ist?
Lösung: In der Zielzeile tritt jedes Element $x \in X$ genau einmal auf!

(2) Wie bestimmt man die Inverse $f^{-1} : X \to X$?

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \quad \Longrightarrow \quad f^{-1} = \begin{bmatrix} 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix}$$

(3) Ist $g : \mathbb{Z}_7 \to \mathbb{Z}_7 : x \mapsto x^5$ bijektiv? (4) Bestimmen Sie $g^{-1} : x \mapsto \sqrt[5]{x}$?

$$g = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 \end{bmatrix} \quad \Longrightarrow \quad g^{-1} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 \end{bmatrix}$$

Permutationen und die symmetrische Gruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition H1B: die symmetrische Gruppe S_X

Eine **Permutation** der Menge X ist eine Selbstbijektion $\sigma : X \xrightarrow{\sim} X$.

$$\mathrm{S}_X = \mathrm{Sym}(X) := \{\sigma : X \xrightarrow{\sim} X\}$$

Die Komposition definiert die Gruppe $(\mathrm{S}_X, \bullet, \mathrm{id}_X)$ bzw. $(\mathrm{S}_X, \circ, \mathrm{id}_X)$.
Speziell für $X = \{1, \dots, n\}$ schreiben wir $\mathrm{S}_n := \mathrm{S}_X$.

Die Komposition auf S_X schreiben wir wahlweise rechts oder links:

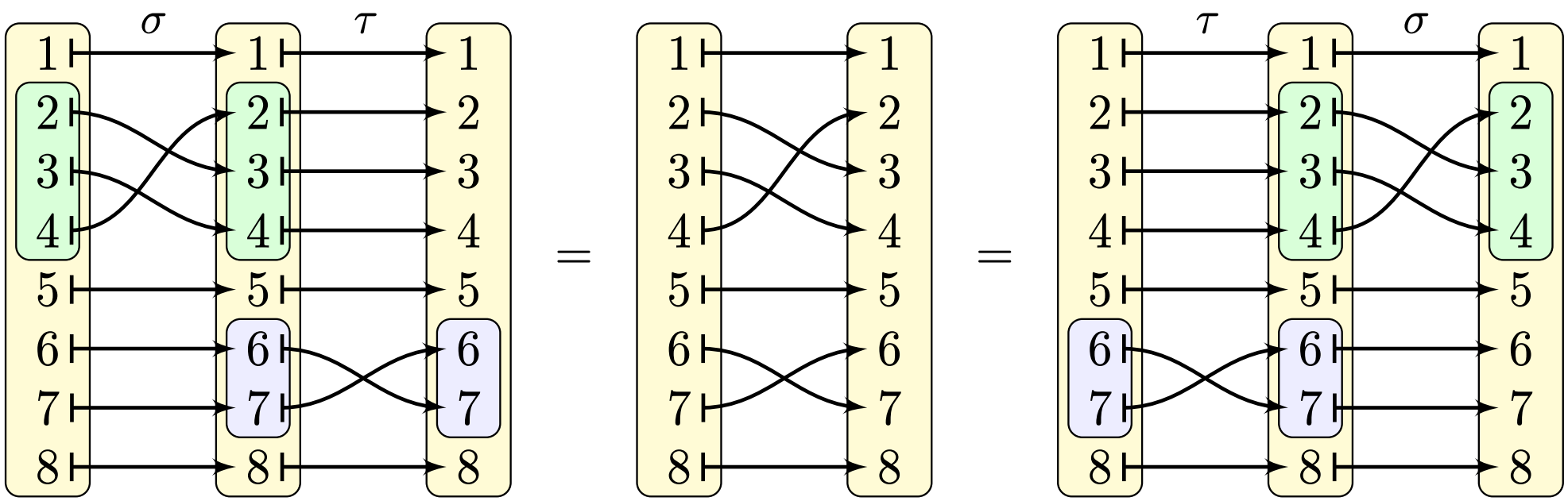
$$\delta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \bullet \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}$$

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

Fixpunktmenge und Träger einer Permutation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Sei $\sigma : X \to X$. Wir definieren

$$\begin{aligned} &\text{die Fixpunktmenge} && \operatorname{fix}(\sigma) &&:= \{\, x \in X \mid \sigma(x) = x \,\} \\ &\text{und den Träger} && \operatorname{supp}(\sigma) &&:= \{\, x \in X \mid \sigma(x) \neq x \,\}. \end{aligned}$$

Lemma H1c: Disjunkte Permutationen kommutieren.

(1) Permutationen $\sigma, \tau : X \xrightarrow{\sim} X$ mit disjunkten Trägern kommutieren.

Zykelschreibweise für Permutationen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Gegeben seien $\ell \geq 2$ verschiedene Elemente $x_1, x_2, \dots, x_\ell \in X$.

$$\sigma = \mathrm{Cyc}_X(x_1, x_2, \dots, x_\ell) : X \xrightarrow{\sim} X : x_1 \mapsto x_2 \mapsto \cdots \mapsto x_\ell \mapsto x_1$$

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 $\mathrm{Cyc}_X(a, b) : a \leftrightarrow b$ heißt **Transposition**.

Die Zykelzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Zerlegen Sie σ in disjunkte Zykel, ebenso σ^{-1} und σ^{2025}.

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 7 & 4 & 6 & 2 & 3 & 8 \end{bmatrix} = (1)\,(2,5,4,7)\,(6)\,(3,9,8)$$

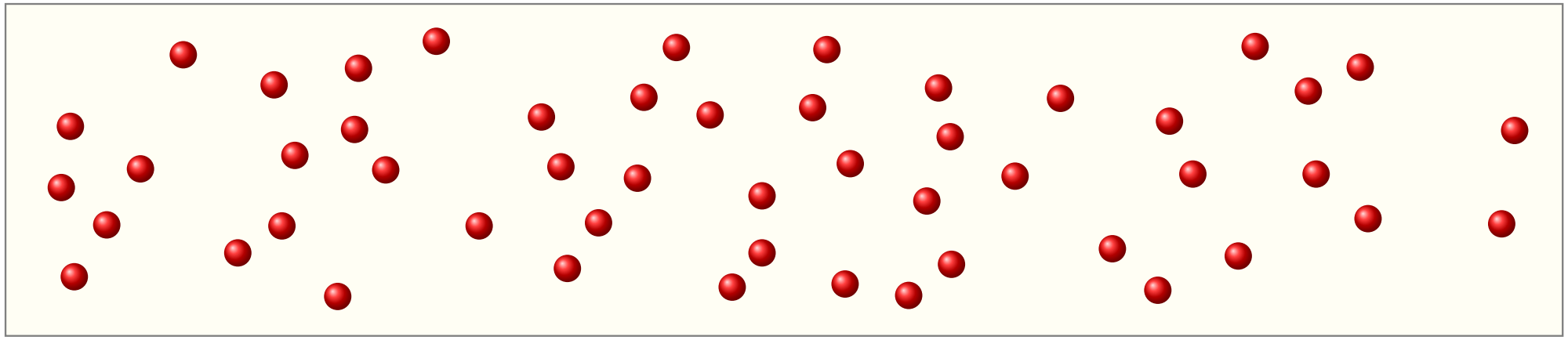
$$\sigma^{-1} = (8,9,3)(7,4,5,2) \overset{\text{H1c}}{=} (2,7,4,5)(3,8,9)$$

$$\sigma^{2025} \overset{\text{H1c}}{=} (2,5,4,7)^{2025}(3,9,8)^{2025} = (2,5,4,7)$$

Satz H1D: eindeutige Zykelzerlegung auf jeder endlichen Menge X

Jede Permutation $\sigma : X \xrightarrow{\sim} X$ zerlegt sich eindeutig in eine Menge $\{c_1, c_2, \dots, c_k\} \subseteq \mathrm{S}_X$ disjunkter Zykel mit $\sigma = c_1 \bullet c_2 \bullet \cdots \bullet c_k$.

Wie viele Elemente hat die vorgelegte Menge?



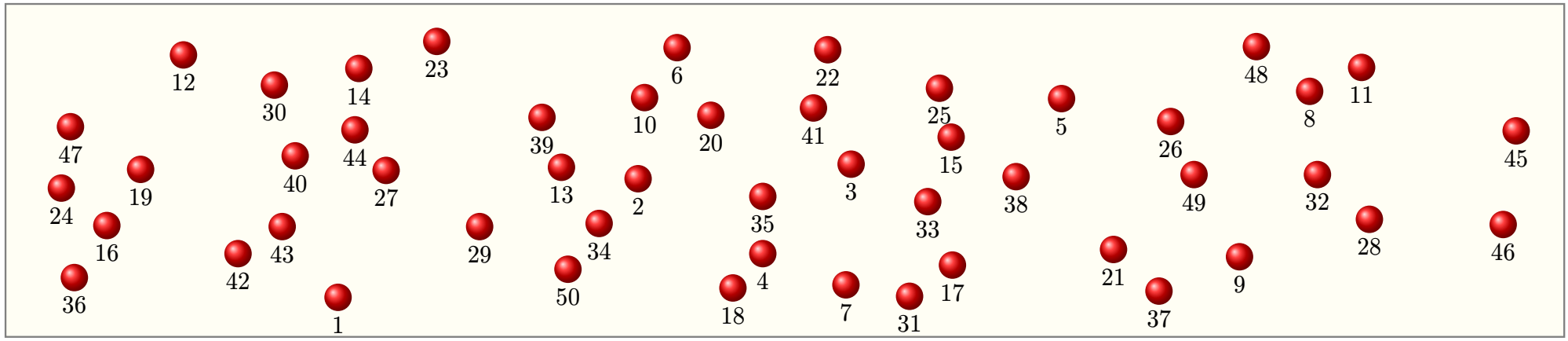
Definition H1E: die Anzahl der Elemente einer Menge

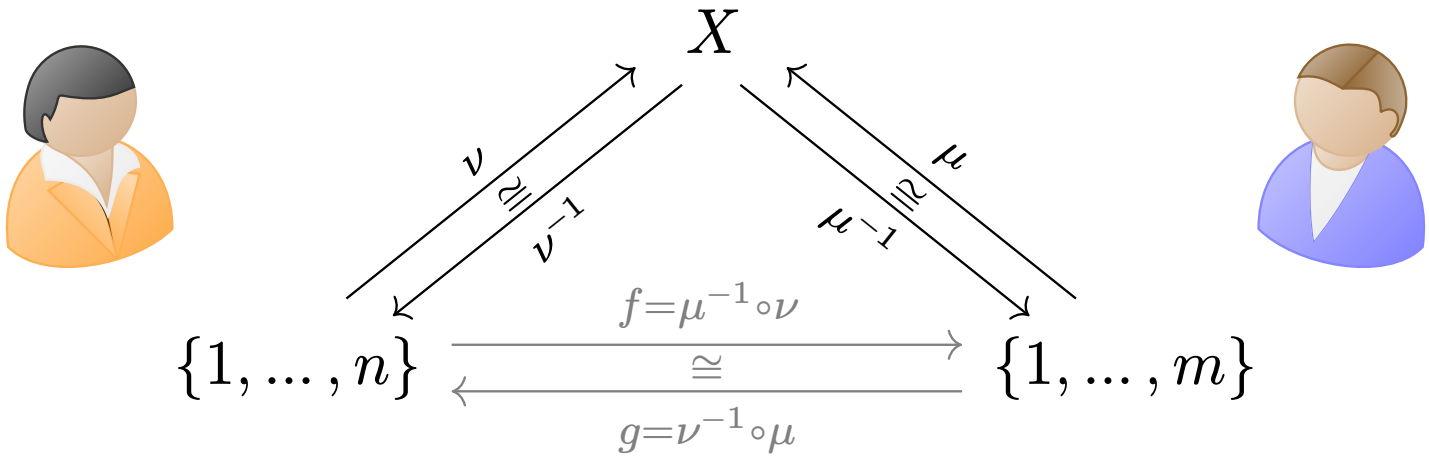
Sei $n \in \mathbb{N}$. Eine Menge X **enthält (genau) n Elemente**, kurz $\sharp X = n$, falls eine Bijektion $\nu : \{1, \dots, n\} \xrightarrow{\sim} X$ existiert .

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Ergibt doppeltes Abzählen dieselbe Elementezahl?





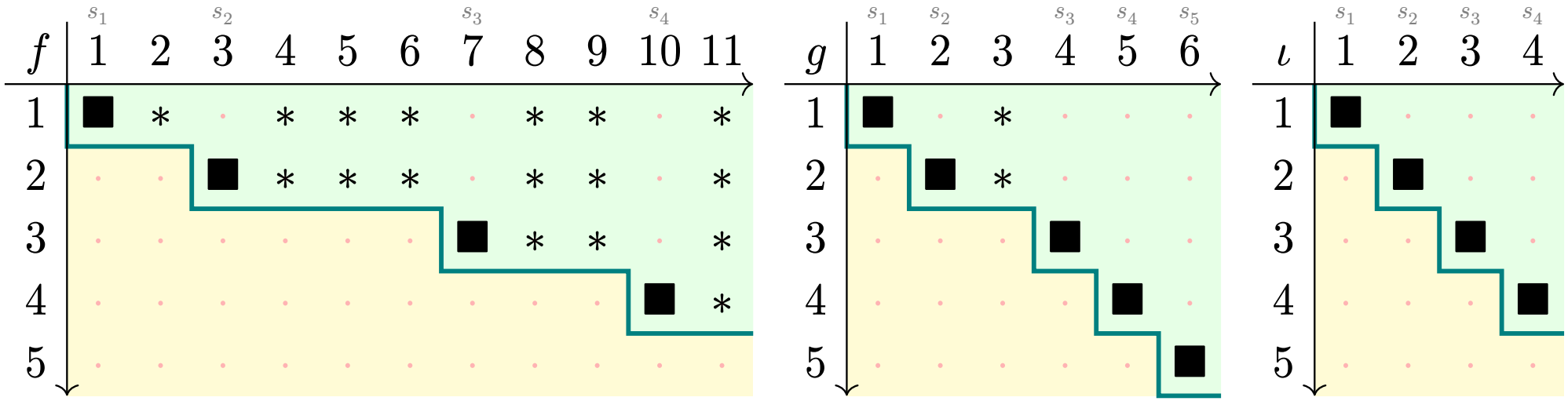
Wir hoffen: Ist $f : \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, m\}$ bijektiv, so gilt $n = m$.

Beispiel: Wie viele Elemente enthält $X = \{0, \{0\}, \{0, 1\}, \{1, 0, 1\}\}$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Abbildungen $f : \{1, \dots, n\} \to \{1, \dots, m\}$ in Stufenform



Die Abbildung $f : \{1, \dots, n\} \to \{1, \dots, m\}$ ist in **Stufenform**, falls gilt:
Wir haben $\mathrm{Im}(f) = \{1, \dots, r\}$ und Stufen $s_1 < \dots < s_r$ in $\{1, \dots, n\}$,
an jeder Stufe s_i gilt $f(s_i) = i$, und für alle $j < s_i$ gilt $f(j) < i$.

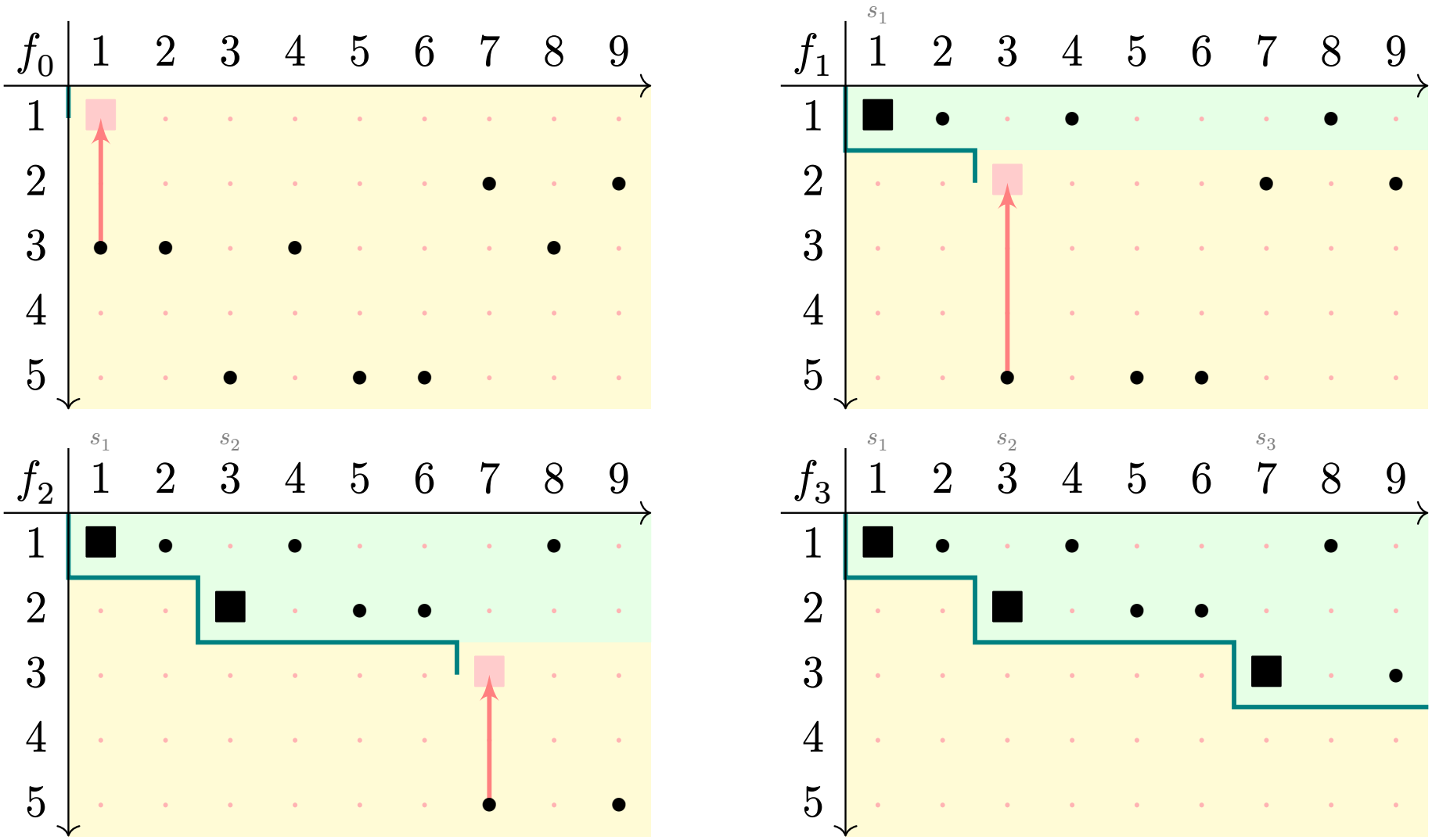
Insbesondere folgt $r \leq n$ und $r \leq m$.
(1) Genau dann ist f surjektiv, wenn $r = m \leq n$ gilt.
(2) Genau dann ist f injektiv, wenn $r = n \leq m$ gilt.
(3) Genau dann ist f bijektiv, wenn $r = n = m$ gilt.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sortieren zur Stufenform à la Gauß

Gauß–Verfahren: Bringen Sie $f : \{1, \dots, n\} \to \{1, \dots, m\}$ in Stufenform!



Hier ist $f_3 = \sigma \circ f_0$ in Stufenform, $\sigma = (3,5) \circ (2,5) \circ (1,3) = (1,5,2,3)$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sur/In/Bijektivität von $f : \{1, \dots, n\} \to \{1, \dots, m\}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H1G: Sur/In/Bijektivität von $f : \{1, \dots, n\} \to \{1, \dots, m\}$

Wir bringen f in Stufenform $f' = \sigma \circ f$ mit $\sigma \in \mathrm{S}_m$ und Rang r.
Genau dann ist f sur/in/bijektiv, wenn f' dies ist:

(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.

$$\begin{tikzcd}
\underline{n} \arrow[r, "f"'] & \underline{m} \arrow[d, "\sigma"'] \\
\underline{n} \arrow[u, "\mathrm{id}"] \arrow[r, "f'"'] & \underline{m}
\end{tikzcd}$$

Doppeltes Abzählen: Die Elementezahl ist wohldefiniert.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{tikzcd}
 & & X \arrow[dl, shift right, "\nu^{-1}"'] \arrow[dr, shift right, "\mu^{-1}"'] & & \\
\text{Count} & \{1,\dots,n\} \arrow[ur, shift right, "\nu"'] \arrow[rr, shift left, "f=\mu^{-1}\circ\nu"] \arrow[rr, phantom, "\cong"] & & \{1,\dots,m\} \arrow[ul, shift right, "\mu"'] \arrow[ll, shift left, "g=\nu^{-1}\circ\mu"] & \text{Recount}
\end{tikzcd}
$$

Korollar H1H: der Zählsatz

(1) Ist $f : \{1,\dots,n\} \twoheadrightarrow \{1,\dots,m\}$ surjektiv, so gilt $n \geq m$.
(2) Ist $f : \{1,\dots,n\} \hookrightarrow \{1,\dots,m\}$ injektiv, so gilt $n \leq m$.
(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.

Invarianz der Elementezahl und Dirichlets Schubfachprinzip

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H1ɟ: Invarianz der Elementezahl

Seien X und Y endliche Mengen und $f : X \to Y$ eine Abbildung.
Für den Rang $r = \sharp\,\mathrm{Im}(f)$ gilt $r \leq \sharp X$ und $r \leq \sharp Y$.

(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.

Für $\sharp X = \sharp Y$ folgt: f surjektiv $\Leftrightarrow$ f injektiv $\Leftrightarrow$ f bijektiv.

Als Spezialisierung erhalten wir insbesondere:
(1') Ist $f : X \twoheadrightarrow Y$ surjektiv, so gilt $\sharp X \geq \sharp Y$.
(2') Ist $f : X \hookrightarrow Y$ injektiv, so gilt $\sharp X \leq \sharp Y$.
(3') Ist $f : X \xrightarrow{\sim} Y$ bijektiv, so gilt $\sharp X = \sharp Y$.

$$\begin{tikzcd}
X \arrow[r, "f"'] \arrow[d, shift left, "\nu^{-1}"] & Y \arrow[d, shift left, "\mu^{-1}"] \\
\{1,\dots,n\} \arrow[r, "g"] \arrow[u, shift left, "\nu"] \arrow[u, phantom, "\cong"] & \{1,\dots,m\} \arrow[u, shift left, "\mu"] \arrow[u, phantom, "\cong"]
\end{tikzcd}$$

Korollar H1κ: Dirichlets Schubfachprinzip

Sei $f : X \to Y$ eine Abbildung. Gilt $\sharp X > \sharp Y$, so ist f nicht injektiv:
Es existieren also zwei Elemente $a \neq b$ in X mit $f(a) = f(b)$ in Y.

Illustration zu Dirichlets Schubfachprinzip

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel H1o: haargenau!

Gibt es aktuell in Stuttgart zwei Menschen, die genau dieselbe Anzahl von Haaren auf dem Kopf haben?

Ja! Menschen haben um 100 000 Kopfhaare, von 0 bis etwa 120 000, aber sicher weniger als 200 000. Stuttgart hat derzeit $N > 600\,000$ Einwohner. Wir nutzen H1κ für die Haarzahl $f : \{1, \dots, N\} \to \{0, \dots, 199\,999\}$.

Anwendung: Welche Transformationen sind Permutationen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$e = \begin{bmatrix} 1 & 2 & 3 & \dots & 8 \\ 2 & 2 & 1 & \dots & 3 \end{bmatrix}, \quad f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & 5 & 7 & 8 & 6 & 3 \end{bmatrix} \quad \in \mathrm{T}_8$$

1. Bijektivität: In der Zielzeile steht jedes Element $x \in X$ *genau* einmal.
2. Injektivität: ... *höchstens* einmal.
3. Surjektivität: ... *mindestens* einmal.

Jeder endliche Integritätsring ist ein Körper.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H1s: endliche Integritätsringe

Jeder endliche Integritätsring $(R, +, 0, \cdot, 1)$ ist ein Körper.

Beweis: Zu $a \in R \smallsetminus \{0\}$ 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 H1J.
Insbesondere existiert zur Gleichung $a \cdot x = 1$ eine Lösung $x \in R$. $\boxed{\text{QED}}$

Unendlich oft gleich?

Rufen Sie „Stopp!“, sobald Sie beweisen können, dass zwei der folgenden Zahlen an unendlich vielen Nachkommastellen übereinstimmen.

$$
\begin{aligned}
0 &= 0.\,00000\;00000\;00000\;00000\;00000\;00000\;00000\;00000\;00000\;00000\ldots\\
1/3 &= 0.\,33333\;33333\;33333\;33333\;33333\;33333\;33333\;33333\;33333\;33333\ldots\\
2/3 &= 0.\,66666\;66666\;66666\;66666\;66666\;66666\;66666\;66666\;66666\;66666\ldots\\
1/7 &= 0.\,14285\;71428\;57142\;85714\;28571\;42857\;14285\;71428\;57142\;85714\ldots\\
\sqrt{2} &= 1.\,41421\;35623\;73095\;04880\;16887\;24209\;69807\;85696\;71875\;37694\ldots\\
\sqrt{3} &= 1.\,73205\;08075\;68877\;29352\;74463\;41505\;87236\;69428\;05253\;81038\ldots\\
\sqrt{5} &= 2.\,23606\;79774\;99789\;69640\;91736\;68731\;27623\;54406\;18359\;61152\ldots\\
\ln 2 &= 0.\,69314\;71805\;59945\;30941\;72321\;21458\;17656\;80755\;00134\;36025\ldots\\
\mathrm{e} &= 2.\,71828\;18284\;59045\;23536\;02874\;71352\;66249\;77572\;47093\;69995\ldots\\
\pi &= 3.\,14159\;26535\;89793\;23846\;26433\;83279\;50288\;41971\;69399\;37510\ldots\\
\pi^2 &= 9.\,86960\;44010\;89358\;61883\;44909\;99876\;15113\;53136\;99407\;24079\ldots
\end{aligned}
$$

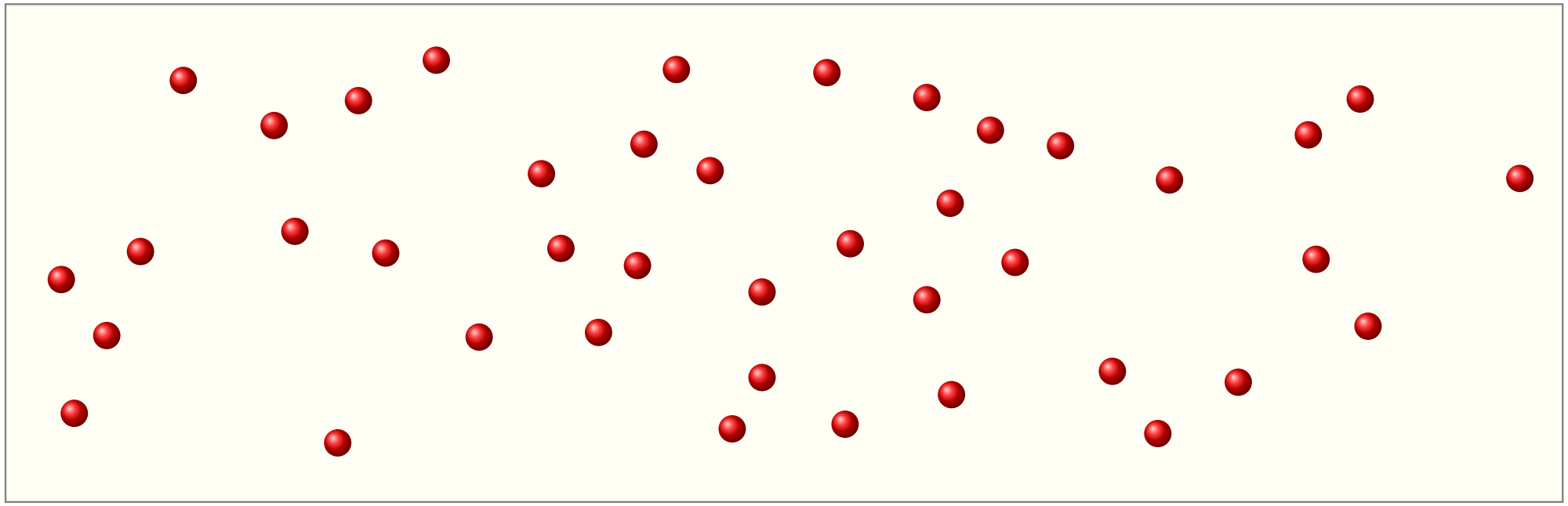
Stopp! **Beweis:** Gegeben sind $f_1, \ldots, f_p : \mathbb{N} \to \mathbb{Z}_q$ mit $q = 10 < p = 11$.
Schubfachprinzip 1: An jeder Stelle $k \in \mathbb{N}$ haben wir $\{1, \ldots, p\} \to \mathbb{Z}_q$ mit $i \mapsto f_i(k)$. Wegen $p > q$ existiert ein Paar $i < j$ mit $f_i(k) = f_j(k)$.

Die Mengen $E_{i,j} := \{\, k \in \mathbb{N} \mid f_i(k) = f_j(k) \,\}$ überdecken $\mathbb{N} = \bigcup_{i<j} E_{i,j}$.
Es gibt nur endlich viele Indexpaare $i < j$, genauer $\binom{p}{2} = p(p-1)/2 = 55$.
Schubfachprinzip 2: Also muss eine der Mengen $E_{i,j}$ unendlich sein. $\boxed{\text{QED}}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

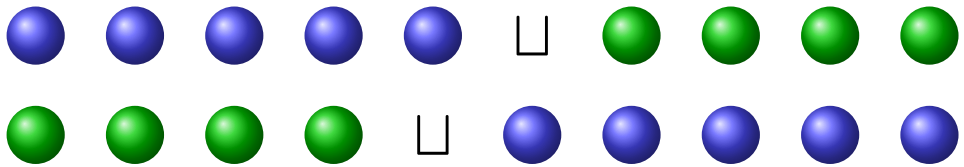
Mächtigkeit von Mengen: immer durch Abzählen!



Dies ist nur die Saalversion ohne Erläuterungen.

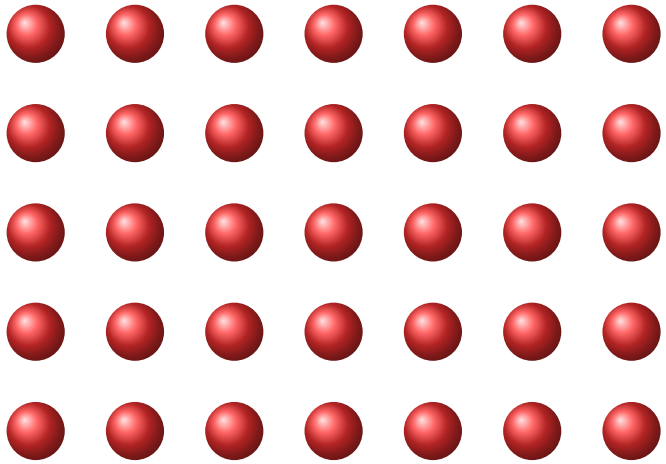
Ausführliche Erläuterungen bietet die Vollversion.

Strukturiertes Abzählen: Grundrechenarten



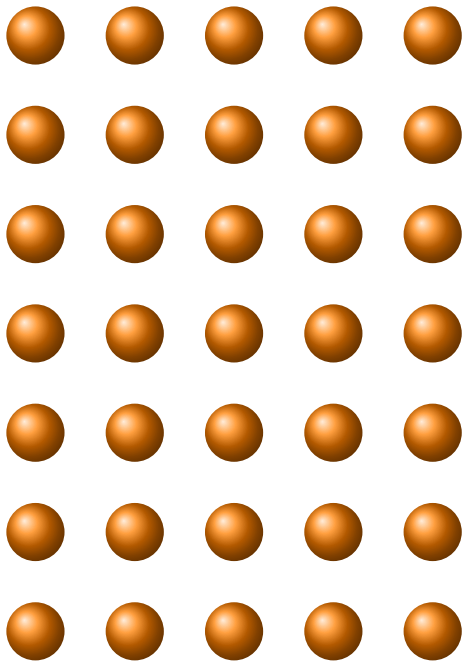
$\sharp X = 5 + 4$

$\sharp X = 4 + 5$



$\sharp Y = 7 \cdot 5$

$\cong$



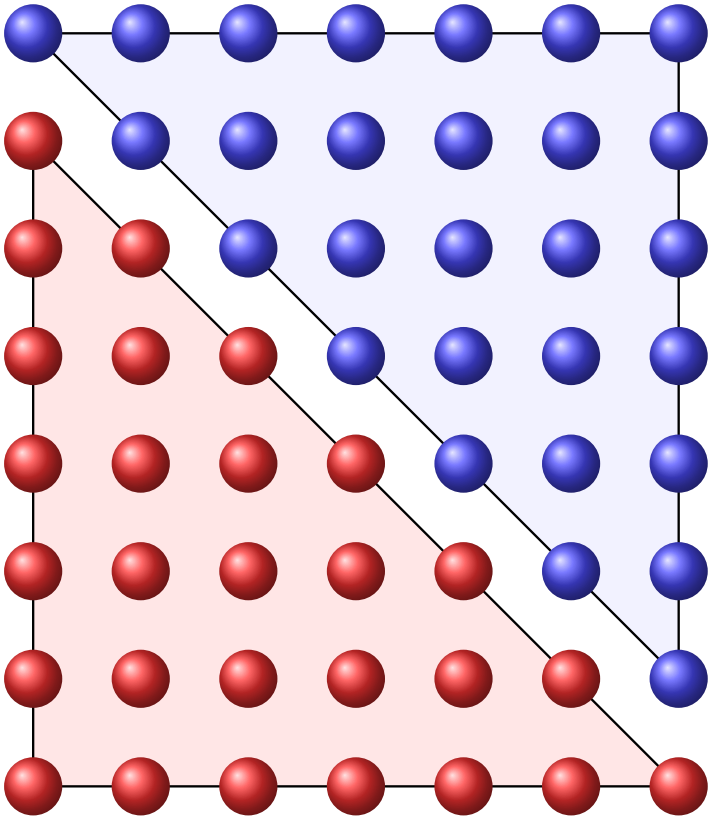
$\sharp Z = 5 \cdot 7$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Doppeltes Abzählen: der kleine Gauß

$$1 + 2 + 3 + \quad \ldots \quad + n =: S(n)$$

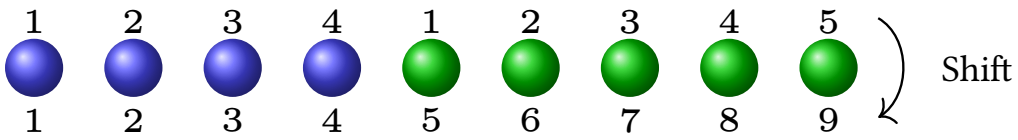


$$2S(n) = n(n+1)$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Mächtigkeit disjunkter Vereinigungen



Satz H2A: Mächtigkeit einer disjunkten Vereinigung

Seien X und Y endliche Mengen mit $X \cap Y = \emptyset$. Dann gilt:

$$\boxed{\sharp(X \sqcup Y) = (\sharp X) + (\sharp Y)}$$

Explizite Konstruktion: Gegeben seien die Abzählungen

$$\mu : \{1, \dots, p\} \xrightarrow{\sim} X \quad \text{und} \quad \nu : \{1, \dots, q\} \xrightarrow{\sim} Y.$$

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 $y \in Y$.

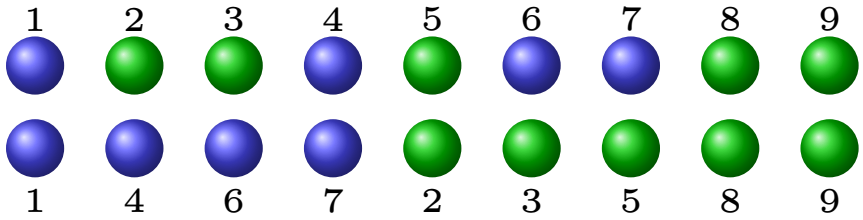
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Mächtigkeit von Teilmengen und Vereinigungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Satz H2B: Mächtigkeit von Teilmengen und Vereinigungen

(1) Ist Z endlich, so auch jede Teilmenge $X \subseteq Z$. Genauer gilt:

$$\boxed{X \subseteq Z \implies \sharp X \leq \sharp Z, \quad \sharp(Z \setminus X) = (\sharp Z) - (\sharp X)}$$

(2) Für alle endlichen Mengen X, Y folgt:

$$\boxed{\sharp(X \cup Y) = \sharp X + \sharp Y - \sharp(X \cap Y)}$$

Mächtigkeit kartesischer Produkte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H2c: Mächtigkeit eines kartesischen Produkts

Seien X und Y endliche Mengen. Dann gilt:

$$\boxed{\sharp(X \times Y) = (\sharp X) \cdot (\sharp Y)}$$

Mächtigkeit von Summen und Produkten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H2D: Mächtigkeit von Summen und Produkten

$$\sharp(X_1 \sqcup X_2 \sqcup \cdots \sqcup X_n) = (\sharp X_1) + (\sharp X_2) + \ldots + (\sharp X_n).$$
$$\sharp(X_1 \times X_2 \times \cdots \times X_n) = (\sharp X_1) \cdot (\sharp X_2) \cdot \ldots \cdot (\sharp X_n).$$

Mächtigkeit von Abbildungsmengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel Zahlenschloss: Wie viele Abbildungen $f : X \to Y$ gibt es von der Startmenge $X = \{1, 2, 3, 4\}$ in die Zielmenge $Y = \{0, \dots, 9\}$?

Satz H2F: Mächtigkeit der Abbildungsmenge

Sind X und Y endlich, so auch $Y^X = \mathrm{Fun}(X, Y) = \{ f : X \to Y \}$:

$$\boxed{\sharp(Y^X) = (\sharp Y)^{(\sharp X)}}$$

Mächtigkeit von Potenzmengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H2G: Mächtigkeit der Potenzmenge

Ist die Menge X endlich, so auch ihre Potenzmenge $\mathfrak{P}(X) = \{\, A \subseteq X \,\}$:

$$\boxed{\sharp\mathfrak{P}(X) = 2^{\sharp X}}$$

$$\begin{aligned} (\mathbf{1}, \mathrm{supp}) : \mathfrak{P}(X) &\cong 2^X = \mathrm{Fun}(X, \{0,1\}) \\ A &\mapsto \mathbf{1}_A \\ \mathrm{supp}(f) &\leftarrow\!\shortmid f \end{aligned}$$

Mächtigkeit von Potenzmengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: (1) Wie viele Relationen gibt es zwischen $X = \{1, 2, 3\}$ und $Y = \{0, 1, \dots, 99\}$? (2) Wie viele davon sind Funktionen?

Lösung: (1) Relation bedeutet $F \subseteq X \times Y$, also $F \in \mathfrak{P}(X \times Y)$:

$$\sharp\mathfrak{P}(X \times Y) = 2^{3 \cdot 100} = 1024^{30} \gtrapprox 10^{90}$$

(2) Funktion bedeutet zudem linkstotal und rechtseindeutig:

$$\sharp(Y^X) = 100^3 = 10^6$$

Anzahl der Abbildungen, Injektionen und Bijektionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H2H: Anzahl der Abbildungen, Injektionen und Bijektionen

(1) Für je zwei Mengen X, Y mit $\sharp X = k$ und $\sharp Y = n$ gilt:

$$\boxed{\sharp\,\mathrm{Fun}(X,Y) = n^k}$$

Die Anzahl der injektiven Abbildungen ist:

$$\boxed{\sharp\,\mathrm{Inj}(X,Y) \;=\; n\cdot(n-1)\cdot\ldots\cdot(n-k+1) \;=:\; n^{\underline{k}}}$$

(2) Im Spezialfall $k = n$ erhalten wir

$$\boxed{\sharp\,\mathrm{Fun}(X,Y) = n^n}$$

sowie die Anzahl der Bijektionen:

$$\boxed{\sharp\,\mathrm{Bij}(X,Y) \;=\; n\cdot(n-1)\cdot\ldots\cdot 3\cdot 2\cdot 1 \;=\; n^{\underline{n}} \;=:\; n!}$$

Die symmetrische Gruppe $\mathrm{S}_n = \mathrm{Aut}(\{1,\ldots,n\})$ hat genau $n!$ Elemente.

Binomialkoeffizienten: Definition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Für $z \in \mathbb{C}$ und $k \in \mathbb{N}$ definieren wir den **Binomialkoeffizienten**

$$\boxed{\binom{z}{k} := \frac{z(z-1)\cdots(z-k+1)}{k(k-1)\cdots 1}}$$

Speziell für natürliche Zahlen $n \in \mathbb{N}$ und $0 \leq k \leq n$ gilt:

$$\binom{n}{k} \overset{\mathbb{Q}}{=} \frac{n!}{k!(n-k)!} \overset{\mathbb{Q}}{=} \binom{n}{n-k}$$

Aus der Definition folgt sofort:

$$\binom{z}{k+1} \overset{\mathbb{C}}{=} \binom{z}{k}\frac{z-k}{k+1} \qquad \text{und} \qquad \binom{z+1}{k+1} \overset{\mathbb{C}}{=} \binom{z}{k}\frac{z+1}{k+1}$$

Daraus erhalten wir **Pascals Rekursionsformel**:

$$\boxed{\binom{z}{k} + \binom{z}{k+1} = \binom{z+1}{k+1}}$$

Binomialkoeffizienten: Rekursion zum Pascal–Dreieck

$\binom{n}{k}$	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

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

$\binom{0}{0} = 1$ und $\binom{0}{k} = 0$ für $k \neq 0$

Dies ist nur die Saalversion ohne Erläuterungen.

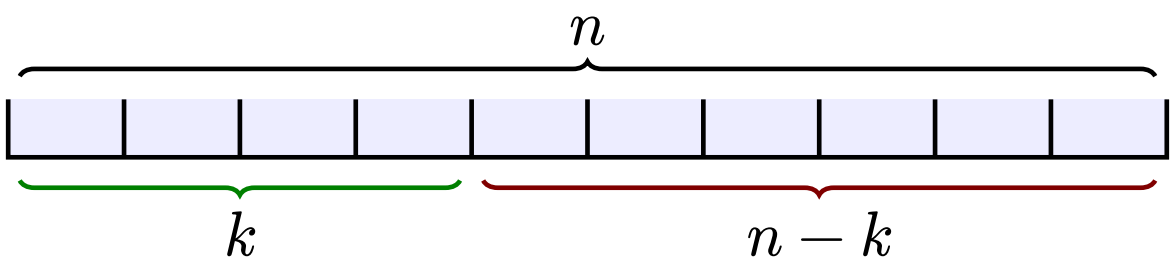
Ausführliche Erläuterungen bietet die Vollversion.

Binomialkoeffizienten: Interpretation durch k–Teilmengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Auf wie viele Arten können wir aus n Objekten k auswählen?



$n!$

$k!(n-k)!$

Lösung: Die Gesamtzahl der Möglichkeiten ist

$$\boxed{\binom{n}{k} = \frac{n!}{k!(n-k)!}.}$$

Binomialkoeffizienten: Interpretation durch k–Teilmengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H2J: Teilmengenformel dank Binomialkoeffizient

Wir betrachten eine Menge X und ihre k–elementigen Teilmengen:

$$\mathfrak{P}_k(X) := \{\, A \subseteq X \mid \sharp A = k \,\} := \binom{X}{k}$$

Ist X endlich, so auch $\binom{X}{k}$, und es gilt:

$$\boxed{\sharp \binom{X}{k} = \binom{\sharp X}{k}}$$

Beispiel: Wie viele 4–elementige Teilmengen hat $\{1, \dots, 9\}$? Genau 126.

Der binomische Lehrsatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\boxed{(\mathrm{klim} + \mathrm{bim})^2 = \mathrm{klim}^2 + 2\,\mathrm{klim}\,\mathrm{bim} + \mathrm{bim}^2}$$

$$(a+b)^0 = \mathbf{1}$$
$$(a+b)^1 = \mathbf{1} \cdot a + \mathbf{1} \cdot b$$
$$(a+b)^2 = \mathbf{1} \cdot a^2 + \mathbf{2} \cdot ab + \mathbf{1} \cdot b^2$$
$$(a+b)^3 = \mathbf{1} \cdot a^3 + \mathbf{3} \cdot a^2b + \mathbf{3} \cdot ab^2 + \mathbf{1} \cdot b^3$$
$$(a+b)^4 = \mathbf{1} \cdot a^4 + \mathbf{4} \cdot a^3b + \mathbf{6} \cdot a^2b^2 + \mathbf{4} \cdot ab^3 + \mathbf{1} \cdot b^4$$
$$(a+b)^5 = \mathbf{1} \cdot a^5 + \mathbf{5} \cdot a^4b + \mathbf{10} \cdot a^3b^2 + \mathbf{10} \cdot a^2b^3 + \mathbf{5} \cdot a^1b^4 + \mathbf{1} \cdot b^5$$

☺ Der Koeffizient vor $a^k b^{n-k}$ ist genau der Binomialkoeffizient $\binom{n}{k}$.

Der binomische Lehrsatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H2κ: der binomische Lehrsatz

Sei $(R, +, \cdot)$ ein Halbring und $a, b \in R$ mit $ab = ba$. Für alle $n \in \mathbb{N}$ gilt:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Kombinatorischer Beweis: Wir multiplizieren $(a+b)^n$ aus und erhalten

$$(a+b)(a+b)\cdots(a+b) \quad = \quad \boxed{?}\, a^0 b^n + \cdots + \boxed{?}\, a^k b^{n-k} + \cdots + \boxed{?}\, a^n b^0.$$

Aus jedem der n Faktoren wird entweder a oder b verwendet.
Dank $ab = ba$ ist jeder Summand von der Form $a^k b^{n-k}$.
Der Summand $a^k b^{n-k}$ tritt genau $\binom{n}{k}$ mal auf. QED

Beispiel: Speziell für $a = b = 1$ in $\mathbb{N}$ erhalten wir

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \quad \text{entsprechend} \quad \mathfrak{P}(\{1, \dots, n\}) = \bigsqcup_{k=0}^{n} \mathfrak{P}_k(\{1, \dots, n\}).$$

Ein genialer Abzähltrick: *stars and bars*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H2L: die Anzahl monotoner k–Tupel in $\{1,\dots,n\}^k$

$$I = \{1,\dots,n\}^k_< = \{\,(i_1 < i_2 < \dots < i_k) \in \{1,\dots,n\}^k\,\} \qquad \Longrightarrow \qquad \sharp I = \binom{n}{k}$$

Beispiel: $\sharp\{\,(\,a < b < c\,) \in \{1,\dots,7\}^3\,\} = \binom{7}{3} = 35$

$$J = \{1,\dots,n\}^k_\leq = \{\,(j_1 \leq j_2 \leq \dots \leq j_k) \in \{1,\dots,n\}^k\,\} \Longrightarrow \sharp J = \binom{n+k-1}{k}$$

Beispiel: $\sharp\{\,(\,a \leq b \leq c\,) \in \{1,\dots,7\}^3\,\} = \binom{9}{3} = 84$

$$\begin{aligned}
(v,u) \;&:\; \{1,\dots,n\}^k_< \;\cong\; \mathfrak{P}_k(\{1,\dots,n\}) \\
(i_1 < i_2 < \dots < i_k) \;&\mapsto\; \{i_1, i_2, \dots, i_k\}^! \\
(s,t) \;&:\; \{1,\dots,n\}^k_\leq \;\cong\; \{1,\dots,n+k-1\}^k_< \\
(j_1 \leq j_2 \leq \dots \leq j_k) \;&\mapsto\; (j_1 + 0 < j_2 + 1 < \dots < j_k + k - 1)
\end{aligned}$$

Zerlegungen aka Partitionen: erste Beispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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-Zerlegungen: $\{\{1,2,3,4\}\}$,

2-Zerlegungen: $\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$, $\{\{1,4\},\{2,3\}\}$,
$\{\{1\},\{2,3,4\}\}$, $\{\{2\},\{1,3,4\}\}$, $\{\{3\},\{1,2,4\}\}$, $\{\{4\},\{1,2,3\}\}$,

3-Zerlegungen: $\{\{1,2\},\{3\},\{4\}\}$, $\{\{1,3\},\{2\},\{4\}\}$, $\{\{1,4\},\{2\},\{3\}\}$,
$\{\{2,3\},\{1\},\{4\}\}$, $\{\{2,4\},\{1\},\{3\}\}$, $\{\{3,4\},\{1\},\{2\}\}$,

4-Zerlegungen: $\{\{1\},\{2\},\{3\},\{4\}\}$.

Zerlegungen rekursiv aufbauen: Systematik

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede k–Zerlegung Q von $\{1, \dots, n\}$ erhalten wir auf eine von zwei Arten:

1. Wir nehmen eine $(k-1)$–Zerlegung P von $\{1, \dots, n-1\}$ und fügen ihr die neue Klasse $\{n\}$ hinzu: So erhalten wir $Q = P \cup \{\{n\}\}$.
2. Wir nehmen eine k–Zerlegung P von $\{1, \dots, n-1\}$ und fügen einer Klasse $C \in P$ das neue Element n hinzu: $Q = (P \setminus \{C\}) \cup \{C \cup \{n\}\}$.

Satz H2M: Zerlegungen und Stirling–Zahlen

Wir betrachten eine Menge X und ihre k–elementigen Zerlegungen:

$$\left\{ {X \atop k} \right\} := \left\{ Q \subseteq \mathfrak{P}(X)^* \;\middle|\; X = \bigsqcup Q \text{ mit } \sharp Q = k \right\}$$

Für $n = \sharp X \in \mathbb{N}$ und $k \in \mathbb{Z}$ definieren wir die **Stirling–Zahl** $\left\{ {n \atop k} \right\} := \sharp \left\{ {X \atop k} \right\}$.
Für $n = 0$ gilt $\left\{ {0 \atop 0} \right\} = 1$ sowie $\left\{ {0 \atop k} \right\} = 0$ für $k \neq 0$. Für $n \geq 1$ gilt rekursiv:

$$\boxed{\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}}$$

Zerlegungszahlen: Rekursion zum Stirling–Dreieck

$\left\{ {n \atop k} \right\}$	k=0	1	2	3	4	5	6	7	8	9	10
n=0	1										
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

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}$$

$\left\{ {0 \atop 0} \right\} = 1$ und $\left\{ {0 \atop k} \right\} = 0$ für $k \neq 0$

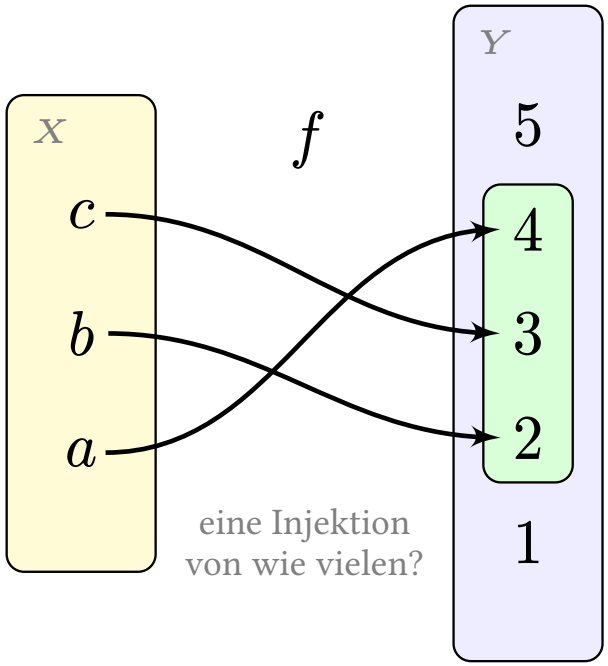
Dies ist nur die Saalversion ohne Erläuterungen.

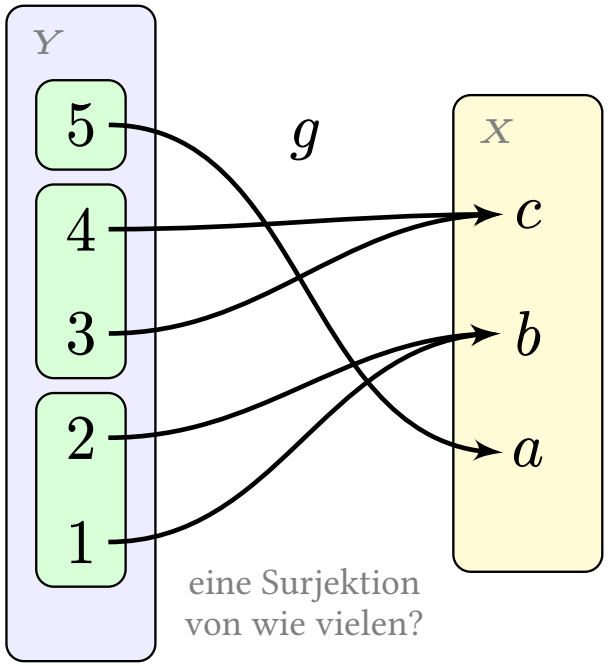
Ausführliche Erläuterungen bietet die Vollversion.

Anzahl der Injektionen und der Surjektionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Aufgabe: (1) Wie viele Injektionen $f : \{a, b, c\} \hookrightarrow \{1, 2, 3, 4, 5\}$ gibt es?

$$\binom{5}{3} \cdot 3! \;=\; 10 \cdot 6 \;=\; 60$$

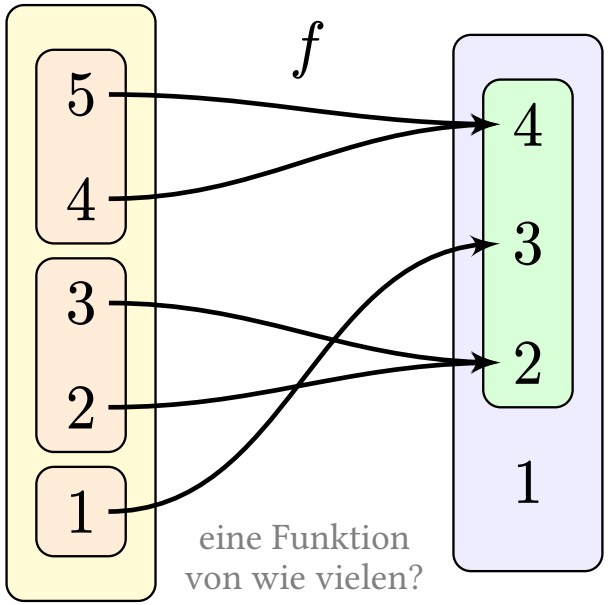
(2) Wie viele Surjektionen $g : \{1, 2, 3, 4, 5\} \twoheadrightarrow \{a, b, c\}$ gibt es?

$$\left\{ {5 \atop 3} \right\} \cdot 3! \;=\; 25 \cdot 6 \;=\; 150$$

Anzahl der Abbildungen mit vorgegebenem Rang

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Aufgabe: Wie viele Abbildungen $f : \{1, \dots, k = 5\} \to \{1, \dots, n = 4\}$ treffen genau $r = 3$ Bildpunkte?

$$\left\{ {k \atop r} \right\} \cdot r! \cdot \binom{n}{r} = \left\{ {5 \atop 3} \right\} \cdot 3! \cdot \binom{4}{3} = 25 \cdot 6 \cdot 4 = 600$$

Zerlegung und Quotient

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Zu $X = \{1, \dots, 7\}$ und $Q = \{\, A{=}\{1,4\},\ B{=}\{2,3,6,7\},\ C{=}\{5\} \,\}$ gehört $q : X \twoheadrightarrow Q : 1 \mapsto A,\ 2 \mapsto B,\ 3 \mapsto B,\ 4 \mapsto A,\ 5 \mapsto C,\ 6 \mapsto B,\ 7 \mapsto B.$

Definition H3A: Zerlegung und Quotient

Eine **Zerlegung** der Menge X ist eine Familie $Q \subseteq \mathfrak{P}(X)^*$ mit $X = \bigsqcup Q$. Jedes Element $x \in X$ liegt in genau einer Klasse $C \in Q$. Dies definiert

$$q : X \twoheadrightarrow Q : x \mapsto [x] := C \ \text{ mit } \ x \in C \in Q.$$

Repräsentanten: die Qual der Wahl

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Zu $X = \{1, \dots, 7\}$ und $Q = \{\, A{=}\{1,4\},\ B{=}\{2,3,6,7\},\ C{=}\{5\}\,\}$ ist $R = \{4,3,5\}$ ein Repräsentantensystem, ebenso $R' = \{1,2,5\}$ uvm.

Definition H3A: Repräsentantensystem

Eine Teilmenge $R \subseteq X$ heißt **Repräsentantensystem** zu Q, falls gilt:

$$\forall C \in Q \;\; \exists! x \in R : x \in C$$

Das bedeutet, die Einschränkung $q|_R : X \supseteq R \to Q : x \mapsto [x]$ ist bijektiv.

Klassengleichung durch doppeltes Abzählen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Für $X = \bigsqcup Q$ mit $Q = \{\{1,4\},\{2,3,5\}\}$ gilt $\sharp X = 2 + 3 = 5$.
Für $X = \bigsqcup Q$ mit $Q = \{\{1,6\},\{2,5\},\{3,4\}\}$ gilt $\sharp X = 2 \cdot \sharp Q_2 = 6$.

Satz H3B: Klassengleichung / Kassensturz / Schäfergleichung

Wir zerlegen $X = \bigsqcup Q$ und $Q = \bigsqcup_{n\in\mathbb{N}} Q_n$ in $Q_n := \{\, C \in Q \mid \sharp C = n \,\}$.

$$\boxed{X = \bigsqcup Q = \bigsqcup \bigsqcup_{n\in\mathbb{N}} Q_n \quad \Longrightarrow \quad \sharp X = \sum_{C\in Q} \sharp C = \sum_{n\in\mathbb{N}} n \cdot \sharp Q_n}$$

Haben alle Klassen $C \in Q$ dieselbe Größe $n > 0$, also $Q = Q_n$, so gilt

$$\sharp X = n \cdot \sharp Q, \quad \text{also} \quad \sharp Q = (\sharp X)/n.$$

Anwendungsbeispiel: Multinomialkoeffizienten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Auf wie viele Arten können wir n Studierende aufteilen in ℓ Übungsgruppen $X_1, \dots, X_\ell$ von gegebener Größe $k_1, \dots, k_\ell$?

$$\overbrace{\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ \hline 5 & 7 & 1 & 4 & 11 & 12 & 6 & 3 & 9 & 10 & 8 & 2 \end{array}}^{\sharp X = n} \quad \sigma \qquad n!$$

$$\underbrace{\qquad\qquad}_{\sharp X_1 = k_1} \quad \underbrace{\qquad\qquad\qquad}_{\sharp X_2 = k_2} \quad \underbrace{\qquad\qquad}_{\sharp X_3 = k_3} \qquad k_1!\, k_2! \cdots k_\ell!$$

Lösung: Die Gesamtzahl der Möglichkeiten ist

$$\boxed{\binom{n}{k_1, \dots, k_\ell} := \frac{n!}{k_1! \cdots k_\ell!}.}$$

Anwendungsbeispiel: Multinomialkoeffizienten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H3c: Teilmengenformel dank Multinomialkoeffizient

Für $\sharp X = n = k_1 + \cdots + k_\ell$ definieren wir

$$\binom{X}{k_1, \dots, k_\ell} := \left\{ (X_1, \dots, X_\ell) \in \mathfrak{P}(X)^\ell \;\middle|\; \begin{array}{c} X = X_1 \sqcup \cdots \sqcup X_\ell, \\ \sharp X_1 = k_1, \dots, \sharp X_\ell = k_\ell \end{array} \right\}.$$

Dann gilt

$$\sharp \binom{X}{k_1, \dots, k_\ell} = \binom{n}{k_1, \dots, k_\ell} := \frac{n!}{k_1! \cdots k_\ell!}$$

Beweis: Wir fixieren $X = A_1 \sqcup \cdots \sqcup A_\ell$ mit $\sharp A_i = k_i$ und nutzen

$$f : \mathrm{S}_X \to \binom{X}{k_1, \dots, k_\ell} : \sigma \mapsto (\, X_1 = \sigma(A_1), \dots, X_\ell = \sigma(A_\ell)\,).$$

Die Abbildung f ist surjektiv. Jede Faser hat $k_1! \cdots k_\ell!$ Elemente.
Die Klassengleichung H3B liefert die Anzahl $n!/k_1! \cdots k_\ell!$. QED

Äquivalenz und Quotient

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede Teilmenge $R \subseteq X \times X$ heißt (binäre) **Relation auf X**. Für $(a, b) \in R$ schreiben wir infix $a\,R\,b$ und sagen „a und b stehen in der Relation R“.

Beispiel: Jede Abbildung $f : X \to Y$ definiert ihre zugehörige Relation

$$R_f = (\sim_f) := \{\, (a, b) \in X \times X \mid f(a) = f(b) \,\}, \quad a \sim b :\Leftrightarrow f(a) = f(b).$$

Reflexivität,	**Refl**(X, R):	$\Delta_X \subseteq R$,	$a\,R\,a$
Symmetrie,	**Sym**(X, R):	$R = R^{\mathsf{T}}$,	$a\,R\,b \Rightarrow b\,R\,a$
Transitivität,	**Tran**(X, R):	$R \bullet R \subseteq R$,	$a\,R\,b \wedge b\,R\,c \Rightarrow a\,R\,c$

Definition H3D: Äquivalenzrelation

Eine Relation $R \subseteq X \times X$ heißt **Äquivalenzrelation**, falls sie reflexiv, symmetrisch und transitiv ist.

Äquivalenz und Quotient

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die **Äquivalenzklasse** von $a \in X$ bezüglich R ist

$$[a]_R := \{ b \in X \mid a \, R \, b \}.$$

Dank Reflexivität gilt $[a]_R \ni a$. Aus $[a]_R \ni b$ folgt $[a]_R \supseteq [b]_R$ dank Transitivität, und $[a]_R \subseteq [b]_R$ dank Symmetrie, also $[a]_R = [b]_R$.

☺ Je zwei Äquivalenzklassen sind entweder gleich oder disjunkt.

☺ Jedes Element $a \in X$ liegt in genau einer Klasse, nämlich $[a]$.

Die **Quotientenmenge** von (X, R) ist die Zerlegung

$$X/R := \{ [a]_R \mid a \in X \}.$$

Die zugehörige **Quotientenabbildung** ist

$$q_R : X \twoheadrightarrow X/R : a \mapsto [a]_R.$$

Statt mit Elementen $a \in X$ arbeiten wir mit Äquivalenzklassen $k \in X/R$.

Äquivalenzen entsprechen Zerlegungen.

Dies ist nur die Saalversion ohne Erläuterungen.

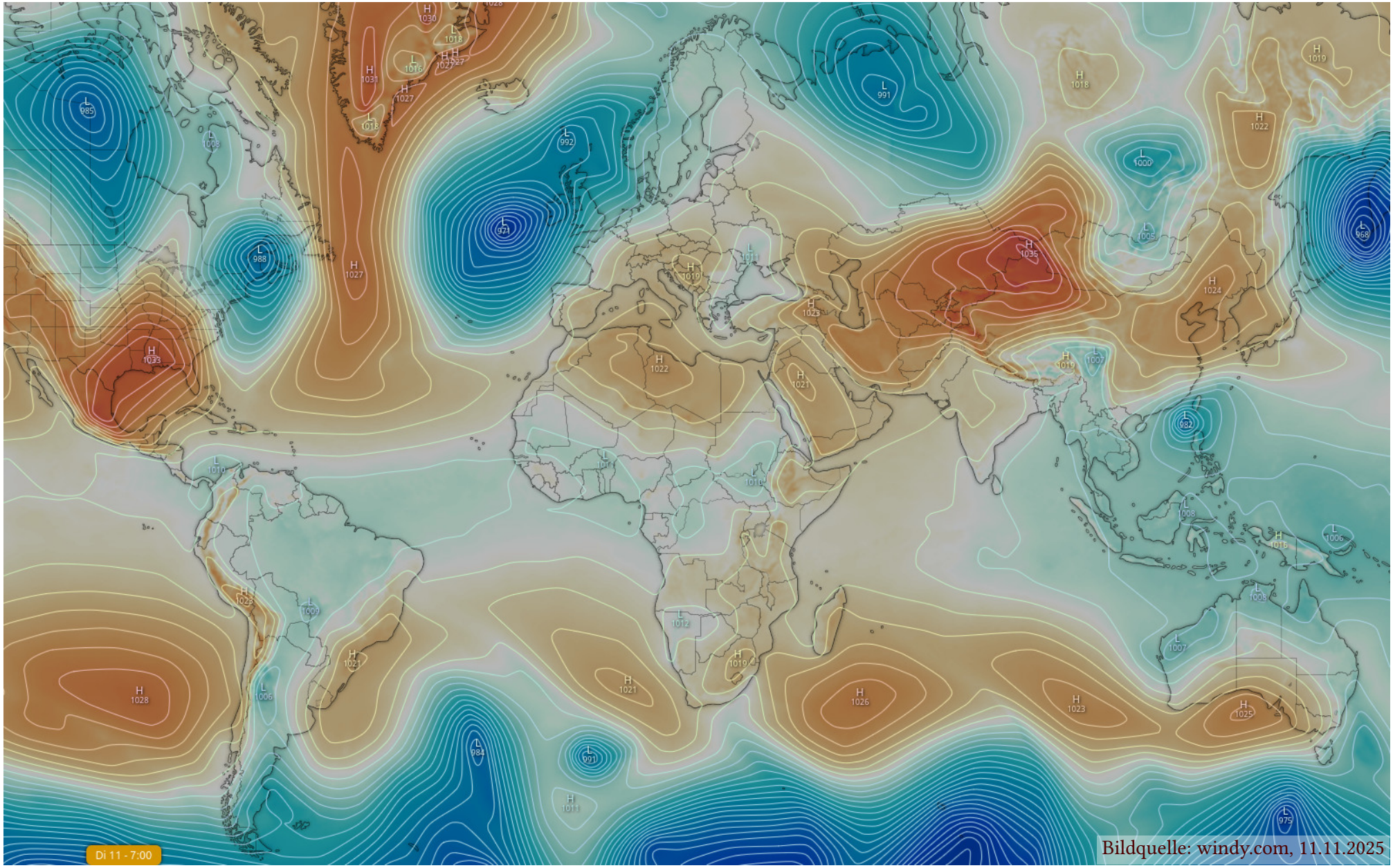
Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: (1) Wie viele Relationen gibt es auf $X = \{1, \dots, n = 4\}$?
(2) Wie viele dieser Relationen sind Äquivalenzrelationen?

Lösung: (1) Die Menge $\mathfrak{P}(X \times X)$ hat $2^{n \cdot n} = 2^{16} = 65536$ Elemente.

(2) Äquivalenzen auf X entsprechen Zerlegungen von X.
Die Menge X hat $\sum_{k=0}^{n} \left\{ {n \atop k} \right\} = 15$ Zerlegungen.

Äquivalenzklassen: Niveaumengen, Isolinien



Bildquelle: windy.com, 11.11.2025

Der Luftdruck $f : \mathbb{R}^2 \supseteq U \twoheadrightarrow I \subseteq \mathbb{R}$ zerlegt in Isobare, $U = \bigsqcup_{c \in I} f^{-1}(\{c\})$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Äquivalenzrelationen: einfache Beispiele

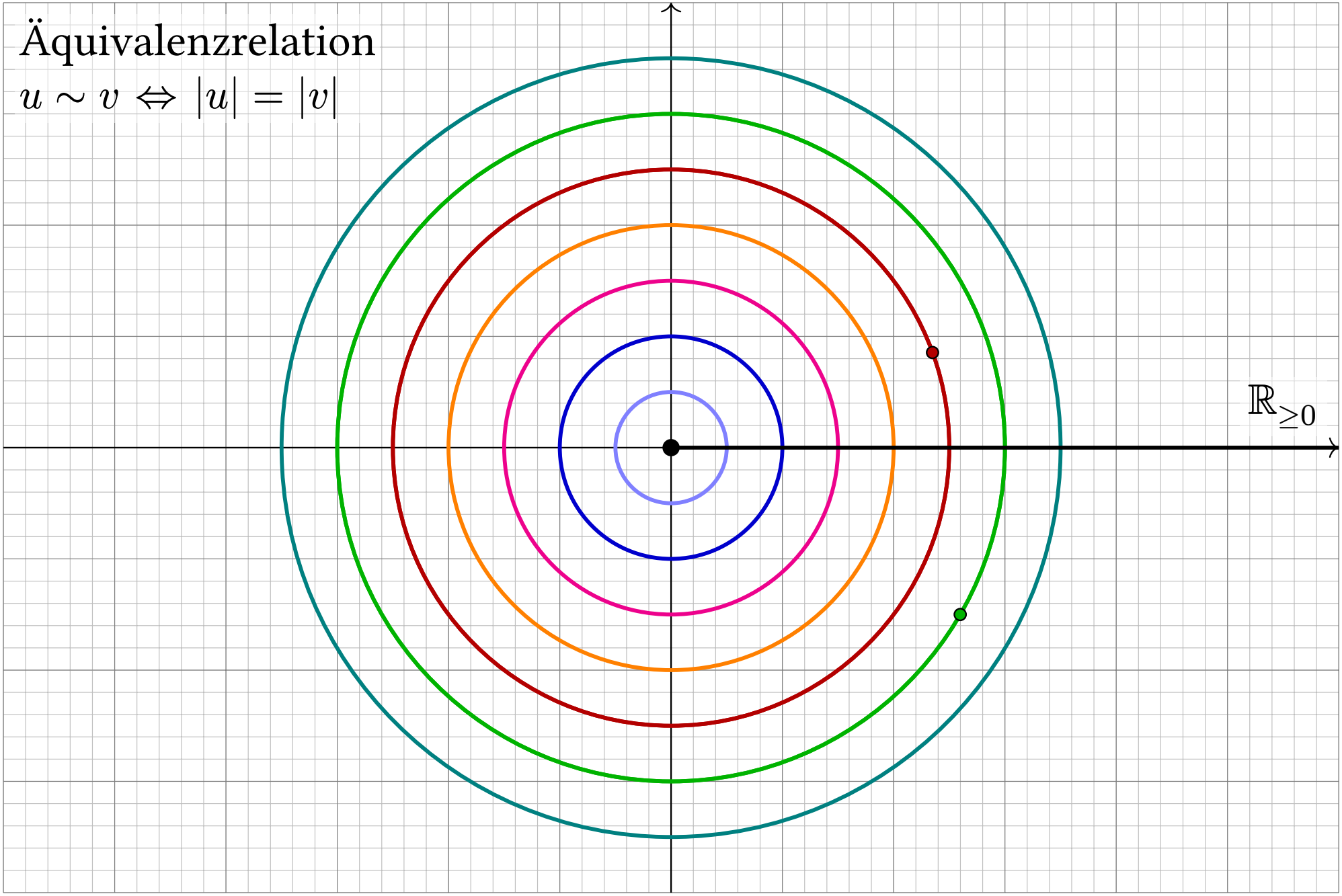
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Die feinste Äquivalenz auf X ist $F = \Delta_X = \{\,(x,x) \mid x \in X\,\}$:
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.

Beispiel: Die gröbste Äquivalenzrelation auf X ist $G = X \times X$.
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.

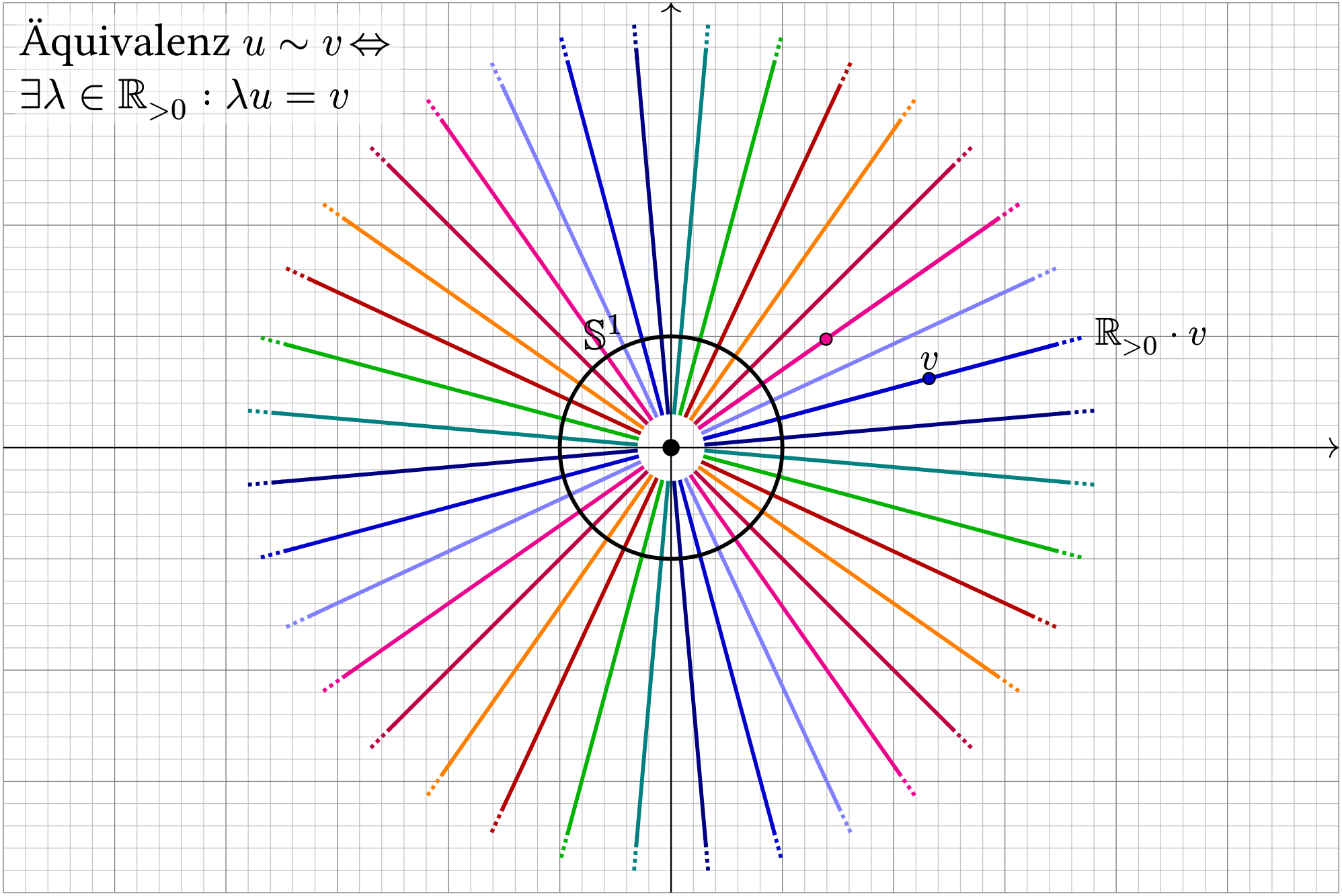
Zerlegung der Ebene $\mathbb{R}^2$ in Kreislinien



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zerlegung der Ebene $\mathbb{R}^2$ in Halbgeraden



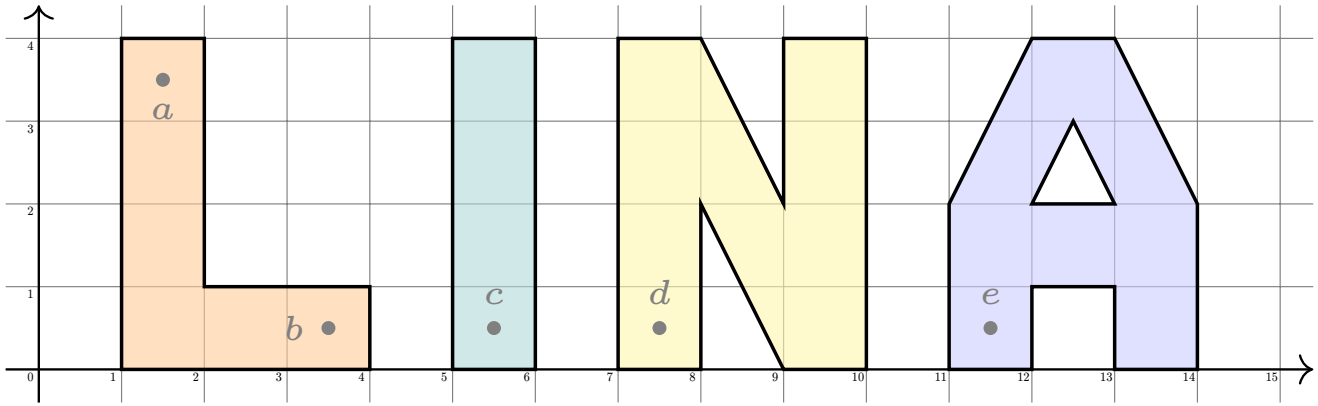
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Anwendungsbeispiel: Wegkomponenten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Sei $X \subseteq \mathbb{R}^n$. Punkte a und b in X sind **verbindbar**, falls ein Weg von a nach b in X existiert. Die Zerlegung im Beispiel ist $\pi_0(X) = \{L, I, N, A\}$.

? Ist gerade Verbindbarkeit $a \approx b :\Leftrightarrow [a, b] \subseteq X$ eine Äquivalenzrelation?

Erzeugung von Äquivalenzrelationen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H3F: die erzeugte Äquivalenzrelation

Jede Relation $P \subseteq X \times X$ erzeugt eine Äquivalenzrelation $T \subseteq X \times X$:

$$\begin{aligned} P &\mapsto R := P \cup \Delta_X \\ &\mapsto S := R \cup R^{\mathsf{T}} = P \cup \Delta_X \cup P^{\mathsf{T}} \\ &\mapsto T := \textstyle\bigcup_{n\in\mathbb{N}} S^{\bullet n} = \Delta_X \cup S \cup (S \bullet S) \cup (S \bullet S \bullet S) \cup \ldots \end{aligned}$$

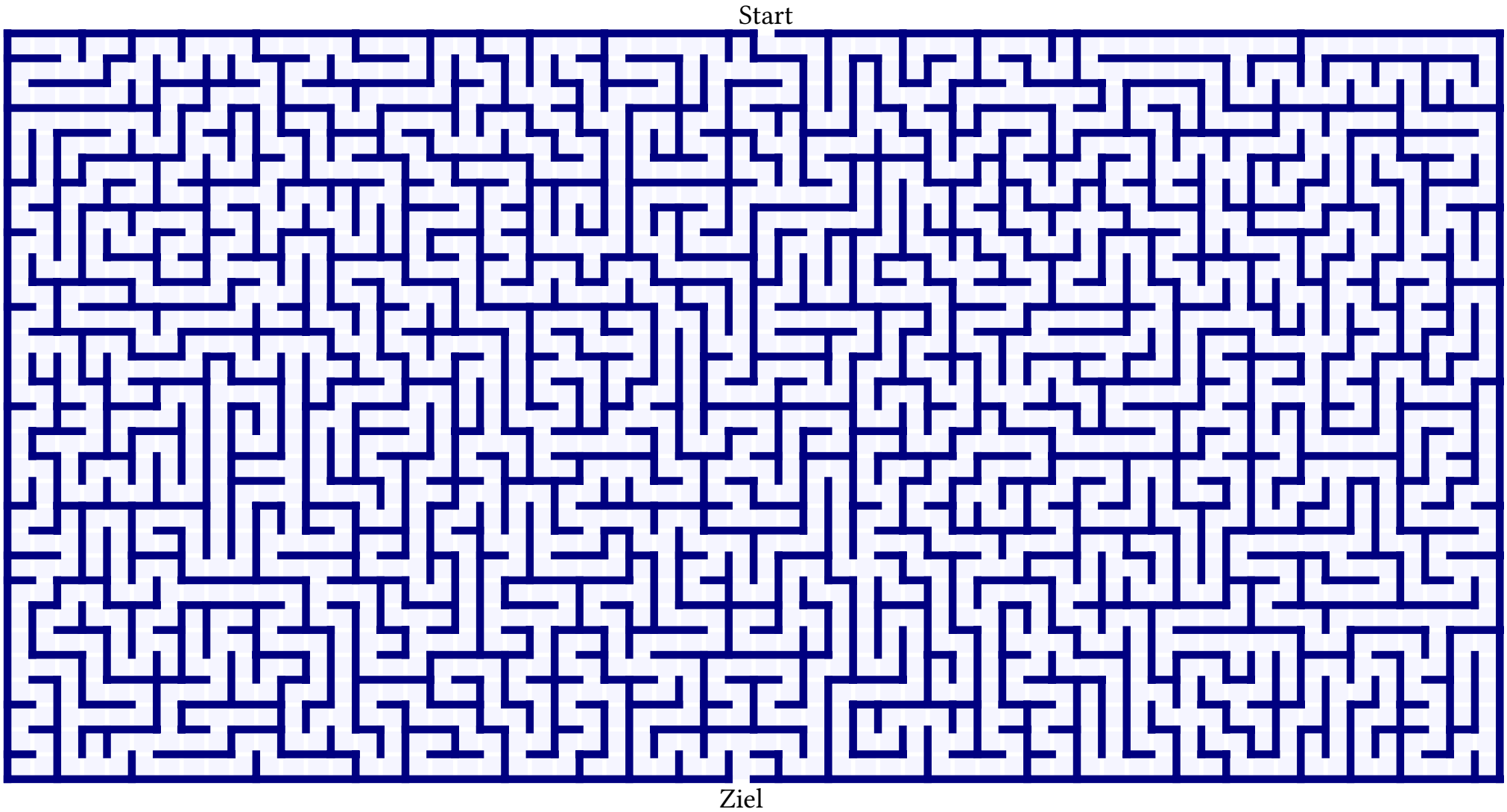
Aufgabe: Auf $X = \mathbb{R}$ gelte $a\,P\,b \Leftrightarrow b - a = 1$. Bestimmen Sie R, S, T.

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.

Anwendungsbeispiel: Wege in einem Labyrinth

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

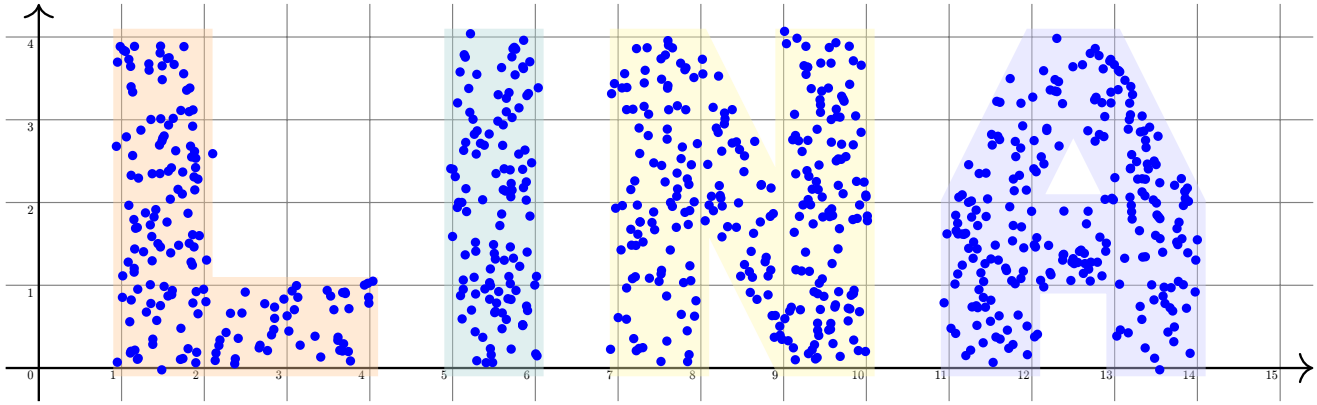


Gegeben: lokale Verbindbarkeit S. — Gesucht: globale Verbindbarkeit T.

Anwendungsbeispiel: topologische Datenanalyse (TDA)

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Wie klassifizieren wir $X \subseteq \mathbb{R}^n$ in ε–zusammenhängende Komponenten?
Wir definieren die Relation $x \approx y$ durch die Bedingung $d(x, y) \leq \varepsilon = 0.5$.

Faktorisierung über eine Injektion: Beispiel

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd} \mathbb{R} \arrow[r, "f"] \arrow[dr, dashed, "g"'] & \mathbb{R} \\ & \mathbb{R}_{\geq 0} \arrow[u, hook, "i"'] \end{tikzcd}$$

$$f_1(x) = x^5$$
$$f_2(x) = x^6$$
$$i(x) = x^2$$

Aufgabe: Finden Sie alle Faktorisierungen $g : \mathbb{R} \to \mathbb{R}_{\geq 0}$ mit $f = i \circ g$.

Lösung: (1) Es gibt keine Lösung, denn $\operatorname{Im} f_1 = \mathbb{R} \not\subseteq \mathbb{R}_{\geq 0} = \operatorname{Im} i$.
(2) Hier gilt $\operatorname{Im} f_2 \subseteq \operatorname{Im} i$, und wir finden die Lösung $g_2(x) = |x|^3$.

Faktorisierung über eine Injektion: Konstruktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, dashed, "\exists! g"'] & Y \\ & U \arrow[u, hook, "i"'] \end{tikzcd}$$

Satz H3κ: eindeutige Faktorisierung über eine Injektion

Zu jeder Abbildung $f : X \to Y$ und Injektion $i : U \hookrightarrow Y$ existiert $g : X \to U$ mit $f = i \circ g$ gdw $\operatorname{Im} f \subseteq \operatorname{Im} i$; diesenfalls gilt $g = i^{\top} \circ f$.

In Worten: Zu jedem $x \in X$ und seinem Bild $y = f(x)$ wählen wir das (eindeutig existente) Urbild $u \in U$ mit $i(u) = y$ und setzen $g(x) := u$.

Faktorisierung über eine Surjektion: Beispiel

$$\begin{tikzcd} \mathbb{R} \arrow[r, "f"] \arrow[d, two heads, "q"'] & {[-1,1]} \\ \mathbb{R}_{\geq 0} \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

$$f_1(x) = \sin(x)$$
$$f_2(x) = \cos(x)$$
$$q(x) = x^2$$

Aufgabe: Finden Sie alle Faktorisierungen $g : \mathbb{R}_{\geq 0} \to [-1, 1]$ mit $f = g \circ q$.

Lösung: (1) Es gibt keine Lösung, denn $q(-x) = q(x)$ für alle $x \in \mathbb{R}$, aber im Allgemeinen $\sin(-x) \neq \sin(x)$, etwa $\sin(-\pi/2) = -1 \neq 1 = \sin(\pi/2)$.
(2) Hier gilt $\cos(-x) = \cos(x)$ für alle $x \in \mathbb{R}$, und $g_2(y) = \cos(\sqrt{y})$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Faktorisierung über eine Surjektion: Konstruktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, two heads, "q"'] & Y \\ Q \arrow[ur, dashed, "\exists! g"'] & \end{tikzcd}$$

Satz H3L: eindeutige Faktorisierung über eine Surjektion

Zu $f : X \to Y$ und $q : X \twoheadrightarrow Q$ existiert $g : Q \to Y$ mit $f = g \circ q$ gdw $R_q \subseteq R_f$, also $q(x) = q(x') \Rightarrow f(x) = f(x')$; diesenfalls gilt $g = f \circ q^\top$.

In Worten: Zu jedem $\overline{x} \in Q$ wählen wir willkürlich ein Urbild $x \in X$ mit $q(x) = \overline{x}$ und setzen $g(\overline{x}) := f(x)$. Dies ist wohldefiniert dank $R_q \subseteq R_f$.

Surjektiv und injektiv machen dank Faktorisierung

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, two heads, "\hat{f}\colon x \mapsto f(x)"'] & Y \\
& f(X) \arrow[u, hook, "\iota"']
\end{tikzcd}$$

$$f(X) := \{\, f(x) \in Y \mid x \in X \,\}$$

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, two heads, "q"'] & Y \\
X/R_f \arrow[ur, hook, "\check{f}\colon [x] \mapsto f(x)"'] &
\end{tikzcd}$$

$$R_f := \{\, (x, x') \mid f(x) = f(x') \,\}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

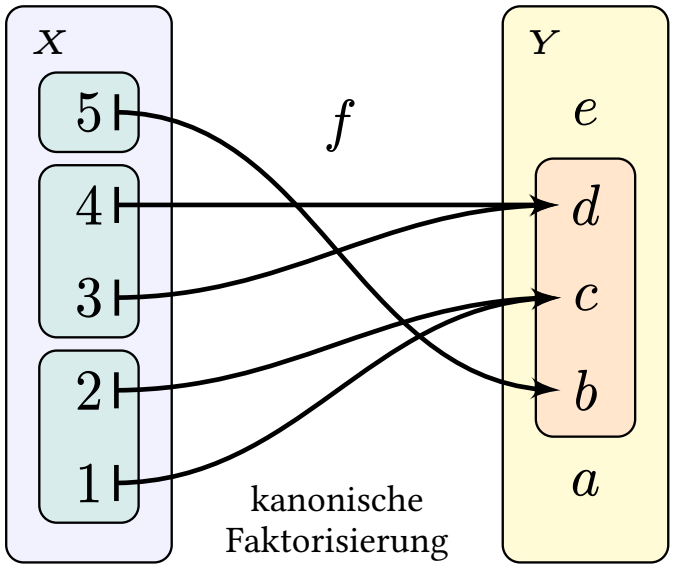
Bijektiv machen dank kanonischer Faktorisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{tikzcd}
X \arrow[rr, "f"] \arrow[d, two heads, "{[x] \leftarrow\!\shortmid x : q}"'] \arrow[dr, "\hat{f}"] & & Y \\
X/R_f \arrow[rr, "\bar{f} : [x] \mapsto f(x)"] \arrow[ur, "\check{f}"] & & f(X) \arrow[u, hook, "{y \hookleftarrow\!\shortmid y : \iota}"']
\end{tikzcd}
$$

$\{\, [x] = f^{-1}(f(x)) \mid x \in X \,\}$ $\qquad$ $\{\, f(x) \mid x \in X \,\}$



Satz H3M: die kanonische Faktorisierung

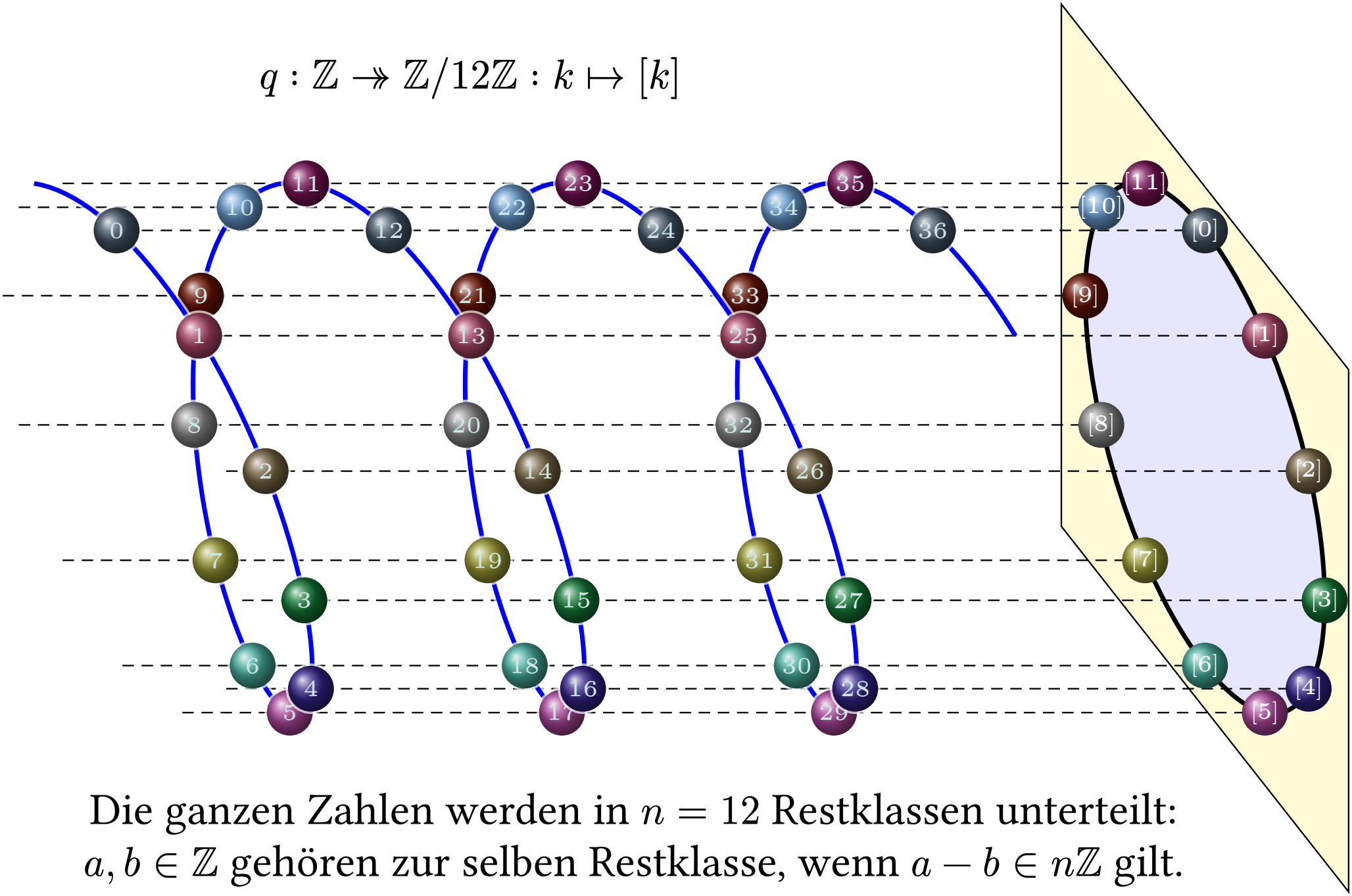
Jede Abbildung $f : X \to Y$ faktorisiert eindeutig gemäß $f = \iota \circ \bar{f} \circ q$ in die Quotientenabbildung $q : X \twoheadrightarrow X/R_f$, die kanonische Bijektion $\bar{f} : X/R_f \xrightarrow{\sim} f(X) : [x] \mapsto f(x)$ und die Inklusion $\iota : f(X) \hookrightarrow Y$.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/12\mathbb{Z} : k \mapsto [k]$$



Die ganzen Zahlen werden in $n = 12$ Restklassen unterteilt:
$a, b \in \mathbb{Z}$ gehören zur selben Restklasse, wenn $a - b \in n\mathbb{Z}$ gilt.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $n \in \mathbb{Z}$ eine ganze Zahl. Wir betrachten die Menge aller Vielfachen:

$$H = n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$$

1. Es gilt $0 \in H$.
2. Aus $a \in H$ folgt $-a \in H$.
3. Aus $a, b \in H$ folgt $a + b \in H$.

$\Big\}$ $H \leq (\mathbb{Z}, +, 0, -)$ ist Untergruppe

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Auf der Menge $\mathbb{Z}$ definieren wir:

$$a \equiv_n b \quad :\Leftrightarrow \quad a - b \in n\mathbb{Z}$$

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 $a \equiv c$.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zu jeder ganzen Zahl $a \in \mathbb{Z}$ haben wir die zugehörige Äquivalenzklasse:

$$[a]_n = a + n\mathbb{Z} := \{\, a + nk \mid k \in \mathbb{Z} \,\}$$

Alle Äquivalenzklassen fassen wir zur Quotientenmenge zusammen:

$$\mathbb{Z}/n\mathbb{Z} := \{\, [a] = a + n\mathbb{Z} \mid a \in \mathbb{Z} \,\}$$

Die zugehörige Quotientenabbildung ist demnach:

$$q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} : a \mapsto [a]$$

Beispiel: Es gilt $\mathbb{Z}/0\mathbb{Z} = \{\, \{a\} \mid a \in \mathbb{Z} \,\}$.
Die Quotientenabbildung $q : \mathbb{Z} \to \mathbb{Z}/0\mathbb{Z} : a \mapsto \{a\}$ ist bijektiv.

Beispiel: Es gilt $\mathbb{Z}/1\mathbb{Z} = \{\, [0] = \mathbb{Z} \,\}$.
Die Quotientenabbildung $q : \mathbb{Z} \to \mathbb{Z}/1\mathbb{Z} : a \mapsto \mathbb{Z}$ ist konstant.

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Für $n = 2$ haben wir genau zwei Äquivalenzklassen:

$$\begin{aligned}\mathbb{Z}/2\mathbb{Z} = \{\ 0 + 2\mathbb{Z} &= \{\dots, -4, -2, 0, 2, 4, 6, \dots\},\\ 1 + 2\mathbb{Z} &= \{\dots, -3, -1, 1, 3, 5, 7, \dots\}\ \}\end{aligned}$$

Beispiel: Für $n = 3$ haben wir genau drei Äquivalenzklassen:

$$\begin{aligned}\mathbb{Z}/3\mathbb{Z} = \{\ 0 + 3\mathbb{Z} &= \{\dots, -6, -3, 0, 3, 6, 9, \dots\},\\ 1 + 3\mathbb{Z} &= \{\dots, -5, -2, 1, 4, 7, 10, \dots\},\\ 2 + 3\mathbb{Z} &= \{\dots, -4, -1, 2, 5, 8, 11, \dots\}\ \}\end{aligned}$$

Bemerkung: Für jede ganze Zahl $n \in \mathbb{Z}_{\geq 1}$ erhalten wir die Zerlegung

$$\mathbb{Z} = \bigsqcup \mathbb{Z}/n\mathbb{Z} = \bigsqcup_{k=0}^{n-1} (k + n\mathbb{Z})$$

Das kanonische Repräsentantensystem ist hier $\mathbb{Z}_n = \{0, \dots, n-1\}$.
Statt mit Repräsentanten a arbeiten wir mit Äquivalenzklassen $[a]$!

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sind Addition α und Multiplikation μ in $\mathbb{Z}$ kompatibel mit q?

$$\begin{tikzcd}
\mathbb{Z} \times \mathbb{Z} \arrow[r, "\alpha", "(a,b)\mapsto a+b"'] \arrow[d, two heads, "q"'] \arrow[dr, "q\circ\alpha"] & \mathbb{Z} \arrow[d, two heads, "q"'] \\
\mathbb{Z}/n \times \mathbb{Z}/n \arrow[r, dashed, "\bar{\alpha}", "([a],[b])\mapsto[a+b]"'] & \mathbb{Z}/n
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{Z} \times \mathbb{Z} \arrow[r, "\mu", "(a,b)\mapsto a\cdot b"'] \arrow[d, two heads, "q"'] \arrow[dr, "q\circ\mu"] & \mathbb{Z} \arrow[d, two heads, "q"'] \\
\mathbb{Z}/n \times \mathbb{Z}/n \arrow[r, dashed, "\bar{\mu}", "([a],[b])\mapsto[a\cdot b]"'] & \mathbb{Z}/n
\end{tikzcd}$$

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? Ja!

Lemma H3n: Wohldefiniertheit von Addition und Multiplikation

Aus $a \equiv a'$ und $b \equiv b'$ in $\mathbb{Z}$ folgt $a + b \equiv a' + b'$ und $a \cdot b \equiv a' \cdot b'$.

Beweis: Aus $a = a' + nk$ und $b = b' + n\ell$ mit $a, a', k, b, b', \ell \in \mathbb{Z}$ folgt $a + b = a' + b' + n(k + \ell)$ und $a \cdot b = a' \cdot b' + n(kb' + a'\ell + nk\ell)$. QED

Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz H3o: Konstruktion des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

(1) Dank Lemma H3N erhalten wir auf $\mathbb{Z}/n$ die Verknüpfungen

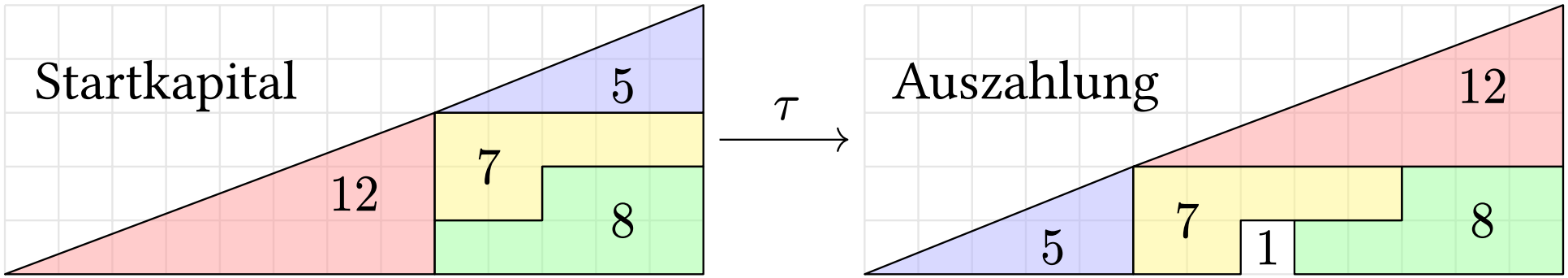
$$\begin{aligned} + &: \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n : [a] + [b] := [a+b], \\ \cdot &: \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n : [a] \cdot [b] := [a \cdot b]. \end{aligned}$$

(2) Damit ist $(\mathbb{Z}/n, +, [0], \cdot, [1])$ ein kommutativer Ring.

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel H

Bonusmaterial



Wer zählen kann, ist klar im Vorteil.

humoristisches Sprichwort

Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels H

5 Strukturiertes Abzählen

6 Anwendung des Schubfachprinzips

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel I

Ordnungsrelationen und Mächtigkeit

Alles sollte so einfach wie möglich gemacht werden
— aber nicht noch einfacher.

Albert Einstein (1879–1955)

Inhalt dieses Kapitels I

1 Ordnungsrelationen

2 Wohlordnungen und Ordinalzahlen

3 Die Mächtigkeit von Mengen

4 Übungsaufgaben und Anwendungsbeispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Was ist eine Ordnungsrelation?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Auf $X = \mathbb{N}$ definieren wir die Relation

$$R = (\leq) = \{ (a, b) \in \mathbb{N} \times \mathbb{N} \mid \exists a' \in \mathbb{N} : a + a' = b \}.$$

Diese erfreut sich folgender Eigenschaften für alle $a, b, c \in X$:

Reflexivität,	**Refl**(X, R):	$\Delta_X \subseteq R$,	$a \leq a$
Transitivität,	**Tran**(X, R):	$R \bullet R \subseteq R$,	$a \leq b \land b \leq c \Rightarrow a \leq c$
Antisymmetrie,	**Asym**(X, R):	$R \cap R^{\mathsf{T}} \subseteq \Delta_X$,	$a \leq b \land b \leq a \Rightarrow a = b$
Totalität,	**Total**(X, R):	$R \cup R^{\mathsf{T}} = X \times X$,	$a \leq b \lor b \leq a$

Definition I1A: Ordnungsrelation

Eine Relation $R \subseteq X \times X$ auf der Menge X heißt… falls… gilt:

Name \ geforderte Eigenschaften	**Refl**	**Tran**	**Asym**	**Total**
totale Ordnung, lineare Ordnung, Toset	✓	✓	✓	✓
(partielle) **Ordnung**, Halbordnung, Poset	✓	✓	✓	
totale Präordnung, Präferenzordnung	✓	✓		✓
(partielle) **Präordnung**, Quasiordnung	✓	✓		

Ordnungsrelationen: unvergleichbare Elemente $a \parallel b$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Sei $\mathscr{A} = \mathfrak{P}(\Omega)$ mit Inklusionsrelation $\subseteq$.

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 nicht: weder $\{1\} \subseteq \{2\}$ noch $\{2\} \subseteq \{1\}$, kurz $\{1\} \parallel \{2\}$.

Ordnungsrelationen: assoziierte Elemente $a \approx b$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Auf $\mathbb{Z}$ definieren wir $a \mid_{\mathbb{Z}} b$ durch $\exists a' \in \mathbb{Z} : aa' = b$.

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 nicht: Aus $a \mid_{\mathbb{Z}} b$ und $b \mid_{\mathbb{Z}} a$ folgt nur $a = \pm b$.

Ordnungsrelationen: Striktordnung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition I1D: zugehörige Striktordnung

(1) Zu $(\preceq) = R$ ist $(\succeq) = R^{\mathsf{T}}$ die **umgekehrte Relation**: $a \succeq b \Leftrightarrow b \preceq a$.
(2) Die **Striktordnung** $(\prec) = S$ zu $(\preceq) = R$ ist $a \prec b \Leftrightarrow a \preceq b \wedge b \not\preceq a$.

Wichtige Beispiele sind $(\mathbb{N}, <_{\mathbb{N}}) \subseteq (\mathbb{Z}, <_{\mathbb{Z}}) \subseteq (\mathbb{Q}, <_{\mathbb{Q}}) \subseteq (\mathbb{R}, <_{\mathbb{R}})$.

Ordnungsrelationen: Einschränkung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition I1E: eingeschränkte Ordnungsrelation

(1) Sei $U \subseteq X$. Ist (X, R) eine total / partiell prä/geordnete Menge, so auch ihre **Einschränkung** (U, R_U) auf U mit $R_U = R \cap (U \times U)$.

(2) Wir nennen U in $(X, \leq)$ eine **Kette**, wenn $(U, \leq_U)$ total geordnet ist.

Beispiel: In $(\mathfrak{P}(\mathbb{N}), \subseteq)$ haben wir die Kette

$$U = \{\, \emptyset \subset \{0\} \subset \{0,1\} \subset \{0,1,2\} \subset \{0,1,2,3\} \,\}.$$

Ordnungsrelationen: Erzeugung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz I1F: die erzeugte Präordnung

Jede Relation $R \subseteq X \times X$ erzeugt eine Präordnung $P \subseteq X \times X$ auf X:

$$P = \bigcup_{n \in \mathbb{N}} R^{\bullet n} = \Delta_X \cup R \cup (R \bullet R) \cup (R \bullet R \bullet R) \cup \ldots$$

Beispiel: Auf $\mathbb{N}$ betrachten wir $R = \{\,(a, a+1) \mid a \in \mathbb{N}\}$. Dann gilt $R^{\bullet n} = \{\,(a, a+n) \mid a \in \mathbb{N}\}$, also $P = \{\,(a, a+n) \mid a, n \in \mathbb{N}\} = (\leq)$.

Hasse–Diagramm als graphische Darstellung

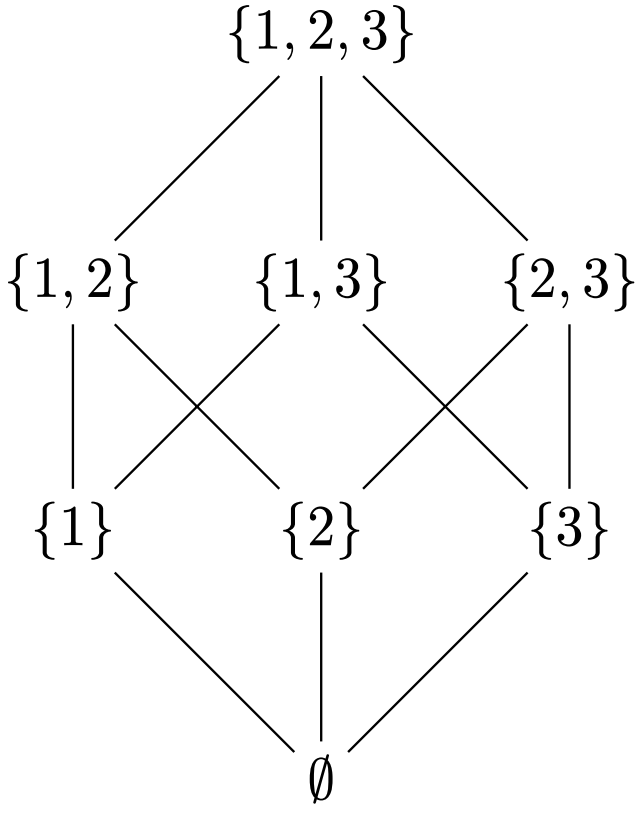
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Relation $\leq$ für natürliche Zahlen

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5 \longrightarrow 6 \longrightarrow 7 \longrightarrow \cdots$$

Inklusion von Mengen
in $\mathfrak{P}(\{1,2,3\})$



Ordnungsrelationen: kleine Beispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Für jede Menge X vereinbaren wir

$$\mathbb{O}(X) := \{\, R \subseteq X \times X \text{ totale Ordnung auf } X \,\} \quad \text{(tran. \& asym. \& total)}$$
$$\mathbb{P}(X) := \{\, R \subseteq X \times X \text{ totale Präordnung auf } X \,\} \quad \text{(tran. \& total)}$$

(1) Bestimmen Sie $\mathbb{O}(X)$ und $\mathbb{P}(X)$ für $X = \{a, b\}$.

Lösung: (1) Auf $X = \{a, b\}$ gibt es genau drei Präferenzen, nämlich:

$$\mathbb{O} = \left\{ \begin{array}{ll} \{(a,a),(a,b),(b,b)\} & \text{kurz: } a \prec b \\ \{(a,a),(b,a),(b,b)\} & \text{kurz: } a \succ b \\ \{(a,a),(a,b),(b,a),(b,b)\} & \text{kurz: } a \approx b \end{array} \right\} = \mathbb{P}$$

$\prec$	a	b
a	1	1
b	0	1

$$\begin{array}{c} b \\ | \\ a \end{array}$$

$\succ$	a	b
a	1	0
b	1	1

$$\begin{array}{c} a \\ | \\ b \end{array}$$

$\approx$	a	b
a	1	1
b	1	1

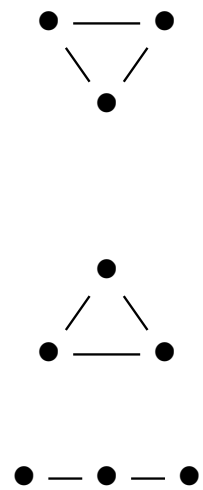
$$a \text{ —— } b$$

Ordnungsrelationen: kleine Beispiele

Dies ist nur die Saalversion ohne Erläuterungen.

(2) Auf $X = \{a, b, c\}$ gibt es genau 13 Präferenzen, nämlich

$$\mathbb{O} = \left\{ \begin{array}{ll} a \prec b \prec c & a \prec b \approx c \\ a \prec c \prec b & b \prec a \approx c \\ b \prec a \prec c & c \prec a \approx b \\ b \prec c \prec a & a \approx b \prec c \\ c \prec a \prec b & a \approx c \prec b \\ c \prec b \prec a & b \approx c \prec a \\ & a \approx b \approx c \end{array} \right\} = \mathbb{P}$$



☺ Die totalen Prä/Ordnungen auf X entsprechen den Bijektionen $f : X \xrightarrow{\sim} \{1, \dots, n\}$ bzw. den Surjektionen $f : X \twoheadrightarrow \{1, \dots, k\}$.

(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

Ausführliche Erläuterungen bietet die Vollversion.

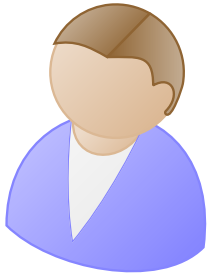
Efrons intransitive Würfel: Welcher ist der beste?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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

$$\mathbf{P}(A > B) = 12/36 = 1/3, \qquad \mathbf{P}(B > C) = 12/36 = 1/3,$$
$$\mathbf{P}(C > D) = 12/36 = 1/3, \qquad \mathbf{P}(D > A) = 12/36 = 1/3.$$

☺ Es gibt keinen „besten“ Würfel: Jeder wird vom nächsten geschlagen!

Untere und obere Schranken

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition I1G: untere und obere Schranken

Sei $(X, \leq)$ eine geordnete Menge (Poset), darin $U \subseteq X$ und $s \in X$.

$$s \text{ ist eine untere Schranke, } \quad s \leq U \quad :\Leftrightarrow \quad \forall x \in U : s \leq x$$

$$s \text{ ist eine obere Schranke, } \quad U \leq s \quad :\Leftrightarrow \quad \forall x \in U : x \leq s$$

Kleinste und größte Elemente

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition I1H: kleinste und größte Elemente

Sei $(X, \leq)$ eine geordnete Menge (Poset), darin $U \subseteq X$ und $s \in X$.

$$s \text{ ist kleinstes Element von } U \quad :\Leftrightarrow \quad s \in U \wedge s \leq U,$$

$$s \text{ ist größtes Element von } U \quad :\Leftrightarrow \quad s \in U \wedge U \leq s.$$

Minimale und maximale Elemente

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition I1ı: minimale und maximale Elemente

Sei $(X, \leq)$ eine geordnete Menge (Poset), darin $U \subseteq X$ und $s \in X$.

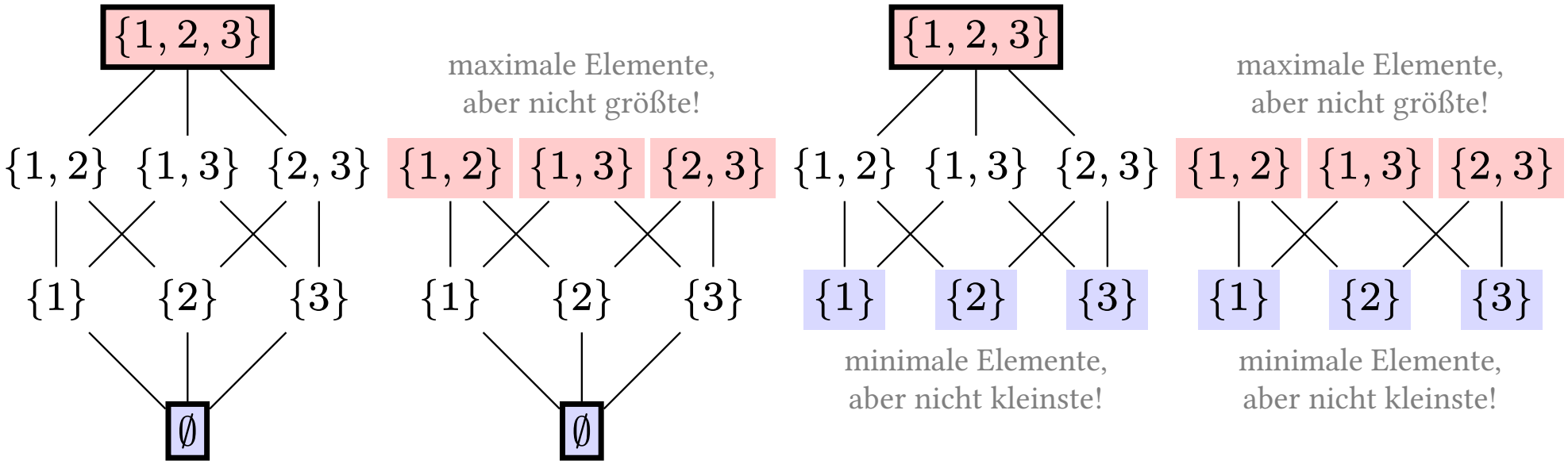
$$s \text{ ist minimal in } U \quad :\Leftrightarrow \quad s \in U \wedge \forall t \in U : t \leq s \Rightarrow t = s$$

$$s \text{ ist maximal in } U \quad :\Leftrightarrow \quad s \in U \wedge \forall t \in U : s \leq t \Rightarrow s = t$$

Minimale und maximale Elemente

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Aufgabe: Markieren Sie minimale Elemente blau, maximale rot. Rahmen Sie kleinste bzw. größte Elemente ein.

Verband und Vollständigkeit

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: In der Potenzmenge $\mathfrak{P}(\Omega)$ mit Inklusion $\subseteq$ gilt:

$$A \cap B = \inf\{A, B\}, \quad \text{allgemein} \quad \bigcap_{i \in I} A_i = \inf\{\, A_i \mid i \in I\}$$

$$A \cup B = \sup\{A, B\}, \quad \text{allgemein} \quad \bigcup_{i \in I} A_i = \sup\{\, A_i \mid i \in I\}$$

Monotone Abbildungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition I1o: isotone und antitone Abbildung

(1) Sei $f : (X, \leq) \to (Y, \preceq)$ eine Abbildung geordneter Mengen.

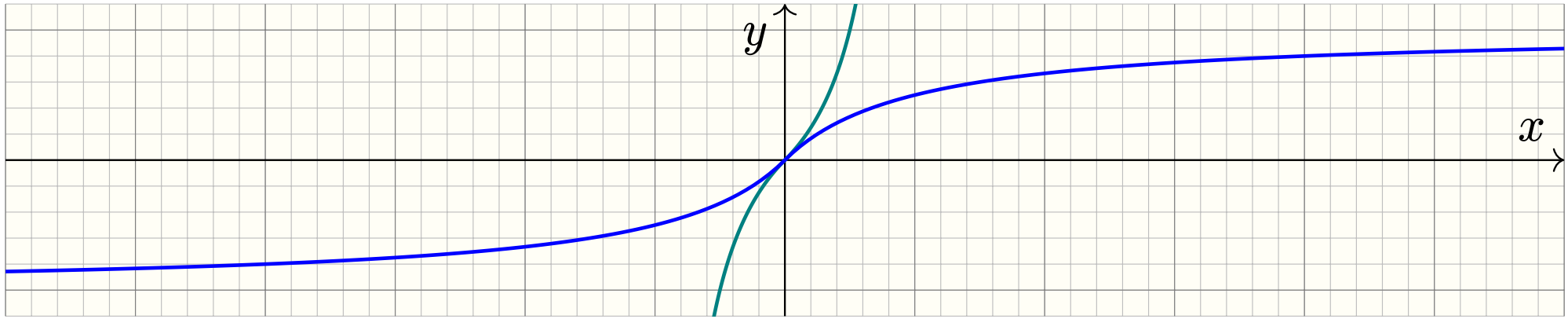
$$
\begin{aligned}
f \text{ ist isoton} \quad &:\Leftrightarrow \quad \forall a, b \in X : a \leq b \Rightarrow f(a) \preceq f(b) \\
f \text{ ist strikt isoton} \quad &:\Leftrightarrow \quad \forall a, b \in X : a < b \Rightarrow f(a) \prec f(b) \\
f \text{ ist antiton} \quad &:\Leftrightarrow \quad \forall a, b \in X : a \leq b \Rightarrow f(a) \succeq f(b) \\
f \text{ ist strikt antiton} \quad &:\Leftrightarrow \quad \forall a, b \in X : a < b \Rightarrow f(a) \succ f(b)
\end{aligned}
$$

(2) Ein (Ordnungs-)**Isomorphismus** $(f, g) : (X, \leq) \cong (Y, \preceq)$ ist ein ordnungserhaltendes Bijektionspaar, also $f : (X, \leq) \to (Y, \preceq)$ isoton und $g : (Y, \preceq) \to (X, \leq)$ isoton mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$.

Existiert ein Ordnungsisomorphismus $\mathbb{R} \cong \,]-1,1[$?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Beispiel I1P: Zahlengerade und Intervall

Es gilt $(\mathbb{R}, \leq) \cong (]-1,1[, \leq)$ vermöge des isotonen Bijektionspaars

$$f : \mathbb{R} \to \,]-1,1[\, : x \mapsto x/(1+|x|),$$
$$g : \,]-1,1[\, \to \mathbb{R} : y \mapsto y/(1-|y|).$$

Wir setzen dies fort auf $\bar{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$ durch $+\infty \mapsto +1$ und $-\infty \mapsto -1$:

$$(f_{\bar{\mathbb{R}}}, g_{\bar{\mathbb{R}}}) : (\bar{\mathbb{R}}, \leq) \cong ([-1,1]_{\mathbb{R}}, \leq)$$

Die natürlichen Zahlen sind wohlgeordnet.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz I2A: Die natürlichen Zahlen sind wohlgeordnet.

In $(\mathbb{N}, \leq)$ hat jede nicht-leere Teilmenge $U \subseteq \mathbb{N}$ ein kleinstes Element m.

Beweis: (1) Dank $U \neq \emptyset$ existiert ein Element $a \in U$, also gilt $(a+1) \not\leq U$.

(2) Es gibt ein Element $m \in \mathbb{N}$ mit $m \leq U$ und $(m+1) \not\leq U$. Andernfalls:
Für alle $n \in \mathbb{N}$ gilt $n \not\leq U \vee (n+1) \leq U$, also $n \leq U \Rightarrow (n+1) \leq U$.
Mit $0 \leq U$ folgt per Induktion $\mathbb{N} \leq U$, im Widerspruch zu (1).

(3) Für dieses Element $m \in \mathbb{N}$ gilt $m \in U$.
Andernfalls wäre $(m+1) \leq U$, im Widerspruch zu (2). QED

Wohlgeordnete Mengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition I2B: Wohlordnung

Eine geordnete Menge $(X, \leq)$ heißt **wohlgeordnet**, kurz *Woset*, falls jede nicht-leere Teilmenge $U \subseteq X$ ein kleinstes Element $s \in U$ besitzt, $s \leq U$.

Beispiel: Die natürlichen Zahlen $(\mathbb{N}, \leq)$ sind wohlgeordnet (Satz I2A). Hingegen sind $(\mathbb{Z}, \leq)$ und $(\mathbb{Q}, \leq)$ und $(\mathbb{R}, \leq)$ nicht wohlgeordnet.

Die Ordinalzahlen sind wohlgeordnet.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{aligned}
0 &= \emptyset = \bigcup \emptyset \quad \text{(Anfang / Limes)} \\
1 &= \{0\} \\
2 &= \{0 < 1\} \\
3 &= \{0 < 1 < 2\} \\
&\vdots \\
\omega &= \{0 < 1 < 2 < \ldots\} = \bigcup \omega \quad \text{(Limes)} \\
\omega + 1 &= \{0 < 1 < 2 < \ldots < \omega\} \\
\omega + 2 &= \{0 < 1 < 2 < \ldots < \omega < \omega + 1\} \\
&\vdots \\
\omega 2 &= \{0 < 1 < 2 < \ldots < \omega < \omega + 1 < \ldots\} = \bigcup \omega 2 \quad \text{(Limes)} \\
\omega 2 + 1 &= \{0 < 1 < 2 < \ldots < \omega < \omega + 1 < \ldots < \omega 2\} \\
\omega 2 + 2 &= \{0 < 1 < 2 < \ldots < \omega < \omega + 1 < \ldots < \omega 2 < \omega 2 + 1\} \\
&\vdots
\end{aligned}
$$

Die Klasse $\mathbf{Ord} \subseteq \mathcal{U}$ der Ordinalzahlen (G1E) ist wohlgeordnet (I2C).

Sind alle natürlichen Zahlen interessant?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Quatz I2D: interessante Zahlen

Jede natürliche Zahl ist interessant.

Beweis: Angenommen, es gäbe uninteressante natürliche Zahlen.
Dann gäbe es darunter eine kleinste… und die wäre interessant! QED

Quatz I2E: uninteressante Zahlen

Jede natürliche Zahl ist uninteressant.

Beweis: Angenommen, es gäbe interessante natürliche Zahlen.
Dann gäbe es darunter eine kleinste… doch wen interessiert das? QED

Sind die natürlichen Zahlen endlich? (Berry–Paradox)

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir nutzen das lateinische Alphabet `a,b,c,…,z,A,B,C,…,Z`, mit Ziffern `0,1,…,9` und Sonderzeichen. Insgesamt genügen uns 100 Zeichen.

Quatz I2F: Die natürlichen Zahlen sind endlich. (Berry–Paradox)

(1) Jede natürliche Zahl lässt sich mit höchstens 99 Zeichen definieren.
(2) Die Menge $\mathbb{N}$ ist daher endlich: Für ihre Elementezahl gilt $\sharp\mathbb{N} \leq 100^{99}$.

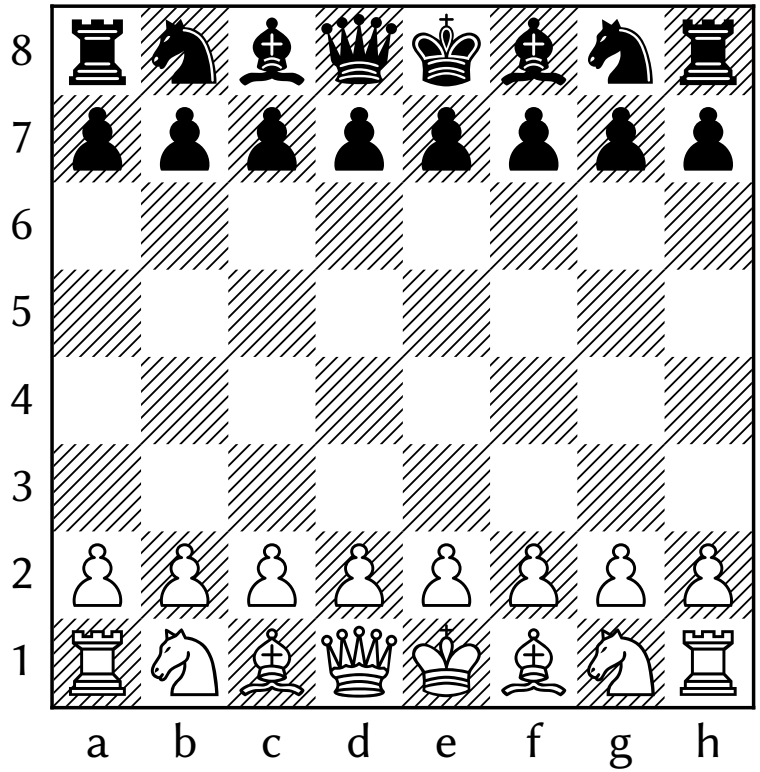
Beweis: (1) Angenommen, es gäbe natürliche Zahlen, die sich nur mit mehr als 99 Zeichen definieren lassen. Wir untersuchen die Kleinste:

`Die kleinste natürliche Zahl, die sich nur mit mehr als 99 Zeichen definieren lässt`

Diese Zahl haben wir soeben mit 83 Zeichen definiert. Widerspruch! QED

Hat Schach eine Gewinnstrategie? (Zermelo 1912)

Dies ist nur die Saalversion ohne Erläuterungen.



Die Relation $\to$ auf der Zustandsmenge X bezeichne legale Züge $s \to t$.
Sie erlaubt keine unendlichen Zugfolgen $s_0 \to s_1 \to \ldots$.

Jeder *Endzustand* t ist determiniert: Der Ziehende gewinnt, $u(t) := +1$, oder verliert, $u(t) := -1$, oder es endet unentschieden (remis), $u(t) := 0$.

Jeder *aktive Zustand* ist determiniert durch $u(s) := -\min\{\, u(t) \mid s \to t \,\}$.

☺ Insbesondere ist der Startzustand determiniert!

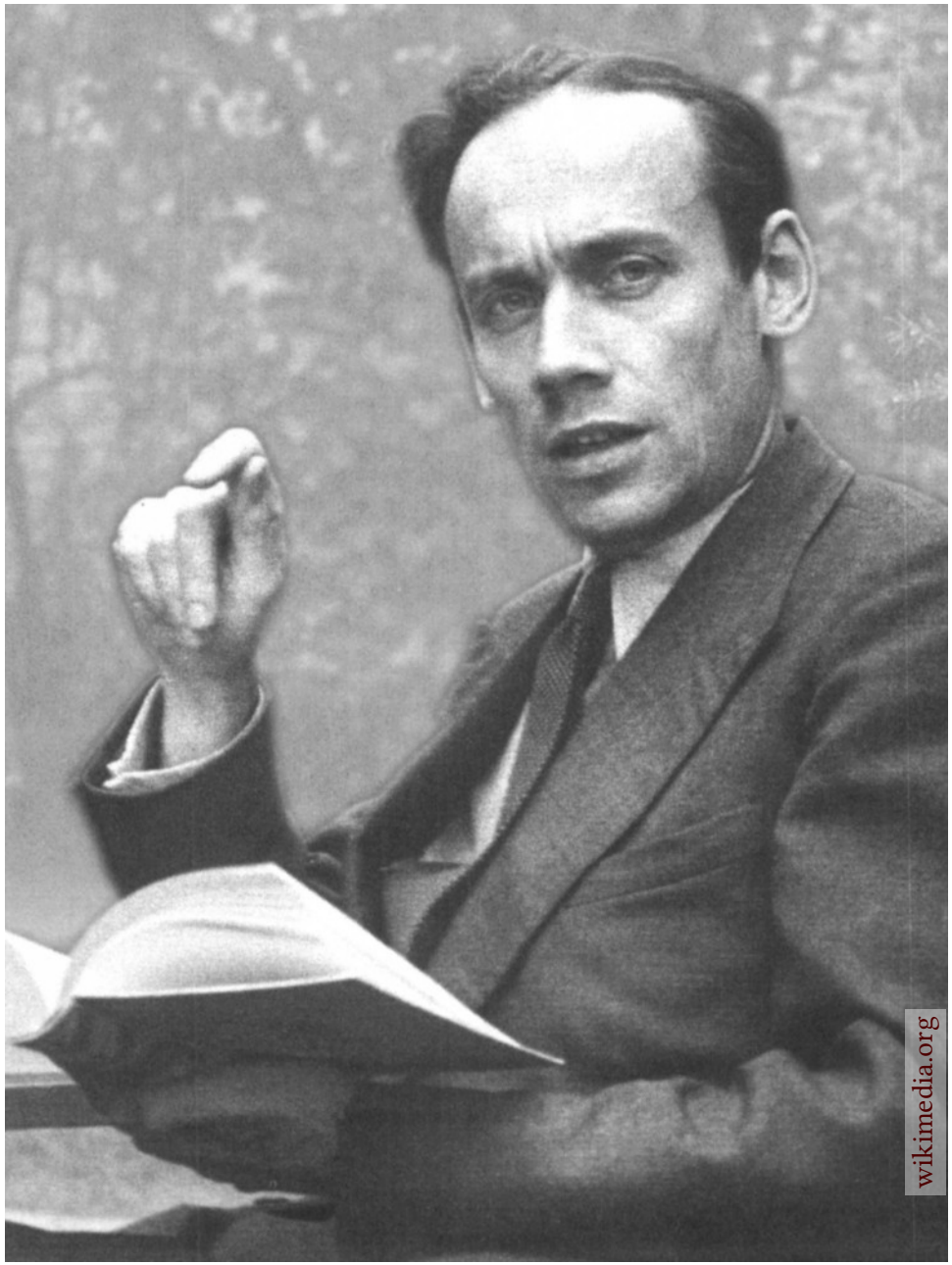
Ausführliche Erläuterungen bietet die Vollversion.

Induktive Beweise und rekursive Konstrukionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Emmy Noether (1882–1935)



Emil Artin (1898–1962)

Artinsche Graphen und noethersche Induktion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei (X, R) eine Menge X mit Relation $R \subseteq X^2$. Für $(t, s) \in R$ schreiben wir $t \prec s$ „kleiner“, $s \succ t$ „größer“ oder $s \to t$ „über“, $t \leftarrow s$ „unter“.

Definition I2G: artinsch aka wohlfundiert

Ein **unendlicher Abstieg** ist eine Kette $s_0 \to s_1 \to s_2 \to s_3 \to \dots$.
Wir nennen $(X, \leftarrow)$ **artinsch**, falls es keinen unendlichen Abstieg gibt.

Beispiel: $(\mathbb{N}, <)$ ist artinsch, nicht jedoch $(\mathbb{Z}, <)$, ebensowenig $([0, 1], <)$.

Satz I2H: noethersche Induktion

Sei $(X, \leftarrow)$ artinsch. Um für jedes $s \in X$ die Aussage $A(s)$ zu beweisen, genügt schon der Induktionschritt: Gilt $A(t)$ für alle $t \leftarrow s$, so folgt $A(s)$.

Beweis: Angenommen, es existiert ein Gegenbeispiel $s_0 \in X$ mit $\neg A(s_0)$.
Per Induktionschritt, contraponiert, existiert ein $s_1 \leftarrow s_0$ und $\neg A(s_1)$.
So fortfahrend erhalten wir $s_0 \to s_1 \to s_2 \to \dots$. Widerspruch! QED

Artins Prinzip des kleinsten Verbrechers

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dramatisch: Wir fürchten ein Gegenbeispiel $s_0 \in X$ mit $\neg A(s_0)$.
Gibt es ein kleineres $s_1 \leftarrow s_0$ mit $\neg A(s_1)$, so wählen wir dies.
So fortfahrend erreichen wir, da $(X, \leftarrow)$ artinsch ist,
schließlich einen „kleinsten Verbrecher“ $s \in X$.
Für alle $t \leftarrow s$ gilt $A(t)$. Der Induktionsschritt
garantiert $A(s)$. Es gibt gar keinen Verbrecher!

(I) Per *Induktion* I2H beweisen wir Aussagen $A(s)$ für alle $s \in X$.
(R) Per *Rekursion* I2I konstruieren wir Abbildungen $f : X \to Z$.

Beispiel: Es gibt $f : \mathbb{N} \to \mathbb{N}$ mit $f(0) = 1$ und $f(n) = n \cdot f(n-1)$ für $n \geq 1$,
$F : \mathbb{N} \to \mathbb{N}$ mit $F(0) = F(1) = 1$ und $F(n) = F(n-1) + F(n-2)$ für $n \geq 2$.

Der Wohlordnungssatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Die Menge $\mathbb{Z}$ lässt sich wohlordnen, etwa durch

$$(\mathbb{Z}, \preceq_1) = \{0 \prec 1 \prec -1 \prec 2 \prec -2 \prec 3 \prec -3 \prec \ldots\} \cong \omega \quad \text{oder}$$
$$(\mathbb{Z}, \preceq_2) = \{0 \prec 1 \prec 2 \prec 3 \prec \ldots \prec -1 \prec -2 \prec -3 \prec \ldots\} \cong \omega 2.$$

Satz I2L: Wohlordnungssatz (in ZFC)

Auf jeder Menge X existiert eine Wohlordnung $\leq$.

Das Lemma von Zorn

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz I2M: Max Zorn 1933, Kuratowski 1922, Hausdorff 1914 (in ZFC)

Sei $(X, \leq)$ eine geordnete Menge (Poset), in der jede Kette $K \subseteq X$ eine obere Schranke besitzt, also $s \in X$ mit $K \leq s$ existiert. Dann enthält $(X, \leq)$ ein maximales Element, also $m \in X$ mit $\nexists x \in X : m < x$.

Wie vergleichen wir die Größe von Mengen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition I3A: Mächtigkeit von Mengen

1. Äquipotenz $X \cong Y$ bedeutet, es existiert eine Bijektion $(h, k) : X \cong Y$.
2. Die Relation $X \preceq Y$ bedeutet, es existiert eine Injektion $f : X \hookrightarrow Y$.

Gilt $X \cong \{1, \dots, n\}$, so ist X **endlich**, mit Elementezahl $\sharp X = n$.
Gilt $X \cong \mathbb{N}$, so nennen wir die Menge X **abzählbar unendlich**.
Abzählbar bedeutet $X \preceq \mathbb{N}$, andernfalls ist X **überabzählbar**.

Fundamentales Beispiel: endliche Mengen

$$\{1, \dots, m\} \cong \{1, \dots, n\} \quad \Leftrightarrow \quad m = n$$
$$\{1, \dots, m\} \preceq \{1, \dots, n\} \quad \Leftrightarrow \quad m \leq n$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: effizienter Vergleich ohne Abzählen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Im Hörsaal sind höchstens so viele Personen X wie Sitze Y.
Dazu muss ich weder X noch Y zählen... Hinsetzen $X \hookrightarrow Y$ genügt!

Beispiel: Galileis Paradox (1638)

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Ist die Menge $Q = \{0, 1, 4, 9, 16, 25, \dots\}$ der Quadratzahlen kleiner als die Menge $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$ der natürlichen Zahlen?

Lösung: (1) Im Sinne der Mengeninklusion gilt offensichtlich $Q \subsetneq \mathbb{N}$.
(2) Wir haben die Bijektion $(h, k) : \mathbb{N} \cong Q$ mit $h(x) = x^2$ und $k(y) = \sqrt{y}$.

Der Äquivalenzsatz von Cantor–Bernstein

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz I3B: Cantor–Bernstein, $X \preceq Y \wedge Y \preceq X \Rightarrow X \cong Y$

Aus $f : X \hookrightarrow Y$ und $g : Y \hookrightarrow X$ können wir $(h, k) : X \cong Y$ konstruieren.

Jedes Element $x_0 \in X$ hat seine Urbildkette $x_0 \overset{g}{\leftarrowtail} y_1 \overset{f}{\leftarrowtail} x_2 \overset{g}{\leftarrowtail} y_3 \overset{f}{\leftarrowtail} \dots$ maximaler Länge $n \in \mathbb{N} \cup \{\infty\}$. Die Elemente der Länge n bilden die Teilmenge $X_n \subseteq X$. Entsprechend definieren wir $Y_n \subseteq Y$. Wir erhalten:

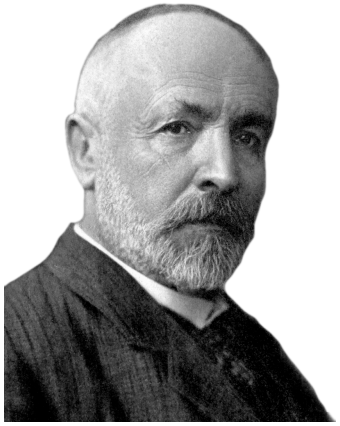
$$\begin{tikzcd}
X \arrow[d, bend right, "f"'] & = & X_0 \arrow[dr, "f_0"] & \sqcup & X_1 \arrow[dr, "g_0"] & \sqcup & X_2 \arrow[dr, "f_1"] & \sqcup & X_3 \arrow[dr, "g_1"] & \sqcup & \dots \arrow[dr, "f_2"] & \sqcup & X_\infty \arrow[d, bend left, "g_\infty"] \\
Y \arrow[u, bend right, "g"'] \arrow[u, phantom, "\text{inj}"] & = & Y_0 \arrow[ur, "g_3"] & \sqcup & Y_1 \arrow[ur, "f_3"] & \sqcup & Y_2 \arrow[ur, "g_4"] & \sqcup & Y_3 & \sqcup & \dots & \sqcup & Y_\infty \arrow[u, bend left, "f_\infty"]
\end{tikzcd}$$

Cantors Reißverschluss: Wir konstruieren daraus $(h, k) : X \cong Y$ vermöge $h = f_0 \sqcup g_0^{-1} \sqcup f_2 \sqcup g_2^{-1} \sqcup \dots \sqcup f_\infty$ und $k = g_0 \sqcup f_0^{-1} \sqcup g_2 \sqcup f_2^{-1} \sqcup \dots \sqcup f_\infty^{-1}$.

Mächtigkeit des Produkts $\mathbb{N} \times \mathbb{N}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Georg Cantor
(1845–1918)

$(0,4) \mapsto 10$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	…
$(0,3) \mapsto 6$	$(1,3) \mapsto 11$	$(2,3)$	$(3,3)$	$(4,3)$	…
$(0,2) \mapsto 3$	$(1,2) \mapsto 7$	$(2,2) \mapsto 12$	$(3,2)$	$(4,2)$	…
$(0,1) \mapsto 1$	$(1,1) \mapsto 4$	$(2,1) \mapsto 8$	$(3,1)$	$(4,1)$	…
$(0,0) \mapsto 0$	$(1,0) \mapsto 2$	$(2,0) \mapsto 5$	$(3,0) \mapsto 9$	$(4,0)$	…

Carl-Friedrich Gauß
(1777–1855)

Es existieren Bijektionen $(f, g) : \mathbb{N}^2 \cong \mathbb{N}$. Sogar verblüffend elegant:

Satz I3G: Cantors erstes Diagonalargument

Die Abbildung $f : \mathbb{N}^2 \to \mathbb{N} : (a, b) \mapsto a + (a + b)(a + b + 1)/2$ ist bijektiv.

Abzählbare Vereinigung abzählbarer Mengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz I3H: abzählbare Vereinigung abzählbarer Mengen

Jede abzählbare Vereinigung abzählbarer Mengen ist abzählbar.

Beweis: Gegeben seien $f : I \hookrightarrow \mathbb{N}$ und $g_i : A_i \hookrightarrow \mathbb{N}$ für jedes $i \in I$.

$$\begin{tikzcd}
A = \bigcup_{i\in I} A_i \arrow[r, hook, dashed, "h"] \arrow[d, two heads, shift right, "\mathrm{pr}_2"'] & \mathbb{N} \\
A' = \bigsqcup_{i\in I}\{i\} \times A_i \arrow[u, hook, shift right, "r"'] \arrow[r, hook, "(i,a_i)\mapsto(f(i),g_i(a_i))"] & \mathbb{N}\times\mathbb{N} \arrow[u, hook, "\mathrm{I3G}"']
\end{tikzcd}$$

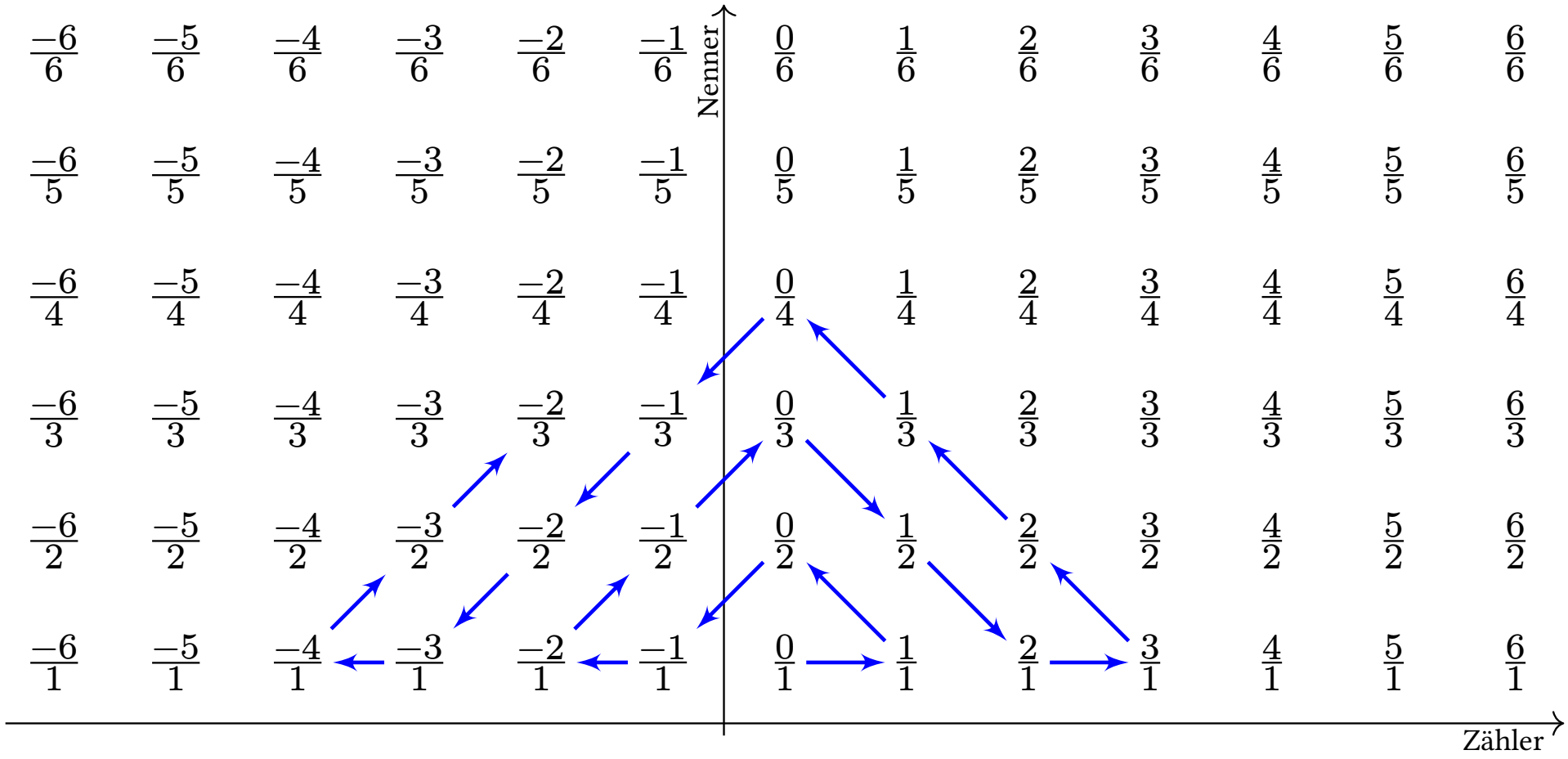
Beispiel: Abzählbar sind $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ und $\mathbb{Q} = \bigcup_{n\in\mathbb{N}^*}\{\, z/n \mid z \in \mathbb{Z}\,\}$.

Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Dies ist nur die Saalversion ohne Erläuterungen.

Satz I3J: Mächtigkeit von $\mathbb{Q}$

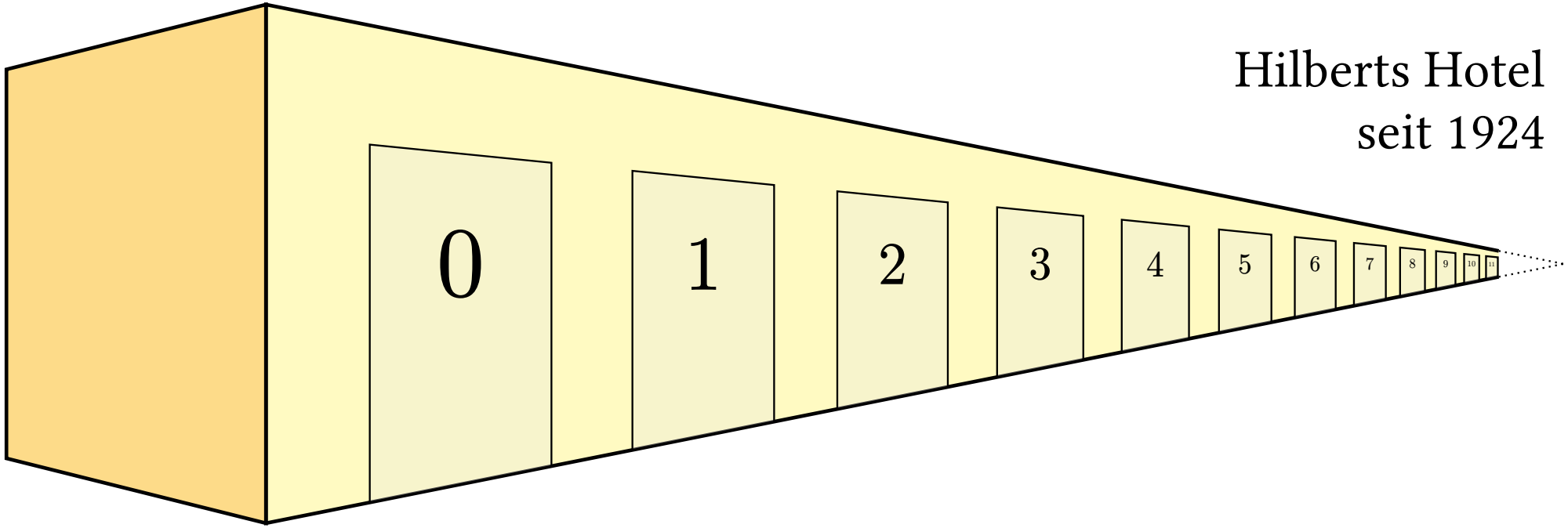
Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar unendlich, kurz $\mathbb{Q} \cong \mathbb{N}$.



Ausführliche Erläuterungen bietet die Vollversion.

Hilberts Hotel — Platz in der Herberge!

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 $\mathbb{N}^2 \hookrightarrow \mathbb{N} : (a, b) \mapsto a + (a + b)(a + b + 1)/2$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Hilberts Hotel — sagenhaft, gesungen!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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 — sagenhaft, gesungen!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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!"

Mächtigkeit der Potenzmenge

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Cantors zweites Diagonalargument: Kann $f : X \to \mathfrak{P}(X)$ surjektiv sein? Nein! Gegeben sei eine beliebige Funktion $f : X \to \mathfrak{P}(X)$. Wir betrachten

$$A := \{ x \in X \mid x \notin f(x) \} \subseteq X.$$

Gilt $A \in \operatorname{Im}(f)$? Angenommen $x \in X$ erfüllt $f(x) = A$. Es gibt zwei Fälle:
(1) Aus $x \in A$ folgt $x \notin f(x) = A$. ↯ (2) Aus $x \notin A$ folgt $x \in f(x) = A$. ↯
Demnach existiert kein $x \in X$ mit $f(x) = A$, also $A \in \mathfrak{P}(X) \setminus \operatorname{Im}(f)$.

Satz I3L: Cantors zweites Diagonalargument

Zu jeder Menge X ist die Potenzmenge $\mathfrak{P}(X)$ mächtiger, kurz $X \prec \mathfrak{P}(X)$.

Beweis: Wir haben $X \hookrightarrow \mathfrak{P}(X) : x \mapsto \{x\}$, aber $X \not\cong \mathfrak{P}(X)$ wie oben. QED

Beispiele: Zu $\mathbb{N}$ ist die Potenzmenge $\mathfrak{P}(\mathbb{N}) \cong \{0,1\}^{\mathbb{N}}$ überabzählbar!
Noch mächtiger als $\mathbb{N}$ ist $\mathfrak{P}(\mathbb{N})$ dann $\mathfrak{P}\mathfrak{P}(\mathbb{N})$ und dann $\mathfrak{P}\mathfrak{P}\mathfrak{P}(\mathbb{N})$ usw.

Entwicklung reeller Zahlen in Basis B

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $B \in \mathbb{N}_{\geq 2}$, etwa binär $B = 2$, ternär $B = 3$ oder dezimal $B = 10$:

$$\pi = 3.14159\,26535\,89793\,23846\,26433\,83279\ \ldots$$
$$0.1 = 0.09999\,99999\,99999\,99999\,99999\,99999\ \ldots$$

♦ Satz E1F: B–adische Entwicklung als Retraktion $(q, r) : \mathbb{Z}_B^{\mathbb{N}} \rightleftarrows [0, 1]$

(0) Jede Ziffernfolge $a = (a_0, a_1, a_2, \ldots) \in \mathbb{Z}_B^{\mathbb{N}}$ definiert eine reelle Zahl

$$x = q(a) := \sum_{k=0}^{\infty} a_k B^{-k-1} \quad \in \quad [0, 1].$$

$$q_B \ : \ \mathbb{Z}_B^{\mathbb{N}} \twoheadrightarrow [0, 1] \ : \ a \mapsto x$$

$$r_B \ : \ [0, 1] \hookrightarrow \mathbb{Z}_B^{\mathbb{N}} \ : \ x \mapsto a$$

Mächtigkeit der reellen Zahlen $\mathbb{R}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz I3M: Mächtigkeit von $\mathbb{R}$

(1) Die Menge $\mathbb{R}$ ist überabzählbar, genauer gilt $\mathbb{R} \cong \{0,1\}^{\mathbb{N}} \cong \mathfrak{P}(\mathbb{N})$.
(2) In jeder Dimension $d \in \mathbb{N}_{\geq 1}$ gilt somit $\mathbb{R} \cong \mathbb{R}^d \cong \mathbb{R}^{\mathbb{N}} = \{\, f : \mathbb{N} \to \mathbb{R} \,\}$.
(3) Strikt mächtiger sind hingegen $\mathfrak{P}(\mathbb{R}) \cong \{0,1\}^{\mathbb{R}} \subset \mathbb{R}^{\mathbb{R}} = \{\, f : \mathbb{R} \to \mathbb{R} \,\}$.

Beweis: (1) Wir konstruieren Injektionen $\mathbb{R} \hookrightarrow \{0,1\}^{\mathbb{N}}$ und $\{0,1\}^{\mathbb{N}} \hookrightarrow \mathbb{R}$; Cantor–Bernstein I3B konstruiert daraus eine Bijektion $\mathbb{R} \cong \{0,1\}^{\mathbb{N}}$.

Explizit: (1a) Wir haben $f : \mathbb{R} \xrightarrow{\sim} \,]-1,+1[\, : x \mapsto x/(1+|x|)$ (B1H) sowie $g : \,]-1,+1[\, \xrightarrow{\sim} \,]0,1[\, : x \mapsto (x+1)/2$. Die Binärentwicklung stiftet die Injektion $r_2 : \,]0,1[\, \hookrightarrow \{0,1\}^{\mathbb{N}}$ dank Satz E1F für $B = 2$.

(1b) Satz E1F für $B = 3$ stiftet $q_3 : \{0,1,2\}^{\mathbb{N}} \supset \{0,1\}^{\mathbb{N}} \hookrightarrow \,]0,1[\, \subset \mathbb{R}$.

(2) Wir haben Bijektionen $\mathbb{N} \cong \mathbb{N} \times \{1,\dots,d\} \cong \mathbb{N} \times \mathbb{N}$. Aus $\mathbb{R} \cong \{0,1\}^{\mathbb{N}}$ folgt $\mathbb{R}^d \cong \{0,1\}^{\mathbb{N}\times\{1,\dots,d\}} \cong \{0,1\}^{\mathbb{N}}$ und $\mathbb{R}^{\mathbb{N}} \cong \{0,1\}^{\mathbb{N}\times\mathbb{N}} \cong \{0,1\}^{\mathbb{N}}$. $\boxed{\text{QED}}$

Turing: Lässt sich jede reelle Zahl berechnen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means.

Alan Turing fragte 1936: Können wir jede reelle Zahl $x \in \mathbb{R}$ berechnen?
Nein! Es gibt nur abzählbar viele Programme, doch $\mathbb{R}$ ist überabzählbar.

Das Alphabet $\mathscr{A}$ ist abzählbar, somit auch die Menge $\mathscr{A}^* := \bigsqcup_{n \in \mathbb{N}} \mathscr{A}^n$.

Cantor: algebraische vs transzendente Zahlen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Ist jede Zahl $\alpha \in \mathbb{R}$ Nullstelle eines rationalen Polynoms $A \in \mathbb{Q}[X]^*$?
Nein! Es gibt nur abzählbar viele rationale Polynome und Nullstellen.

Abzählbar ist $\mathbb{Q}$, somit $\mathbb{Q}[X] = \bigcup_{n\in\mathbb{N}} \mathbb{Q}[X]_{<n}$ und $\mathbb{A} := \bigcup_{P\in\mathbb{Q}[X]^*} P^{-1}(\{0\})$.

Cantor: algebraische vs transzendente Zahlen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz I3o: Die algebraischen Zahlen sind abzählbar.

Eine reelle Zahl $\alpha \in \mathbb{R}$ heißt **algebraisch** über $\mathbb{Q}$, wenn sie Nullstelle eines rationalen Polynoms $P \in \mathbb{Q}[X]^*$ ist. Andernfalls heißt α **transzendent**.

$$\mathbb{A} := \bigcup_{P \in \mathbb{Q}[X]^*} \{\, \alpha \in \mathbb{R} \mid P(\alpha) = 0 \,\}$$

Die Menge $\mathbb{A} \subseteq \mathbb{R}$ der algebraischen Zahlen ist abzählbar, kurz $\mathbb{A} \cong \mathbb{N}$. Somit ist das Komplement $\mathbb{T} = \mathbb{R} \smallsetminus \mathbb{A}$ überabzählbar, genauer $\mathbb{T} \cong \mathbb{R}$.

Beweis: Die Menge aller Polynome vom Grad $< n$ ist abzählbar:

$$\mathbb{Q}[X]_{<n} \underset{\text{Def}}{\cong} \mathbb{Q}^n \underset{\text{I3J}}{\cong} \mathbb{N}^n \underset{\text{I3I}}{\cong} \mathbb{N}$$

Demnach ist auch der Polynomring $\mathbb{Q}[X] = \bigcup_{n \in \mathbb{N}} \mathbb{Q}[X]_{<n}$ abzählbar (I3H). Jedes Polynom $P \in \mathbb{Q}[X]^*$ hat in $\mathbb{R}$ eine endliche Nullstellenmenge (C2C). Somit ist $\mathbb{A}$ abzählbar (I3H). Mit $\mathbb{N} \subseteq \mathbb{A}$ folgt $\mathbb{A} \cong \mathbb{N}$ (I3B). QED

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel I

Bonusmaterial

The two most engaging powers of an author are to make new things familiar and familiar things new.

Samuel Johnson (1709–1784)

Inhalt dieses Kapitels I

5 Isomorphiespiele: Samson vs Delila

6 Hausdorff: die Ordnung der rationalen Zahlen $(\mathbb{Q}, \leq)$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Isomorphiespiele: Samson gegen Delila

Samson und Dalila, Gemälde von Peter Paul Rubens um 1610, National Gallery London

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Isomorphiespiele: Samson gegen Delila

Dies ist nur die Saalversion ohne Erläuterungen.

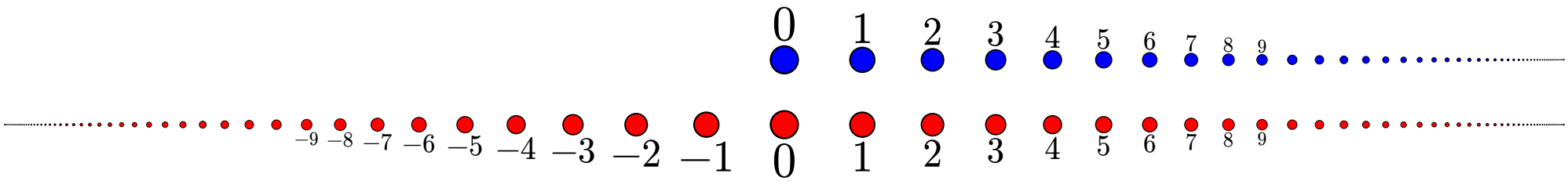
Ausführliche Erläuterungen bietet die Vollversion.

$$X = \{0 < 1 < 2 < 3 < 4 < 5 < 6 < 7\}$$
$$Y = \{0 < 1 < 2 < 3 < 4 < 5 < 6 < 7 < 8 < 9\}$$

In Runde $n = 1, 2, 3, \dots$ ziehen die Spieler Elemente $(a_n, b_n) \in X \times Y$:
(0) Verfügbar sind $X_n = X \setminus \{a_1, \dots, a_{n-1}\}$ und $Y_n = Y \setminus \{b_1, \dots, b_{n-1}\}$.
(1) Samson (*spoiler*) wählt ein Element, entweder $a_n \in X_n$ oder $b_n \in Y_n$.
(2) Delila (*duplicator*) wählt komplementär dazu $b_n \in Y_n$ oder $a_n \in X_n$.

Dabei muss stets Monotonie gelten, also $a_i < a_j \Leftrightarrow b_i < b_j$ für alle i, j.
Samson bekommt anfangs 5€ und zahlt 1€ an Delila für jede Antwort.

Isomorphiespiele: Samson gegen Delila



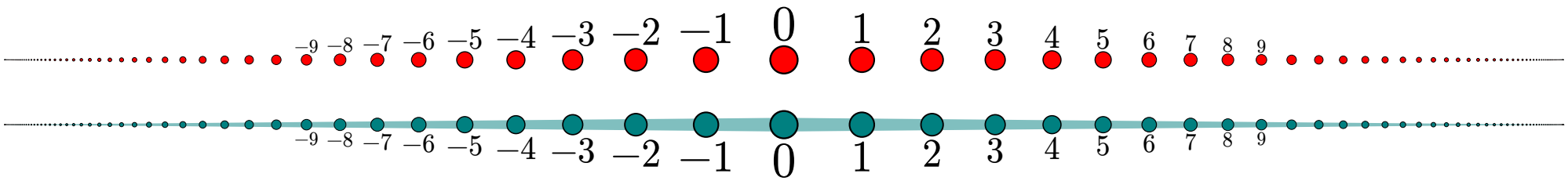
Wir spielen $(\mathbb{N}, \leq)$ gegen $(\mathbb{Z}, \leq)$. Samsons Gewinnstrategie als Formel:

$$\exists a_1 \in \mathbb{N} \;\; \forall a_2 \in \mathbb{N} : a_1 \leq a_2$$
$$\forall b_1 \in \mathbb{Z} \;\; \exists b_2 \in \mathbb{Z} \;\; : b_1 > b_2$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Isomorphiespiele: Samson gegen Delila



Wir spielen $(\mathbb{Z}, \leq)$ gegen $(\mathbb{Q}, \leq)$. Samsons Gewinnstrategie als Formel:

$$\exists a_1 \in \mathbb{Z}\ \ \exists a_2 \in \mathbb{Z}\ \ \forall a_3 \in \mathbb{Z} : [\, a_1 < a_2 \ \wedge\ (a_1 \geq a_3 \ \vee\ a_3 \geq a_2)\,]$$

$$\forall b_1 \in \mathbb{Q}\ \ \forall b_2 \in \mathbb{Q}\ \ \exists b_3 \in \mathbb{Q} : [\, b_1 \geq b_2 \ \vee\ (b_1 < b_3 \ \wedge\ b_3 < b_2)\,]$$

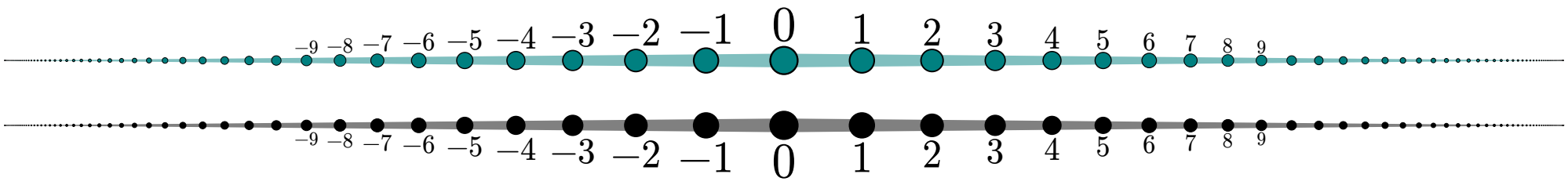
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Isomorphiespiele: Samson gegen Delila

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



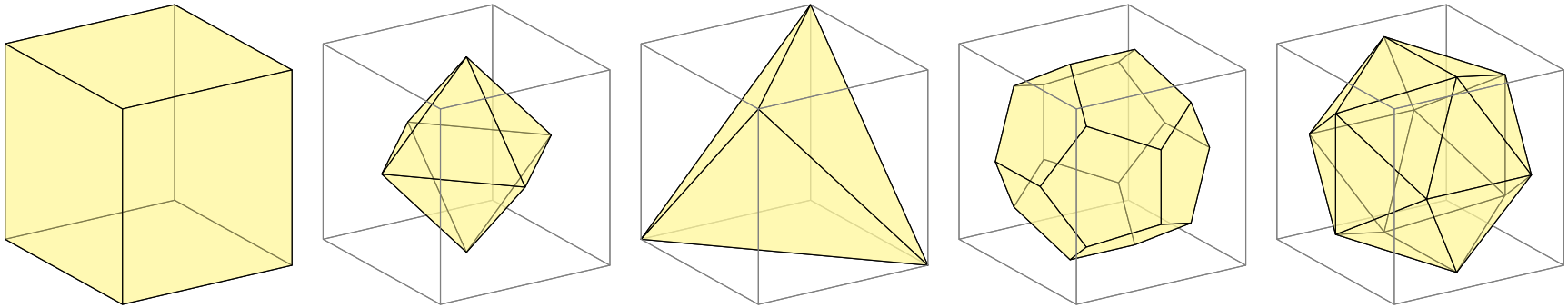
Wir spielen $(\mathbb{Q}, \leq)$ gegen $(\mathbb{R}, \leq)$. Hier kommt das Spiel nie zum Ende!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel J

Monoide und Gruppen



Wherever groups disclosed themselves, or could be introduced, simplicity crystallized out of comparative chaos.

Eric Temple Bell (1883–1960)

Inhalt dieses Kapitels J

1 Richtig rechnen!

2 Struktur erhalten!

3 Gruppen wollen operieren!

4 Quotientengruppen und Homomorphiesatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Monoide und Gruppen: Grundlage des Rechnens

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vertraute Beispiele:

$$(\mathbb{Z}, +, 0, -), \quad (\mathbb{Q}, +, 0, -), \quad (\mathbb{R}, +, 0, -), \quad (\mathbb{C}, +, 0, -), \quad \ldots$$
$$(\mathbb{Z}, \cdot, 1), \quad (\mathbb{Q}, \cdot, 1), \quad (\mathbb{R}, \cdot, 1), \quad (\mathbb{C}, \cdot, 1), \quad \ldots$$

Rechenrenegeln für jede **Gruppe** $(G, *, e, ')$ und ihre Elemente $a, b, c \in G$:

Assoziativität:	$(a * b) * c = a * (b * c)$
Neutrales:	$a * e = a = e * a$
Inverse:	$a * a' = e = a' * a$

Ohne die Inversion $'$ zu verlangen, haben wir nur ein **Monoid** $(G, *, e)$.

Was ist eine Verknüpfung?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J1A: Verknüpfung

Jede Abbildung

$$* : A \times B \to C : (a, b) \mapsto c = a * b = ab$$

nennen wir eine **Verknüpfung** oder **Operation**.

$*$	b_1	…	b_j	…
a_1	$a_1 * b_1$	…	$a_1 * b_j$	…
$\vdots$	$\vdots$		$\vdots$	
a_i	$a_i * b_1$	…	$a_i * b_j$	…
$\vdots$	$\vdots$		$\vdots$	

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

Grundrechenarten sind Verknüpfungen.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{array}{lll}
\text{Addition} & + : \mathbb{K} \times \mathbb{K} \to \mathbb{K} : (a,b) \mapsto a + b, \\
\text{Subtraktion} & - : \mathbb{K} \times \mathbb{K} \to \mathbb{K} : (a,b) \mapsto a - b, \\
\text{Multiplikation} & \cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K} : (a,b) \mapsto a \cdot b, \\
\text{Division} & / : \mathbb{K} \times \mathbb{K}^\times \to \mathbb{K} : (a,b) \mapsto a \,/\, b.
\end{array}
$$

$$
\begin{array}{ll}
3 - 5 \neq 5 - 3, & (8-4)-2 \neq 8-(4-2), \\
3 \,/\, 5 \neq 5 \,/\, 3, & (8 \,/\, 4) \,/\, 2 \neq 8 \,/\, (4 \,/\, 2).
\end{array}
$$

Was ergibt $25 - 5 \,/\, 5$? Die Antwort ist 4!.

Verknüpfung von Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\bullet : \mathbb{K}^{p\times q} \times \mathbb{K}^{q\times r} \to \mathbb{K}^{p\times r} : (A, B) \mapsto C = A \bullet B, \quad c_{ik} = \sum_{j=1}^{q} a_{ij} \cdot b_{jk}$$

So formulieren wir lineare Gleichungssysteme bequem als $Ax = y$.
Ist A invertierbar, so existiert genau ein Lösung, nämlich $x = A^{-1}y$.

Kommutieren und Zentrum

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J1D: Kommutieren und Zentrum

Sei $* : A \times A \to C$. Elemente $x, y \in A$ **kommutieren**, falls $x * y = y * x$. Gilt dies für alle $x, y \in A$, so ist die Verknüpfung $*$ **kommutativ**.

Ein Element $z \in A$ ist **zentral**, falls es mit allen $x \in A$ kommutiert.

$$Z(A, *) := \left\{ z \in A \,\middle|\, \forall x \in A : x * z = z * x \right\}$$

Beispiel: $Z(\mathbb{K}^{n \times n}, \cdot) = \left\{ \lambda \cdot 1_{n \times n} \,\middle|\, \lambda \in Z(\mathbb{K}, \cdot) \right\}$.

Assoziativität vereinfacht!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Drei Faktoren können wir auf genau zwei Weisen klammern:

$$(ab)c \quad \text{und} \quad a(bc)$$

Vier Faktoren können wir auf genau fünf Weisen klammern:

$$((ab)c)d, \quad (a(bc))d, \quad (ab)(cd), \quad a((bc)d), \quad a(b(cd))$$

Satz J1F: Umklammern und Umordnen

(1) Eine Verknüpfung $* : A \times A \to A$ heißt **assoziativ**, falls

$$(a * b) * c = a * (b * c)$$

für alle $a, b, c \in A$ gilt. In diesem Falle ist jedes Produkt $a_1 * a_2 * \cdots * a_n$ klammerunabhängig: Jede Klammerung führt zum selben Ergebnis.

(2) Kommutieren zudem die Faktoren $a_1, a_2, \ldots, a_n$ in $(A, *)$ paarweise, so können wir sie beliebig umordnen, ihr Produkt bleibt dabei gleich.

Umklammern und Umordnen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Anwendungsbeispiel: Wir suchen eine geschlossene Formel für

$$S(n) \;:=\; \textstyle\sum_{k=1}^{n} k.$$

Dank Assoziativität und Kommutativität erhalten wir

$$\begin{aligned} 2S(n) &= (1+2+\cdots+n-1+n)+(1+2+\cdots+n-1+n) \\ &= (1+2+\cdots+n-1+n)+(n+n-1+\cdots+2+1) \\ &= (1+n)+(2+n-1)+\cdots+(n-1+2)+(n+1) \;=\; n(n+1) \end{aligned}$$

Komplexoperation: elementweise Verknüpfung von Mengen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{aligned} 2\mathbb{N} &= 2\cdot\mathbb{N} &&:= \{2\cdot n \,|\, n\in\mathbb{N}\} &&= \{0,2,4,6,8,\dots\} \\ 2\mathbb{N}+1 &= 2\cdot\mathbb{N}+1 &&:= \{2\cdot n+1 \,|\, n\in\mathbb{N}\} &&= \{1,3,5,7,9,\dots\} \end{aligned}$$

Definition J1G: Komplexoperation

$$\begin{aligned} * &: A \times B \to C : (a,b) \mapsto a*b \quad \text{setzen wir fort zu} \\ \boxed{*} &: A \times \mathfrak{P}(B) \to \mathfrak{P}(C) : (a,T) \mapsto a \boxed{*} T := \{a*b \,|\, b\in T\}, \\ \boxed{*} &: \mathfrak{P}(A) \times B \to \mathfrak{P}(C) : (S,b) \mapsto S \boxed{*} b := \{a*b \,|\, a\in S\}, \\ \boxed{*} &: \mathfrak{P}(A) \times \mathfrak{P}(B) \to \mathfrak{P}(C) : (S,T) \mapsto S \boxed{*} T := \{a*b \,|\, a\in S,\ b\in T\}. \end{aligned}$$

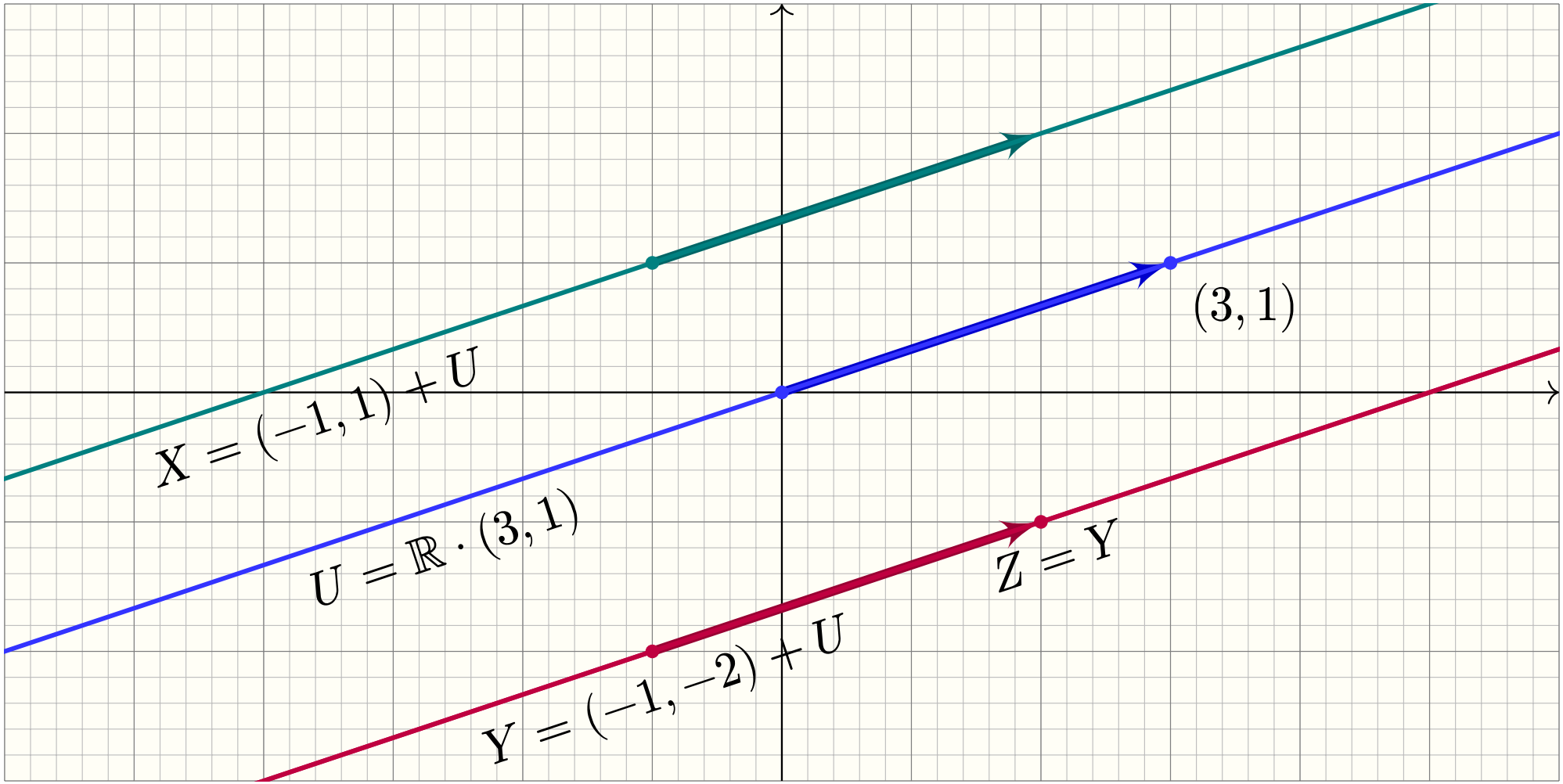
Beispiel: Es gilt $\mathbb{N}+\mathbb{N}=\mathbb{N}$ und $\mathbb{N}-\mathbb{N}=\mathbb{Z}$ und $\mathbb{N}_{\geq 2} \setminus (\mathbb{N}_{\geq 2}\cdot\mathbb{N}_{\geq 2}) = \mathbb{P}$.

Komplexoperation: erste geometrische Anwendungen

Dies ist nur die Saalversion ohne Erläuterungen.

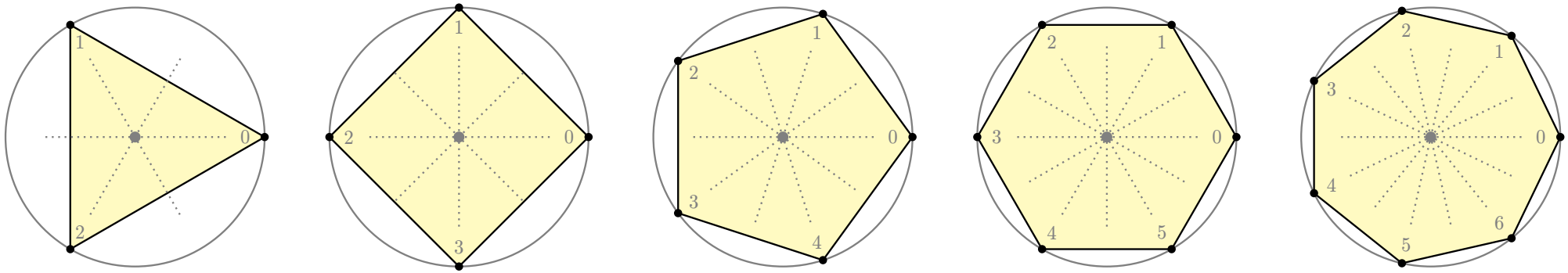
Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Zeichnen Sie in der Ebene $\mathbb{R}^2$ die Menge $U = \mathbb{R} \cdot (3,1)$ sowie $X = (-1,1) + U$ und $Y = (-1,-2) + U$ und $Z = (+2,-1) + U$.



Die Diedergruppe als Isometrien des regulären n–Ecks

Wir betrachten das reguläre n–Eck $P_n \subseteq \mathbb{R}^2 = \mathbb{C}$, wobei $n \in \mathbb{N}_{\geq 3}$:



Die **Diedergruppe** D_n^{I} besteht aus den euklidischen Isometrien von P_n:

$$D_n^{\mathrm{I}} = \Big\{ \underbrace{\rho_k : z \mapsto z\,\mathrm{e}^{2\pi \mathrm{i} k/n}}_{\text{genau } n \text{ Drehungen}},\ \underbrace{\sigma_k : z \mapsto \overline{z}\,\mathrm{e}^{2\pi \mathrm{i} k/n}}_{\text{... und } n \text{ Spiegelungen}} \ \Big|\ k = 0, \dots, n-1 \Big\} \leq \mathrm{Isom}(\mathbb{R}^2)$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Diedergruppe in Matrixdarstellung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Drehungen und Spiegelungen können wir durch Matrizen darstellen:

$$R_k = \begin{bmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{bmatrix}, \quad S_k = \begin{bmatrix} \cos(2\pi k/n) & \sin(2\pi k/n) \\ \sin(2\pi k/n) & -\cos(2\pi k/n) \end{bmatrix}$$

Diese $2n$ Matrizen fassen wir zusammen zur **Dieder-Matrixgruppe**:

$$D_n^{\mathrm{M}} = \{\, \mathrm{id} = R_0,\, R_1,\, \dots,\, R_{n-1},\, S_0,\, S_1,\, \dots,\, S_{n-1} \,\} \;\leq\; \mathrm{GL}_2\,\mathbb{R}$$

Die Diedergruppe in Permutationsdarstellung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir können die Isometrien durch Permutationen der Ecken darstellen:

$$r_k : \mathbb{Z}_n \to \mathbb{Z}_n : x \mapsto k + x, \qquad s_k : \mathbb{Z}_n \to \mathbb{Z}_n : x \mapsto k - x$$

Diese fassen wir zusammen zur **Dieder-Permutationsgruppe**:

$$D_n^{\mathrm{P}} = \{\, \mathrm{id} = r_0,\, r_1,\, \dots,\, r_{n-1},\; s_0,\, s_1,\, \dots,\, s_{n-1} \,\} \;\leq\; \mathrm{S}_n$$

Diese drei Darstellungen sind isomorph.

$$
\begin{tikzcd}
(\mathrm{GL}_2\,\mathbb{R}, \cdot) \arrow[d, phantom, "\vee\!|"] & & (\mathrm{Isom}(\mathbb{R}^2), \circ) \arrow[d, phantom, "\vee\!|"] & & (\mathrm{S}_n, \circ) \arrow[d, phantom, "\vee\!|"] \\
(D_n^{\mathrm{M}}, \cdot) \arrow[rr, shift right, "\varphi^{-1}"'] \arrow[rr, phantom, "\cong"] & & (D_n^{\mathrm{I}}, \circ) \arrow[ll, shift right, "\varphi"'] \arrow[rr, shift left, "\psi"] \arrow[rr, phantom, "\cong"] & & (D_n^{\mathrm{P}}, \circ) \arrow[ll, shift left, "\psi^{-1}"] \\
R_k, S_k & & \rho_k, \sigma_k & & r_k, s_k
\end{tikzcd}
$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Monoide und Gruppen: explizite Definition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J1ı: Monoid und Gruppe, explizite Formulierung

Ein **Magma** $(G, *)$ besteht aus einer Menge G mit innerer Verknüpfung

$$* : G \times G \to G : (a, b) \mapsto a * b.$$

(G0) Eine **Halbgruppe** $(G, *)$ erfüllt zudem die Assoziativität:

$$\mathbf{Ass}(G, *) \quad :\Leftrightarrow \forall a, b, c \in G : (a * b) * c = a * (b * c)$$

(G1) Ein **Monoid** $(G, *, e)$ besitzt zudem ein neutrales Element $e \in G$:

$$\mathbf{Ntr}(G, *, e) \quad :\Leftrightarrow \forall a \in G : e * a = a = a * e$$

$$\mathbf{Mon}(G, *, e) \quad :\Leftrightarrow \mathbf{Ass}(G, *) \wedge \mathbf{Ntr}(G, *, e)$$

(G2) Eine **Gruppe** $(G, *, e, \iota)$ besitzt zudem eine Inversion $\iota : G \to G$:

$$\mathbf{Inv}(G, *, e, \iota) \quad :\Leftrightarrow \forall a \in G : a * \iota(a) = e = \iota(a) * a$$

$$\mathbf{Grp}(G, *, e, \iota) \quad :\Leftrightarrow \mathbf{Ass}(G, *) \wedge \mathbf{Ntr}(G, *, e) \wedge \mathbf{Inv}(G, *, e, \iota)$$

(GA) Wir nennen $(G, *)$ **kommutativ** oder **abelsch**, falls gilt:

$$\mathbf{Com}(G, *) \quad :\Leftrightarrow \forall a, b \in G : a * b = b * a$$

$$\mathbf{AbGrp}(G, *, e, \iota) \quad :\Leftrightarrow \mathbf{Grp}(G, *, e, \iota) \wedge \mathbf{Com}(G, *)$$

Die Elementezahl $\sharp G = |G| =: \operatorname{ord}(G)$ heißt **Ordnung** von G.

Monoide und Gruppen: erste Beispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Triviales Beispiel: Die Menge $\{e\}$ wird auf genau eine Weise ein Magma $(\{e\}, *)$, $e * e = e$, ein Monoid $(\{e\}, *, e)$, eine Gruppe $(\{e\}, *, e, \iota)$, $\iota(e) = e$.

Beispiele: Monoide: $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{K}^{n\times n}, \cdot, 1_{n\times n})$, $(\mathrm{T}_n, \circ, \mathrm{id})$, ...
Gruppen: $(\mathbb{Z}, +, 0, -)$, $(\mathbb{Q}^*, \cdot, 1, {}^{-1})$, $(\mathrm{GL}_n\,\mathbb{K}, \cdot, 1_{n\times n}, {}^{-1})$, $(\mathrm{S}_n, \circ, \mathrm{id}, {}^{-1})$, ...

Sind Neutrale eindeutig?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma J1J: Eindeutigkeit des Neutralen in einem Magma $(M, *)$

Wir nennen $e \in M$ **linksneutral**, falls $e * a = a$ für alle $a \in M$ gilt.
Wir nennen $e' \in M$ **rechtsneutral**, falls $a * e' = a$ für alle $a \in M$ gilt.
Gilt beides, so ist $e = e'$ beidseitig **neutral**:

$$e \overset{\text{rNtr}}{=} e * e' \overset{\text{lNtr}}{=} e'$$

Sind Inverse eindeutig?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma J1κ: Eindeutigkeit des Inversen in einem Monoid $(M, *, e)$

Wir nennen $b \in M$ **linksinvers** zu $a \in M$, falls $b * a = e$ gilt.
Wir nennen $c \in M$ **rechtsinvers** zu $a \in M$, falls $a * c = e$ gilt.

(1) Gilt beides, so folgt $b = c$, denn

$$b \overset{\text{rNtr}}{=} b * e \overset{\text{rInv}}{=} b * (a * c) \overset{\text{Ass}}{=} (b * a) * c \overset{\text{lInv}}{=} e * c \overset{\text{lNtr}}{=} c.$$

(2) Wir nennen b **invers** zu a, falls $b * a = e$ und $a * b = e$ gilt.
Dank (1) ist b eindeutig durch a bestimmt, und wir schreiben $a^{-1} := b$.

$$M^\times = (M, *)^\times = (M, *, e)^\times := \left\{ a \in M \,\middle|\, \exists b \in M : a * b = e = b * a \right\}.$$

Invertierbarkeit und Inverse in einem Monoid

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele: (1) $(\mathbb{N}, +, 0)^\times = \{0\}$ und $(\mathbb{N}, \cdot, 1)^\times = \{1\}$.

(2) $(\mathbb{Z}, +, 0)^\times = \mathbb{Z}$ und $(\mathbb{Z}, \cdot, 1)^\times = \{-1, 1\}$.

(3) $(\mathbb{Q}, +, 0)^\times = \mathbb{Q}$ und $(\mathbb{Q}, \cdot, 1)^\times = \mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$.

(4) $\mathbb{Z}_n^\times = (\mathbb{Z}_n, \cdot_n, 1)^\times = \{\, a \in \mathbb{Z}_n \mid \mathrm{ggT}(a, n) = 1 \,\}$.

(5) $(\mathbb{K}^{n \times n}, \bullet, 1)^\times = \mathrm{GL}_n\, \mathbb{K}$.

(6) $(\mathrm{T}_X, \circ, \mathrm{id}_X)^\times = \mathrm{S}_X$.

Monoide und Gruppen: implizite Definition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J1M: 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:

$$\mathbf{Ass}(G, *) \quad :\Leftrightarrow \forall a, b, c \in G : (a * b) * c = a * (b * c)$$

(G1) Ein **Monoid** $(G, *)$ besitzt zudem ein neutrales Element:

$$\mathbf{Mon}(G, *) \quad :\Leftrightarrow \exists e \in G : \mathbf{Mon}(G, *, e)$$

$$\Leftrightarrow \begin{cases} \forall a, b, c \in G : (a * b) * c = a * (b * c) \\ \exists e \in G \;\; \forall a \in G : e * a = a = a * e \end{cases}$$

(G2) Eine **Gruppe** $(G, *, e)$ bzw. $(G, *)$ besitzt zudem eine Inversion:

$$\mathbf{Grp}(G, *, e) \quad :\Leftrightarrow \exists (\iota : G \to G) : \mathbf{Grp}(G, *, e, \iota)$$

$$\mathbf{Grp}(G, *) \quad :\Leftrightarrow \exists e \in G \;\; \exists (\iota : G \to G) : \mathbf{Grp}(G, *, e, \iota)$$

$$\Leftrightarrow \begin{cases} \forall a, b, c \in G : (a * b) * c = a * (b * c) \\ \exists e \in G \;\; \forall a \in G : \big[\, e * a = a = a * e \\ \qquad\qquad \wedge \exists b \in G : \;\; b * a = e = a * b \,\big] \end{cases}$$

Monoide und Gruppen: explizite vs implizite Definition

explizit $(G, *, e, \iota)$	implizit $(G, *, e)$ bzw. $(G, *)$
$(\mathbb{Z}, +, 0, -)$, $(\mathbb{Q}^*, \cdot, 1, {}^{-1})$, $(\mathrm{GL}_n\,\mathbb{R}, \cdot, 1_{n\times n}, {}^{-1})$, $(\mathrm{S}_n, \circ, \mathrm{id}, {}^{-1})$	$(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathrm{GL}_n\,\mathbb{R}, \cdot)$, $(\mathrm{S}_n, \circ)$

Pars pro toto: Oft sagen wir „die Gruppe G“, meinen aber $(G, *, e, \iota)$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lösung von Gleichungen in Gruppen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

In $(\mathbb{R}, +, 0, -)$ lösen Sie Gleichungen wie in der Schule gelernt:

$$x + 5 = 3 \xRightarrow{\text{addiere } -5} x = 3 + (-5) = -2$$

Ebenso lösen Sie Gleichungen in jeder Gruppe $(G, *, e, ')$:

$$x * a = b \xRightarrow{\text{multipliziere } a' \text{ von rechts}} x = b * a'$$
$$a * y = b \xRightarrow{\text{multipliziere } a' \text{ von links}} y = a' * b$$

Satz J1N: Lösung von Gleichungen in Gruppen

Sei $G \neq \emptyset$ und $* : G \times G \to G$ assoziativ. 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 $a * y = b$.

Lösung von Gleichungen in Gruppen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: „(1) ⇒ (2)“: Wir haben Lösungen $x = b * a'$ und $y = a' * b$:

$$x = b * a' \quad \Longrightarrow \quad x * a \overset{\text{Vor}}{=} (b * a') * a \overset{\text{G0}}{=} b * (a' * a) \overset{\text{G2}}{=} b * e \overset{\text{G1}}{=} b$$

$$y = a' * b \quad \Longrightarrow \quad a * y \overset{\text{Vor}}{=} a * (a' * b) \overset{\text{G0}}{=} (a * a') * b \overset{\text{G2}}{=} e * b \overset{\text{G1}}{=} b$$

Diese Lösungen $b * a'$ bzw. $a' * b$ sind zudem sogar eindeutig:

$$b = x * a \quad \Longrightarrow \quad b * a' \overset{\text{Vor}}{=} (x * a) * a' \overset{\text{G0}}{=} x * (a * a') \overset{\text{G2}}{=} x * e \overset{\text{G1}}{=} x$$

$$b = a * y \quad \Longrightarrow \quad a' * b \overset{\text{Vor}}{=} a' * (a * y) \overset{\text{G0}}{=} (a' * a) * y) \overset{\text{G2}}{=} e * y \overset{\text{G1}}{=} y$$

„(2) ⇒ (1)“: Dank $G \neq \emptyset$ existiert $a \in G$. Dank (2) existiert $e \in G$ mit $e * a = a$. Zu jedem $b \in G$ existiert $y \in G$ mit $a * y = b$. Daraus folgt:

$$e * b \overset{\text{Vor}}{=} e * (a * y) \overset{\text{Ass}}{=} (e * a) * y \overset{\text{Vor}}{=} a * y \overset{\text{Vor}}{=} b$$

Also ist e in $(G, *)$ linksneutral. Ebenso finden wir $\tilde{e} \in G$ rechtsneutral. Dank Eindeutigkeit J1J gilt $e = \tilde{e}$. Zu $a \in G$ existiert $a' \in G$ mit $a' * a = e$, ebenso $a'' \in G$ mit $a * a'' = e$. Dank Eindeutigkeit J1K gilt dann $a' = a''$. Somit ist $(G, *, e, ')$ eine Gruppe. QED

Endliche Summen und Produkte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J1R: endliche Summen und Produkte

(1) Sei $(M, +, 0)$ bzw. $(M, \cdot, 1)$ ein Monoid.

$$\sum_{i=1}^{0} a_i := 0, \qquad \sum_{i=1}^{n} a_i := \left[\sum_{i=1}^{n-1} a_i\right] + a_n = (\ldots(a_1 + a_2) + \ldots) + a_n$$

$$\prod_{i=1}^{0} a_i := 1, \qquad \prod_{i=1}^{n} a_i := \left[\prod_{i=1}^{n-1} a_i\right] \cdot a_n = (\ldots(a_1 \cdot a_2) \cdot \ldots) \cdot a_n$$

Kommutierende Summen und Produkte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J1R: kommutierende Summen und Produkte

(2) Seien $(a_i)_{i\in J}$ kommutierende Elemente in $(M,+,0)$ bzw. $(M,\cdot,1)$.

(2a) Ist $I=\{i_1,\dots,i_n\}^! \subseteq J$ eine n–elementige Menge, so definieren wir

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

(2b) Gilt $a_j=0$ für alle $j\in J\smallsetminus I$, so definieren wir $\sum_{i\in J} a_i := \sum_{i\in I} a_i$.

Ganzzahlige Vielfache und Potenzen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J1R: ganzzahlige Vielfache und Potenzen

(3) Für $n \in \mathbb{N}$ definieren wir das n-te Vielfache und die n-te Potenz durch

$$a \cdot n := \sum_{i=1}^{n} a \quad \text{bzw.} \quad a^n := \prod_{i=1}^{n} a.$$

Ist $-a$ das Negative zu a in $(M, +, 0)$, so setzen wir $a \cdot (-n) := (-a) \cdot n$.
Ist a^{-1} das Inverse zu a in $(M, \cdot, 1)$, so setzen wir $a^{-n} := (a^{-1})^n$.

Rechenregeln für Vielfache und Potenzen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J1R: Modulgesetze und Potenzgesetze

$$
\begin{array}{lrr}
(1) & a \bullet 1 = a, & a^1 = a, \\
(2) & a \bullet (m \cdot n) = (a \bullet m) \bullet n, & a^{m \cdot n} = (a^m)^n, \\
(3) & a \bullet (m + n) = a \bullet m + a \bullet n, & a^{m+n} = a^m \cdot a^n.
\end{array}
$$

$$
\begin{array}{lrcl}
(4) & a + b = b + a & \Longrightarrow & (a + b) \bullet n = a \bullet n + b \bullet n, \\
 & a \cdot b = b \cdot a & \Longrightarrow & (a \cdot b)^n = a^n \cdot b^n.
\end{array}
$$

Was ist ein Gruppenhomomorphismus?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir betrachten die Gruppen $(\mathbb{R}, +, 0, -)$ und $(\mathbb{R}_{>0}, \cdot, 1, {}^{-1})$.

$$\begin{tikzcd}
\mathbb{R} \arrow[d, shift right, "\exp"'] & \times & \mathbb{R} \arrow[d, shift right, "\exp"'] \arrow[rr, "+", "(a,b)\mapsto a+b"'] & & \mathbb{R} \arrow[d, shift right, "\exp"'] \\
\mathbb{R}_{>0} \arrow[u, shift right, "\ln"'] & \times & \mathbb{R}_{>0} \arrow[u, shift right, "\ln"'] \arrow[rr, "\cdot", "(x,y)\mapsto x\cdot y"'] & & \mathbb{R}_{>0} \arrow[u, shift right, "\ln"']
\end{tikzcd}
\qquad
\begin{tikzcd}
0 \arrow[d, shift right, "\exp"'] \\
1 \arrow[u, shift right, "\ln"']
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{R} \arrow[d, shift right, "\exp"'] \arrow[r, "-", "a\mapsto -a"'] & \mathbb{R} \arrow[d, shift right, "\exp"'] \\
\mathbb{R}_{>0} \arrow[u, shift right, "\ln"'] \arrow[r, "{}^{-1}", "x\mapsto x^{-1}"'] & \mathbb{R}_{>0} \arrow[u, shift right, "\ln"']
\end{tikzcd}$$

Die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}_{>0} : a \mapsto \mathrm{e}^a = \sum_{k=0}^{\infty} a^k/k!$ erfüllt $\exp(a+b) = \exp(a) \cdot \exp(b)$, somit $\exp(0) = 1$ und $\exp(-a) = \exp(a)^{-1}$.

Umgekehrt, die Logarithmusfunktion $\ln : \mathbb{R}_{>0} \to \mathbb{R} : x \mapsto \ln(x)$ erfüllt $\ln(x \cdot y) = \ln(x) + \ln(y)$ und somit $\ln(1) = 0$ und $\ln(x^{-1}) = -\ln(x)$.

Homomorphismen sind strukturerhaltende Abbildungen.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J2A: Homomorphismen

Ein **Homomorphismus** $f : G \to H$ ist eine strukturerhaltende Abbildung.

$$\left.\begin{array}{l} f : (G, *) \to (H, \bullet) \\ \text{Magmahomomorphismus} \end{array}\right\} :\Longleftrightarrow \left\{\begin{array}{l} f : G \to H \text{ Abbildung und} \\ \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \end{array}\right.$$

$$\left.\begin{array}{l} f : (G, *, e) \to (H, \bullet, e') \\ \text{Monoidhomomorphismus} \end{array}\right\} :\Longleftrightarrow \left\{\begin{array}{l} f : G \to H \text{ mit } f(e) = e' \text{ und} \\ \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \end{array}\right.$$

$$\left.\begin{array}{l} f : (G, *, e, \iota) \to (H, \bullet, e', \iota') \\ \text{Gruppenhomomorphismus} \end{array}\right\} :\Longleftrightarrow \left\{\begin{array}{l} f : G \to H \text{ Abbildung und} \\ \forall a, b \in G : f(a * b) = f(a) \bullet f(b) \end{array}\right.$$

Daraus folgt (1) $f(e) = e'$ und damit (2) $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G^\times$.

Gruppenhomomorphismen respektieren Neutrales & Inverse.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: (1) Aus $e' \cdot f(a) \overset{\text{Ntr}}{=} f(a) \overset{\text{Ntr}}{=} f(e * a) \overset{\text{Hom}}{=} f(e) \cdot f(a)$ folgt $e' = f(e)$.

(2) Aus $e' \overset{(1)}{=} f(e) \overset{\text{Inv}}{=} f(a * a^{-1}) \overset{\text{Hom}}{=} f(a) \cdot f(a^{-1})$ folgt $f(a^{-1}) = f(a)^{-1}$.

Rechnen mit Homomorphismen — die Kategorie Grp

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$(G, \star) \xrightarrow{\mathrm{id}} (G, \star) \qquad \begin{tikzcd} (G, \star) \arrow[r, "g"] \arrow[rr, bend right, "k = h \circ g"'] & (H, \circledast) \arrow[r, "h"] & (K, \circledast) \end{tikzcd}$$

Lemma J2D: Komposition von Homomorphismen

(1) Für jede Gruppe $(G, \star)$ ist $\mathrm{id}_G : (G, \star) \to (G, \star)$ ein Homomorphismus.

(2) Sind $g : (G, \star) \to (H, \circledast)$ und $h : (H, \circledast) \to (K, \circledast)$ Homomorphismen von Gruppen, so auch ihre Komposition $k = h \circ g : (G, \star) \to (K, \circledast)$.

Beweis: Für alle $a, b \in G$ gilt $\mathrm{id}_G(a \star b) \overset{\text{Def}}{=} a \star b \overset{\text{Def}}{=} \mathrm{id}_G(a) \star \mathrm{id}_G(b)$ sowie $k(a \star b) \overset{\text{Def}}{=} h(g(a \star b)) \overset{\text{Hom}}{=} h(g(a) \circledast g(b)) \overset{\text{Hom}}{=} h(g(a)) \circledast h(g(b)) \overset{\text{Def}}{=} k(a) \circledast k(b)$.

Das kartesische Produkt von Monoiden und Gruppen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wie addieren Sie Vektoren $(\mathbb{R}^n, +, 0, -)$ sowie Matrizen $(\mathbb{R}^{m\times n}, +, 0, -)$ (D1B) und Funktionen $(\mathbb{R}^\Omega, +, 0, -)$ (C1C)? Koordinatenweise! Allgemein:

Satz J2E: das kartesische Produkt von Monoiden und Gruppen

Zu $i \in I$ sei $(G_i, *_i, e_i, {}^{-1})$ ein Magma / ein Monoid / eine Gruppe.

Das **kartesische Produkt** $P = \prod_{i\in I} G_i$ besteht aus allen **I–Tupeln** $a = (a_i)_{i\in I}$ mit **Koordinaten** $a_i \in G_i$, zum Beispiel $e := (e_i)_{i\in I}$.

(0) Auf $P = \prod_{i\in I} G_i$ definieren wir die **koordinatenweise Verknüpfung**

$$* : P \times P \to P \text{ durch } (a * b)_i := a_i *_i b_i.$$

(1) Ist jeder Faktor $(G_i, *_i)$ (a) kommutativ, (b) assoziativ, (c) ein Monoid, (d) eine Gruppe so auch das Produkt $(P, *)$.

(2) Jede Projektion $p_i = \mathrm{pr}_i : P \twoheadrightarrow G_i : a \mapsto a_i$ ist ein Homomorphismus.

Die Summe von Monoiden und Gruppen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J2E: die Summe von Monoiden und Gruppen

Sei $(G_i, *_i, e_i)$ ein Monoid / eine Gruppe für jeden Index $i \in I$.

(3) Zu $a \in \prod_{i \in I} G_i$ ist der **Träger** $\operatorname{supp}(a) := \{\, i \in I \mid a_i \neq e_i \,\}$. Es gilt

$$\operatorname{supp}(e) = \emptyset \quad \text{und} \quad \operatorname{supp}(a * b) \subseteq \operatorname{supp}(a) \cup \operatorname{supp}(b).$$

(4) Das Produkt $P = \prod_{i \in I} G_i$ enthält somit die **Summe**

$$S = \bigoplus_{i \in I} G_i := \left\{\, a \in P \,\middle|\, \sharp \operatorname{supp}(a) < \infty \,\right\} \leq P.$$

(5) Zu jedem $i \in I$ haben wir neben der Projektion $p_i = \mathrm{pr}_i : P \geq S \twoheadrightarrow G_i$ die Einbettung $s_i = \mathrm{inc}_i : G_i \hookrightarrow S \leq P : a_i \mapsto a$ mit $a_j = e_j$ für alle $j \neq i$.

Potenz von Monoiden und Gruppen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J2E: Potenz von Monoiden und Gruppen

(6) Im Spezialfall $(G_i, *_i, e_i, {}^{-1}) = (G, *, e, {}^{-1})$ für alle $i \in I$ erhalten wir:

$$\begin{aligned} G^I &= \textstyle\prod_{i\in I} G = \{\, a : I \to G : i \mapsto a_i \,\} \\ G^{(I)} &= \textstyle\bigoplus_{i\in I} G = \{\, a : I \to G \mid \sharp \operatorname{supp} a < \infty \,\} \end{aligned}$$

Beispiel: Die Gruppe $(\mathbb{R}, +, 0, -)^{\mathbb{N}}$, kurz $\mathbb{R}^{\mathbb{N}}$, besteht aus allen Folgen

$$f : \mathbb{N} \to \mathbb{R} : k \mapsto f_k.$$

Darin ist $\mathbb{R}^{(\mathbb{N})} < \mathbb{R}^{\mathbb{N}}$ die Unter/Gruppe der endlich getragenen Folgen f.

$$\sharp \operatorname{supp}(f) < \infty \quad \Longleftrightarrow \quad f = \textstyle\sum_k f_k X^k \in \mathbb{R}[X]$$

Isomorphe Gruppen haben dieselbe Struktur.

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

$\cong$

$\cdot$	$+1$	-1
$+1$	$+1$	-1
-1	-1	$+1$

$$(\varphi, \psi) : (\mathbb{Z}_2, +_2) \cong (\{\pm 1\}, \cdot) : a \mapsfrom\!\!\!\!\to (-1)^a$$

$$\varphi = \begin{Bmatrix} 0 \mapsto +1 \\ 1 \mapsto -1 \end{Bmatrix} \text{ und } \psi = \begin{Bmatrix} +1 \mapsto 0 \\ -1 \mapsto 1 \end{Bmatrix}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Was ist ein Isomorphismus?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J2H: Isomorphismus von Gruppen

(1) Ein **Isomorphismuspaar** $(\varphi, \psi) : (G, *) \cong (H, \bullet)$ von zwei Gruppen besteht aus zueinander inversen Homomorphismen, $\varphi : (G, *) \to (H, \bullet)$ und $\psi : (H, \bullet) \to (G, *)$ mit $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_H$.

(2) Wir nennen allein schon $\varphi : (G, *) \rightsquigarrow (H, \bullet)$ einen Isomorphismus, falls hierzu ein inverser Isomorphismus $\psi : (H, \bullet) \rightsquigarrow (G, *)$ existiert.

Beispiel: $(\exp, \ln) : (\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$ ist ein Isomorphismuspaar.

Morphismen: Homo, Iso, Endo, Auto

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J2H: Homo/Iso/Endo/Automorphismen

(3) Zu je zwei Gruppen $(G,*)$ und $(H,\bullet)$ definieren wir:

$$\begin{aligned}
\mathrm{Hom}(G,*;H,\bullet) &:= \{\varphi : G \to H \mid \forall a,b \in G : \varphi(a*b) = \varphi(a)\bullet\varphi(b)\} \\
\mathrm{Hom}(G,*;H,\bullet)^\times &:= \{\varphi \in \mathrm{Hom}(G,H) \mid \varphi \text{ ist invertierbar gemäß (2)}\}
\end{aligned}$$

(4) Im Spezialfall $(G,*) = (H,\bullet)$ stimmen Start und Ziel überein:

$$\begin{aligned}
\mathrm{End}(G,*) &:= \mathrm{Hom}(G,*;G,*) && \text{ist ein Monoid (J2D)}, \\
\mathrm{Aut}(G,*) &:= \mathrm{End}(G,*)^\times && \text{ist eine Gruppe (J1L)}.
\end{aligned}$$

Wie erkennen wir Isomorphismen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J2I: Jeder bijektive Homomorphismus ist ein Isomorphismus.

Ist $\varphi : (G, *) \to (H, \bullet)$ ein Homomorphismus und bijektiv, so ist auch seine Umkehrung $\psi = \varphi^{-1} : (H, \bullet) \to (G, *)$ ein Homomorphismus.

Beweis: Zu $x, y \in H$ setzen wir $a := \psi(x)$ und $b := \psi(y)$ in G und finden $\psi(x \bullet y) \overset{\text{Def}}{=} \psi(\varphi(a) \bullet \varphi(b)) \overset{\text{Hom}}{=} \psi(\varphi(a * b)) \overset{\text{Inv}}{=} a * b \overset{\text{Def}}{=} \psi(x) * \psi(y)$. $\boxed{\text{QED}}$

Beispiel: Zu jedem Exponenten $n \in \mathbb{N}$ ist $p_n : (\mathbb{R}_{\geq 0}, \cdot) \to (\mathbb{R}_{\geq 0}, \cdot) : x \mapsto x^n$ ein Homomorphismus, $(x \cdot y)^n = x^n \cdot y^n$ (J1R), für $n \geq 1$ zudem bijektiv, also invertierbar durch $w_n(y) = \sqrt[n]{y}$. Dank J2I folgt $\sqrt[n]{x \cdot y} = \sqrt[n]{x} \cdot \sqrt[n]{y}$.

Der Fundamentalsatz der Arithmetik als Isomorphismus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel J2J: Fundamentalsatz der Arithmetik

Sei $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$ die Menge aller positiven Primzahlen in $(\mathbb{Z}, \cdot)$.
Zu $e : \mathbb{P} \to \mathbb{N}$ endlich getragen haben wir $\prod_p p^{e(p)} = 2^{e(2)}\, 3^{e(3)}\, 5^{e(5)} \cdots$.

(1) Dies definiert einen Monoidhomomorphismus,

$$\Phi : (\mathbb{N}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{Z}_{>0}, \cdot) : e \mapsto \textstyle\prod_{p \in \mathbb{P}} p^{e(p)}.$$

Dank Fundamentalsatz der Arithmetik B3J ist Φ ein Isomorphismus.

(2) Übergang zu Brüchen ergibt einen Gruppenisomorphismus,

$$\Phi : (\mathbb{Z}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{Q}_{>0}, \cdot) : e \mapsto \textstyle\prod_{p \in \mathbb{P}} p^{e(p)}.$$

Unterstrukturen durch Einschränkung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition J2M: Unterstrukturen durch Einschränkung

Sei $(G, * : G \times G \to G)$ ein Magma. Einschränkung auf $U \subseteq G$ ergibt

$$
\begin{aligned}
*|_{U\times G} &: U \times G \to G : (u,a) \mapsto u * a && \text{Linksoperation von } U \text{ auf } G,\\
*|_{G\times U} &: G \times U \to G : (a,u) \mapsto a * u && \text{Rechtsoperation von } U \text{ auf } G,\\
*|_{U\times U} &: U \times U \to G : (u,v) \mapsto u * v && \text{äußere Verknüpfung auf } U.
\end{aligned}
$$

(G0) Ein **Untermagma** $U \leq (G, *)$ ist eine Menge $U \subseteq G$ mit $U * U \subseteq U$, also $\forall a, b \in U : a * b \in U$. Dies definiert auf U eine innere Verknüpfung,

$$*_U := *|^U_{U\times U} : U \times U \to U : (u,v) \mapsto u * v.$$

(G1) Für ein **Untermonoid** $U \leq (G, *, e)$ fordern wir zusätzlich $e \in U$.
(G2) Für eine **Untergruppe** $U \leq (G, *, e, \iota)$ fordern wir zudem $\iota(U) \subseteq U$.

Einfache Gegen/Beispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: In jeder Gruppe $(G, *, e, \iota)$ sind $\{e\}$ und G Untergruppen.

Warnung: Im Monoid $(\mathbb{Z}, \cdot, 1)$ ist $\{0\}$ multiplikativ abgeschlossen. Daher ist $(\{0\}, \cdot, 0)$ ein Monoid, aber kein Untermonoid von $(\mathbb{Z}, \cdot, 1)$.

Beispiele: In der Gruppe $(\mathbb{Z}, +, 0, -)$ gilt:

1. Die Menge $X = 2\mathbb{Z} + 1$ ist kein Untermagma, denn $X + X \not\subseteq X$.
2. Die Menge $\mathbb{N}_{\geq 5}$ ist eine Unterhalbgruppe, aber kein Untermonoid.
3. Die Menge $\mathbb{N}$ ist ein Untermonoid in $\mathbb{Z}$, aber keine Untergruppe.
4. Die Menge $U = n\mathbb{Z}$ mit $n \in \mathbb{N}$ ist eine Untergruppe.

Untergruppen: Verkürzung auf zwei Bedingungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma J2o: verkürzte Untergruppenbedingung

Sei $(G, *, e, \iota)$ eine Gruppe. Für jede Teilmenge $U \subseteq G$ gilt:

$$\begin{aligned} U \leq (G, *, e, \iota) &\overset{\text{Def}}{\iff} e \in U \wedge \forall a, b \in U : a * b \in U \wedge \forall b \in U : \iota(b) \in U \\ &\overset{!}{\iff} U \neq \emptyset \wedge \forall a, b \in U : a * \iota(b) \in U \end{aligned}$$

Beweis: Die Implikation „$\Rightarrow$“ ist klar. Wir zeigen die Umkehrung „$\Leftarrow$“: Wegen $U \neq \emptyset$ existiert ein Element $a \in U$, damit folgt $U \ni a * \iota(a) = e$. Für alle $a, b \in U$ folgt $U \ni e * \iota(b) = \iota(b)$ und $U \ni a * \iota(\iota(b)) = a * b$. $\boxed{\text{QED}}$

Die erzeugte Untergruppe $\langle S \rangle \leq G$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel J2R: erzeugte Untergruppe

Das von $S \subseteq M$ **erzeugte Untermonoid** ist

$$[S] := \{ s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n} \mid n \in \mathbb{N},\ s_i \in S,\ e_i \in \mathbb{N} \}.$$

Die von $S \subseteq M^\times$ **erzeugte Untergruppe** ist

$$\langle S \rangle := \{ s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n} \mid n \in \mathbb{N},\ s_i \in S,\ e_i \in \mathbb{Z} \}.$$

Speziell für $S = \{a\}$ erhalten wir die **zyklische Untergruppe** $\langle a \rangle \leq M$.

Beispiel: Permutationen und Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Wir betrachten die Elementartranspositionen:

$$\mathscr{E} = \{ (1,2), (2,3), \dots, (n-1,n) \} \quad \subseteq \mathrm{T}_n$$

Diese erzeugen die Permutationsgruppe $\langle \mathscr{E} \rangle = \mathrm{S}_n$. Sortieren H1F!

Beispiel: Über einem Körper $\mathbb{K}$ betrachten wir die Elementarmatrizen:

$$\mathscr{E} = \{ P_{ij}, S_i(\mu), T_{ij}(\lambda) \} \quad \subseteq \mathbb{K}^{n \times n}$$

Diese erzeugen die Matrixgruppe $\langle \mathscr{E} \rangle = \mathrm{GL}_n\, \mathbb{K}$. Gauß–Algorithmus D2H!

Klassifikation aller Untergruppen von $(\mathbb{Z}, +)$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Für jedes $n \in \mathbb{N}$ ist $\langle n \rangle = n\mathbb{Z} = \{\, nq \mid q \in \mathbb{Z} \,\}$ eine Untergruppe in $(\mathbb{Z}, +)$.
Gibt es noch weitere Beispiele? Oder kennen wir damit bereits alle?

Satz J2T: Klassifikation aller Untergruppen von $(\mathbb{Z}, +)$ – Minimalelement

Jede Untergruppe $U \leq (\mathbb{Z}, +)$ ist zyklisch: Es existiert $n \in \mathbb{N}$ mit $U = n\mathbb{Z}$.

Beweis: (0) Für $U = \{0\}$ genügt $n = 0$. (1) Im Folgenden sei also $U \supsetneq \{0\}$.
Dann existiert $n \in U \smallsetminus \{0\}$, ohne Einschränkung $n > 0$, zudem minimal.

(2) Wir behaupten $U = n\mathbb{Z}$. Aus $n \in U \leq (\mathbb{Z}, +)$ folgt $n\mathbb{Z} \subseteq U$.
Wie zeigen wir die Umkehrung $U \subseteq n\mathbb{Z}$? Hierzu sei $a \in U$ beliebig.
Euklidische Division B3A ergibt $a = nq + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < n$.
Es folgt $r = a - nq \in U$, somit $r = 0$, denn n ist minimal gemäß (1).
Also gilt $a = nq \in n\mathbb{Z}$. Das zeigt $U \subseteq n\mathbb{Z}$. Wir schließen $U = n\mathbb{Z}$. QED

Bild und Kern sind Untergruppen.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J2u: Bild und Kern sind Untergruppen.

Sei $\varphi : (G, *, e) \to (H, \cdot, 1)$ ein Homomorphismus von Gruppen.

(1) Ist $U \leq G$ eine Untergruppe, so auch ihr Bild $V = \varphi(U) \leq H$.
Ist $V \leq H$ eine Untergruppe, so auch ihr Urbild $U = \varphi^{-1}(V) \leq G$.

Beweis: (1a) Es gilt $1 = \varphi(e) \in V$. Zu $x, y \in V$ existieren Urbilder $a, b \in U$ mit $\varphi(a) = x$, $\varphi(b) = y$, also gilt $x \cdot y^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a * b^{-1}) \in V$.

(1b) Wegen $\varphi(e) = 1 \in V$ gilt $e \in U$. Seien $a, b \in U$, also $\varphi(a), \varphi(b) \in V$.
Dann gilt $a * b^{-1} \in U$, denn $\varphi(a * b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} \in V$.

Insbesondere sind das Bild und der Kern von φ jeweils Untergruppen:

$$\begin{aligned} G \leq G \quad &\Longrightarrow \quad \mathrm{Im}(\varphi) \ := \varphi(G) \qquad \leq (H, \cdot, 1) \\ \{1\} \leq H \quad &\Longrightarrow \quad \mathrm{Ker}(\varphi) := \varphi^{-1}(\{1\}) \leq (G, *, e) \end{aligned}$$

Faser und Injektivität

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J2U: die Faser über einem Bildpunkt als Nebenklasse des Kerns

(2) Für $a \in G$ und $b = \varphi(a)$ gilt $\varphi^{-1}(\{b\}) = a\,\mathrm{Ker}(\varphi) = \mathrm{Ker}(\varphi)\,a$.

Beweis: Für $x \in G$ ist die Bedingung $\varphi(x) = \varphi(a) = b$ äquivalent zu:
(2a) $1 = \varphi(a)^{-1}\varphi(x) = \varphi(a^{-1}x)$, also $a^{-1}x \in \mathrm{Ker}(\varphi)$, somit $x \in a\,\mathrm{Ker}(\varphi)$.
(2b) $1 = \varphi(x)\varphi(a)^{-1} = \varphi(xa^{-1})$, also $xa^{-1} \in \mathrm{Ker}(\varphi)$, somit $x \in \mathrm{Ker}(\varphi)\,a$.

Satz J2U: Kern-Kriterium zur Injektivität von Gruppenhomomorphismen

(3) Genau dann ist $\varphi : G \to H$ injektiv, wenn $\mathrm{Ker}(\varphi) = \{e\}$ gilt.

Beweis: „$\Rightarrow$“: Ist φ injektiv, so hat $\varphi(x) = 1$ nur die Lösung $x = e$.
„$\Leftarrow$“: Gilt $\varphi(x) = \varphi(a)$, so folgt $xa^{-1} \in \mathrm{Ker}(\varphi) = \{e\}$, also $x = a$. QED

Klassifikation zyklischer Monoide $[a]$

$$a^0 \longmapsto a^1 \longmapsto \ldots \longmapsto a^{m-1} \longmapsto a^m \longmapsto a^{m+1} \longmapsto \ldots \longmapsto a^{n-1}$$

Vorperiode der Länge m

Periode der Länge $\ell = n - m$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Klassifikation zyklischer Gruppen $\langle a \rangle$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J2v: zyklische Untergruppe und Ordnung eines Elements

Sei $(G, \cdot)$ eine Gruppe und $a \in G$. Wir haben den Homomorphismus

$$\varphi : (\mathbb{Z}, +) \to (G, \cdot) : k \mapsto a^k.$$

Es gilt $\operatorname{Im}(\varphi) = \langle a \rangle \leq G$ und $\operatorname{Ker}(\varphi) \leq (\mathbb{Z}, +)$, dank Klassifikation J2T also $\operatorname{Ker}(\varphi) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$. Wir erhalten $\varphi^{-1}(a^k) = k + n\mathbb{Z}$, somit:

$$\bar{\varphi} : (\mathbb{Z}/n\mathbb{Z}, +) \xrightarrow{\sim} (\langle a \rangle, \cdot) : k + n\mathbb{Z} \mapsto a^k$$

In Worten: Genau dann gilt $a^k = a^\ell$ in G, wenn $k \equiv \ell \bmod n$ in $\mathbb{Z}$.

$$\begin{tikzcd}
(\mathbb{Z}, +) \arrow[r, "\varphi", "k \mapsto a^k"'] \arrow[d, two heads, "q"'] \arrow[dr, two heads, "\varphi"] & (G, \cdot) \\
\mathbb{Z}/n\mathbb{Z} \arrow[r, "\bar{\varphi}", "\cong"'] & \langle a \rangle \arrow[u, hook, "\mathrm{inc}"']
\end{tikzcd}$$

Im Falle $n \geq 1$ hat a endliche Ordnung, $\operatorname{ord}(a) := \sharp\langle a \rangle = n < \infty$.
Im Falle $n = 0$ hat a unendliche Ordnung, $\operatorname{ord}(a) := \sharp\langle a \rangle = \infty$.

Klassifikation zyklischer Gruppen $\langle a \rangle$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Bestimmen Sie zu $\sigma = (1,2)(3,4,5) \in \mathrm{S}_5$ die Gruppe $\langle \sigma \rangle \leq \mathrm{S}_5$.

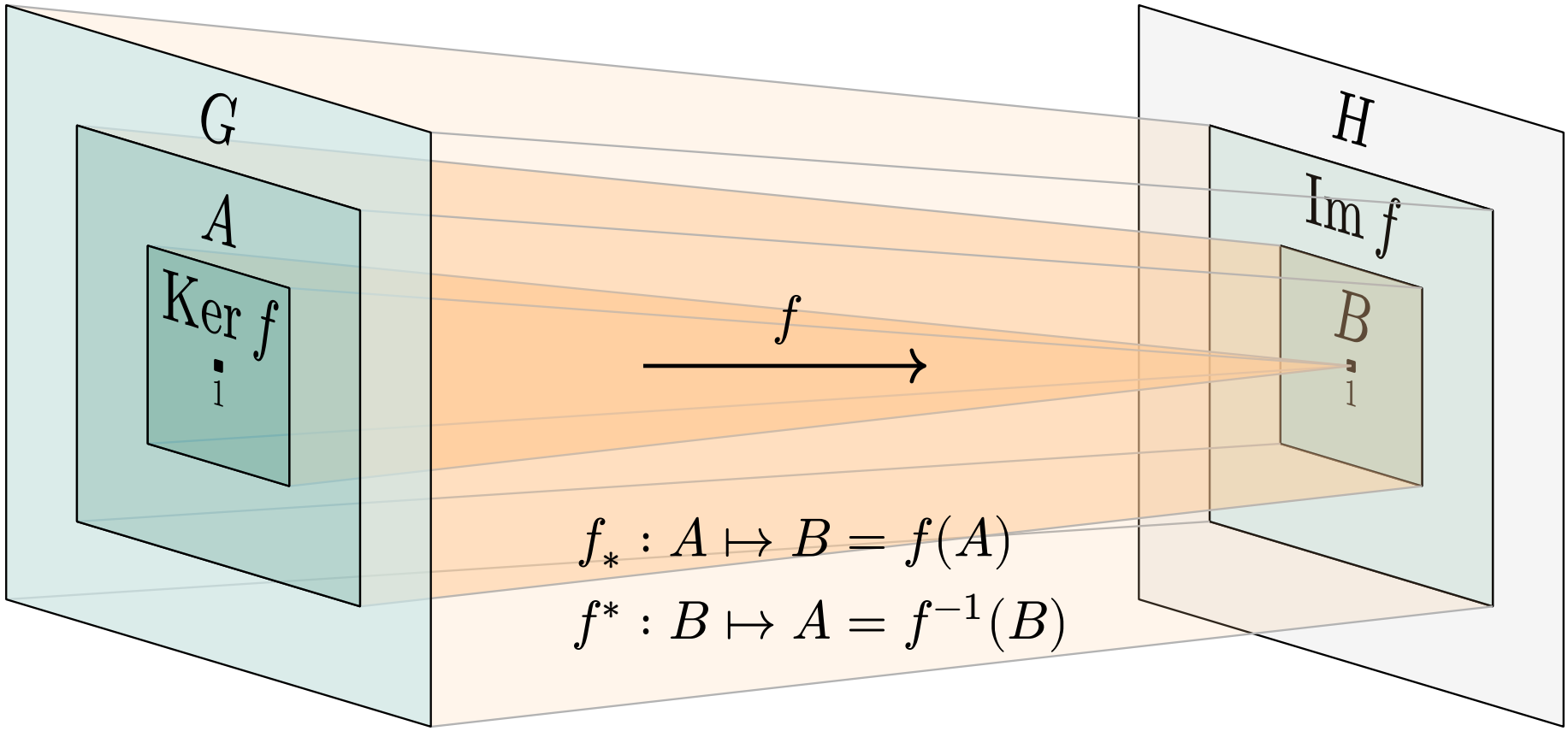
Lösung: Für $k \in \mathbb{Z}$ gilt $\sigma^k = (1,2)^k(3,4,5)^k$, also $\mathrm{ord}(\sigma) = \mathrm{kgV}(2,3) = 6$. In $(\mathrm{S}_5, \circ, \mathrm{id})$ erhalten wir so die Untergruppe $(\langle \sigma \rangle, \circ, \mathrm{id}) \cong (\mathbb{Z}/6\mathbb{Z}, +, 0)$.

$$\sigma^0 = \mathrm{id}, \qquad \sigma^1 = (1,2)(3,4,5), \qquad \sigma^2 = (3,5,4),$$
$$\sigma^3 = (1,2), \qquad \sigma^4 = (3,4,5), \qquad \sigma^5 = (1,2)(3,5,4), \qquad \sigma^6 = \mathrm{id}, \ldots$$

Korrespondenzsatz für Untergruppen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Satz J2w: Untergruppen-Korrespondenz

(0) Jeder Gruppenhomomorphismus $f : G \to H$ stiftet eine Bijektion

$$(f_*, f^*) : \{ A \mid \mathrm{Ker}(f) \leq A \leq G \} \cong \{ B \mid \{1\} \leq B \leq \mathrm{Im}(f) \}.$$

(1) Für jede Untergruppe $A \leq G$ gilt $f^{-1}(f(A)) = A\,\mathrm{Ker}(f) = \mathrm{Ker}(f)\,A$.
(2) Für jede Untergruppe $B \leq H$ gilt $f(f^{-1}(B)) = B \cap \mathrm{Im}(f)$.

Korrespondenzsatz für Untergruppen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: (1) Für jede Untergruppe $A \leq G$ gilt:

$$f^{-1}(f(A)) \overset{\text{Def}}{=} \bigcup_{x \in A} f^{-1}(f(\{x\})) \overset{\text{J2u}}{=} \bigcup_{x \in A} x\,\mathrm{Ker}(f) \overset{\text{Def}}{=} A\,\mathrm{Ker}(f)$$

(0a) Zusammen mit $\mathrm{Ker}(f) \leq A$ erhalten wir $f^{-1}(f(A)) = A$.

(2) Für jede Untergruppe $B \leq H$ gilt:

$$f(f^{-1}(B)) \overset{\text{Def}}{=} \bigcup_{y \in B} f(f^{-1}(\{y\})) \overset{\text{Bild}}{=} B \cap \mathrm{Im}(f)$$

(0b) Zusammen mit $B \leq \mathrm{Im}(f)$ erhalten wir $f(f^{-1}(B)) = B$. $\boxed{\text{QED}}$

Alle Untergruppen von $\mathbb{Z}/12\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Bestimmen Sie alle Untergruppen $B \leq \mathbb{Z}/n\mathbb{Z}$ für $n = 12$.

Lösung: Wir nutzen den surjektiven Gruppenhomomorphismus

$$f : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} : a \mapsto [a] = a + n\mathbb{Z}.$$

Dank Korrespondenz J2w entspricht jede Untergruppe $B \leq \mathbb{Z}/n\mathbb{Z}$ eindeutig einer Untergruppe $A = f^{-1}(B) \leq \mathbb{Z}$ mit $A \geq \operatorname{Ker}(f) = n\mathbb{Z}$.

Dank Klassifikationsatz J2T gilt $A = d\mathbb{Z}$ für ein $d \in \mathbb{N}$.
Die Inklusion $n\mathbb{Z} \leq d\mathbb{Z}$ bedeutet $n \in d\mathbb{Z}$, also $d \mid n$.

$$n = 12 \quad \Longrightarrow \quad d \in \{1, 2, 3, 4, 6, 12\}$$

Alle Untergruppen von $\mathbb{Z}/12\mathbb{Z}$ — der Untergruppenverband

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd}
 & 1\mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\
2\mathbb{Z} \arrow[d, dash] \arrow[drr, dash] & & 3\mathbb{Z} \arrow[d, dash] \\
4\mathbb{Z} \arrow[dr, dash] & & 6\mathbb{Z} \arrow[dl, dash] \\
 & 12\mathbb{Z} &
\end{tikzcd}
\quad
\overset{\text{Korrespondenz}}{\underset{\text{Satz J2w}}{\longleftrightarrow}}
\quad
\begin{tikzcd}
 & 1\mathbb{Z}/12\mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\
2\mathbb{Z}/12\mathbb{Z} \arrow[d, dash] \arrow[drr, dash] & & 3\mathbb{Z}/12\mathbb{Z} \arrow[d, dash] \\
4\mathbb{Z}/12\mathbb{Z} \arrow[dr, dash] & & 6\mathbb{Z}/12\mathbb{Z} \arrow[dl, dash] \\
 & 12\mathbb{Z}/12\mathbb{Z} &
\end{tikzcd}$$

alle Untergruppen
$12\mathbb{Z} \leq A \leq \mathbb{Z}$

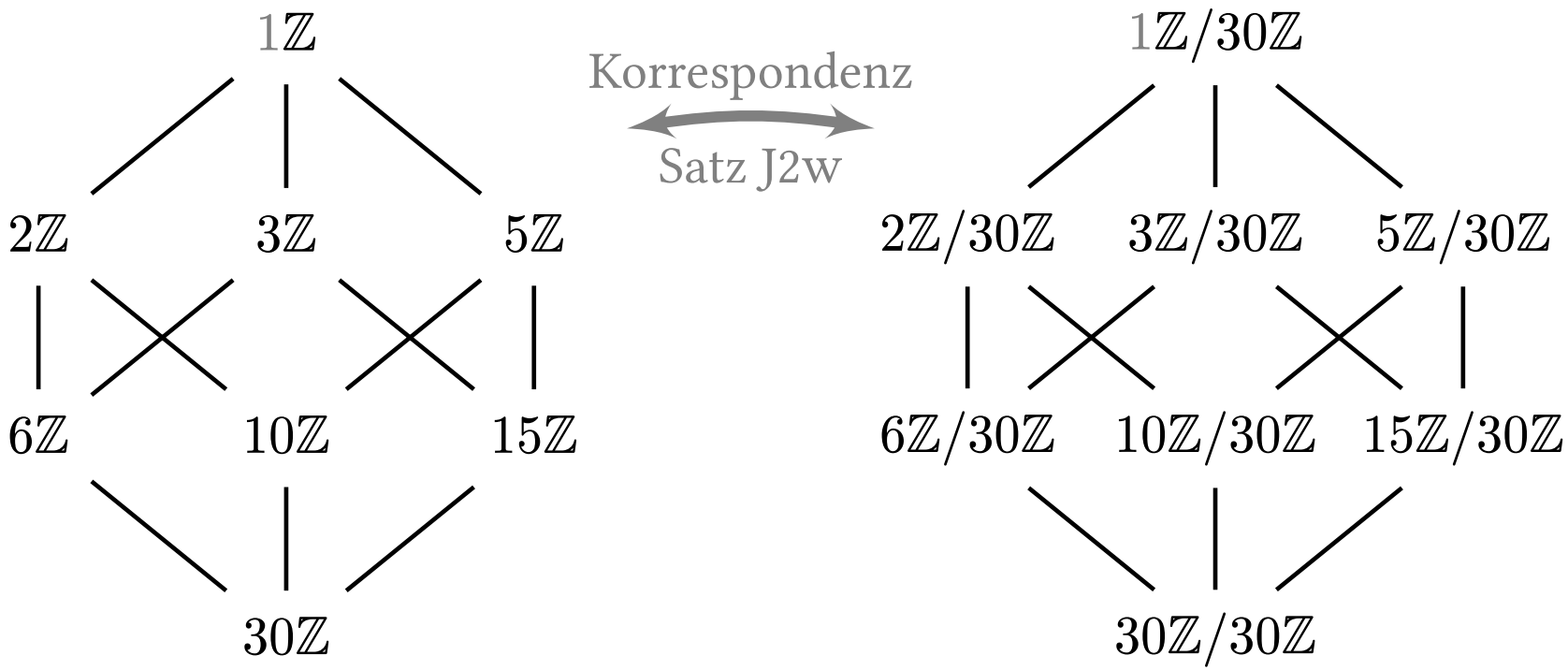
alle Untergruppen
$\{\bar{0}\} \leq B \leq \mathbb{Z}/12\mathbb{Z}$

Alle Untergruppen von $\mathbb{Z}/30\mathbb{Z}$ — der Untergruppenverband

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Bestimmen Sie alle Untergruppen $B \leq \mathbb{Z}/n\mathbb{Z}$ für $n = 30$.



alle Untergruppen
$30\mathbb{Z} \leq A \leq \mathbb{Z}$

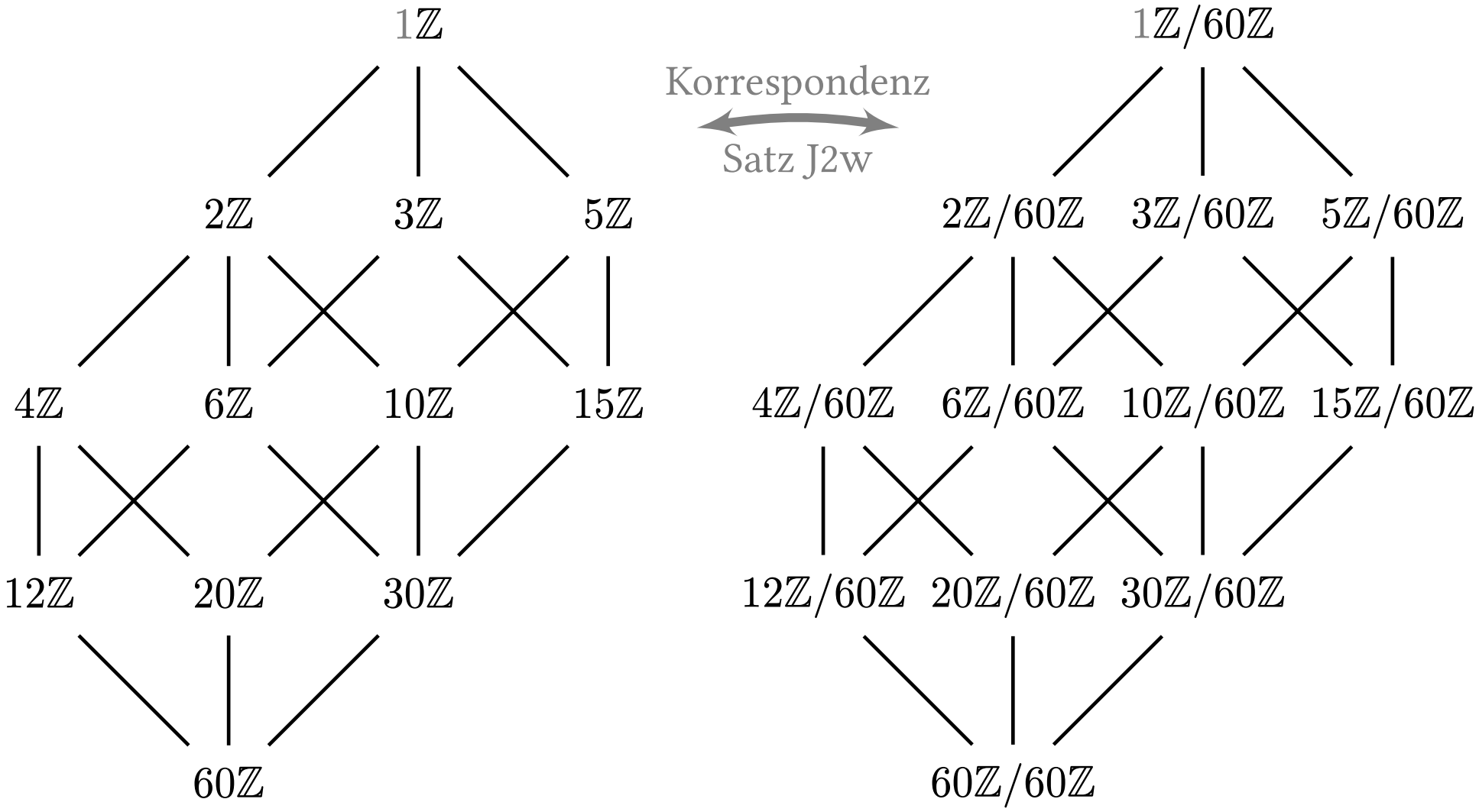
alle Untergruppen
$\{\bar{0}\} \leq B \leq \mathbb{Z}/30\mathbb{Z}$

Alle Untergruppen von $\mathbb{Z}/60\mathbb{Z}$ — der Untergruppenverband

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Bestimmen Sie alle Untergruppen $B \leq \mathbb{Z}/n\mathbb{Z}$ für $n = 60$.



alle Untergruppen
$60\mathbb{Z} \leq A \leq \mathbb{Z}$

alle Untergruppen
$\{\bar{0}\} \leq B \leq \mathbb{Z}/60\mathbb{Z}$

Was ist eine Operation aka Wirkung... von rechts?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Auf den Vektoren $v \in \mathbb{K}^n$ operieren die Skalare $\lambda \in (\mathbb{K}, \cdot, 1)$ von rechts durch Skalierung $(v, \lambda) \mapsto v \bullet \lambda$ mit $(v \bullet \lambda)_i = v_i \cdot \lambda$.

Definition J3A: Rechtsoperation eines Monoids / einer Gruppe

Eine **Rechtsoperation** des Monoids $(G, *, e)$ auf der Menge X ist eine Abbildung $\psi : X \times G \to X : (x, a) \mapsto x \bullet a = xa$, für die gilt:

$$\text{(R1)} \quad x \bullet e = x \quad \text{und} \quad \text{(R2)} \quad (x \bullet a) \bullet b = x \bullet (a * b)$$

Wir schreiben hierfür

$$X \overset{\psi}{\curvearrowleft} (G, *, e) \quad \text{oder kurz} \quad X \overset{\bullet}{\curvearrowleft} G.$$

Für $a \in G^\times$ folgt daraus: $(x \bullet a) \bullet a^{-1} \overset{\text{R2}}{=} x \bullet (a * a^{-1}) \overset{\text{Inv}}{=} x \bullet e \overset{\text{R1}}{=} x.$

Was ist eine Operation aka Wirkung... von links?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Matrizen wirken auf Vektoren, $(\mathbb{K}^{n\times n}, \cdot, 1) \curvearrowright \mathbb{K}^n : (A, v) \mapsto Av$.
Ist A invertierbar, so lösen wir $Ax = y$ eindeutig durch $x = A^{-1}y$.

Definition J3A: Linksoperation eines Monoids / einer Gruppe

Eine **Linksoperation** des Monoids $(G, *, e)$ auf der Menge X ist eine Abbildung $\varphi : G \times X \to X : (a, x) \mapsto a \circ x = ax$, für die gilt:

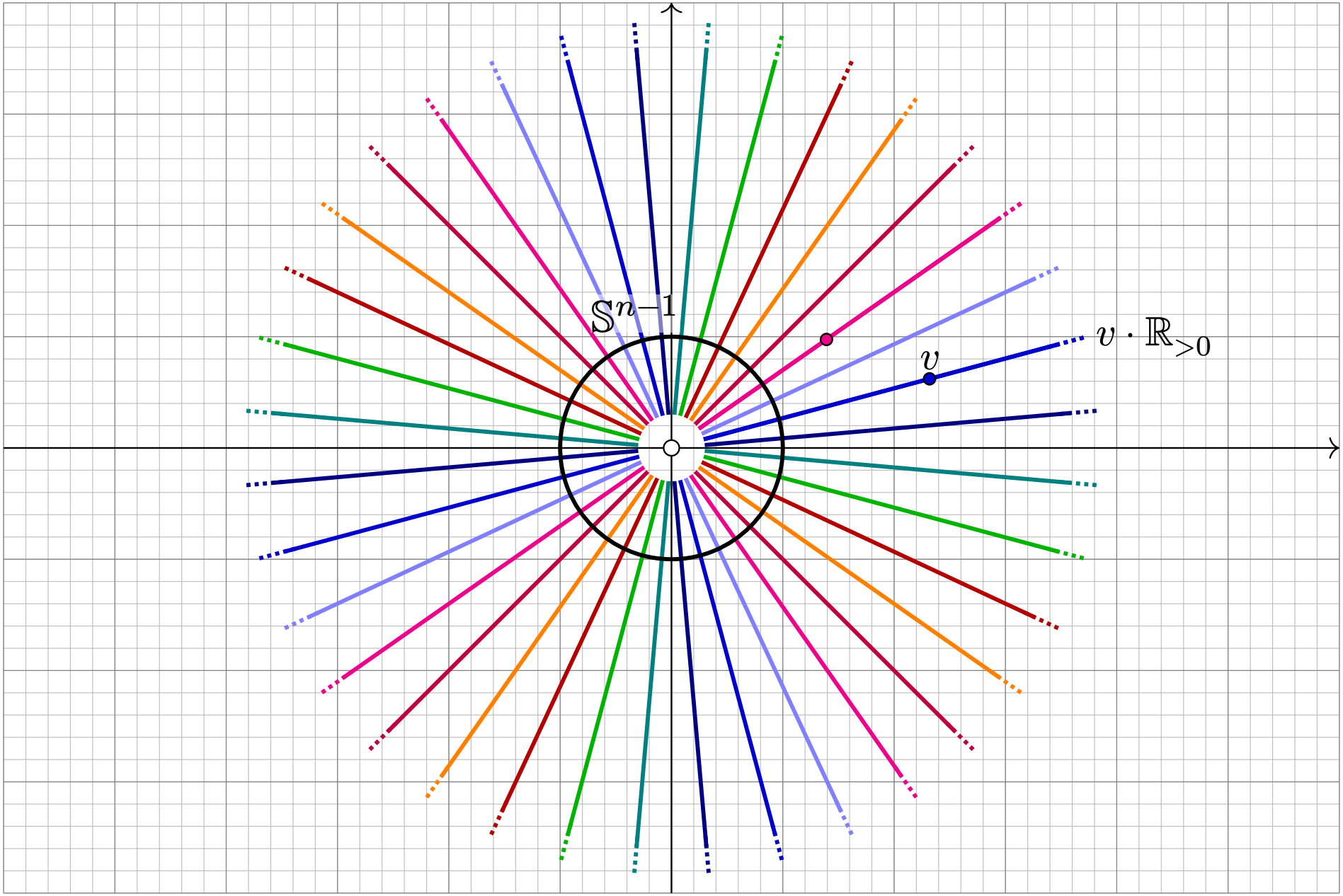
$$\text{(L1)} \quad e \circ x = x \quad \text{und} \quad \text{(L2)} \quad b \circ (a \circ x) = (b * a) \circ x$$

Wir schreiben hierfür

$$(G, *, e) \overset{\varphi}{\curvearrowright} X \quad \text{oder kurz} \quad G \overset{\circ}{\curvearrowright} X.$$

Räumliche Polarkoordinaten: radiale Operation

Auf $X = \mathbb{R}^n \setminus \{0\}$ operiert die Gruppe $G = (\mathbb{R}_{>0}, \cdot)$ durch Skalierung.

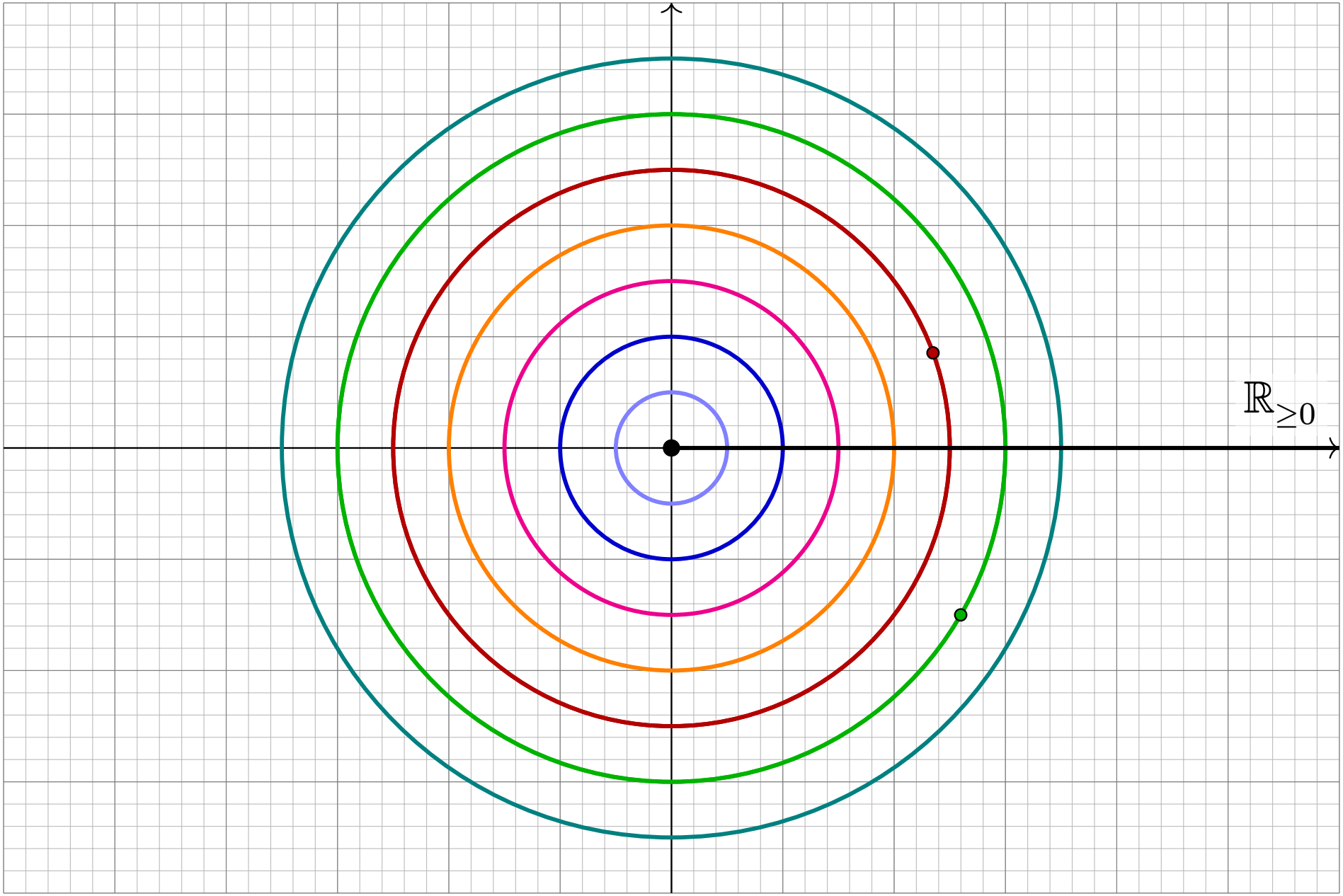


Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Ebene Polarkoordinaten: zirkuläre Operation

Auf $\mathbb{C}$ operiert die Gruppe $(\mathbb{R}, +)$ vermöge $(\mathbb{R}, +) \curvearrowright \mathbb{C} : (\theta, z) \mapsto \mathrm{e}^{\mathrm{i}\theta} \cdot z$.



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Gruppenoperation und Bahnenzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma J3G: Gruppenoperation induziert G–Äquivalenz

Jede Gruppenoperation $(G, \cdot, 1) \curvearrowright X : (g, x) \mapsto gx$ definiert auf der Menge X die zugehörige Äquivalenzrelation $\underset{G}{\sim}$ vermöge

$$x \underset{G}{\sim} y \quad :\Leftrightarrow \quad \exists g \in G : gx = y.$$

Beweis: Die Relation $\underset{G}{\sim}$ auf X erfüllt (R) Reflexivität: $1x = x$.
(S) Symmetrie: Aus $gx = y$ folgt $g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = x$.
(T) Transitivität: Aus $gx = y$ und $hy = z$ folgt $(hg)x = h(gx) = z$. QED

Definition J3G: disjunkte Zerlegung in Bahnen

Die Äquivalenzklasse $Gx = \{\, gx \mid g \in G \,\}$ nennen wir die **Bahn** von x.
Der **Bahnenraum** ist die Quotientenmenge $G\backslash X := \{\, Gx \mid x \in X \,\}$.
Die **Quotientenabbildung** ist $q : X \to G\backslash X : x \mapsto Gx$. Kurzum:

$$G \curvearrowright X \xrightarrow{q} G\backslash X.$$

Operation, links und rechts

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Für jedes Monoid $(G, \cdot, 1)$ erklären wir Operationen links und rechts:

Linksoperation $G \overset{\circ}{\curvearrowright} X$	Rechtsoperation $X \overset{\bullet}{\curvearrowleft} G$
$\circ : G \times X \to X : (g, x) \mapsto g \circ x$	$\bullet : X \times G \to X : (x, g) \mapsto x \bullet g$
$1 \circ x = x, \;\; h \circ (g \circ x) = (h \cdot g) \circ x$	$x \bullet 1 = x, \;\; (x \bullet g) \bullet h = x \bullet (g \cdot h)$
$G \circ x := \{ g \circ x \mid g \in G \}$	$x \bullet G := \{ x \bullet g \mid g \in G \}$

Ist $(G, \cdot, 1)$ sogar eine Gruppe, so zerlegt dies die Menge X in Bahnen:

Bahnenzerlegung links	Bahnenzerlegung rechts
$x \underset{G}{\sim} y \;\; :\Leftrightarrow \;\; \exists g \in G : g \circ x = y$	$x \underset{G}{\backsim} y \;\; :\Leftrightarrow \;\; \exists g \in G : x \bullet g = y$
$G \backslash X := \{ [x] = G \circ x \mid x \in X \}$	$X / G := \{ [x] = x \bullet G \mid x \in X \}$
$G \overset{\circ}{\curvearrowright} X \xrightarrow{q} G \backslash X$	$X / G \xleftarrow{q} X \overset{\bullet}{\curvearrowleft} G$

Fixpunktmenge und Standgruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vorgelegt sei eine Gruppenoperation $X \curvearrowleft (G, \cdot, 1) : (x, g) \mapsto xg$.
Die **Fixpunktmenge** von $g \in G$ ist $\operatorname{fix}(g) = X_g := \{\, x \in X \mid xg = x \,\}$.

Lemma J3H: Standgruppe aka Stabilisator

(a) Zu $x \in X$ ist $\operatorname{stab}(x) = {}_xG := \{\, g \in G \mid xg = x \,\}$ eine Untergruppe.

Beweis: (1) Es gilt $1 \in {}_xG$, denn $x1 = x$.
(2) Für $a, b \in {}_xG$ gilt $ab \in {}_xG$, denn $x(ab) = (xa)b = xb = x$.
(3) Für $a \in {}_xG$ gilt $a^{-1} \in {}_xG$, denn $xa^{-1} = (xa)a^{-1} = x(aa^{-1}) = x$. $\boxed{\text{QED}}$

Triviale Standgruppe bedeutet freie Bahn.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(b) Sei $x \in X$ und $g, h \in G$. Genau dann gilt $xg = xh$, wenn $gh^{-1} \in {}_xG$.

Beweis: Dank J3A(R) gilt $\quad xg = xh \quad \Longleftrightarrow \quad xgh^{-1} = x \quad \Longleftrightarrow \quad gh^{-1} \in {}_xG.$

(c) Genau dann ist $\mu_x : G \twoheadrightarrow xG : g \mapsto xg$ bijektiv, wenn ${}_xG = \{1\}$ gilt.
Wir nennen die Bahn xG dann **frei** oder auch einen **regulären Orbit**.
Sind alle Bahnen frei, so heißt die gesamte Operation $X \curvearrowleft G$ **frei**.

Die freie Bahnengleichung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J31: freie Bahnengleichung

(0) Jedes Repräsentantensystem $R \subseteq X$ bezüglich G–Äquivalenz $\underset{G}{\backsim}$ stiftet eine Bijektion $R \xrightarrow{\sim} X/G : x \mapsto xG$ und somit eine Surjektion

$$\boxed{\mu : R \times G \twoheadrightarrow X : (x, g) \mapsto xg.}$$

(1) Genau dann ist μ bijektiv, wenn die Operation frei ist; daraus folgt:

$$\boxed{|X/G| \cdot |G| = |X|}$$

Beweis: (0) Jeder Punkt $y \in X$ liegt in genau einer Bahn $B \in X/G$ (J3G). Dazu gehört genau ein Repräsentant: $B \cap R = \{x\}$. Zu $y \in xG$ existiert $g \in G$ mit $y = xg$. (1) Eindeutig ist g gdw die Bahn frei ist. QED

Anwendung: Wie viele Geraden gibt es in $V = \mathbb{F}_q^n$?

Die Menge $V^* = \mathbb{F}_q^n \setminus \{0\}$ hat $q^n - 1$ Elemente (ohne den Nullpunkt).
Jede Gerade $v\mathbb{F}_q^\times$ hat genau $q - 1$ Elemente (ohne den Nullpunkt).

$$|V^*/\mathbb{F}_q^\times| = |V^*|/|\mathbb{F}_q^\times| = (q^n - 1)/(q - 1).$$

Beispiel: Für $V = \mathbb{F}_5^3$ über $\mathbb{F}_5$ gilt $(5^3 - 1)/(5 - 1) = 124/4 = 31$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Illustration zum Satz von Lagrange

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: In $G = (\mathrm{S}_3, \bullet, \mathrm{id})$ betrachten wir $U = \langle (1,2) \rangle = \{\mathrm{id}, (1,2)\} \leq G$.

$G/U = \{\, g \bullet U \mid g \in G \,\}$

id	$(2,3)$	$(1,3,2)$
$\mathrm{id}\, U$	$a\, U$	$b\, U$
$(1,2)$	$(1,2,3)$	$(1,3)$

Linksnebenklassen

$U \leq G$

id	$(2,3)$ $(1,3,2)$
$U \leq G$	$G \setminus U$
$(1,2)$	$(1,2,3)$ $(1,3)$

Gruppenelemente

$U \backslash G = \{\, U \bullet g \mid g \in G \,\}$

id	$(2,3)_{U\,a}(1,3,2)$
$U\,\mathrm{id}$	
$(1,2)$	$(1,2,3)^{U\,b}(1,3)$

Rechtsnebenklassen

Für $a = (2,3)$ gilt $aU \neq Ua$: Demnach ist $U \leq G$ **nicht normal** (J4A).

Illustration zum Satz von Lagrange

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Wir betrachten $K = \langle (1,2,3) \rangle \leq G = (\mathrm{S}_3, \bullet, \mathrm{id})$.

$$G/K = \begin{array}{|ccc|} \hline \mathrm{id} & (1,2,3) & (1,3,2) \\ \hline (1,2) & (1,3) & (2,3) \\ \hline \end{array} = K \backslash G$$

Die Untergruppe $K \leq G$ ist **normal** (J4A): Für alle $a \in G$ gilt $aK = Ka$.

Der Satz von Lagrange

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J3J: Satz von Lagrange

Sei $(G, \cdot, 1)$ eine Gruppe. Jede Untergruppe $U \leq G$ operiert vermöge

$$\cdot : G \times U \to G : (g, u) \mapsto gu.$$

Diese Operation ist frei, denn $gu = g$ impliziert $u = 1$. Dank J3I gilt:

$$\boxed{|G| = |G/U| \cdot |U|}$$

Wir nennen $[G : U] := |G/U|$ den **Index** der Untergruppe U in G.

Satz von Lagrange: graphische Darstellung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$G \geq U$	r_1U	r_2U	r_3U	r_4U	r_5U	$\dots$	r_kU
u_ℓ	r_1u_ℓ	r_2u_ℓ	r_3u_ℓ	r_4u_ℓ	r_5u_ℓ	$\dots$	r_ku_ℓ
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\iddots$	$\vdots$
u_3	r_1u_3	r_2u_3	r_3u_3	r_4u_3	r_5u_3	$\dots$	r_ku_3
u_2	r_1u_2	r_2u_2	r_3u_2	r_4u_2	r_5u_2	$\dots$	r_ku_2
u_1	r_1u_1	r_2u_1	r_3u_1	r_4u_1	r_5u_1	$\dots$	r_ku_1
	r_1	r_2	r_3	r_4	r_5	$\dots$	r_k

$R \subseteq G$

Anwendung: Elementordnung teilt Gruppenordnung.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar J3K: Elementordnung $\operatorname{ord}(a) = |\langle a \rangle|$ teilt Gruppenordnung.

(1) Für jede endliche Gruppe $(G, \cdot)$ und $a \in G$ gilt $|G| = [G : \langle a \rangle] \cdot |\langle a \rangle|$.

Beispiel: Gibt es in S_6 Elemente der Ordnung 7? Nein, denn $7 \nmid 6! = 720$.

Anwendung: Gruppen von Primordnung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar J3κ: Gruppen von Primordnung

(2) Jede Gruppe $(G, \cdot, 1)$ von Primordnung $|G| = p$ ist zyklisch.
Genauer: Jedes Element $a \in G \smallsetminus \{1\}$ erzeugt $G = \langle a \rangle \cong \mathbb{Z}/p\mathbb{Z}$.

Beweis: Dank Lagrange J3J gilt $|G| = [G : \langle a \rangle] \cdot |\langle a \rangle|$, also $|\langle a \rangle| \in \{1, p\}$. Für $a \neq 1$ folgt $|\langle a \rangle| = p$, somit $\langle a \rangle = G$. Dank Satz J2v erhalten wir

$$\varphi_a : (\mathbb{Z}/p\mathbb{Z}, +) \xrightarrow{\sim} (G, \cdot) : k + p\mathbb{Z} = [k] \mapsto a^k.$$

Beispiel: Bestimmen Sie alle Gruppen G der Ordnung 1999.
Lösung: Die Zahl $p = 1999$ ist prim. Also gilt $G = \langle a \rangle \cong \mathbb{Z}/p\mathbb{Z}$.

Bahn und Standgruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J3N: Orbit-Stabilisator-Satz

Für jede Gruppenoperation $(G, \cdot, 1) \curvearrowright X : (g, x) \mapsto gx$ und $x \in X$ gilt:

$$\begin{array}{llll} \mu_x & : G & \twoheadrightarrow Gx & : a \mapsto ax \\ \bar{\mu}_x & : G/G_x & \xrightarrow{\sim} Gx & : aG_x \mapsto ax \end{array}$$

Daraus folgt $|Gx| = [G : G_x]$, dank Lagrange J3J also $|G| = |Gx| \cdot |G_x|$.

☺ Die Gruppenordnung ist gleich Bahnlänge mal Stabilisatorordnung.

Beweis: Nach Konstruktion ist die Abbildung μ_x surjektiv.
Weiterhin gilt $ax = bx \Leftrightarrow x = a^{-1}bx \Leftrightarrow a^{-1}b \in G_x \Leftrightarrow b \in aG_x$.
Somit ist $\bar{\mu}_x$ wohldefiniert (dank „$\Leftarrow$“) und injektiv (dank „$\Rightarrow$“). QED

Bahn und Standgruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Die symmetrische Gruppe $G = (\mathrm{S}_n, \circ, \mathrm{id})$ operiert auf der Punktmenge $X = \{1, \dots, n\}$ vermöge $G \curvearrowright X : (\sigma, x) = \sigma(x)$ mit Orbit $Gn = X$ und Stabilisator $G_n = \{\sigma \in G \mid \sigma(n) = n\} \cong \mathrm{S}_{n-1}$. So finden wir $|\mathrm{S}_n| = |X| \cdot |S_{n-1}|$, also rekursiv $|\mathrm{S}_n| = n \cdot (n-1)! = n!$.

Die Ordnung kommutierender Elemente

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma J3o: Ordnung kommutierender Elemente

(1) Seien $a, b \in G$ Gruppenelemente mit $\operatorname{ord}(a) =: k$ und $\operatorname{ord}(b) =: \ell$ in $\mathbb{N}$. Gilt $ab = ba$ in G und $\operatorname{ggT}(k, \ell) = 1$ in $\mathbb{Z}$, so folgt $\operatorname{ord}(ab) = k\ell$.

Beweis: (1a) Sei $n = \operatorname{ord}(ab)$. Wir haben $(ab)^{k\ell} = a^{k\ell}\, b^{\ell k} = 1$, also $n \mid k\ell$.
(1b) Dank Bézout B3E existieren $u, v \in \mathbb{Z}$ mit $uk + v\ell = 1$. Demnach gilt $(ab)^{uk} = a^{uk}\, b^{1-v\ell} = b$ und $(ab)^{v\ell} = a^{1-uk}\, b^{v\ell} = a$, also $a, b \in \langle ab \rangle$.
Dank Lagrange J3K folgt $k, \ell \mid n$, also $k\ell = \operatorname{kgV}(k, \ell) \mid n$. QED

Der Exponent einer abelschen Gruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Der **Exponent** einer Gruppe $(G, \cdot)$ ist

$$\boxed{\exp(G) := \operatorname{kgV}\{\operatorname{ord}(a) \mid a \in G\}.}$$

Beispiel: Es gilt $\exp(\mathrm{S}_n) = \operatorname{kgV}\{1, \dots, n\}$. Warum? Zykelzerlegung H1D!

Ist die Gruppe endlich, so folgt $\exp(G) \mid \operatorname{ord}(G)$ dank Lagrange J3K und $\exp(G) = \min\{n \in \mathbb{N}_{\geq 1} \mid \forall a \in G : a^n = 1\}$.

Lemma J3O: Exponent einer abelschen Gruppe

(2) Ist G abelsch und endlich, dann folgt $\exp(G) = \max\{\operatorname{ord}(a) \mid a \in G\}$.

Beweis: Wir primzerlegen $\exp(G) = p_1^{e_1} \cdots p_\ell^{e_\ell}$. Zu jedem Index $i = 1, \dots, \ell$ existiert $x_i \in G$ mit $\operatorname{ord}(x_i) = p_i^{e_i} k$. Für $a_i := x_i^k$ folgt dann $\operatorname{ord}(a_i) = p_i^{e_i}$. Dank (1) hat $a = a_1 \cdots a_\ell$ die Ordnung $\operatorname{ord}(a) = p_1^{e_1} \cdots p_\ell^{e_\ell} = \exp(G)$. $\boxed{\text{QED}}$

Charakterisierung zyklischer Gruppen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma J3o: Charakterisierung zyklischer Gruppen

(3) Eine endliche abelsche Gruppe G ist zyklisch gdw $\exp(G) = \operatorname{ord}(G)$.

Beweis: „$\Rightarrow$“: Für $G = \langle a \rangle$ gilt $\operatorname{ord}(a) \mid \exp(G) \mid \operatorname{ord}(G) = \operatorname{ord}(a)$, also $\exp(G) = \operatorname{ord}(G)$. „$\Leftarrow$“: Angenommen $\exp(G) = \operatorname{ord}(G)$. Dank (2) existiert $a \in G$ mit $\operatorname{ord}(a) \overset{(2)}{=} \exp(G) \overset{\text{Vor}}{=} \operatorname{ord}(G)$, also $\langle a \rangle = G$. $\boxed{\text{QED}}$

Die multiplikative Gruppe $(\mathbb{F}_q^\times, \cdot)$ ist zyklisch.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele: $\mathbb{F}_2^\times = \langle [1] \rangle$

$\mathbb{F}_3^\times = \langle [2] \rangle$: $a = [2],\ a^2 = [1]$

$\mathbb{F}_5^\times = \langle [2] \rangle$: $a = [2],\ a^2 = [4],\ a^3 = [3],\ a^4 = [1]$

$\mathbb{F}_7^\times = \langle [3] \rangle$: $a = [3],\ a^2 = [2],\ a^3 = [6],\ a^4 = [4],\ a^5 = [5],\ a^6 = [1]$

Primitivwurzel: Zu $p \in \mathbb{P}$ suchen wir $\alpha \in \mathbb{N}$ (minimal) mit $\mathbb{F}_p^\times = \langle [\alpha] \rangle$.

p	2	3	5	7	11	13	17	19	23	29
α	1	2	2	3	2	2	3	2	5	2

p	31	37	41	43	47	53	59	61	67	71
α	3	2	6	3	5	2	2	2	2	7

p	73	79	83	89	97	101	103	107	109	113
α	5	3	2	3	5	2	5	2	6	3

Zyklische Untergruppen $W_n \leq (\mathbb{K}^\times, \cdot)$ und Primitivwurzeln

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

In $\mathbb{C}$ haben wir zu jeder gewünschten Ordnung $n \in \mathbb{N}_{\geq 1}$ die Untergruppe $W_n = \{\, z \in \mathbb{C} \mid z^n = 1 \,\} = \{\, \mathrm{e}^{2\pi \mathrm{i} k/n} \mid k = 0, \dots, n-1 \,\}^! = \langle \mathrm{e}^{2\pi \mathrm{i}/n} \rangle \leq (\mathbb{C}^\times, \cdot)$.
In $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ finden wir nur $W_1 = \{1\}$ und $W_2 = \{\pm 1\} = \langle -1 \rangle$.

Satz J3P: zyklische Untergruppen und Primitivwurzeln

(1) Sei $(\mathbb{K}, +, \cdot)$ ein Körper oder allgemeiner ein Integritätsring.

Zu jeder Ordnung $n \in \mathbb{N}_{\geq 1}$ existiert höchstens eine Untergruppe $W_n \leq (\mathbb{K}^\times, \cdot)$, nämlich $W_n = \{\, x \in \mathbb{K} \mid x^n = 1 \,\}$. (2) Diese ist zyklisch.

(3) Für jeden endlichen Körper $(\mathbb{F}_q, +, \cdot)$ ist demnach $\mathbb{F}_q^\times = \langle a \rangle$ zyklisch: Es gibt eine **Primitivwurzel** $a \in \mathbb{F}_q^\times$ mit $\langle a \rangle = \mathbb{F}_q^\times = \{\, a, a^2, \dots, a^{q-1} = 1 \,\}^!$.

Beweis: (1) „$\subseteq$“: Elementordnung teilt Gruppenordnung (Lagrange, J3K).
„$=$“: Das Polynom $X^n - 1$ hat in $\mathbb{K}$ höchstens n Nullstellen. (Satz C2C).

(2) Für $m := \exp(W_n)$ gilt $W_n \subseteq \{\, x \in \mathbb{K} \mid x^m = 1 \,\}$. Daraus folgt $m = n$.
Dank Lemma J3O ist W_n zyklisch. QED

Jeder Kern ist ein Normalteiler.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

? Wie charakterisieren wir die Kerne von Gruppenhomomorphismen?

♦ Satz J2U: Kern und Faser

Vorgelegt sei ein Gruppenhomomorphismus $\varphi : (G, \cdot, 1) \to (H, \bullet, e)$.
(1) Sein Kern ist eine Untergruppe, $K = \operatorname{Ker}(\varphi) := \varphi^{-1}(\{e\}) \leq (G, \cdot)$.
(2) Für jedes Element $a \in G$ und $b = \varphi(a)$ gilt $\varphi^{-1}(\{b\}) = aK = Ka$.

Die Bedingung $aK = Ka$ ist äquivalent zu $K = a^{-1}Ka$, das heißt K ist stabil unter Konjugation $x \mapsto x^a := a^{-1}xa$, also $K \mapsto K^a := \{\, x^a \mid x \in K \,\}$.

Definition J4A: normale Untergruppe aka Normalteiler

Sei $(G, \cdot, 1)$ eine Gruppe. Eine Untergruppe $N \leq G$ heißt **normal** in G, geschrieben $N \trianglelefteq G$, falls $N^g = N$ für alle $g \in G$ gilt, also $gN = Ng$.

Beispiele: In jeder Gruppe $(G, \cdot)$ sind $\{1\}$ und G normale Untergruppen.
Für jeden Gruppenhomomorphismus $\varphi : G \to H$ ist $\operatorname{Ker}\varphi \trianglelefteq G$ normal.
In S_3 ist $\langle (1,2,3) \rangle \trianglelefteq \mathrm{S}_3$ normal (J334), doch $\langle (1,2) \rangle \leq \mathrm{S}_3$ nicht (J333).
Ist $(G, \cdot)$ abelsch, so ist jede Untergruppe $N \leq G$ normal da $a^g = a$.

Jeder Normalteiler ist ein Kern.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J4A: Quotientengruppe zu einem Normalteiler

(0) Zu jeder Untergruppe $K \leq (G, \cdot, 1, ^{-1})$ haben wir den Quotienten H3A

$$\pi : G \twoheadrightarrow G/K : g \mapsto [g] := gK.$$

(1) Gilt $K \trianglelefteq G$, so erbt $Q = G/K$ die (wohldefinierte!) Verknüpfung

$$\bullet : Q \times Q \to Q : [a] \bullet [b] = [a \cdot b].$$

(2) Damit ist $(Q, \bullet)$ eine Gruppe und π ein Homomorphismus mit Kern K.

Beweis: (1) Für $a' \in [a]$ und $b' \in [b]$ gilt $a' = ah$ und $b' = bk$ mit $h, k \in K$, also $a' \cdot b' = ah \cdot bk = ab \cdot (b^{-1}hb)k \in ab \cdot K$, somit $[a'b'] = [ab]$.

Konstruktion der Quotientengruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(2a) Unser Produkt $\bullet : Q \times Q \to Q$ ist assoziativ:

$$([a] \bullet [b]) \bullet [c] \overset{\text{Def}}{=} [(a \cdot b) \cdot c] \overset{\text{Ass}}{=} [a \cdot (b \cdot c)] \overset{\text{Def}}{=} [a] \bullet ([b] \bullet [c])$$

(2b) In $(Q, \bullet)$ ist das Element $[1]$ neutral:

$$[1] \bullet [a] \overset{\text{Def}}{=} [1 \cdot a] \overset{\text{Ntr}}{=} [a]$$
$$[a] \bullet [1] \overset{\text{Def}}{=} [a \cdot 1] \overset{\text{Ntr}}{=} [a]$$

(2c) In $(Q, \bullet, [1])$ ist $[a^{-1}]$ invers zu $[a]$:

$$[a] \bullet [a^{-1}] \overset{\text{Def}}{=} [a \cdot a^{-1}] \overset{\text{Ntr}}{=} [1]$$
$$[a^{-1}] \bullet [a] \overset{\text{Def}}{=} [a^{-1} \cdot a] \overset{\text{Ntr}}{=} [1]$$

Faktorisierung über eine Surjektion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J4c: Wir faktorisieren φ über π zu $\bar{\varphi}$.

Vorgelegt seien Gruppenhomomorphismen $\pi : G \twoheadrightarrow Q$ surjektiv und $\varphi : G \to H$ beliebig. Gilt $\operatorname{Ker}(\pi) \subseteq \operatorname{Ker}(\varphi)$, so existiert genau ein Homomorphismus $\bar{\varphi} : Q \to H$ mit $\varphi = \bar{\varphi} \circ \pi$.

$$\begin{tikzcd} (G,\cdot) \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & (H,*) \\ (Q,\bullet) \arrow[ur, dashed, "\exists!\bar{\varphi}"'] & \end{tikzcd}$$

Beweis: *Eindeutigkeit:* Aus $\bar{\varphi} \circ \pi = \tilde{\varphi} \circ \pi$ folgt $\bar{\varphi} = \tilde{\varphi}$, da π surjektiv ist.

Konstruktion: Zu jedem $\bar{x} \in Q$ wählen wir *willkürlich* ein Urbild $x \in G$ mit $\pi(x) = \bar{x}$ und setzen $\bar{\varphi}(\bar{x}) := \varphi(x)$. Ist das Ergebnis *wohldefiniert*? Ja, aus $\pi(x) = \pi(x')$ folgt $x^{-1}x' \in \operatorname{Ker}(\pi) \subseteq \operatorname{Ker}(\varphi)$, also $\varphi(x) = \varphi(x')$.

Homomorphie: Für alle $\bar{x}, \bar{y} \in Q$ und Urbilder $x, y \in G$ gilt $\pi(x \cdot y) \overset{\text{Hom}}{=} \bar{x} \bullet \bar{y}$, nach Konstuktion also $\bar{\varphi}(\bar{x} \bullet \bar{y}) \overset{\text{Def}}{=} \varphi(x \cdot y) \overset{\text{Hom}}{=} \varphi(x) * \varphi(y) \overset{\text{Def}}{=} \bar{\varphi}(\bar{x}) * \bar{\varphi}(\bar{y})$. $\boxed{\text{QED}}$

Injektiv und surjektiv machen: kanonische Faktorisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{tikzcd}
(G,\cdot) \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"', "{[x]\leftarrow\!\shortmid x}"] & (H,*) \\
G/\operatorname{Ker}(\varphi) \arrow[r, "\bar\varphi", "{[x]\mapsto\varphi(x)}"'] & \operatorname{Im}(\varphi) \arrow[u, hook, "\iota", "{y\mapsto y}"']
\end{tikzcd}
$$

Satz J4D: kanonische Faktorisierung aka Homomorphiesatz

Jeder Homomorphismus $\varphi : G \to H$ faktorisiert gemäß $\varphi = \iota \circ \bar\varphi \circ \pi$ in

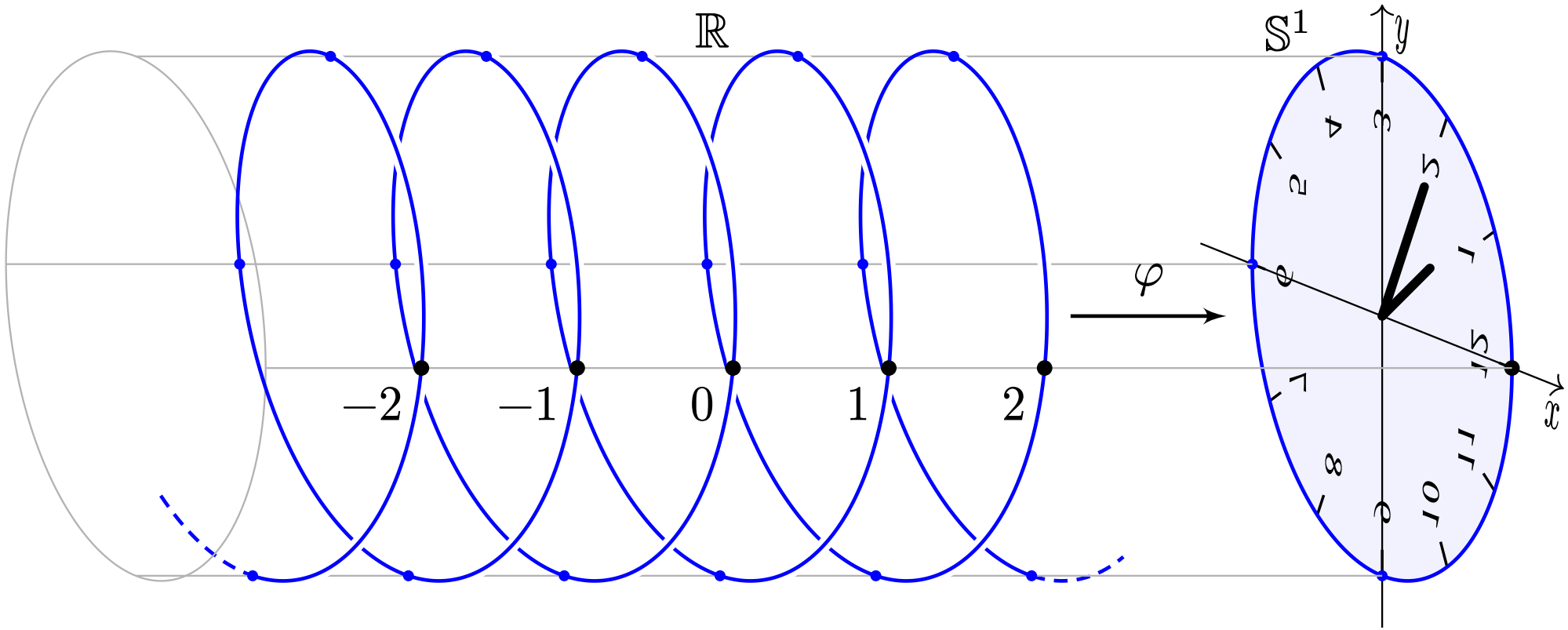
1. die Quotientenabbildung $\pi : G \twoheadrightarrow G/\operatorname{Ker}(\varphi) : x \mapsto [x]$,
2. die Bijektion $\bar\varphi : G/\operatorname{Ker}(\varphi) \xrightarrow{\sim} \operatorname{Im}(\varphi) : [x] \mapsto \varphi(x)$,
3. die Inklusion $\iota : \operatorname{Im}(\varphi) \hookrightarrow H : y \mapsto y$.

Dies sind Homomorphismen. Dank Satz J2I ist $\bar\varphi$ ein Isomorphismus. Dank Lagrange J3J gilt $|\operatorname{Im}\varphi| = [G : \operatorname{Ker}\varphi]$ und $|G| = |\operatorname{Ker}\varphi| \cdot |\operatorname{Im}\varphi|$.

Anwendungsbeispiel: die Gruppe $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Wir parametrisieren die Kreislinie $\mathbb{S}^1$ in Polarkoordinaten durch

$$\varphi : (\mathbb{R}, +) \to (\mathbb{C}^\times, \cdot) : t \mapsto \mathrm{e}^{2\pi \mathrm{i} t} = \cos(2\pi t) + \mathrm{i}\sin(2\pi t)$$

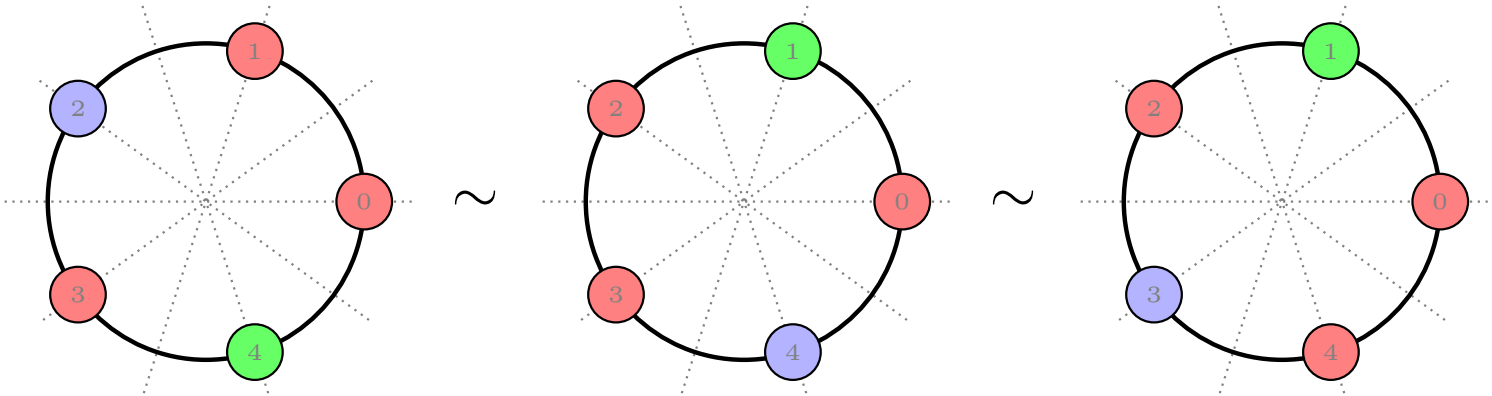
und erhalten den Isomorphismus $\bar{\varphi} : (\mathbb{R}/\mathbb{Z}, +) \xrightarrow{\sim} (\mathbb{S}^1, \cdot) : t + \mathbb{Z} \mapsto \mathrm{e}^{2\pi \mathrm{i} t}$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel J

Bonusmaterial



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)

Inhalt dieses Kapitels J

5 Gruppen: Beispiele und Anwendungen

6 Birkhoffs universelle Algebra: *abstract nonsense*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zusammenfassung: Lagrange & Orbit-Stabilisator-Satz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J3J von Lagrange: Für jede Untergruppe $U \leq G$ gilt

$$\boxed{|G| = |G/U| \cdot |U|}$$

In Worten: „Gruppenordnung gleich Index mal Untergruppenordnung.“
Falls endlich: „Die Untergruppenordnung $|U|$ teilt Gruppenordnung $|G|$.“
Spezialfall: „Die Elementordnung $|\langle a \rangle|$ teilt die Gruppenordnung $|G|$.“

Orbit-Stabilisator-Satz J3N für $G \curvearrowright X$ und $x \in X$:

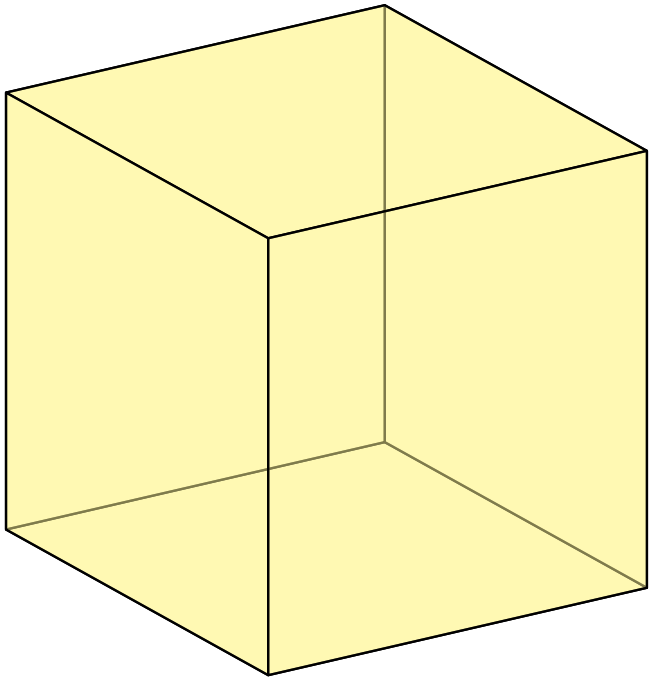
$$\boxed{|G| = |Gx| \cdot |G_x|}$$

In Worten: „Gruppenordnung gleich Orbitlänge mal Stabilisatorordnung.“

Wie viele Symmetrien hat der Würfel aka Hexaeder?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



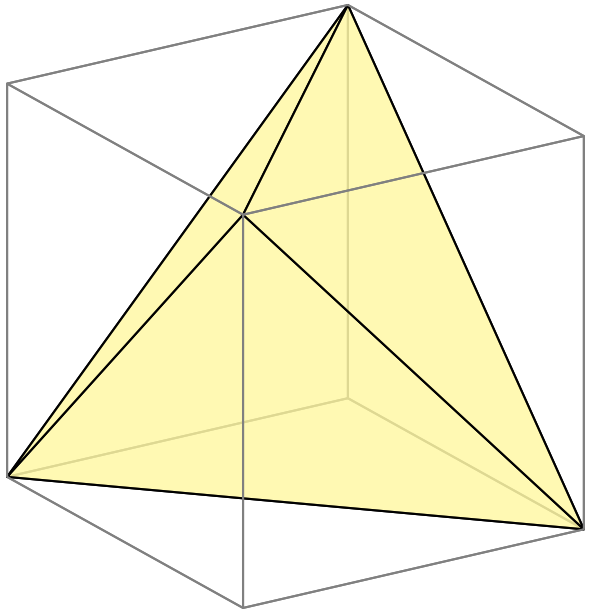
$$G = \mathrm{Isom}^{+}(\mathbb{R}^3, W) \quad \Longrightarrow \quad |G| = |Gv| \cdot |G_v| = 8 \cdot 3 = 24$$

$$H = \mathrm{Isom}^{\pm}(\mathbb{R}^3, W) \quad \Longrightarrow \quad |H| = |Hv| \cdot |H_v| = 8 \cdot 6 = 48$$

Wie viele Symmetrien hat das Tetraeder?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



$$G = \mathrm{Isom}^{+}(\mathbb{R}^3, T) \quad \Longrightarrow \quad |G| = |Gv| \cdot |G_v| = 4 \cdot 3 = 12$$

$$H = \mathrm{Isom}^{\pm}(\mathbb{R}^3, T) \quad \Longrightarrow \quad |H| = |Hv| \cdot |H_v| = 4 \cdot 6 = 24$$

Was ist die mittlere Fixpunktzahl?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sie ziehen zufällig, gleichverteilt eine Permutation aus S_5. Wie viele Fixpunkte erwarten Sie?

Repräsentant	Anzahl	Fixpunkte
id	1	5
$(1,2)$	10	3
$(1,2,3)$	20	2
$(1,2,3,4)$	30	1
$(1,2)(3,4)$	15	1
$(1,2,3,4,5)$	24	0
$(1,2,3)(4,5)$	20	0

Damit finden wir $(1 \cdot 5 + 10 \cdot 3 + 20 \cdot 2 + 30 \cdot 1 + 15 \cdot 1)/120 = 1$.

Der Abzählsatz aka Burnside–Lemma

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz J5E: Abzählsatz nach Cauchy–Frobenius–Burnside

Für jede Operation $X \curvearrowleft G : (x, g) \mapsto xg$ einer endlichen Gruppe G gilt:

$$\boxed{|X/G| = \frac{1}{|G|} \sum_{g \in G} \big|\mathrm{fix}(g)\big|}$$

Beweis: (1) Wir betrachten die Menge

$$\big\{ (x, g) \in X \times G \,\big|\, xg = x \big\} \;=\; \bigsqcup_{g \in G} X_g \times \{g\} \;=\; \bigsqcup_{x \in X} \{x\} \times {}_x G.$$

Hier ist $X_g = \mathrm{fix}(g) = \{ x \in X \,|\, xg = x \}$ die Fixpunktmenge von $g \in G$ und ${}_x G = \mathrm{stab}(x) = \{ g \in G \,|\, xg = x \}$ die Stabilisatorgruppe von $x \in X$.

$$\sum_{g \in G} |X_g| \overset{(1)}{=} \sum_{x \in X} |{}_x G| \overset{\text{J3N}}{=} \sum_{B \in X/G} \sum_{x \in B} |G|/|B| \overset{\mathbb{Q}}{=} \sum_{B \in X/G} |G| \overset{\mathbb{Z}}{=} |X/G| \cdot |G|$$

Der Abzählsatz aka Burnside–Lemma

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

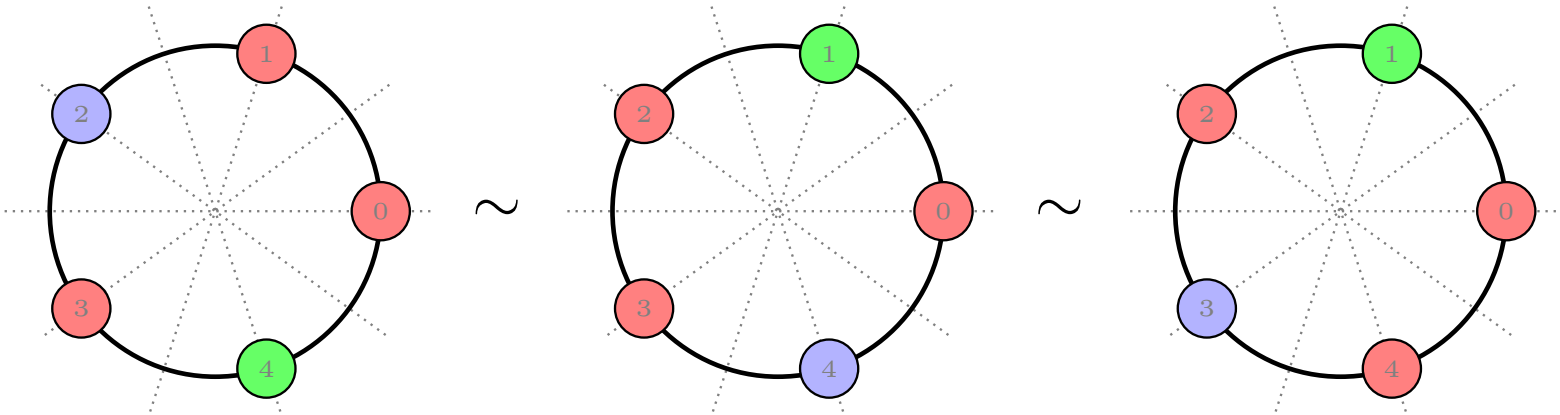
Aufgabe: Sie ziehen zufällig, gleichverteilt ein Element aus $G = \mathrm{S}_n$. Wie viele Fixpunkte erwarten Sie?

Lösung: Dank Abzählsatz erhalten wir $\sum_{g \in G} |\mathrm{fix}(g)| / |G| = \left|X/G\right| = 1$.

Anwendung: *the bracelet counting problem*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Aufgabe: Sie haben genug Perlen in $c = 3$ Farben. Wie viele *verschiedene* Armbänder mit $n = 5$ Perlen können Sie herstellen? Genauer gefragt:

Wir färben die Eckpunkte $n = \{0, \dots, n-1\}$ eines regulären n–Ecks mit $C = \{1, \dots, c\}$. Färbungen $f, f' : n \to C$ sind *äquivalent*, $f \sim f'$, falls sie durch Drehen oder Spiegeln ineinander übergehen, also $f' = f \circ g$ mit $g \in D_n^{\mathrm{P}}$ (J145). In wie viele Äquivalenzklassen zerfällt $C^n \circlearrowleft D_n^{\mathrm{P}}$?

Anwendung: *the bracelet counting problem*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lösung: Wir wenden Burnsides Abzählsatz J5E auf $C^n = X \curvearrowleft D_n$ an.
Zu jedem Gruppenelement $g \in D_n$ bestimmen wir die Fixpunktzahl $|X_g|$:

$g \in D_5$	r_0	r_1	r_2	r_3	r_4	s_0	s_1	s_2	s_3	s_4
$\lvert X_g \rvert$	c^5	c^1	c^1	c^1	c^1	c^3	c^3	c^3	c^3	c^3

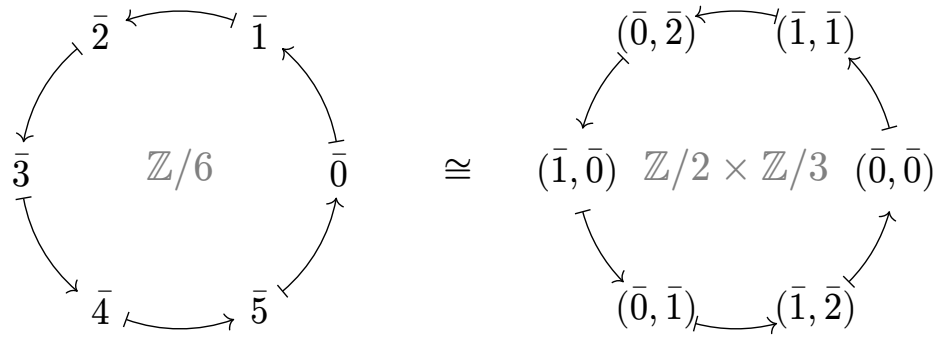
Wir finden $B(5,c) := |C^n/D_n| = \sum_{g \in D_n} |X_g|/|D_n| = (c^5 + 5c^3 + 4c)/10$.
Zahlenbeispiel: Für $c = 3$ gilt $|C^5| = 243$ und $B(5,3) = |C^n/D_n| = 39$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel K

Ringe und Körper



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, on the other hand, are usually considered by specialists only.

Paul Halmos (1916–2006), *Linear Algebra Problem Book*

Inhalt dieses Kapitels K

1 Ringe und Körper

2 Konstruktion: neue Ringe aus alten!

3 Matrizen, Polynome, Brüche

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Ringe und Körper: Definition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition K1A: Ring und Körper

Ein **Ring** $(R, +, 0, \cdot, 1)$ besteht aus (A) einer abelschen Gruppe $(R, +, 0)$ und (M) einem Monoid $(R, \cdot, 1)$, sodass $\cdot$ über $+$ distribuiert (D).

(C) Zwei Ringelemente $a, b \in R$ **kommutieren**, falls $a \cdot b = b \cdot a$ gilt. Gilt dies für alle $a, b \in R$, so heißt der Ring **kommutativ**, kurz CRing.

Wir setzen $R^* := R \setminus \{0\}$. Gilt $a \cdot b = 0$ für $a, b \in R^*$, so nennen wir a und b einen **(Links/Rechts)Nullteiler**. Der Ring $(R, +, 0, \cdot, 1)$ heißt...

1. **Bereich** oder **nullteilerfrei**, falls $R^* < (R, \cdot, 1)$ ein Monoid ist,
2. **Integritätsring**, kurz **IRing**, falls $(R, \cdot)$ zudem kommutativ ist;
3. **Divisionsring**, kurz **DRing**, falls $R^* < (R, \cdot, 1)$ eine Gruppe ist,
4. **Körper**, frz. *corps*, engl. *field*, falls $(R, \cdot)$ zudem kommutativ ist.

Ringe und Körper: Beispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele: Der Nullring $(\{0\}, +, 0, \cdot, 1)$ ist der einzige Ring mit $1 = 0$.

Sie kennen bereits die Ringe $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ sowie $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Zum Ring $\mathbb{K}$ haben wir den Polynomring $\mathbb{K}[X]$ und den Matrixring $\mathbb{K}^{n\times n}$.

Rechenregeln für Ringe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma K1c: Vorzeichenregeln

Für jeden Ring $(R, +, 0, \cdot, 1)$ und alle Elemente $a, b \in R$ gilt:

0 $0 \cdot a = 0 = a \cdot 0$

1 Aus $0 = 1$ folgt $R = \{0\}$.

2 $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$

3 $(-a) \cdot (-b) = a \cdot b$

Beweis: (0) Es gilt $(0 \cdot a) + (0 \cdot a) \overset{\text{Dst}}{=} (0 + 0) \cdot a \overset{\text{Ntr}}{=} 0 \cdot a \overset{\text{Ntr}}{=} 0 + (0 \cdot a)$.
Kürzung / Subtraktion von $(0 \cdot a)$ ergibt $0 \cdot a = 0$. Ebenso folgt $a \cdot 0 = 0$.

(1) Aus $0 = 1$ folgt $a \overset{\text{Ntr}}{=} 1 \cdot a \overset{\text{Vor}}{=} 0 \cdot a \overset{(0)}{=} 0$.

(2) Es gilt $(a \cdot b) + ((-a) \cdot b) \overset{\text{Dst}}{=} (a + (-a)) \cdot b \overset{\text{Neg}}{=} 0 \cdot b \overset{(0)}{=} 0$.
Ebenso gilt $(a \cdot b) + (a \cdot (-b)) \overset{\text{Dst}}{=} a \cdot (b + (-b)) \overset{\text{Neg}}{=} a \cdot 0 \overset{(0)}{=} 0$.

(3) Es folgt $(-a) \cdot (-b) \overset{(2)}{=} -(a \cdot (-b)) \overset{(2)}{=} -(-(a \cdot b)) \overset{\text{Neg}}{=} a \cdot b$. QED

Rechenregeln für Körper

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma K1c: Kürzungsregel

In jedem Körper / DRing / IRing / Bereich $(R, +, 0, \cdot, 1)$ gilt zudem:

4. Das Untermonoid $R^* = R \setminus \{0\}$ enthält das Einselement, also $1 \neq 0$.
5. Die multiplikative Abgeschlossenheit von $R^* < (R, \cdot, 1)$ bedeutet:
   $a \neq 0 \ \wedge \ b \neq 0 \quad \Longrightarrow \quad a \cdot b \neq 0$
   $a \cdot b = 0 \quad \Longrightarrow \quad a = 0 \ \vee \ b = 0$
6. Daraus folgt multiplikative Kürzbarkeit:
   $a \cdot x = a \cdot y \ \wedge \ a \neq 0 \quad \Longrightarrow \quad x = y$
   $x \cdot b = y \cdot b \ \wedge \ b \neq 0 \quad \Longrightarrow \quad x = y$

Beweis: (4) und (5) wiederholen die Definition. (6) Aus $a \cdot x = a \cdot y$ folgt $0 \overset{\text{Neg}}{=} (a \cdot x) - (a \cdot y) \overset{(2)}{=} (a \cdot x) + (a \cdot (-y)) \overset{\text{Dst}}{=} a \cdot (x - y)$. Dank $a \neq 0$ und (5) folgt $x - y = 0$, somit $x = y$. $\boxed{\text{QED}}$

Allgemeine Distributivität und binomische Formeln

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz K1G: allgemeine Distributivität und binomische Formeln

(1) In jedem Ring R gilt das **allgemeine Distributivitätsgesetz**:

$$\Big(\sum_{i\in I} a_i\Big)\cdot\Big(\sum_{j\in J} b_j\Big) \;=\; \sum_{(i,j)\in I\times J} a_i\cdot b_j$$

Seien $a, b \in R$ kommutierende Elemente, also $ab = ba$. Dann folgt

$$(2)\;\; (a+b)^2 = a^2 + 2ab + b^2 \quad \text{und} \quad (3)\;\; (a-b)(a+b) = a^2 - b^2.$$

Allgemein für alle $n \in \mathbb{N}$ gilt hierzu (2) der **binomische Lehrsatz**

$$(a+b)^n \;=\; \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

sowie (3) die **geometrische Teleskopsumme**

$$(a-b)\cdot\sum_{i=0}^{n} a^{n-i}b^i \;=\; a^{n+1} - b^{n+1}.$$

Die geometrische Teleskopsumme

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(3) Induktion über $n \in \mathbb{N}$ (Übung!) oder anschaulich wie folgt:

$$\begin{aligned}
(a^n b^0 + a^{n-1} b^1 + \ldots + a^0 b^n) \cdot (a - b) &= \\
a^{n+1} b^0 + a^n b^1 + \ldots + a^1 b^n & \\
- a^n b^1 - \ldots - a^1 b^n - a^0 b^{n+1} &= a^{n+1} - b^{n+1}
\end{aligned}$$

Beispiel: Für $q \in \mathbb{C} \setminus \{1\}$ finden wir die geometrische Summenformel

$$1 + q + q^2 + \ldots + q^{n-1} = \frac{1 - q^n}{1 - q}.$$

Anwendungsbeispiel: ein Trick zur Faktorisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(1) Ist $u := 2^{77} - 1 = 151\,115\,727\,451\,828\,646\,838\,271$ prim?
(2) Ist $v := 2^{80} + 1 = 1\,208\,925\,819\,614\,629\,174\,706\,177$ prim?

Lösung: Wir wissen $(a - b) \mid (a^s - b^s)$, also

$$(2^7 - 1) \mid (2^{77} - 1^{11}), \qquad 127 \mid u,$$
$$(2^{16} - (-1)) \mid (2^{80} - (-1)^5), \qquad 65537 \mid v.$$

Korollar K1H: Mersenne–Zahlen und Fermat–Zahlen

Sei $n \in \mathbb{N}_{\geq 1}$. (1) Ist $u = 2^n - 1$ prim, dann auch n. Kontraposition:
Für $n = rs$ mit $1 < r < n$ gilt $2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + \ldots + 2^r + 1)$.

(2) Ist $v = 2^n + 1$ prim, dann gilt $n = 2^k$ für ein $k \in \mathbb{N}$. Kontraposition:
Für $n = rs$ mit $s \geq 3$ ungerade gilt $2^{rs} + 1 = (2^r + 1)(2^{r(s-1)} \mp \ldots - 2^r + 1)$.

Homomorphismen von Ringen und Körpern

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition K11: Homomorphismen von Ringen und Körpern

Ein **Ringhomomorphismus**

$$\varphi : (R, +_R, 0_R, \cdot_R, 1_R) \to (S, +_S, 0_S, \cdot_S, 1_S)$$

ist eine Abbildung $\varphi : R \to S$, so dass für alle $a, b \in R$ gilt:

$$\begin{aligned} \varphi(a +_R b) &= \varphi(a) +_S \varphi(b), & \varphi(0_R) &= 0_S, \\ \varphi(a \cdot_R b) &= \varphi(a) \cdot_S \varphi(b), & \varphi(1_R) &= 1_S. \end{aligned}$$

Homomorphismen von Ringen und Körpern

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Warnung: Die Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z} : n \mapsto 0$ ist additiv und multiplikativ, erfüllt aber $\varphi(1) = 0 \neq 1$. Demnach ist φ *kein* Ringhomomorphismus.

Die Inklusionen $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \mathbb{H}$ sind Ringhomomorphismen, ebenso die Quotientenabbildung $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} : a \mapsto [a]_n = a + n\mathbb{Z}$.

Die komplexe Konjugation $^{-} : \mathbb{C} \to \mathbb{C} : z = x + \mathrm{i}y \mapsto \overline{z} = x - \mathrm{i}y$ ist ein Automorphismus des Körpers $(\mathbb{C}, +, \cdot)$: Sie erfüllt $\overline{\overline{z}} = z$, $\overline{0} = 0$ und $\overline{z + w} = \overline{z} + \overline{w}$ sowie $\overline{1} = 1$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

Unterringe und Unterkörper

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition K1M: Unterring und Unterkörper

Sei $(R, +, 0, \cdot, 1)$ ein Ring und darin $S \subseteq R$ eine Teilmenge. Wir nennen S einen **Unterring** oder **Teilring**, geschrieben $S \leq (R, +, 0, \cdot, 1)$, falls gilt:

1. $S \leq (R, +, 0)$ ist eine Untergruppe, also $S \neq \emptyset$ und $S - S \subseteq S$ (J2O),
2. $S \leq (R, \cdot, 1)$ ist ein Untermonoid, also $1 \in S$ und $S \cdot S \subseteq S$ (J2M).

In diesem Falle ist $(S, +_S, 0, \cdot_S, 1)$ selbst ein Ring durch Einschränkung und die Inklusion $\mathrm{inc}_S^R : S \hookrightarrow R$ ein Ringhomomorphismus.

Gegenbeispiel: In $(\mathbb{Z}, +, 0, \cdot, 1)$ ist die Teilmenge $\mathbb{N} \subset \mathbb{Z}$ kein Teilring.

Beispiele: $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{H}$ sind Teilringe bzw. Teilkörper.

Unterringe und Unterkörper

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz K1N: Bild eines Ringhomomorphismus

Für jeden Ringhomomorphismus $\varphi : (R, +, 0, \cdot, 1) \to (S, +, 0, \cdot, 1)$ ist das Bild ein Unterring, also $\varphi(R) \leq (S, +, 0, \cdot, 1)$

Beweis: Dank J2U ist die Bildmenge $\varphi(R) \subseteq S$ eine additive Untergruppe in $(S, +, 0)$ und ein multiplikatives Untermonoid in $(S, \cdot, 1)$. $\boxed{\text{QED}}$

Beispiele: Im Polynomring $\mathbb{R}[X]$ ist $1 \cdot \mathbb{R} \leq \mathbb{R}[X]$ ein Teilring (Teilkörper). Auch im Matrixring $\mathbb{R}^{n\times n}$ ist $1_{n\times n} \cdot \mathbb{R} \leq \mathbb{R}^{n\times n}$ ein Teilring (Teilkörper).

Der charakteristische Unterring

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz K1Q: charakteristischer Unterring und Charakteristik

Zu jedem Ring $(R, +, 0, \cdot, 1)$ existiert genau ein Ringhomomorphismus

$$\varphi : (\mathbb{Z}, +, 0, \cdot, 1) \to (R, +, 0, \cdot, 1), \quad \text{nämlich } \varphi(k) = 1_R \cdot k$$

dank Satz J1R. Sein Bild in R ist der **charakteristische Unterring**

$$\mathrm{Char}(R, +, \cdot) := \{1_R \cdot k \mid k \in \mathbb{Z}\} \leq (R, +, \cdot).$$

Wir haben $\mathrm{Ker}(\varphi) := \varphi^{-1}(\{0\}) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ dank J2T, also

$$\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{Char}(R) : [k] \mapsto 1_R \cdot k.$$

Die Zahl $\mathrm{char}(R) := n \in \mathbb{N}$ nennen wir die **Charakteristik** des Rings R.
Ist R nullteilerfrei, so ist n null oder prim, also $n \in \{0, 2, 3, 5, 7, 11, 13, \dots\}$.

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 $\mathrm{char}(R) = n$.

Der Frobenius–Endomorphismus: *a freshman's dream*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $(R,+,\cdot)$ ein Ring. Aus $ab = ba$ in R folgt $(a+b)^2 = a^2 + 2ab + b^2$.
In Charakteristik $\operatorname{char}(R) = 2$ gilt $1_R + 1_R = 0_R$, also $(a+b)^2 = a^2 + b^2$.

Satz K1R: Frobenius–Endomorphismus in Charakteristik p

Sei $(R,+,\cdot)$ ein kommutativer Ring von Primcharakteristik $p > 0$.
Die Potenzierung $\mathfrak{f}_R : (R,+,\cdot) \to (R,+,\cdot) : a \mapsto a^p$ ist dann additiv,

$$(a+b)^p = a^p + b^p \quad \text{für alle } a, b \in R.$$

Beweis: Es gilt $\mathfrak{f}(0) = 0$, $\mathfrak{f}(1) = 1$ und $\mathfrak{f}(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = \mathfrak{f}(a) \cdot \mathfrak{f}(b)$.
Erstaunlich ist $(a+b)^p = a^p + b^p$: Für alle $k \in \mathbb{N}$ mit $0 < k < p$ haben wir

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1} \in p\mathbb{Z}.$$

Dank K1G folgt $\mathfrak{f}(a+b) = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p = \mathfrak{f}(a) + \mathfrak{f}(b)$. $\boxed{\text{QED}}$

Kartesisches Produkt mit koordinatenweiser Verknüpfung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz K2A: Das Produkt $P = \prod_{i\in I} R_i$ von Ringen ist ein Ring.

Ist $(R_i, +_i, 0_i, \cdot_i, 1_i)$ ein Ring für $i \in I$, so auch das kartesische Produkt

$$(P, +, 0, \cdot, 1) =: \prod_{i\in I}(R_i, +_i, 0_i, \cdot_i, 1_i) \quad \text{mit} \quad P := \prod_{i\in I} R_i,$$

$$(a_i)_{i\in I} + (b_i)_{i\in I} := (a_i +_i b_i)_{i\in I}, \qquad 0 := (0_i)_{i\in I},$$

$$(a_i)_{i\in I} \cdot (b_i)_{i\in I} := (a_i \cdot_i b_i)_{i\in I}, \qquad 1 := (1_i)_{i\in I}.$$

(1) Die Projektion $\mathrm{pr}_i : P \twoheadrightarrow R_i : a \mapsto a_i$ ist ein Ringhomomorphismus.

Funktionen mit punktweiser Verknüpfung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Die reellen Funktionen $f : \mathbb{R}^n \supseteq \Omega \to \mathbb{R}$ bilden den Ring $\mathbb{R}^\Omega$.

Beispiel K2B: Potenz R^Ω eines Rings, Funktionenring

Sei Ω eine Menge. Ist $(R, +, \cdot)$ ein Ring, so auch die Potenz

$$(P, +, \cdot) = (R, +, \cdot)^\Omega := \prod_{x \in \Omega} (R, +, \cdot) \text{ mit } P = \{ f : \Omega \to R \},$$
$$(f + g)(x) = f(x) + g(x) \text{ und } (f \cdot g)(x) = f(x) \cdot g(x).$$

Beispiel: Die Potenzmenge $(\mathfrak{P}(\Omega), \triangle, \emptyset, \cap, \Omega)$ ist ein Ring.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel K2c: Die Potenzmenge $(\mathfrak{P}(\Omega), \triangle, \emptyset, \cap, \Omega)$ ist ein Ring.

Zu jeder Menge Ω ist $(\mathbb{F}_2^\Omega, +, 0, \cdot, 1)$ ein CRing, ebenso $(\mathfrak{P}(\Omega), \triangle, \emptyset, \cap, \Omega)$, und diese beiden Ringe sind isomorph vermöge $(\mathbf{1}, \mathrm{supp}) : \mathfrak{P}(\Omega) \cong \mathbb{F}_2^\Omega$.

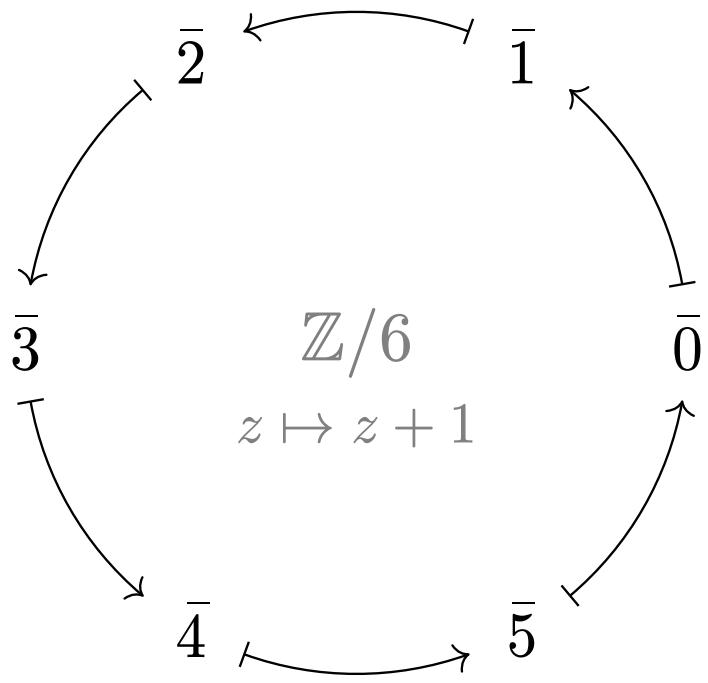
Wann sind $\mathbb{Z}/p \times \mathbb{Z}/q$ und $\mathbb{Z}/pq$ isomorph?

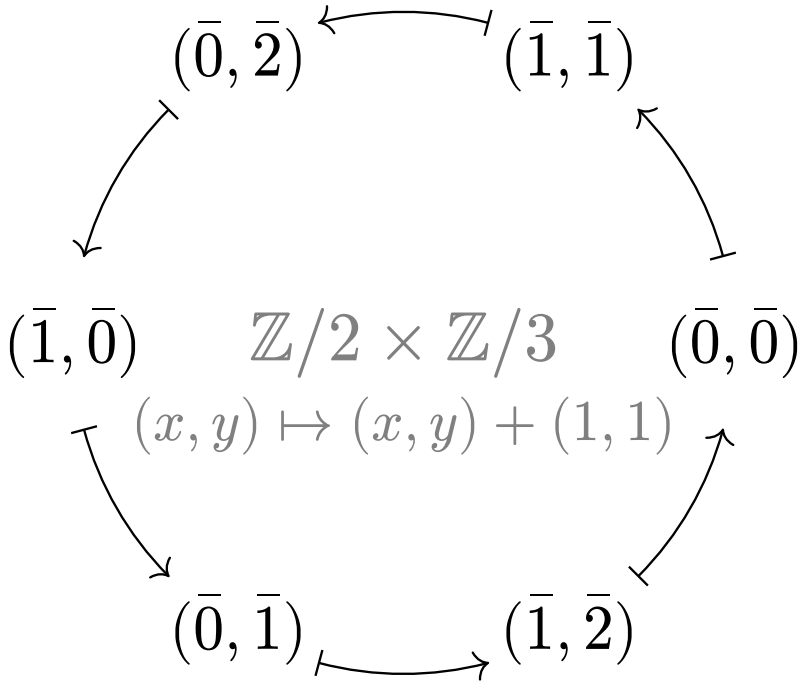
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Die Gruppen $A = \mathbb{Z}/2 \times \mathbb{Z}/2$ und $B = \mathbb{Z}/4$ sind nicht isomorph. Warum? Hier trennt die Invariante $\exp(A, +) = 2$ vs $\exp(B, +) = 4$.

Beispiel: Die Gruppen $C = \mathbb{Z}/2 \times \mathbb{Z}/3$ und $D = \mathbb{Z}/6$ sind isomorph.





Der chinesische Restsatz über $\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz K2E: chinesischer Restsatz über $\mathbb{Z}$

(1) Zu $p_1, \dots, p_n \in \mathbb{Z}_{\geq 1}$ haben wir den Ringhomomorphismus

$$\tilde{\pi} : \mathbb{Z} \to \mathbb{Z}/p_1 \times \cdots \times \mathbb{Z}/p_n : a \mapsto ([a]_{p_1}, \dots, [a]_{p_n}).$$

Sein Kern ist $\operatorname{Ker}(\tilde{\pi}) = p\mathbb{Z}$ mit $p = \operatorname{kgV}(p_1, \dots, p_n)$. Er induziert also

$$\pi : \mathbb{Z}/p \hookrightarrow \mathbb{Z}/p_1 \times \cdots \times \mathbb{Z}/p_n : [a]_p \mapsto ([a]_{p_1}, \dots, [a]_{p_n}).$$

(2) Genau dann ist π ein Isomorphismus, wenn $p = p_1 \cdots p_n$ gilt. (H1J)
Letzteres ist äquivalent zu $\operatorname{ggT}(p_i, p_j) = 1$ für alle $i \neq j$.

Anwendung des chinesischen Restsatzes: Euler

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz K2G: die Ordnung der Gruppe $\mathbb{Z}_n^\times$

Die **eulersche Funktion** $\varphi : \mathbb{N}_{\geq 1} \to \mathbb{N}_{\geq 1}$ ist die Gruppenordnung

$$\varphi(n) := \left|\mathbb{Z}_n^\times\right| = \sharp\{\, a \in \mathbb{N} \,\big|\, 0 \leq a < n \,\wedge\, \mathrm{ggT}(a,n) = 1 \,\}.$$

(1) Für $n = p^\alpha$ mit p prim und $\alpha \in \mathbb{N}_{\geq 1}$ gilt $\mathbb{Z}_{p^\alpha} = p\mathbb{Z}_{p^\alpha} \sqcup \mathbb{Z}_{p^\alpha}^\times$, also

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1).$$

(2) Für $n = ab$ mit $\mathrm{ggT}(a,b) = 1$ induziert der Ringisomorphismus K2E $(\pi,\sigma) : \mathbb{Z}_n \cong \mathbb{Z}_a \times \mathbb{Z}_b$ den Gruppenisomorphismus $\mathbb{Z}_n^\times \cong \mathbb{Z}_a^\times \times \mathbb{Z}_b^\times$, also

$$\varphi(ab) = \varphi(a)\varphi(b).$$

(3) Für $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ mit $p_1 < \ldots < p_k$ prim und $\alpha_1, \ldots, \alpha_k \in \mathbb{N}_{\geq 1}$ folgt:

$$\varphi(n) = \textstyle\prod_{i=1}^k p_i^{\alpha_i - 1}(p_i - 1)$$

Beispiel: Es gilt $\mathbb{Z}_{99} \cong \mathbb{Z}_9 \times \mathbb{Z}_{11}$ somit $\mathbb{Z}_{99}^\times \cong \mathbb{Z}_9^\times \times \mathbb{Z}_{11}^\times$ also $\varphi(99) = 60$.

Anwendung des chinesischen Restsatzes: Euler

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz K2H: Euler–Fermat dank Lagrange

Für alle $a \in \mathbb{Z}$ teilerfremd zu $n \in \mathbb{N}_{\geq 1}$, also $[a] \in \mathbb{Z}_n^\times$, gilt dank J3K:

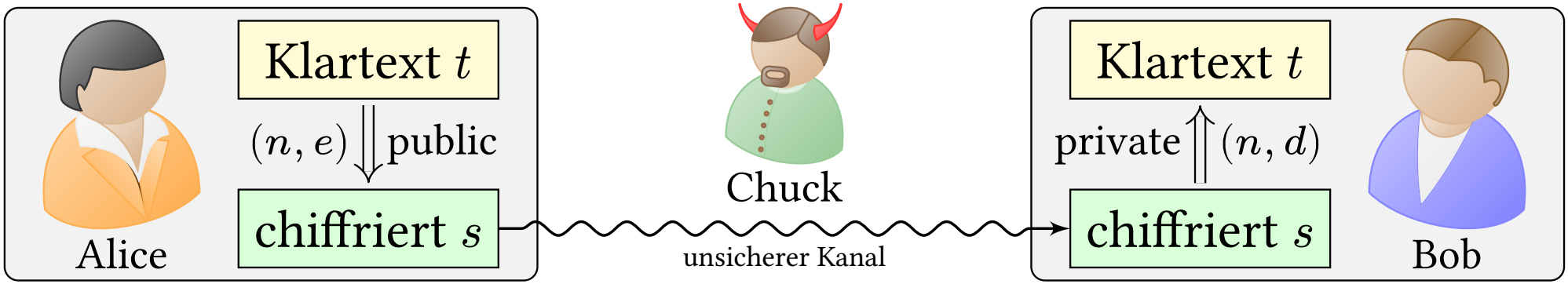
$$(1) \qquad a^{\varphi(n)} \equiv 1 \bmod n$$

$$(2) \qquad a^{\varphi(n)k+1} \equiv a \bmod n$$

Anwendung des chinesischen Restsatzes: RSA

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



$$\text{encrypt} : \mathbb{Z}_n \to \mathbb{Z}_n : t \mapsto s = t^e \text{ rem } n$$

$$\text{decrypt} : \mathbb{Z}_n \to \mathbb{Z}_n : s \mapsto t = s^d \text{ rem } n$$

Satz K21: Korrektheit des RSA–Kryptosystems

Gegeben seien $(n, e, d) \in \mathbb{N}^3$ mit $n = pq$ und $p < q$ in $\mathbb{N}$ prim sowie $ed \equiv 1 \bmod (p-1)(q-1)$. Dann gilt $(t^e)^d = t^{ed} = t$ für alle $t \in \mathbb{Z}_n$.

Polynome $P \in \mathbb{K}[X]$ auswerten durch Einsetzen $X \mapsto a$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel K3c: der Einsetzungshomomorphismus für Matrizen

Sei $\mathbb{K}$ ein kommutativer Ring und $\mathbb{K}[X]$ sein Polynomring.

(1) In Polynome können wir jedes Ringelement $a \in \mathbb{K}$ einsetzen:

$$\Phi_a : \mathbb{K}[X] \to \mathbb{K} : \; P = \textstyle\sum_k p_k X^k \;\mapsto\; P(a) = \sum_k p_k a^k$$

(2) Allgemein können wir jede quadratische Matrix $A \in \mathbb{K}^{n\times n}$ einsetzen:

$$\Phi_A : \mathbb{K}[X] \to \mathbb{K}^{n\times n} : \; P = \textstyle\sum_k p_k X^k \;\mapsto\; P(A) = \sum_k p_k A^k$$

Dies ist ein Ringhomomorphismus: Für alle $P, Q \in \mathbb{K}[X]$ gilt

$$\begin{aligned} (P+Q)(A) &= P(A) + Q(A), & 0(A) &= 0_{n\times n}, \\ (P\cdot Q)(A) &= P(A)\cdot Q(A), & 1(A) &= 1_{n\times n}. \end{aligned}$$

Zahlenbeispiele: Über $\mathbb{K} = \mathbb{Z}$ betrachten wir die Matrix $A = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right] \in \mathbb{Z}^{2\times 2}$.

$$\begin{aligned} P = X^2 + X \quad &\Longrightarrow \quad P(A) = 0_{2\times 2} + A \;\; = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right] \\ Q = 3X + 1 \quad &\Longrightarrow \quad Q(A) = 3A + 1_{2\times 2} = \left[\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right] \end{aligned}$$

Die universelle Abbildungseigenschaft des Polynomrings

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd}
R \arrow[r, hook, "\mathrm{inc}"] \arrow[dr, "\varphi"'] & R[X] \arrow[d, dashed, "\exists!\Phi"'] & \{X\} \arrow[l, hook', "\mathrm{inc}"'] \arrow[dl, "a \leftarrow\!\shortmid X"] \\
& S &
\end{tikzcd}$$

Satz K3D: der Einsetzungshomomorphismus

Sei $\varphi : R \to S$ ein Ringhomomorphismus und $a \in S$ zentral über $\varphi(R)$. Zu diesen Daten (φ, a) existiert genau ein Ringhomomorphismus $\Phi : R[X] \to S$ mit $\Phi|_R = \varphi$ und $\Phi(X) = a$, nämlich die Abbildung

$$\Phi \ : \ R[X] \to S \ : \ \Phi(\textstyle\sum_k p_k X^k) = \sum_k \varphi(p_k) a^k$$

Anwendungsbeispiel zur UAE des Polynomrings

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel K3F: $(Z(R), +, 0) \hookrightarrow (\mathrm{Aut}(R[X]), \circ, \mathrm{id})$

Sei R ein Ring. (1) Dank UAE haben wir die Ringautomorphismen

$$G_a : R[X] \to R[X] : X \mapsto X + a \quad \text{mit } a \in Z(R) \text{ und } G_a|_R = \mathrm{inc}_R.$$

Eindeutigkeit des Polynomrings bis auf Isomorphismus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar K3G: Eindeutigkeit bis auf Isomorphismus

Je zwei Polynomringe $R[X]$ und $R[Y]$ sind kanonisch isomorph.

Dank UAE existiert genau ein Isomorphismuspaar $(\varphi, \psi) : R[X] \cong R[Y]$ zu den Vorgaben $\varphi|_R = \psi|_R = \mathrm{inc}_R$ sowie $\varphi(X) = Y$ und $\psi(Y) = X$.

Vom Ring $\mathbb{Z}$ zum Körper $\mathbb{Q}$: Rechnen mit Brüchen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Problem: Im Ring $(\mathbb{Z}, +, \cdot)$ können wir Gleichungen wie $3 \cdot x = 2$ zwar formulieren, aber noch nicht lösen. **Ziel:** Wir erweitern den Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen zum Bruchkörper $(\mathbb{Q}, +, \cdot)$ der rationalen Zahlen.

Satz K3H: vom Ring $\mathbb{Z}$ zum Bruchkörper $\mathbb{Q}$

(1) Zum Ring $\mathbb{Z}$ der ganzen Zahlen existiert ein **Bruchkörper** $\mathbb{Q}$ mit folgender Eigenschaft: Der Körper $\mathbb{Q}$ enthält $\mathbb{Z} \leq \mathbb{Q}$ als Teilring, und jedes Element $a \in \mathbb{Q}$ schreibt sich $a = z/n$ mit $z \in \mathbb{Z}$ und $n \in \mathbb{Z}^*$.

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook, "\mathrm{inc}"] \arrow[dr, hook, "\varphi"'] & \mathbb{Q} \arrow[d, dashed, "\exists!\psi"] \\ & K \end{tikzcd} \qquad \begin{tikzcd} a = z/n \arrow[d, mapsto] \\ \varphi(z)/\varphi(n) \end{tikzcd}$$

(2) Jeder injektive Ringhomomorphismus $\varphi : \mathbb{Z} \hookrightarrow K$ in einen Körper K setzt sich eindeutig fort zu einem Körperhomomorphismus $\psi : \mathbb{Q} \to K$.

Der Bruchkörper eines Integritätsrings

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zum Polynomring $\mathbb{R}[X]$ konstruieren wir ebenso den Bruchkörper $\mathbb{R}(X)$.

Satz K31: der Bruchkörper eines Integritätsrings

(1) Zu jedem Integritätsring R existiert ein **Bruchkörper** $Q = \mathrm{Frac}(R)$ mit folgender Eigenschaft: Der Körper Q enthält $R \leq Q$ als Teilring, und jedes Element $a \in Q$ schreibt sich $a = r/s$ mit $r \in R$ und $s \in R^*$.

$$\begin{tikzcd} R \arrow[r, hook, "\mathrm{inc}"] \arrow[dr, hook, "\varphi"'] & Q \arrow[d, dashed, "\exists!\psi"] \\ & K \end{tikzcd} \qquad \begin{tikzcd} a = r/s \arrow[d, mapsto] \\ \varphi(r)/\varphi(s) \end{tikzcd}$$

(2) Jeder injektive Ringhomomorphismus $\varphi : R \hookrightarrow K$ in einen Körper K setzt sich eindeutig fort zu einem Körperhomomorphismus $\psi : Q \to K$.

(3) Je zwei Bruchkörper Q, Q' von R sind demnach isomorph vermöge des eindeutigen Isomorphismus $(\psi, \psi') : Q \cong Q'$ mit $\psi|_R = \psi'|_R = \mathrm{id}_R$.

Konstruktion des Bruchkörpers

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(0) Vorüberlegung: Wir setzen $S := R^*$. Angenommen, wir hätten einen Körper $(Q, +, \cdot)$ mit $R \leq Q$ und $S \leq Q^\times$. Für $r, r' \in R$ und $s, s' \in S$ gilt

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \qquad \text{und} \qquad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$

Zudem können wir die Gleichheit von Brüchen leicht feststellen:

$$\frac{r}{s} = \frac{r'}{s'} \text{ in } Q \quad \Longleftrightarrow \quad rs' = r's \text{ in } R$$

Konstruktion des Bruchkörpers

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(1) Konstruktion: (A) Auf der Menge $P = R \times S$ definieren wir

$$+ \,:\, P \times P \to P : \, (r,s) + (r',s') = (\, rs' + r's,\; ss' \,),$$
$$\cdot \,:\, P \times P \to P : \, (r,s) \cdot (r',s') = (\, rr',\; ss' \,).$$

(B) Wir erlauben „Erweitern“ und „Kürzen“ durch die Relation

$$(r,s) \sim (r',s') \quad :\Leftrightarrow \quad rs' = r's.$$

- ☺ Dies ist eine Äquivalenzrelation auf der Menge P. (Nachrechnen!)
- ☺ Auf $Q = P/_\sim$ sind $+$ und $\cdot$ wohldefiniert. (Nachrechnen!)
- ☺ Wir erhalten einen Körper $(Q, +, \cdot)$. (Nachrechnen!)

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel K

Bonusmaterial

One of the main objectives of higher mathematics is proving theorems. Theorems are tools that make new and productive applications of mathematics possible. We use examples to give insight into existing theorems and to foster intuitions as to what new theorems might be true. Applications, examples, and proofs are tightly interconnected — much more so than they may seem at first appearance.

Thomas W. Judson: *Abstract Algebra* (2017)

Inhalt dieses Kapitels K

5 Kleine Ringe: Beispiele und Klassifikation

6 Matrizenrechnung und Ringwechsel

7 Der Nim–Körper nach John H. Conway

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel L

Lineare Räume und lineare Abbildungen

$$\forall 🐶 \in 🤣 : 🐶\ 👀\ ☁️ = 🐶$$
$$\forall 🐶 \in 🤣 : \forall 👧, 👦 \in 🤩 : 🐶\ 👀\ (👧\ 👁️\ 👦) = (🐶\ 👀\ 👧)\ 👀\ 👦$$
$$\forall 🐶 \in 🤣 : \forall 👧, 👦 \in 🤩 : 🐶\ 👀\ (👧\ 💖\ 👦) = (🐶\ 👀\ 👧)\ ❤️‍🔥\ (🐶\ 👀\ 👦)$$
$$\forall 🐶, 🐱 \in 🤣 : \forall 👧 \in 🤩 : (🐶\ ❤️‍🔥\ 🐱)\ 👀\ 👧 = (🐶\ 👀\ 👧)\ ❤️‍🔥\ (🐱\ 👀\ 👧)$$

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), *Lineare Algebra*

Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels L

1 Lineare Räume und lineare Abbildungen

2 Lineare Unterräume

3 Universelle Werkzeuge

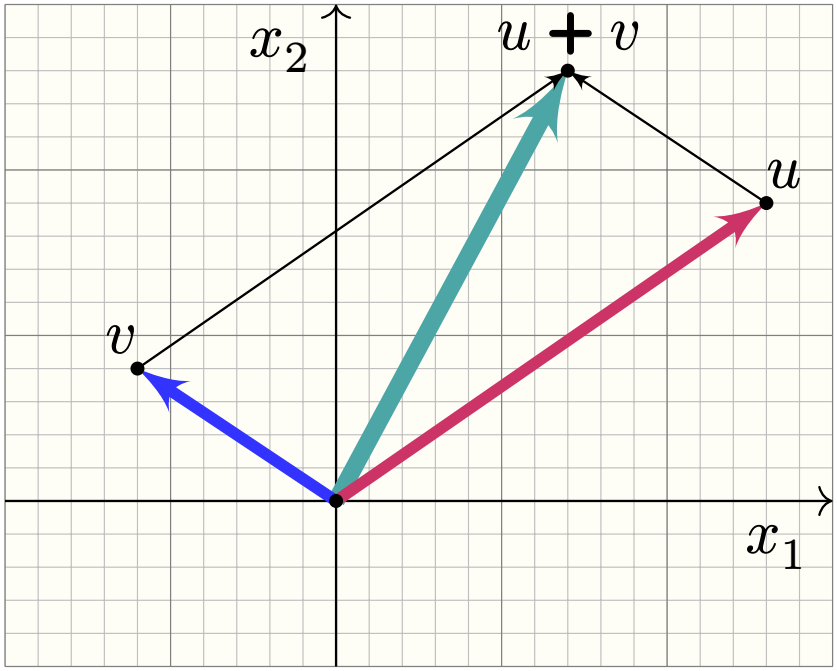
Dies ist nur die Saalversion ohne Erläuterungen.

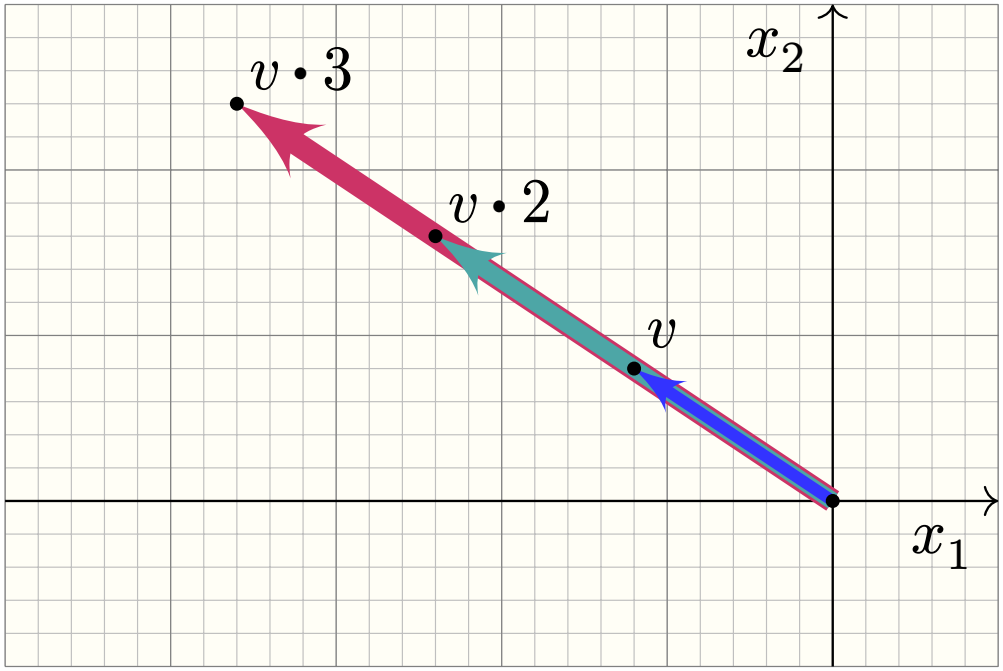
Ausführliche Erläuterungen bietet die Vollversion.

Addition und Skalierung von Vektoren im $\mathbb{R}^n$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





$$+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n : (u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n)$$

$$\bullet : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n : (v_1, \dots, v_n) \bullet \lambda = (v_1 \cdot \lambda, \dots, v_n \cdot \lambda)$$

$$\circ : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n : \lambda \circ (v_1, \dots, v_n) = (\lambda \cdot v_1, \dots, \lambda \cdot v_n)$$

Addition und Multiplikation von Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $(K, +, 0, \cdot, 1)$ ein Ring, etwa $\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \ldots$, und $m, n \in \mathbb{N}_{\geq 1}$.
Matrizen passender Größe können wir addieren und multiplizieren:

$$\underset{\in K^{m\times n}}{v} + \underset{\in K^{m\times n}}{v'} = \underset{\in K^{m\times n}}{v + v'}$$

$$\underset{\in K^{m\times n}}{v} \cdot \underset{\in K^{n\times n}}{r} = \underset{\in K^{m\times n}}{v \cdot r}$$

$$\underset{\in K^{m\times m}}{s} \circ \underset{\in K^{m\times n}}{v} = \underset{\in K^{m\times n}}{s \circ v}$$

Addition und Multiplikation von Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(A) Die $m \times n$–Matrizen bilden die abelsche Gruppe $(V = K^{m\times n}, \mathbf{+}, \mathbf{0}, \mathbf{-})$:

(A0)	$v \mathbf{+} v' = v' \mathbf{+} v,$	(A2)	$v \mathbf{+} \mathbf{0} = v,$
(A1)	$(v \mathbf{+} v') \mathbf{+} v'' = v \mathbf{+} (v' \mathbf{+} v''),$	(A3)	$v \mathbf{+} (\mathbf{-}v) = \mathbf{0}.$

(R) Der Matrixring $(R = K^{n\times n}, +, 0, \cdot, 1)$ operiert distributiv von rechts:

(R1)	$v \bullet 1 = v,$	(R3)	$v \bullet (r + r') = (v \bullet r) \mathbf{+} (v \bullet r'),$
(R2)	$v \bullet (r \cdot r') = (v \bullet r) \bullet r',$	(R4)	$(v \mathbf{+} v') \bullet r = (v \bullet r) \mathbf{+} (v' \bullet r).$

(L) Der Matrixring $(S = K^{m\times m}, +, 0, \cdot, 1)$ operiert distributiv von links:

(L1)	$1 \circ v = v,$	(L3)	$(s + s') \circ v = (s \circ v) \mathbf{+} (s' \circ v),$
(L2)	$(s \cdot s') \circ v = s \circ (s' \circ v),$	(L4)	$s \circ (v \mathbf{+} v') = (s \circ v) \mathbf{+} (s \circ v').$

Beide Operationen sind miteinander verträglich: $(s \circ v) \bullet r = s \circ (v \bullet r)$.

Lineare Räume, rechts und links

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition L1A: linearer Raum über einem Ring

(1) Ein **rechtslinearer Raum** $(V, \boldsymbol{+}, \bullet)$ über dem Ring $(R, +, \cdot)$ besteht aus einer abelschen Gruppe $(V, \boldsymbol{+})$ mit Skalierung $\bullet : V \times R \to V$ gemäß (R).

(2) Ein **linkslinearer Raum** $(V, \boldsymbol{+}, \circ)$ über dem Ring $(S, +, \cdot)$ besteht aus einer abelschen Gruppe $(V, \boldsymbol{+})$ mit Skalierung $\circ : S \times V \to V$ gemäß (L).

(3) Ein **Vektorraum** ist ein linearer Raum über einem Divisionsring.

(4) Haben wir beide Strukturen (1,2) und sind sie miteinander verträglich, so nennen wir $(V, \boldsymbol{+}, \circ, \bullet)$ einen **(S, R)–linearen Raum**. Gilt $S = R$ und $r \circ v = v \bullet r$ für alle $v \in V$ und $r \in R$, so nennen wir V **zentral** über R.

Lineare Räume, rechts und links

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele: (0) Die einelementige Menge $\{0\}$ ist ein (S, R)–linearer Raum: notgedrungen gilt $0 + 0 = 0$ und $0 \bullet r = 0$ für $r \in R$ und $s \circ 0 = 0$ für $s \in S$.

(2) Der Raum $K^m = K^{m\times 1}$ der Spaltenvektoren ist linkslinear über $K^{m\times m}$ sowie rechtslinear über $K^{1\times 1} = K$, und beides ist verträglich.

(4) Allgemein ist $K^{m\times n}$ linkslinear über $S = K^{m\times m}$ sowie rechtslinear über $R = K^{n\times n}$, und beides ist verträglich, also (S, R)–linear. Zusätzlich ist $K^{m\times n}$ ein (K, K)–linearer Raum, und zentral gdw K kommutativ ist.

Jeder Ring $(R, +, \cdot)$ ist ein linearer Raum über R.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die reellen Zahlen $\mathbb{R}$ sind ein Vektorraum über $\mathbb{R}$, aber auch über $\mathbb{Q}$.

Bemerkung L1D: Jeder Ring ist ein linearer Raum.

(0) Jeder Ring $(V = R, +, \cdot)$ ist automatisch ein (R, R)–linearer Raum:

$$\begin{array}{ll} \text{links} & \circ : R \times V \to R : (s, v) \mapsto s \cdot v \\ \text{rechts} & \bullet : V \times R \to V : (v, r) \mapsto v \cdot r \end{array}$$

(1) Ist der Raum V linear über (S, R), so auch über $(S', R') \leq (S, R)$:

$$\begin{array}{lcl} \circ : S \times V \to V & \Longrightarrow & \circ' : S' \times V \to V : (s, v) \mapsto s \circ v \\ \bullet : V \times R \to V & \Longrightarrow & \bullet' : V \times R' \to V : (v, r) \mapsto v \bullet r \end{array}$$

Beispiel: Die komplexen Zahlen $(\mathbb{C}, +, \cdot)$ sind ein Vektorraum über $\mathbb{C}$, aber auch über $\mathbb{R} \leq \mathbb{C}$ und über $\mathbb{Q} \leq \mathbb{C}$ und ein linearer Raum über $\mathbb{Z} \leq \mathbb{C}$.

Was ist ein Vektorraum? – *emoji math*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: (1) Was bedeutet es, dass (🤣, ❤️‍🔥, 👻) eine abelsche Gruppe ist?
(2) … und (🤣, ❤️‍🔥, 👻, 👀) ein linearer Raum über (🤩, 💖, 💀, 👁️, ☁️)?

Lösung: (1) Das bedeutet, 🤣 ist eine Menge, darauf ist ❤️‍🔥 : 🤣 × 🤣 → 🤣 eine Verknüpfung, und 👻 ∈ 🤣 ist ein Element. Für diese Daten gelte:

∀🐶, 🐱 ∈ 🤣 : 🐶 ❤️‍🔥 🐱 = 🐱 ❤️‍🔥 🐶

∀🐶, 🐱, 🐵 ∈ 🤣 : (🐶 ❤️‍🔥 🐱) ❤️‍🔥 🐵 = 🐶 ❤️‍🔥 (🐱 ❤️‍🔥 🐵)

∀🐶 ∈ 🤣 : 🐶 ❤️‍🔥 👻 = 🐶

∀🐶 ∈ 🤣 : ∃🐱 ∈ 🤣 : 🐶 ❤️‍🔥 🐱 = 👻

(2) Linearer Raum bedeutet, (🤣, ❤️‍🔥, 👻) ist eine abelsche Gruppe wie in (1) mit einer Skalierung 👀 : 🤣 × 🤩 → 🤣. Für diese Daten gelte:

∀🐶 ∈ 🤣 : 🐶 👀 ☁️ = 🐶

∀🐶 ∈ 🤣 : ∀👧, 👦 ∈ 🤩 : 🐶 👀 (👧 👁️ 👦) = (🐶 👀 👧) 👀 👦

∀🐶 ∈ 🤣 : ∀👧, 👦 ∈ 🤩 : 🐶 👀 (👧 💖 👦) = (🐶 👀 👧) ❤️‍🔥 (🐶 👀 👦)

∀🐶, 🐱 ∈ 🤣 : ∀👧 ∈ 🤩 : (🐶 ❤️‍🔥 🐱) 👀 👧 = (🐶 👀 👧) ❤️‍🔥 (🐱 👀 👧)

Was ist ein Vektorraum? – *classic math*

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: (1) Was bedeutet es, dass $(V, \mathbf{+}, \mathbf{0})$ eine abelsche Gruppe ist?
(2) ... und $(V, \mathbf{+}, \mathbf{0}, \bullet)$ ein linearer Raum über $(K, +, 0, \cdot, 1)$?

Lösung: (1) Das bedeutet, V ist eine Menge, darauf ist $\mathbf{+} : V \times V \to V$ eine Verknüpfung, und $\mathbf{0} \in V$ ist ein Element. Für diese Daten gelte:

$$\forall u, v \in V : u \mathbf{+} v = v \mathbf{+} u$$
$$\forall u, v, w \in V : (u \mathbf{+} v) \mathbf{+} w = u \mathbf{+} (v \mathbf{+} w)$$
$$\forall u \in V : u \mathbf{+} \mathbf{0} = u$$
$$\forall u \in V : \exists v \in V : u \mathbf{+} v = \mathbf{0}$$

(2) Linearer Raum bedeutet, $(V, \mathbf{+}, \mathbf{0})$ ist eine abelsche Gruppe wie in (1) mit einer Skalierung $\bullet : V \times K \to V$. Für diese Daten gelte:

$$\forall u \in V : u \bullet 1 = u$$
$$\forall u \in V : \forall \alpha, \beta \in K : u \bullet (\alpha \cdot \beta) = (u \bullet \alpha) \bullet \beta$$
$$\forall u \in V : \forall \alpha, \beta \in K : u \bullet (\alpha + \beta) = (u \bullet \alpha) \mathbf{+} (u \bullet \beta)$$
$$\forall u, v \in V : \forall \alpha \in K : (u \mathbf{+} v) \bullet \alpha = (u \bullet \alpha) \mathbf{+} (v \bullet \alpha)$$

Rechenregeln für lineare Räume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma L1F: Null und Negation

Sei $(V, \mathbf{+}, \cdot)$ ein rechtslinearer Raum über dem Ring $(R, +, \cdot)$.
Für alle Vektoren $v, v' \in V$ und Skalare $r, r' \in R$ erhalten wir:

1. $\rho_r : (V, \mathbf{+}) \to (V, \mathbf{+}) : v \mapsto v \cdot r$
   Es gilt (R4) $\rho_r(v + v') = \rho_r(v) + \rho_r(v')$.
   Es folgt $\mathbf{0} \cdot r = \mathbf{0}$ und $(-v) \cdot r = -(v \cdot r)$.
2. $\lambda_v : (R, +) \to (V, \mathbf{+}) : r \mapsto v \cdot r$
   Es gilt (R3) $\lambda_v(r + r') = \lambda_v(r) + \lambda_v(r')$.
   Es folgt $v \cdot 0 = \mathbf{0}$ und $v \cdot (-r) = -(v \cdot r)$.

Kürzungsregeln für Vektorräume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma L1F: Kürzungsregel

Sei $(V, \mathbf{+}, \cdot)$ ein R–Vektorraum. Für alle $u, v \in V$ und $a, b \in R$ gilt:

3 Torsionsfreiheit:
$v \cdot a = \mathbf{0} \;\Rightarrow\; v = \mathbf{0} \vee a = 0$

4 Kürzungsregel:
$u \cdot a = v \cdot a \wedge a \neq 0 \;\Rightarrow\; u = v$
$v \cdot a = v \cdot b \wedge v \neq \mathbf{0} \;\Rightarrow\; a = b$

Beweis: (3) Gilt $v \cdot a = \mathbf{0}$ und $a \neq 0$, so können wir mit a^{-1} multiplizieren:

$$\mathbf{0} \overset{(1)}{=} \mathbf{0} \cdot a^{-1} \overset{\text{Vor}}{=} (v \cdot a) \cdot a^{-1} \overset{\text{R2}}{=} v \cdot (a \cdot a^{-1}) \overset{\text{Ntr}}{=} v \cdot 1 \overset{\text{R1}}{=} v$$

(4a) Aus $u \cdot a = v \cdot a$ folgt $\mathbf{0} \overset{\text{A3}}{=} (u \cdot a) - (v \cdot a) \overset{\text{R4}}{=} (u - v) \cdot a$.
Dank (3) und $a \neq 0$ folgt $u - v = \mathbf{0}$, somit $u = v$ dank (A3,1) .

(4b) Aus $v \cdot a = v \cdot b$ folgt $\mathbf{0} \overset{\text{A3}}{=} (v \cdot a) - (v \cdot b) \overset{\text{R3}}{=} v \cdot (a - b)$.
Dank (3) und $v \neq \mathbf{0}$ folgt $a - b = 0$, somit $a = b$ in $(R, +)$. QED

Jede Matrix A definiert eine lineare Abbildung $f_A : x \mapsto Ax$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel L1H: von der Matrix A zur linearen Abbildung f_A

Jede Matrix $A \in R^{m\times n}$ definiert ihre zugehörige **lineare Abbildung**

$$f = f_A : R^{n\times 1} \to R^{m\times 1} : x \mapsto Ax.$$

Diese Abbildung ist **additiv**, das heißt für alle Vektoren $x, y \in R^n$ gilt:

$$f(x+y) \overset{\text{Def}}{=} A(x+y) \underset{\text{D1F}}{\overset{\text{Dst}}{=}} Ax + Ay \overset{\text{Def}}{=} f(x) + f(y).$$

Sie ist zudem **R–homogen** bezüglich Skalierung mit $\lambda \in R$ von rechts:

$$f(x\lambda) \overset{\text{Def}}{=} A(x\lambda) \underset{\text{D1F}}{\overset{\text{Ass}}{=}} (Ax)\lambda \overset{\text{Def}}{=} f(x)\lambda.$$

Lineare Abbildungen erhalten die lineare Struktur.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition L11: R–lineare Abbildung

Seien $(U, +, \cdot)$ und $(V, +, \cdot)$ rechtslineare Räume über dem Ring $(R, +, \cdot)$.

(1) Ein **Gruppenhomomorphismus** $f : (U, +_U) \to (V, +_V)$ ist

additiv: $f(u +_U v) = f(u) +_V f(v)$ für alle $u, v \in U$.

Schreibweise: $f \in \mathrm{Hom}(U, V) := \mathrm{Hom}(U, +_U; V, +_V)$

(2) Eine **R–lineare Abbildung** $f : (U, +_U, \cdot_U) \to (V, +_V, \cdot_V)$ ist zudem

R–homogen: $f(u \cdot_U \lambda) = f(u) \cdot_V \lambda$ für alle $u \in U$ und $\lambda \in R$.

Schreibweise: $f \in \mathrm{Hom}_R(U, V) := \mathrm{Hom}_{(R,+,\cdot)}(U, +_U, \cdot_U; V, +_V, \cdot_V)$

Zusammen, $f : U \to V$ ist R–linear gdw für alle $u, v \in U$ und $\lambda, \mu \in R$ gilt:

$$\boxed{f(u\lambda + v\mu) = f(u)\lambda + f(v)\mu}$$

Lineare Abbildungen erhalten die lineare Struktur.

Für jeden Gruppenhomomorphismus $f : (U, +) \to (V, +)$ gilt dank J2A:

$$f(0_U) = 0_V \quad \text{und} \quad f(-u) = -f(u) \quad \text{für alle } u \in U$$

Für jede R–lineare Abbildung $f : (U, +, \cdot) \to (V, +, \cdot)$ gilt noch mehr:

$$f\left(\sum_{i=1}^{n} u_i \lambda_i\right) = \sum_{i=1}^{n} f(u_i)\lambda_i$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Erste Beispiele: linear oder nicht?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede Matrix $A \in R^{m \times n}$ wirkt als R–lineare Abbildung (Beispiel L1H)

$$f_A : R^n \to R^m : x \mapsto Ax.$$

Beispiel: Die Abbildung $f : \mathbb{R} \to \mathbb{R} : x \mapsto 3x$ ist $\mathbb{R}$–linear.

Beispiel: Die Abbildung $g : \mathbb{R} \to \mathbb{R} : x \mapsto 3x + 2$ ist nicht $\mathbb{R}$–linear, nicht einmal additiv, denn dies scheitert bereits an $g(0) = 2 \neq 0$.

Erste Beispiele: linear oder nicht?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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:

$$\mathrm{conj} : \mathbb{R}^2 \to \mathbb{R}^2 : \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} x \\ -y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Hingegen ist conj nicht $\mathbb{C}$–linear: Es gilt $\mathrm{conj}(1 \cdot \mathrm{i}) = -\mathrm{i}$ vs $\mathrm{conj}(1) \cdot \mathrm{i} = \mathrm{i}$.

Erste Beispiele: linear oder nicht?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Welche der folgenden Abbildungen sind $\mathbb{R}$–linear?

$$f_1 : \mathbb{R}^2 \to \mathbb{R} : f_1\begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \frac{4x^2-9y^2}{2x-3y} & \text{falls } 2x \neq 3y, \\ 4x & \text{falls } 2x = 3y, \end{cases}$$

$$f_2 : \mathbb{R}^2 \to \mathbb{R} : f_2\begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \frac{4x^2-9y^2}{2x-3y} & \text{falls } 2x \neq 3y, \\ 5x & \text{falls } 2x = 3y. \end{cases}$$

Lösung: Die Abbildung f_1 ist $\mathbb{R}$–linear, denn $f_1(x, y) = 2x + 3y$, doch f_2 ist nicht mal additiv: Es gilt $f_2(3, 0) = 6$ und $f_2(0, 2) = 6$ vs $f_2(3, 2) = 15$.

Erste Beispiele: linear oder nicht?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir betrachten die Ableitung von Polynomen:

$$P = \sum_{k=0}^{n} p_k X^k \quad \overset{\partial}{\mapsto} \quad P' = \sum_{k=1}^{n} k p_k X^{k-1}$$

Aufgabe: Ist $\partial : \mathbb{R}[X] \to \mathbb{R}[X]$ linear (0) über $\mathbb{R}[X]$? (1) über $\mathbb{R}$?

Lösung: (0) Nein, $\partial(X \cdot 1) = 1$ vs $X \cdot \partial(1) = 0$. (1) Ja, wir rechnen es nach:

$$\begin{aligned}
\partial(\lambda P + \mu Q) &\overset{\mathbb{R}[X]}{=} \partial \sum_k (\lambda p_k + \mu q_k) X^k \\
&\overset{\text{Def}}{=} \sum_k k(\lambda p_k + \mu q_k) X^{k-1} \\
&\overset{\mathbb{R}[X]}{=} \lambda \sum_k k p_k X^{k-1} + \mu \sum_k k q_k X^{k-1} \overset{\text{Def}}{=} \lambda \partial(P) + \mu \partial(Q)
\end{aligned}$$

Homomorphismen von R–linearen Räumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L1J: Identität und Komposition und Umkehrung

(1) Für jeden linearen Raum $(V,+,\cdot)$ über dem Ring $(R,+,\cdot)$ ist die Identität $\mathrm{id}_V : (V,+,\cdot) \to (V,+,\cdot)$ ein Homomorphismus.

(2) Sind $f : (U,+,\cdot) \to (V,+,\cdot)$ und $g : (V,+,\cdot) \to (W,+,\cdot)$ linear über R, so auch ihre Komposition $g \circ f : (U,+,\cdot) \to (W,+,\cdot)$.

(3) Ist $f : (U,+,\cdot) \to (V,+,\cdot)$ linear über R und bijektiv, so auch die Umkehrabbildung $g = f^{-1} : (V,+,\cdot) \to (U,+,\cdot)$.

Beweis: (1) ist klar. (2) Für alle $u, v \in U$ und $\lambda, \mu \in R$ gilt:

$$\begin{aligned}(g \circ f)(u\lambda + v\mu) &\overset{\text{Def}}{=} g(f(u\lambda + v\mu)) \overset{\text{Lin}}{=} g(f(u)\lambda + f(v)\mu) \\ &\overset{\text{Lin}}{=} g(f(u))\lambda + g(f(v))\mu \overset{\text{Def}}{=} (g \circ f)(u)\lambda + (g \circ f)(v)\mu\end{aligned}$$

(3) Zu $x, y \in V$ setzen wir $u := g(x)$ und $v := g(y)$ und finden:

$$\begin{aligned}g(x\lambda + y\mu) &\overset{\text{Def}}{=} g(f(u)\lambda + f(v)\mu) \overset{\text{Lin}}{=} g(f(u\lambda + v\mu)) \\ &\overset{\text{Inv}}{=} u\lambda + v\mu \overset{\text{Def}}{=} g(x)\lambda + g(y)\mu\end{aligned}$$

Morphismen: Homo, Iso, Endo, Auto

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{aligned}\mathrm{Hom}_R(U,V) &= \{\, f : U \to V \text{ linear über } R \,\}\\ \mathrm{Hom}_R(U,V)^\times &= \{\, f : U \to V \text{ linear und bijektiv} \,\}\end{aligned}$$

$$\begin{aligned}\mathrm{End}_R(V) &= \mathrm{Hom}_R(V,V) && \text{ist ein Monoid (L1J),}\\ \mathrm{Aut}_R(V) &= \mathrm{End}_R(V)^\times = \mathrm{GL}(V) && \text{ist eine Gruppe (J1L).}\end{aligned}$$

Jede lineare Abbildung $f : R^n \to R^m$ definiert eine Matrix.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

♦ **Satz D1J:** Jede lineare Abbildung definiert eine Matrix.

(1) Für $f : R^n \to R^m$ linear gilt $f = f_A$ mit $A = (f(e_1), \dots, f(e_n)) \in R^{m \times n}$.

Beweis: (1) Wir müssen $f(x) = Ax$ zeigen für alle $x \in R^n$. Wir rechnen:

$$f(x) \overset{\text{Def}}{=} f\left(\sum_{j=1}^n e_j x_j\right) \overset{\text{Lin}}{=} \sum_{j=1}^n f(e_j) x_j \overset{\text{Def}}{=} Ax$$

Matrizen entsprechen linearen Abbildungen.

$$
\begin{aligned}
(\mathrm{L},\mathrm{M}) : \quad R^{m\times n} &\cong \mathrm{Hom}_R(R^n, R^m) \quad : A \leftrightarrows f \\
(R^{n\times n}, \cdot, 1_{n\times n}) &\cong (\mathrm{End}_R(R^n), \circ, \mathrm{id}_{R^n}) \\
(\mathrm{GL}_n(R), \cdot, 1_{n\times n}) &\cong (\mathrm{Aut}_R(R^n), \circ, \mathrm{id}_{R^n})
\end{aligned}
$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede abelsche Gruppe $(V,+)$ ist ein $\mathbb{Z}$–linearer Raum.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L1κ: $\mathbb{Z}$–lineare Räume und Abbildungen

(1) Jede abelsche Gruppe $(V,+)$ ist ein $\mathbb{Z}$–linearer Raum vermöge

$$\begin{aligned} \bullet : V \times \mathbb{Z} \to V : (v,n) &\mapsto v \bullet n \\ \circ : \mathbb{Z} \times V \to V : (n,v) &\mapsto n \circ v \end{aligned} = \begin{cases} \sum_{k=1}^{+n} (+v) & \text{falls } n \geq 0, \\ \sum_{k=1}^{-n} (-v) & \text{falls } n \leq 0. \end{cases}$$

(2) Jeder Homomorphismus $f : (V,+) \to (W,+)$ abelscher Gruppen ist automatisch $\mathbb{Z}$–linear, das heißt für alle $v \in V$ und $n \in \mathbb{Z}$ gilt:

$$f(v \bullet n) = f(v) \bullet n \quad \text{und} \quad f(n \circ v) = n \circ f(v)$$

Lineare Räume und lineare Abbildungen über $\mathbb{Z}/p$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L1L: $\mathbb{Z}/p$–lineare Räume und Abbildungen

(1) Sei $(V,+)$ eine abelsche Gruppe und $p \in \mathbb{N}$ mit $v \bullet p = 0$ für alle $v \in V$. Dann ist $(V,+)$ ein linearer Raum über dem Ring $\mathbb{Z}/p$ vermöge

$$\bullet : V \times \mathbb{Z}/p \to V : (v,[n]) \mapsto v \bullet [n] := v \bullet n$$

(2) Jeder Gruppenhomomorphismus $f : (V,+) \to (W,+)$ zwischen $\mathbb{Z}/p$–linearen Räumen $(V,+)$ und $(W,+)$ ist automatisch $\mathbb{Z}/p$–linear:

$$f(v \bullet [n]) = f(v) \bullet [n]$$

(3) Speziell für $p > 0$ prim erhalten wir: $\mathbb{F}_p$–Vektorräume $(V,+,\cdot)$ sind abelsche Gruppen $(V,+)$ mit $\sum_1^p v = 0$ für jedes Element $v \in V$.

Lineare Räume und lineare Abbildungen über $\mathbb{Z}/p$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Sei Ω eine Menge. Die Potenzmenge $V = \mathfrak{P}(\Omega)$ wird zur abelschen Gruppe $(V, \vartriangle, \emptyset)$ mit der symmetrischen Differenz

$$A \vartriangle B = (A \smallsetminus B) \cup (B \smallsetminus A).$$

Für jedes Element $A \in V$, also jede Teilmenge $A \subseteq \Omega$, gilt $A \vartriangle A = \emptyset$. Somit ist $(V, \vartriangle)$ ein $\mathbb{F}_2$–Vektorraum, vermöge $A \bullet [0] = \emptyset$ und $A \bullet [1] = A$.

$$(\mathbf{1}, \operatorname{supp}) : \mathfrak{P}(\Omega) \;\cong\; \mathbb{F}_2^{\Omega}.$$

Dies ist ein Isomorphismus $(V, \vartriangle) \cong (\mathbb{F}_2^{\Omega}, +)$ abelscher Gruppen und nach dem vorigen Satz L1L sogar ein Isomorphismus von $\mathbb{F}_2$–Vektorräumen.

Lineare Räume und lineare Abbildungen über $\mathbb{Q}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L1M: $\mathbb{Q}$–lineare Räume und Abbildungen

(1) Sei $(V,+)$ eine abelsche Gruppe und zu jedem $n \in \mathbb{N}_{\geq 1}$ sei

$$\mu_n : V \xrightarrow{\sim} V : u \mapsto u \cdot n \quad \text{bijektiv.}$$

Wir definieren so die Division $v/n := \mu_n^{-1}(v)$ und allgemein die Operation

$$\cdot : V \times \mathbb{Q} \to V : (v, z/n) \mapsto v \cdot (z/n) = (v \cdot z)/n.$$

(2) Jeder Gruppenhomomorphismus $f : (V,+) \to (W,+)$ zwischen $\mathbb{Q}$–Vektorräumen $(V,+)$ und $(W,+)$ ist automatisch $\mathbb{Q}$–linear:

$$f(v \cdot z/n) = f(v) \cdot z/n$$

Was ist ein R–linearer Unterraum?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition L2A: R–linearer Unterraum

Sei $(V, \boldsymbol{+}, \boldsymbol{\cdot})$ ein rechtslinearer Raum über dem Ring $(R, +, \cdot)$.

Ein **R–linearer Unterraum** $U \leq (V, \boldsymbol{+}, \boldsymbol{\cdot})$ ist eine additive Untergruppe $U \leq (V, \boldsymbol{+})$, die zudem abgeschlossen ist unter Skalierung mit R. Kurz:

$U \leq (V, \boldsymbol{+}, \boldsymbol{\cdot})$ bedeutet $U \subseteq V$ mit $0 \in U$ und $U \boldsymbol{+} U \subseteq U$ und $U \boldsymbol{\cdot} R \subseteq U$.

Durch Einschränkung ist dann $(U, \boldsymbol{+}_U, \boldsymbol{\cdot}_U)$ selbst ein R–linearer Raum und die Inklusion $\iota : (U, \boldsymbol{+}_U, \boldsymbol{\cdot}_U) \hookrightarrow (V, \boldsymbol{+}, \boldsymbol{\cdot})$ eine R–lineare Abbildung.

Beispiel: In $(V, +, \cdot)$ sind die Mengen $\{0\}$ und V lineare Unterräume.

☺ Zum Nachweis von $U \leq (V, \boldsymbol{+}, \boldsymbol{\cdot})$ sind drei Eigenschaften zu prüfen:

(U0) *Die Menge U enthält die Null:* Es gilt $0 \in U$.
(U1) *abgeschlossen unter Addition:* Für alle $u, u' \in U$ gilt $u \boldsymbol{+} u' \in U$.
(U2) *abgeschlossen unter Skalierung:* Aus $u \in U$ und $r \in R$ folgt $u \boldsymbol{\cdot} r \in U$.

Erste Beispiele: linearer Unterraum oder nicht?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Übung: Die reelle Gerade $\mathbb{R}$ hat genau zwei $\mathbb{R}$–lineare Unterräume:

(0) den Nullraum $\{0\}$,
(1) die gesamte Gerade $\mathbb{R}$.

Beispiele: In der reellen Ebene $\mathbb{R}^2$ sind $\mathbb{R}$–lineare Unterräume:

(0) der Nullraum $\{0\}$,
(1) jede Ursprungsgerade $v\mathbb{R}$,
(2) die gesamte Ebene $\mathbb{R}^2$.

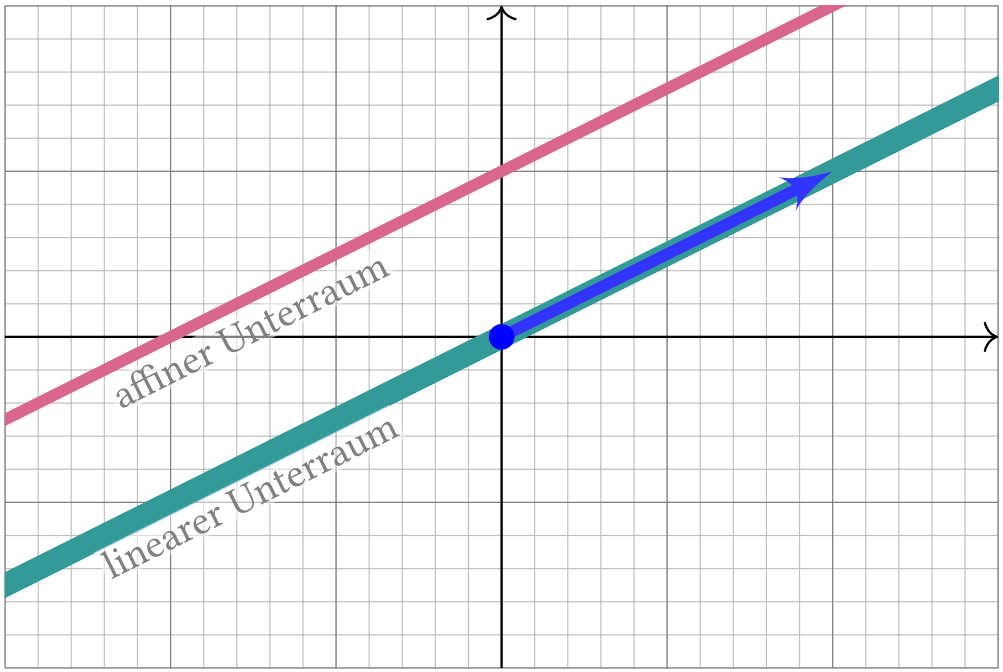
Beispiele: Im reellen Raum $\mathbb{R}^3$ sind $\mathbb{R}$–lineare Unterräume:

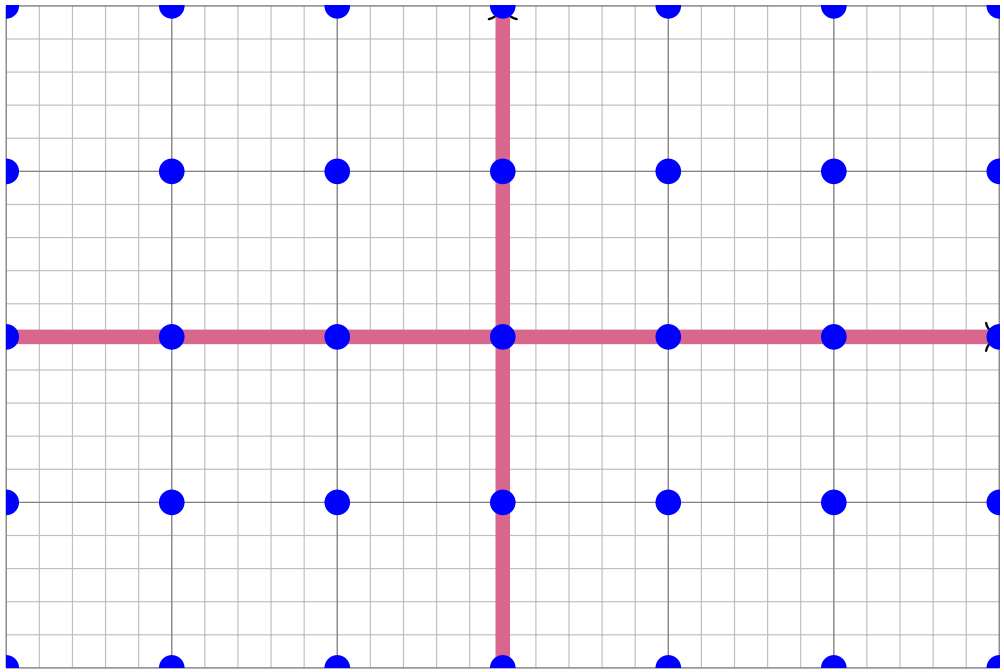
(0) der Nullraum $\{0\}$,
(1) jede Ursprungsgerade $v\mathbb{R}$,
(2) jede Ursprungsebene $u\mathbb{R} + v\mathbb{R}$,
(3) der gesamte Raum $\mathbb{R}^3$.

Erste Beispiele: linearer Unterraum oder nicht?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





? Ist $A = (2,1) \cdot \mathbb{R} + (0,1)$ in $\mathbb{R}^2$ ein $\mathbb{R}$–Unterraum? Nein, denn $0 \notin A$.

? Ist $X = (\mathbb{R} \times \{0\}) \cup (\{0\} \times \mathbb{R})$ in $\mathbb{R}^2$ ein $\mathbb{R}$–Unterraum? Nein! Zwar ist X abgeschlossen unter $\mathbb{R}$–Skalierung, aber nicht unter Addition. Gegenbeispiel: Für $u = (1,0)$ und $u' = (0,1)$ gilt $u + u' \notin U$.

? Ist $U = \mathbb{Z}^2$ in $\mathbb{R}^2$ ein $\mathbb{R}$–Unterraum? Nein! Zwar ist $\mathbb{Z}^2 \leq (\mathbb{R}^2, +)$ eine additive Untergruppe, aber nicht abgeschlossen unter $\mathbb{R}$–Skalierung. Gegenbeispiel: Für $u = (1,0) \in U$ und $r = 1/2 \in \mathbb{R}$ gilt $u \cdot r \notin U$.

Transport von linearen Unterräumen.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L2B: Transport von Unterräumen.

Sei $f : (V, +, \cdot) \to (W, +, \cdot)$ eine R–lineare Abbildung.

(1) Ist $A \leq V$ ein Unterraum, so auch die Bildmenge $B = f(A) \leq W$.
Insbesondere ist das Bild $\mathrm{Im}(f) := f(V) \leq W$ ein Unterraum.

(2) Ist $B \leq W$ ein Unterraum, so auch die Urbildmenge $A = f^{-1}(B) \leq V$.
Insbesondere ist der Kern $\mathrm{Ker}(f) := f^{-1}(\{0\}) \leq V$ eine Unterraum.

Beweis: (1) Dank J2U ist $B = f(A) \leq (W, +)$ eine Untergruppe.
Wir zeigen die Abgeschlossenheit unter Skalierung: $B \cdot R \subseteq B$.
Sei $\lambda \in R$. Zu jedem $w \in B$ existiert ein Urbild $v \in A$ mit $f(v) = w$.
Dank $A \leq (V, +, \cdot,)$ gilt $v\lambda \in A$, also $B = f(A) \ni f(v\lambda) = f(v)\lambda = w\lambda$.

(2) Dank J2U ist $A = f^{-1}(B) \leq (V, +)$ eine Untergruppe.
Wir zeigen die Abgeschlossenheit unter Skalierung: $A \cdot R \subseteq A$.
Sei $\lambda \in R$. Für $v \in A$ gilt $f(v) \in B$. Dank $B \leq (W, +, \cdot,)$
folgt $B \ni f(v)\lambda = f(v\lambda)$, also $v\lambda \in f^{-1}(B) = A$. QED

Kern-Kriterium für Injektivität

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L2B: Kern-Kriterium für Injektivität

(3) Genau dann ist f surjektiv, wenn $\mathrm{Im}(f) = W$ gilt.

(4) Genau dann ist f injektiv, wenn $\mathrm{Ker}(f) = \{0\}$ gilt. Allgemein:

(5) Für $x \in V$ und $y = f(x) \in \mathrm{Im}(f) \leq W$ gilt $f^{-1}(\{y\}) = x + \mathrm{Ker}(f)$.
Jede Faser $f^{-1}(\{y\})$ ist entweder leer oder eine Translation des Kerns.

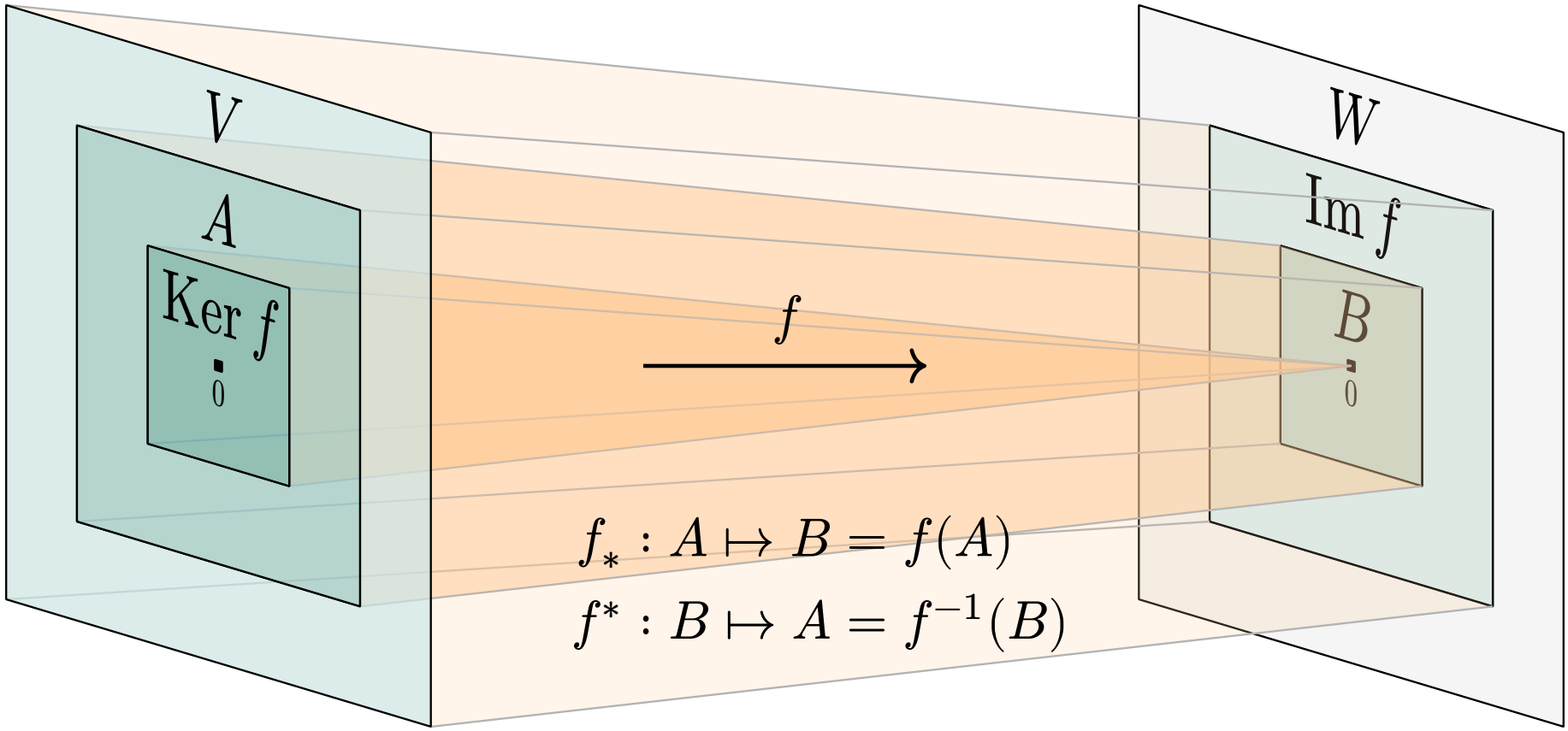
Beweis: Das haben wir bereits in Satz J2U nachgerechnet. QED

Beispiel LGS: Jede Matrix $A \in R^{m \times n}$ definiert $f_A : R^n \to R^m : x \mapsto Ax$.
Wir lösen $Ax = y$ durch $\{x \in R^n \mid Ax = y\} = f_A^{-1}(\{y\}) = x_0 + \mathrm{Ker}\, A$.

Korrespondenzsatz für lineare Unterräume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Satz L2c: Unterraum-Korrespondenz

(0) Jede R–lineare Abbildung $f : V \to W$ stiftet eine Bijektion

$$(f_*, f^*) : \{ A \mid \mathrm{Ker}(f) \leq A \leq V \} \cong \{ B \mid \{0\} \leq B \leq \mathrm{Im}(f) \}.$$

(1) Für jeden Unterraum $A \leq V$ gilt $f^{-1}(f(A)) = A + \mathrm{Ker}(f)$.
(2) Für jeden Unterraum $B \leq W$ gilt $f(f^{-1}(B)) = B \cap \mathrm{Im}(f)$.

Korrespondenzsatz für lineare Unterräume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: (1) Für jeden Unterraum $A \leq V$ gilt:

$$f^{-1}(f(A)) \overset{\text{Def}}{=} \bigcup_{x \in A} f^{-1}(f(\{x\})) \overset{\text{L2B}}{=} \bigcup_{x \in A} x + \operatorname{Ker}(f) \overset{\text{Def}}{=} A + \operatorname{Ker}(f)$$

(0a) Zusammen mit $\operatorname{Ker}(f) \leq A$ 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 $f(f^{-1}(B)) = B$. $\boxed{\text{QED}}$

Superposition: partikuläre und homogene Lösungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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:

$$\left[\begin{array}{ccccc|c} 2 & 0 & 1 & -3 & 3 & 0 \\ 1 & 1 & 0 & -2 & 5 & -1 \\ 2 & 1 & 5 & 1 & 5 & 2 \\ 1 & -3 & 2 & 0 & -9 & 3 \end{array}\right] \xrightarrow[\text{D2H}]{\text{Gauß}} \left[\begin{array}{ccccc|c} 1 & 0 & 0 & -2 & 5/3 & -1/3 \\ 0 & 1 & 0 & 0 & 10/3 & -2/3 \\ 0 & 0 & 1 & 1 & -1/3 & 2/3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Die Lösungsmenge $L(A, b) = \{x \in \mathbb{Q}^5 \mid Ax = b\}$ ist demnach explizit

$$L(A, b) = \begin{bmatrix} -1/3 \\ -2/3 \\ 2/3 \\ 0 \\ 0 \end{bmatrix} + \mathbb{Q} \begin{bmatrix} -2 \\ 0 \\ 1 \\ -1 \\ 0 \end{bmatrix} + \mathbb{Q} \begin{bmatrix} 5/3 \\ 10/3 \\ -1/3 \\ 0 \\ -1 \end{bmatrix} = v + \operatorname{Ker}(A).$$

Kern und Bild des Ableitungsoperators

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Bestimmen Sie Bild und Kern der n–fachen Ableitung ∂^n.

$$\partial : \mathbb{R}[X] \to \mathbb{R}[X] : P = \sum_{k=0}^{n} p_k X^k \mapsto P' = \sum_{k=1}^{n} k p_k X^{k-1}$$

Lösung: (1) Für $n = 1$ haben wir $\mathrm{Ker}(\partial) = \mathbb{R}$ und $\mathrm{Im}(\partial) = \mathbb{R}[X]$.

$$I : \mathbb{R}[X] \to \mathbb{R}[X] : Q = \sum_{k=0}^{n} q_k X^k \mapsto \sum_{k=0}^{n} p_k X^{k+1}/(k+1)$$

(2) Allgemein gilt $\mathrm{Ker}(\partial^n) = \mathbb{R}[X]_{<n}$ und $\mathrm{Im}(\partial^n) = \mathbb{R}[X]$.

Das kartesische Produkt linearer Räume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

? Wie rechnen Sie im Vektorraum $\mathbb{R}^n$? Koordinatenweise! Allgemein:

Satz L2D: das Produkt linearer Räume

Zu jedem Index $i \in I$ sei $(V_i, +_i, 0_i, \circ_i, \bullet_i)$ ein linearer Raum über (S, R).

Das **kartesische Produkt** $V = \prod_{i \in I} V_i$ besteht aus allen **I–Tupeln** $u = (u_i)_{i \in I}$ mit **Koordinaten** $u_i \in V_i$, zum Beispiel $\mathbf{0} := (0_i)_{i \in I}$.

(0) Auf V definieren wir Addition und Skalierung **koordinatenweise**:

$$\begin{aligned}
\mathbf{+} &: V \times V \to V : (u, v) \mapsto u \mathbf{+} v, & (u \mathbf{+} v)_i &:= u_i +_i v_i, \\
\circ &: S \times V \to V : (s, u) \mapsto s \circ u, & (s \circ u)_i &:= s \circ_i u_i, \\
\bullet &: V \times R \to V : (u, r) \mapsto u \bullet r, & (u \bullet r)_i &:= u_i \bullet_i r.
\end{aligned}$$

(1) Damit ist $(V, \mathbf{+}, \mathbf{0}, \circ, \bullet)$ ein linearer Raum über (S, R).

(2) Jede Projektion $p_i = \mathrm{pr}_i : V \twoheadrightarrow V_i : u \mapsto u_i$ ist linear über (S, R).

Die direkte Summe linearer Räume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L2D: die direkte Summe linearer Räume

(3) Der **Träger** von $u \in \prod_{i \in I} V_i$ ist $\operatorname{supp}(u) := \{\, i \in I \mid u_i \neq 0_i \,\}$. Es gilt

$$\operatorname{supp}(\mathbf{0}) = \emptyset, \qquad \operatorname{supp}(u + v) \subseteq \operatorname{supp}(u) \cup \operatorname{supp}(v),$$
$$\operatorname{supp}(s \circ u) \subseteq \operatorname{supp}(u), \qquad \operatorname{supp}(u \bullet r) \subseteq \operatorname{supp}(u).$$

(4) Das Produkt $V = \prod_{i \in I} V_i$ enthält somit als Unterraum die **Summe**

$$U = \bigoplus_{i \in I} V_i := \left\{ u \in V \,\middle|\, \sharp \operatorname{supp}(u) < \infty \right\} \leq V.$$

(5) Zu jedem $i \in I$ haben wir neben der Projektion $p_i = \mathrm{pr}_i : V \geq U \twoheadrightarrow V_i$ die Einbettung $s_i = \mathrm{inc}_i : V_i \hookrightarrow U \leq V : u_i \mapsto u$ mit $u_j = 0_j$ für alle $j \neq i$.

Koordinatenräume sind Potenzen des Grundrings.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L2D: Koordinatenräume

(6) Im Spezialfall $S = V_i = R$ für alle $i \in I$ erhalten wir:

$$\begin{aligned} R^I &= \textstyle\prod_{i\in I} R = \{\, u : I \to R : i \mapsto u_i \,\} \\ R^{(I)} &= \textstyle\bigoplus_{i\in I} R = \{\, u : I \to R \,\big|\, \sharp \operatorname{supp} u < \infty \,\} \end{aligned}$$

Zu $i \in I$ definieren wir $e_i : I \to R$ durch $e_i(i) = 1$ und $e_i(j) = 0$ sonst.

Beispiel: Der lineare Raum $\mathbb{R}^{\mathbb{N}}$ über $\mathbb{R}$ besteht aus allen Folgen

$$f : \mathbb{N} \to \mathbb{R} : k \mapsto f_k \quad \text{geschrieben} \quad (f_k)_{k\in\mathbb{N}} = (f_0, f_1, f_2, \ldots)$$

Darin ist $\mathbb{R}^{(\mathbb{N})} < \mathbb{R}^{\mathbb{N}}$ der Unterraum der endlich getragenen Folgen f:

$$\sharp \operatorname{supp}(f) < \infty \quad \Longleftrightarrow \quad f = \textstyle\sum_k f_k X^k \in \mathbb{R}[X]$$

Erzeugung von Unterräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L2G: Linearkombinationen und erzeugter Unterraum

Sei $(V, +, \cdot)$ ein rechtslinearer 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

$$\Phi_F \;:\; R^{(I)} \to V \;:\; \lambda = (\lambda_i)_{i \in I} \;\mapsto\; v = \textstyle\sum_{i \in I} u_i \lambda_i =: F\lambda.$$

(2) Ihr Bild ist der von $F = (u_i)_{i \in I}$ in V über R **erzeugte Unterraum**:

$$V \;\geq\; \mathrm{Im}(\Phi_F) \;=\; \left\{ \textstyle\sum_{i \in I} u_i \lambda_i \,\middle|\, \lambda \in R^{(I)} \right\} \;=:\; \langle u_i \,|\, i \in I \rangle_R \;=\; U$$

Dies ist der (bezüglich Inklusion) kleinste Unterraum, der F enthält.

(3) Im Spezialfall $I = \{1, \dots, n\}$ gilt $F = (u_1, \dots, u_n)$ und

$$\Phi_F : R^n \to V : (\lambda_1, \dots, \lambda_n) \mapsto u_1\lambda_1 + \cdots + u_n\lambda_n,$$

und $U = \langle u_1, \dots, u_n \rangle_R = u_1 R + \cdots + u_n R$ ist **endlich erzeugt**.

Erzeugung von Unterräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: (1) Die Summe $\sum_{i\in I} u_i\lambda_i$ ist wohldefiniert, da endlich getragen. Die Abbildung Φ_F ist R–linear: Für alle $\lambda, \mu \in R^{(I)}$ und $\alpha, \beta \in R$ gilt:

$$\begin{aligned}
\Phi_F(\lambda\alpha + \mu\beta) &\overset{\text{Def}}{=} \textstyle\sum_{i\in I} u_i(\lambda_i\alpha + \mu_i\beta) \\
&\overset{\text{Dst}}{=} \textstyle\sum_{i\in I} u_i\lambda_i\alpha + u_i\mu_i\beta \\
&\overset{\text{Dst}}{=} (\textstyle\sum_{i\in I} u_i\lambda_i)\alpha + (\sum_{i\in I} u_i\mu_i)\beta \\
&\overset{\text{Def}}{=} \Phi_F(\lambda)\alpha + \Phi_F(\mu)\beta
\end{aligned}$$

(2) Dank Satz L2B ist die Bildmenge $U = \mathrm{Im}(\Phi_F) \leq V$ ein Unterraum. Jeder Unterraum $U' \leq V$, der alle Vektoren u_i mit $i \in I$ umfasst, enthält auch jede Linearkombination $\sum_{i\in I} u_i\lambda_i$. Demnach gilt $U \leq U'$. $\boxed{\text{QED}}$

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 $E = \langle (1,2,5), (0,3,2) \rangle_{\mathbb{R}} = \langle (1,2,5), (0,3,2), (1,5,7) \rangle_{\mathbb{R}}$.

Beispiel: Polynome $R[X]$ über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Der Polynomring $R[X]$ wird über R erzeugt von $(X^n)_{n\in\mathbb{N}}$:

$$R[X] = \langle X^n \mid n \in \mathbb{N} \rangle_R^!$$

Der Raum $R[X]$ kann über R nicht endlich erzeugt werden,
denn $\langle P_1, \dots, P_n \rangle_R \leq R[X]_{\leq m}$ mit $m = \max\{\deg P_1, \dots, \deg P_n\}$.

Was bedeutet Basis?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

♦ Definition M1A: Basis — Vorschau

Ist $\Phi_F : R^{(I)} \xrightarrow{\sim} U$ bijektiv, so ist $F = (u_i)_{i \in I}$ eine **Basis** von U. Kurz:

$$U = \langle u_i \mid i \in I \rangle_R^!$$

Ausführlich in Worten: Jeder Vektor $u \in U$ schreibt sich *eindeutig* (!) als Linearkombination $u = \sum_{i \in I} u_i \lambda_i$ von $F = (u_i)_{i \in I}$ mit $\lambda \in R^{(I)}$.

Beispiele: Für $R[X]$ über R haben wir die Monombasis $(X^k)_{k \in \mathbb{N}}$. Kurz:

$$R[X] = \langle X^k \mid k \in \mathbb{N} \rangle_R^!$$

Für R^n über R haben wir die Standardbasis $(e_1, \dots, e_n)$. Kurz:

$$R^n = \langle e_1, \dots, e_n \rangle_R^!$$

Für $R^{(I)}$ über R haben wir die Standardbasis $(e_i)_{i \in I}$. Kurz:

$$R^{(I)} = \langle e_i \mid i \in I \rangle_R^!$$

Schnitt und Summe von Unterräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L2H: Die Unterräume von V bilden einen vollständigen Verband.

Sei $\mathcal{U} = (U_i)_{i\in I}$ 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.

(2) Die Summe $B = \sum_{i\in I} U_i$ ist ein R–linearer Unterraum in V, dank

$$\Phi : \bigoplus_{i\in I} U_i \to V : (u_i)_{i\in I} \mapsto \sum_{i\in I} u_i, \quad \text{mit dem Bildraum}$$

$$\sum_{i\in I} U_i := \operatorname{Im}(\Phi) = \left\{ \sum_{i\in I} u_i \,\middle|\, u_i \in U_i \ \wedge\ \sharp\operatorname{supp}(u) < \infty \right\}.$$

Schnitt und Summe von Unterräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: Wir haben $0 \in U_i$ 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 $x \cdot \lambda \in A$.

Schnitt und Summe von Unterräumen in $\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$12\mathbb{Z} \cap 15\mathbb{Z} = 60\mathbb{Z}$$
$$12\mathbb{Z} + 15\mathbb{Z} = 3\mathbb{Z}$$

$$12\mathbb{Z} \cap 15\mathbb{Z} \cap 7\mathbb{Z} = 420\mathbb{Z}$$
$$12\mathbb{Z} + 15\mathbb{Z} + 7\mathbb{Z} = 1\mathbb{Z}$$

$$\boxed{\begin{aligned} u_1\mathbb{Z} \cap \cdots \cap u_n\mathbb{Z} &= \mathrm{kgV}(u_1, \dots, u_n)\mathbb{Z} \\ u_1\mathbb{Z} + \cdots + u_n\mathbb{Z} &= \mathrm{ggT}(u_1, \dots, u_n)\mathbb{Z} \end{aligned}}$$

Auch Homomorphismen sind Vektoren.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Seien $(U, +, \cdot)$ und $(V, +, \cdot)$ rechtslineare Räume über R. Ist $\mathrm{Hom}(U, V) \leq (V^U, +, \cdot)$ ein Unterraum? Ebenso $\mathrm{Hom}_R(U, V)$?

Lösung: (0) Die Nullabbildung $0 : U \to V : u \mapsto 0_V$ ist linear über R.

(a) Sind $f, g : U \to V$ linear über R, so auch ihre Summe $f + g : U \to V$:

$$\begin{aligned}
(f+g)(x \cdot \lambda + y \cdot \mu) &\overset{\text{Def}}{=} f(x \cdot \lambda + y \cdot \mu) + g(x \cdot \lambda + y \cdot \mu) \\
&\overset{\text{Lin}}{=} f(x) \cdot \lambda + f(y) \cdot \mu \quad + \quad g(x) \cdot \lambda + g(y) \cdot \mu \\
&\overset{\text{Dst}}{=} [f(x) + g(x)] \cdot \lambda + [f(y) + g(y)] \cdot \mu \\
&\overset{\text{Def}}{=} (f+g)(x) \cdot \lambda + (f+g)(y) \cdot \mu
\end{aligned}$$

Auch Homomorphismen sind Vektoren.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(b) Sei $\rho \in R$. Ist $f : U \to V$ additiv, so auch $f \cdot \rho : U \to V$:

$$\begin{aligned}
(f \cdot \rho)(x + y) &\overset{\text{Def}}{=} f(x + y) \cdot \rho \\
&\overset{\text{Add}}{=} [f(x) + f(y)] \cdot \rho \\
&\overset{\text{Dst}}{=} f(x) \cdot \rho + f(y) \cdot \rho \\
&\overset{\text{Def}}{=} (f \cdot \rho)(x) + (f \cdot \rho)(y)
\end{aligned}$$

(c) Sei $\rho \in R$ zentral. Ist $f : U \to V$ linear über R, so auch $f \cdot \rho : U \to V$:

$$\begin{aligned}
(f \cdot \rho)(x \cdot \lambda) &\overset{\text{Def}}{=} f(x \cdot \lambda) \cdot \rho \\
&\overset{\text{Lin}}{=} f(x) \cdot \lambda \cdot \rho \\
&\overset{\text{Znt}}{=} f(x) \cdot \rho \cdot \lambda \\
&\overset{\text{Def}}{=} (f \cdot \rho)(x) \cdot \lambda
\end{aligned}$$

Auch Homomorphismen sind Vektoren.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L2κ: $\mathrm{Hom}_R(U, V)$ als linearer Raum

Seien $(U, +, \cdot)$ und $(V, +, \cdot)$ rechtslineare Räume über dem Ring $(R, +, \cdot)$.
Im Raum $(V^U, +, \cdot)$ ist $\mathrm{Hom}_R(U, V)$ ein linearer Unterraum über $Z(R)$.
Dank Matrixdarstellung D1J folgt $\mathrm{Hom}_R(R^n, R^m) \cong R^{m \times n}$ über $Z(R)$.

Der Endomorphismenring $\mathrm{End}_R(V)$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L2L: der Endomorphismenring $\mathrm{End}_R(V)$

(1) Komposition von Homomorphismen distribuiert über die Addition: Für alle $f, f' \in \mathrm{Hom}_R(U, V)$ und $g, g' \in \mathrm{Hom}_R(V, W)$ gilt

$$(g + g') \circ f = g \circ f + g' \circ f,$$
$$g \circ (f + f') = g \circ f + g \circ f'.$$

(2) Insbesondere ist somit $(\mathrm{End}_R(V), +, 0, \circ, \mathrm{id}_V)$ ein Ring.

Äquivalenz modulo eines Unterraumes $U \leq V$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vorbild: Zum Unterraum $n\mathbb{Z} \leq \mathbb{Z}$ konstruieren wir den Quotienten $\mathbb{Z}/n\mathbb{Z}$.

$$U \xhookrightarrow{\text{inc}} V \xrightarrow{q} V/U \qquad \text{mit } \operatorname{Ker}(q) = U$$

Sei V ein R–linearer Raum und $U \leq V$ ein Unterraum.
Für Vektoren $x, y \in V$ definieren wir

$$x \underset{U}{\sim} y \quad :\Leftrightarrow \quad x - y \in U.$$

Dies ist eine Äquivalenzrelation:

1. Reflexivität: Es gilt $x \underset{U}{\sim} x$, denn $x - x = 0 \in U$.
2. Symmetrie: $x \underset{U}{\sim} y$ bedeutet $x - y \in U$, also $y - x \in U$, somit $y \underset{U}{\sim} x$.
3. Transitivität: $x \underset{U}{\sim} y$ und $y \underset{U}{\sim} z$ bedeuten $x - y \in U$ und $y - z \in U$, daraus folgt $U \ni (x - y) + (y - z) = x - z$, somit $x \underset{U}{\sim} z$.

Äquivalenzklassen modulo eines Unterraumes $U \leq V$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zu jedem Vektor $x \in V$ haben wir die zugehörige Äquivalenzklasse:

$$[x]_U = x + U := \{\, x + u \mid u \in U \}$$

Alle Äquivalenzklassen fassen wir zur Quotientenmenge zusammen:

$$V/U := \{\, [x] = x + U \mid x \in V \}$$

Die zugehörige Quotientenabbildung ist demnach:

$$q : V \twoheadrightarrow V/U : x \mapsto [x]$$

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 $V/V = \{\, [0] = V \}$.
Die Quotientenabbildung $q : V \to V/V : x \mapsto V$ ist konstant.

Konstruktion der Quotientengruppe $(V/U, +)$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Erinnerung: 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 die (wohldefinierte!) Addition

$$+ : V/U \times V/U \to V/U : ([x], [y]) \mapsto [x] + [y] := [x + y].$$

Konstruktion des Quotientenraumes $(V/U, +, \cdot)$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $\lambda \in R$. Aus $x \sim x'$ 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 die (wohldefinierte!) Skalierung

$$\cdot : V/U \times R \to V/U : ([x], \lambda) \mapsto [x] \cdot \lambda := [x \cdot \lambda].$$

Satz L3A: 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.
Die Quotientenabbildung $q : V \twoheadrightarrow V/U$ ist R–linear mit $\mathrm{Ker}(q) = U$.

Lineare Faktorisierung über eine Surjektion

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L3c: Wir faktorisieren f über π zu $\bar{f}$.

Vorgelegt seien R–lineare Abbildungen $\pi : V \twoheadrightarrow Q$ surjektiv und $f : V \to W$ beliebig. Gilt $\mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(f)$, so existiert genau ein Homomorphismus $\bar{f} : Q \to W$ mit $f = \bar{f} \circ \pi$.

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, two heads, "\pi"'] & W \\ Q \arrow[ur, dashed, "\exists!\bar{f}"'] & \end{tikzcd}$$

Beweis: *Eindeutigkeit:* Aus $\bar{f} \circ \pi = \tilde{f} \circ \pi$ folgt $\bar{f} = \tilde{f}$, da π surjektiv ist.

Konstruktion: Zu jedem $\bar{x} \in Q$ wählen wir *willkürlich* ein Urbild $x \in V$ mit $\pi(x) = \bar{x}$ und setzen $\bar{f}(\bar{x}) := f(x)$. Ist das Ergebnis *wohldefiniert*? Ja, aus $\pi(x) = \pi(x')$ folgt $x - x' \in \mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(f)$, also $f(x) = f(x')$.

Linearität: Seien $\lambda, \mu \in R$ Skalare. Für je zwei Vektoren $\bar{x}, \bar{y} \in Q$ und beliebige Urbilder $x, y \in V$ gilt $\pi(x\lambda + y\mu) \overset{\text{Hom}}{=} \bar{x}\lambda + \bar{y}\mu$, nach Konstuktion also $\bar{f}(\bar{x}\lambda + \bar{y}\mu) \overset{\text{Def}}{=} f(x\lambda + y\mu) \overset{\text{Hom}}{=} f(x)\lambda + f(y)\mu \overset{\text{Def}}{=} \bar{f}(\bar{x})\lambda + \bar{f}(\bar{y})\mu$. $\boxed{\text{QED}}$

Injektiv und surjektiv machen: kanonische Faktorisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd}
V \arrow[r, "f"] \arrow[d, two heads, "q"', "{[x] \leftarrow\!\shortmid x}"] & W \\
V/\operatorname{Ker}(f) \arrow[r, "\bar{f}", "{[x] \mapsto f(x)}"'] & \operatorname{Im}(f) \arrow[u, hook, "\iota", "{y \mapsto y}"']
\end{tikzcd}$$

Satz L3D: kanonische Faktorisierung aka Homomorphiesatz

Jede R–lineare Abbildung $f : V \to W$ faktorisiert gemäß $f = \iota \circ \bar{f} \circ q$ in

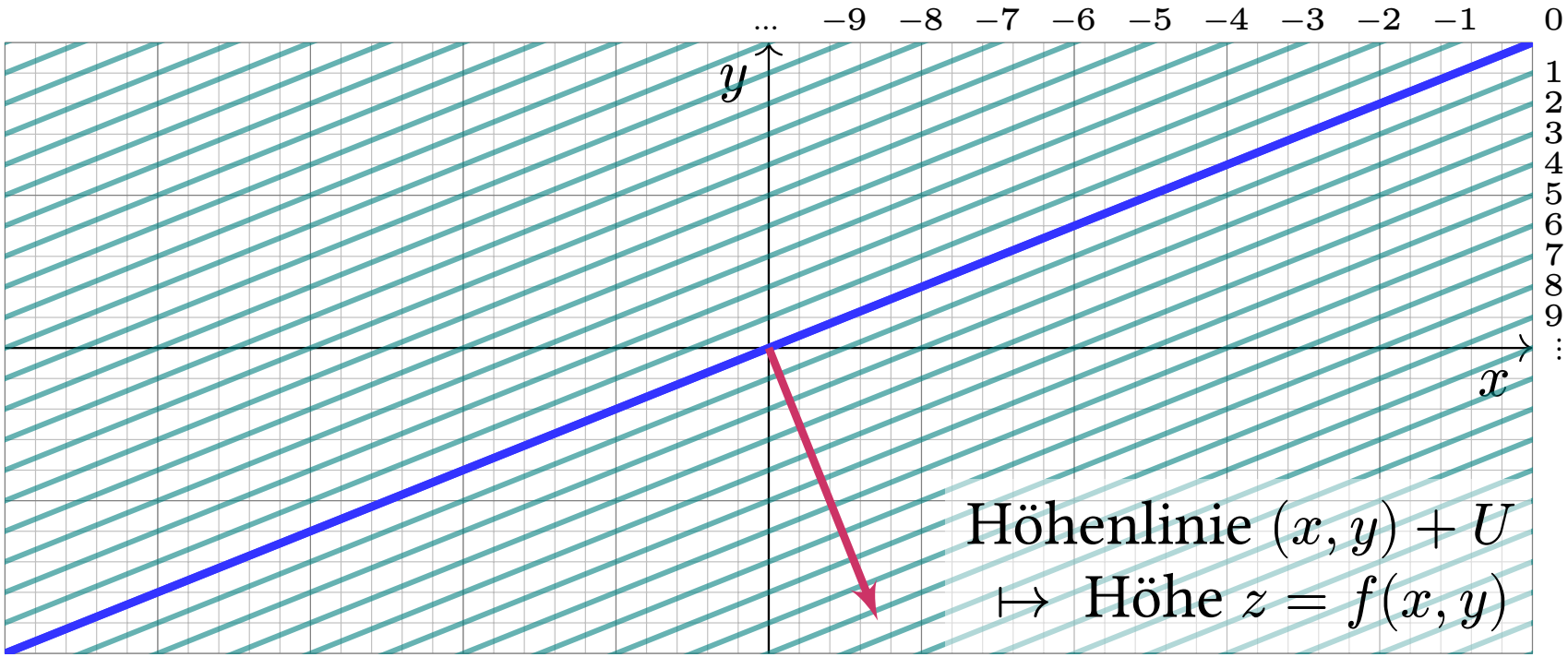
1. die Quotientenabbildung $q : V \twoheadrightarrow V/\operatorname{Ker}(f) : x \mapsto [x]$,
2. die Bijektion $\bar{f} : V/\operatorname{Ker}(f) \xrightarrow{\sim} \operatorname{Im}(f) : [x] \mapsto f(x)$,
3. die Inklusion $\iota : \operatorname{Im}(f) \hookrightarrow W : y \mapsto y$.

Diese sind R–linear. Dank Satz L1J ist $\bar{f}$ ein R–Isomorphismus.

Höhe als Beispiel zur kanonischen Faktorisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Aufgabe: Führen Sie dies aus für $f : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto z = 2x - 5y$.

Lösung: (1) Es gilt $\mathrm{Im}(f) = \mathbb{R}$. (2) Es gilt $\mathrm{Ker}(f) = (5, 2) \cdot \mathbb{R}$. (3) Also:

$$\bar{f} : \mathbb{R}^2/U \xrightarrow{\sim} \mathbb{R} : (x, y) + U \mapsto z = f(x, y).$$

Jeder Höhenlinie $(x, y) + U$ wird ihre Höhe $z = f(x, y)$ zugeordnet.

HDI als analytisches Beispiel zur kanonischen Faktorisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

? Sind Differenzieren und Integrieren zueinander Umkehrungen?

$$\int x^n \,\mathrm{d}x = \frac{x^{n+1}}{n+1} + \text{const}, \qquad \int \mathrm{e}^{\lambda x} \,\mathrm{d}x = \mathrm{e}^{\lambda x}/\lambda + \text{const},$$

$$\begin{tikzcd} \mathbb{R} \arrow[r, hook, "\text{inc}"] & \mathscr{C}^1(X,\mathbb{R}) \arrow[r, shift left, "D"] & \mathscr{C}^0(X,\mathbb{R}) \arrow[l, bend left, "I"] \end{tikzcd}$$

Auf dem Intervall $X =]a,b[\subseteq \mathbb{R}$ haben wir die Ableitung $D : F \mapsto f = F'$ und dazu „umgekehrt“ das Integral $I : f \mapsto F$ mit $F(x) = \int_{t=x_0}^{x} f(t)\,\mathrm{d}t$.
Hauptsatz: Es gilt $D \circ I = \mathrm{id}$, also ist D surjektiv, doch $\mathrm{Ker}(D) = \mathbb{R}$.

$$(\bar{D}, \bar{I}) : \mathscr{C}^1(X,\mathbb{R})/\mathbb{R} \cong \mathscr{C}^0(X,\mathbb{R}) : F + \mathbb{R} = [F] \leftrightarrows f$$

Der Isomorphiesatz für lineare Räume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L3E: 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:

$$\begin{tikzcd}
V \arrow[r, hook, "\mathrm{inc}"] \arrow[d, two heads, "q"'] \arrow[dr, two heads, "f"] & V + U \arrow[d, two heads, "p"] \\
V/(V \cap U) \arrow[r, dashed, "\varphi", "\cong"'] & (V + U)/U
\end{tikzcd}
\qquad
\begin{tikzcd}
W/U \arrow[d, two heads, "r"'] & W \arrow[l, two heads, "q"'] \arrow[d, two heads, "p"] \arrow[dl, two heads, "g"] \\
(W/U)/(V/U) \arrow[r, dashed, "\psi", "\cong"'] & W/V
\end{tikzcd}$$

Unterraum-Korrespondenz und Isomorphiesatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: (1) Im $\mathbb{Z}$–linearen Raum $W = \mathbb{Z}$ sei $V = 4\mathbb{Z}$ und $U = 6\mathbb{Z}$. Hier gilt $V \cap U = 12\mathbb{Z}$ und $V + U = 2\mathbb{Z}$, also $4\mathbb{Z}/12\mathbb{Z} \cong 2\mathbb{Z}/6\mathbb{Z}$.

(2) Für $12\mathbb{Z} \leq 4\mathbb{Z} \leq 2\mathbb{Z}$ gilt $(2\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z}) \cong 2\mathbb{Z}/4\mathbb{Z}$.

Man muss auch Ideale haben: Hauptidealringe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Die $\mathbb{Z}$–linearen Unterräume von $\mathbb{Z}$ sind $n\mathbb{Z}$ mit $n \in \mathbb{N}$ (Satz J2T).

Sei R ein Ring. Ein R–Unterraum $I \leq (R, +, \cdot)$ heißt rechtsseitiges **Ideal**. Das bedeutet $0 \in I$ und $I + I \subseteq I$ und $I \cdot R \subseteq I$ bzgl. Rechtsskalierung.

Beispiel: Jedes Ringelement $a \in R$ erzeugt das **Hauptideal** $\langle a \rangle_R = aR$.

Satz L3F: Klassifikation aller Ideale im Ring $\mathbb{K}[X]$ – Minimalpolynom

Sei $\mathbb{K}$ ein Körper und darüber $R = \mathbb{K}[X]$ der Polynomring. Darin ist jedes Ideal $I \leq (R, +, \cdot)$ ein Hauptideal, also $I = aR$ für ein Element $a \in R$.

Beweis: (0) Für $I = \{0\}$ genügt $a = 0$. (1) Sei $I \supsetneq \{0\}$.
Dann existiert $a \in I \smallsetminus \{0\}$ mit $\deg(a) \in \mathbb{N}$ minimal.

(2) Wir zeigen $I = aR$. Aus $a \in I \leq R$ folgt $aR \subseteq I$. Umgekehrt sei $b \in I$. Polynomdivision C2A ergibt $b = aq + r$ mit $q, r \in R$ und $\deg(r) < \deg(a)$. Es folgt $r = b - aq \in I$, somit $r = 0$, denn $\deg(a)$ ist minimal gemäß (1). Also gilt $b = aq \in aR$. Das zeigt $I \subseteq aR$. Wir schließen $I = aR$. QED

Man muss auch Ideale haben: Quotientenringe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele: Wir kennen bereits die prominenten Quotientenringe

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n \quad \text{und} \quad \mathbb{K}[X]/P\mathbb{K}[X] \cong \mathbb{K}[X]_P.$$

Satz L3G: vom Ring R zum Quotientenring R/I

Sei $(R, +, 0, \cdot, 1)$ ein Ring und $I \trianglelefteq R$ ein beidseitiges Ideal, also

$$0 \in I \quad \text{und} \quad I + I \subseteq I \quad \text{und} \quad R \cdot I \subseteq I \supseteq I \cdot R.$$

(1) Der Quotient $(R/I, +, [0], \cdot, [1])$ ist ein Ring mit

$$\begin{aligned} + &: R/I \times R/I \to R/I : [x] + [y] := [x + y], \\ \cdot &: R/I \times R/I \to R/I : [x] \cdot [y] := [x \cdot y]. \end{aligned}$$

Man muss auch Ideale haben: Quotientenringe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: Aus $x \sim x'$ und $y \sim y'$ folgt $x \cdot y \sim x' \cdot y'$, denn

$$x \cdot y - x' \cdot y' = x \cdot (y - y') + (x - x') \cdot y' \quad \in \quad R \cdot I + I \cdot R \quad \subseteq \quad I$$

Exakt: wie die Faust aufs Auge

$$U \xrightarrow[\operatorname{Im} g \subseteq]{g} V \xrightarrow[\supseteq \operatorname{Ker} f]{f} W$$

$$\operatorname{Im}(g) \subseteq \operatorname{Ker}(f) \quad \Longleftrightarrow \quad f \circ g = 0 \qquad \text{(leicht nachzurechnen)}$$

$$\operatorname{Im}(g) \supseteq \operatorname{Ker}(f) \quad \Longleftrightarrow \quad \operatorname{Ker}(f) = \langle v_i \mid i \in I \rangle_R \ \text{ und } \ v_i = g(u_i)$$

$$\operatorname{Im}(g) = \operatorname{Ker}(f) \quad \Longleftrightarrow: \quad (g, f) \text{ ist exakt}$$

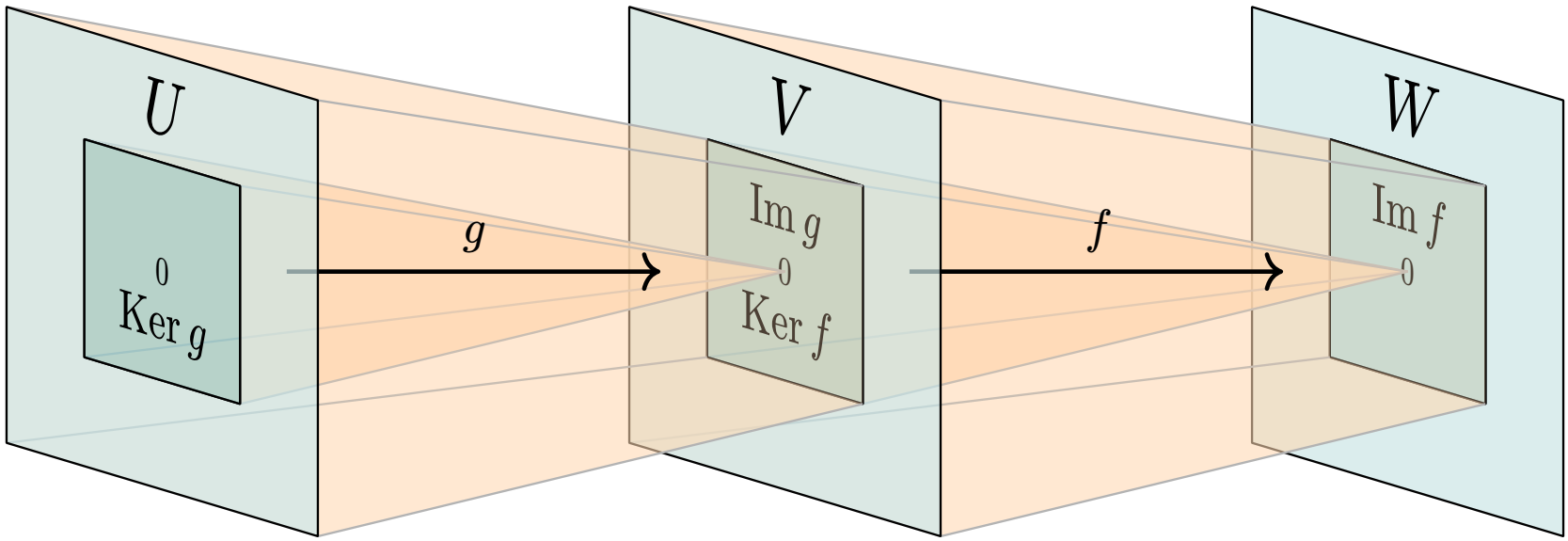
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Exakt: wie die Faust aufs Auge

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



$$0 \xrightarrow{0} V \xrightarrow{f} W \quad \text{exakt} \overset{\text{Def}}{\iff} \operatorname{Ker}(f) = \{0\} \overset{\text{L2B}}{\iff} f \text{ injektiv}$$

$$V \xrightarrow{f} W \xrightarrow{0} 0 \quad \text{exakt} \overset{\text{Def}}{\iff} \operatorname{Im}(f) = W \overset{\text{Def}}{\iff} f \text{ surjektiv}$$

$$0 \xrightarrow{0} V \xrightarrow{f} W \xrightarrow{0} 0 \quad \text{exakt} \overset{\text{L1J}}{\iff} f \text{ ist ein Isomorphismus}$$

Exakte Paare prüfen dank Gauß–Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Welche der folgenden vier Paare sind exakt?

$$\mathbb{R}^4 \xrightarrow[\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\1&0&0&0\end{bmatrix}]{A} \mathbb{R}^4 \xrightarrow[\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&0\end{bmatrix}]{B} \mathbb{R}^4 \xrightarrow[\begin{bmatrix}0&0&1&0\\0&0&0&1\\0&0&0&0\\0&0&0&0\end{bmatrix}]{C} \mathbb{R}^4 \xrightarrow[\begin{bmatrix}0&0&1&0\\0&0&0&1\\0&0&0&0\\0&0&0&0\end{bmatrix}]{D} \mathbb{R}^4 \xrightarrow[\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}]{E} \mathbb{R}^4$$

☺ $\operatorname{Im} A = \operatorname{Ker} B$ ☹ $\operatorname{Im} B \supsetneq \operatorname{Ker} C$ ☺ $\operatorname{Im} C = \operatorname{Ker} D$ ☹ $\operatorname{Im} D \subsetneq \operatorname{Ker} E$

Exakte Paare erstellen dank Gauß–Algorithmus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Wie ergänzen Sie B zu einer exakten Sequenz?

$$0 \xrightarrow{0} \mathbb{R}^1 \xrightarrow[\begin{bmatrix}0\\0\\1\end{bmatrix}]{A} \mathbb{R}^3 \xrightarrow[\begin{bmatrix}1&0&0\\0&1&0\\0&0&0\\0&0&0\end{bmatrix}]{B} \mathbb{R}^4 \xrightarrow[\begin{bmatrix}0&0&1&0\\0&0&0&1\end{bmatrix}]{C} \mathbb{R}^2 \xrightarrow{0} 0$$

$\mathbb{R}^1$: $\operatorname{Ker} A = \{0\}$

$\mathbb{R}^3$: $\operatorname{Im} A = \operatorname{Ker} B$

$\mathbb{R}^4$: $\operatorname{Im} B = \operatorname{Ker} C$

$\mathbb{R}^2$: $\operatorname{Im} C = \mathbb{R}^2$

Exakte Sequenzen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

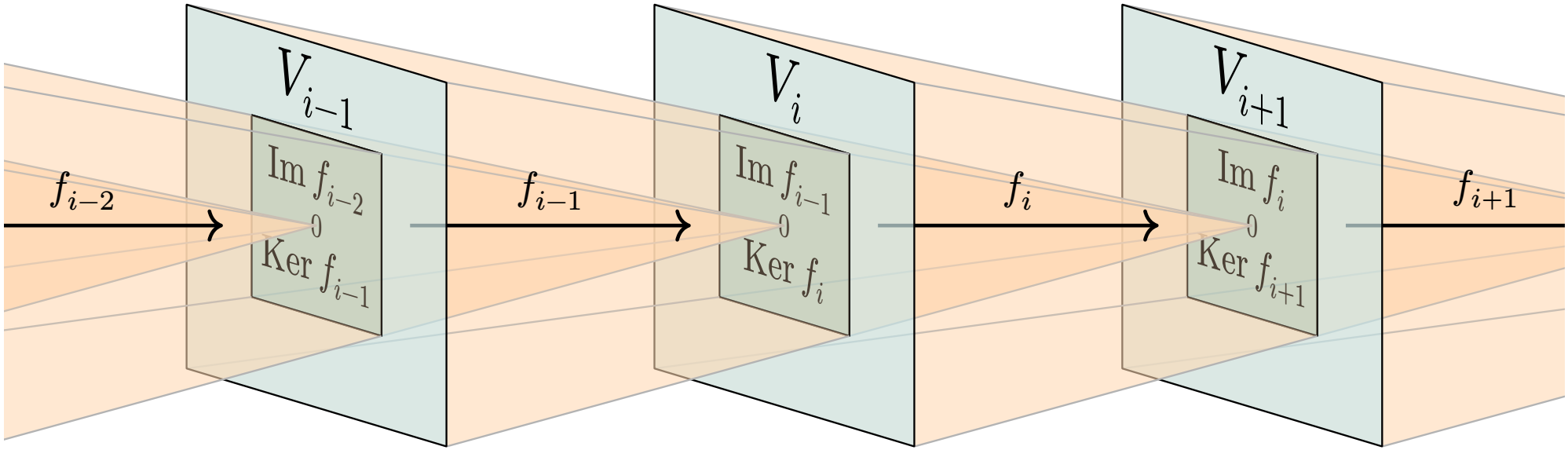
Definition L3H: exakte Sequenz, Bild gleich Kern

Wir betrachten lineare Räume oder Gruppen und ihre Homomorphismen.

$$S: \quad V_0 \xrightarrow{f_0} V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} \dots \longrightarrow V_{n-1} \xrightarrow{f_{n-1}} V_n$$

Wir nennen $S = (f_i : V_i \to V_{i+1})_{i=0}^{n-1}$ eine **Sequenz** mit $n+1$ Termen.
Sie ist **exakt** an der Stelle $i \in \{1, \dots, n-1\}$, falls $\mathrm{Im}(f_{i-1}) = \mathrm{Ker}(f_i)$ gilt.

Exakte Sequenzen



Jede lineare Abbildung $f : V \to W$ definiert eine kurze exakte Sequenz:

$$0 \xrightarrow{0} \mathrm{Ker}(f) \xhookrightarrow{\mathrm{inc}} V \xrightarrow{\hat{f}} \mathrm{Im}(f) \xrightarrow{0} 0$$

Jeder lineare Unterraum $U \leq V$ definiert eine kurze exakte Sequenz:

$$0 \xrightarrow{0} U \xhookrightarrow{\mathrm{inc}} V \xrightarrow{\mathrm{quo}} V/U \xrightarrow{0} 0$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Exakte Sequenzen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: (1) Zu $n = k + \ell$ erhalten wir die folgende exakte Sequenz:

$$\begin{array}{ccccccccc} 0 & \xrightarrow{0} & \mathbb{R}^k & \xrightarrow{\iota} & \mathbb{R}^n & \xrightarrow{\pi} & \mathbb{R}^\ell & \xrightarrow{0} & 0 \\ (a_0, \dots, a_{k-1}) = a & \longmapsto & (a, 0) & & & & & & \\ & & (a, b) & \longmapsto & b = (b_0, \dots, b_{\ell-1}) & & & & \end{array}$$

(2) Für Polynome erhalten wir die folgende exakte Sequenz:

$$0 \xrightarrow{0} \mathbb{R}[X]_{<k} \xrightarrow{\text{inc}} \mathbb{R}[X]_{<n} \xrightarrow{\partial^k} \mathbb{R}[X]_{<\ell} \xrightarrow{0} 0$$

Summenzerlegung und Projektionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei R ein Ring und $(U_i)_{i\in I}$ eine Familie R–linearer Räume mit

$$\begin{aligned} &\text{Produkt} \quad P = \textstyle\prod_{i\in I} U_i := \{\, u = (u_i)_{i\in I} \mid \forall i \in I : u_i \in U_i \,\}, \\ &\text{Summe} \quad S = \textstyle\bigoplus_{i\in I}^{\text{ext}} U_i := \{\, u \in P \mid \sharp\,\mathrm{supp}(u) < \infty \,\} \leq P. \end{aligned}$$

Ist I endlich, etwa $I = \{1, \dots, n\}$, so gilt $S = P = U_1 \times \cdots \times U_n$.

Definition L3J: Summenzerlegung aka interne direkte Summe

(0) Unterräume $(U_i \leq V)_{i\in I}$ erzeugen die interne Summe $\sum_{i\in I} U_i =: U$.
Sie ist Bild der linearen Abbildung $\Phi : \bigoplus_{i\in I}^{\text{ext}} U_i \twoheadrightarrow U : (u_i)_{i\in I} \mapsto \sum_{i\in I} u_i$.

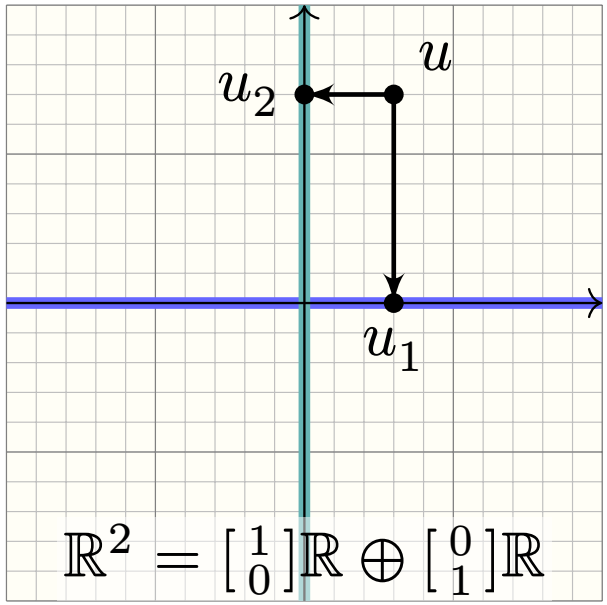
(1) Wir schreiben $U = \bigoplus_{i\in I}^{\text{int}} U_i$ falls Φ injektiv ist, also $\Phi : S \xrightarrow{\sim} U$.
Die Familie $(U_i \leq U)_{i\in I}$ heißt dann eine **Summenzerlegung** von U.

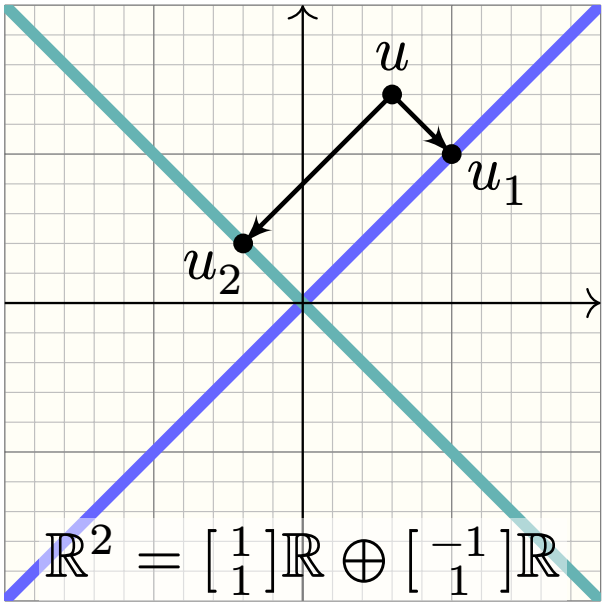
Die **Projektionen** $\pi_i = \mathrm{pr}_i \circ \Phi^{-1} : U \to U_i$ zerlegen jeden Vektor $u \in U$ als Summe $u = \sum_{i\in I} u_i$ der (eindeutigen!) Summanden $u_i = \pi_i(u) \in U_i$.

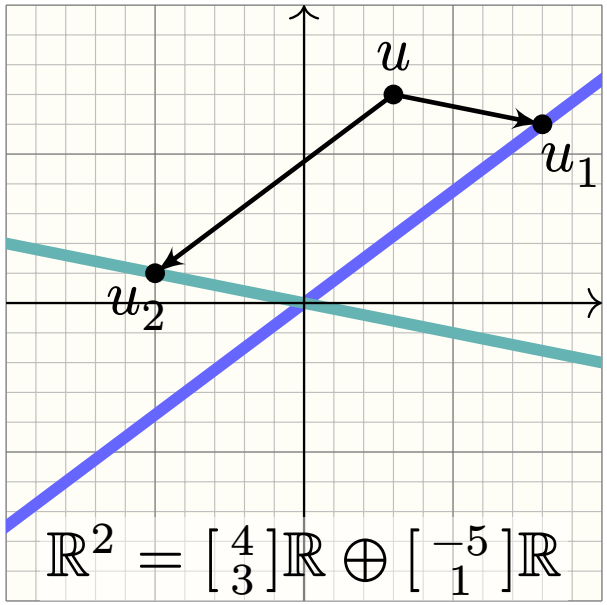
Summenzerlegung und Projektionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.







Beispiel: Im $\mathbb{R}$–Vektorraum $U = \mathbb{R}^2$ liegen als $\mathbb{R}$–lineare Unterräume die **x–Achse** $A_1 = \{\,(x,0) \mid x \in \mathbb{R}\,\}$ und die **y–Achse** $A_2 = \{\,(0,y) \mid y \in \mathbb{R}\,\}$.

Jeder Vektor $u = (x,y) \in \mathbb{R}^2$ zerlegt sich eindeutig als Summe $u = u_1 + u_2$ mit $u_i \in A_i$, nämlich $u_1 = (x,0) =: \pi_1(u)$ und $u_2 = (0,y) =: \pi_2(u)$.

Die Schnittbedingung zur Summenzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Nach Konstruktion ist $\Phi : S \twoheadrightarrow U$ immer surjektiv. Wann ist Φ injektiv?
$u \in \operatorname{Ker} \Phi$ bedeutet $\sum_{i \in I} u_i = 0$, also $-u_j = \sum_{i \neq j} u_i \ \in \ U_j \cap \sum_{i \neq j} U_i$.

Satz L3κ: Unabhängigkeit als Schnittbedingung

(1) Die Summe $U = \sum_{i \in I} U_i$ ist direkt, $U = \bigoplus_{i \in I}^{\text{int}} U_i$, genau dann wenn

$$U_j \cap \sum_{i \neq j} U_i = \{0\} \quad \text{für alle } j \in I.$$

(2) Für $I = \{1, 2\}$ bedeutet das $U_1 \cap U_2 = \{0\}$. Folgende Sequenz ist exakt:

$$0 \longrightarrow U_1 \cap U_2 \xrightarrow[u \mapsto (-u, u)]{\Psi} U_1 \times U_2 \xrightarrow[(u_1, u_2) \mapsto u_1 + u_2]{\Phi} U_1 + U_2 \longrightarrow 0.$$

Projektoren zur direkten Summenzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel L3N: Zerlegung in gerade und ungerade

Jede Funktion $f : \mathbb{R} \to \mathbb{R}$ schreibt sich eindeutig als Summe $f = g + u$ einer geraden Funktion $g : \mathbb{R} \to \mathbb{R}$, also $g(-x) = g(x)$, und einer ungeraden Funktion $u : \mathbb{R} \to \mathbb{R}$, also $u(-x) = -u(x)$. Somit:

$$\mathrm{Fun}(\mathbb{R}, \mathbb{R}) = \mathrm{Fun}(\mathbb{R}, \mathbb{R})^+ \oplus \mathrm{Fun}(\mathbb{R}, \mathbb{R})^-$$

Diese Zerlegung folgt aus den $\mathbb{R}$–linearen Projektoren

$$p_1 = p_+ : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}^{\mathbb{R}} : f \mapsto g \quad \text{mit} \quad g(x) = \tfrac{1}{2}\big[f(x) + f(-x)\big],$$

$$p_2 = p_- : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}^{\mathbb{R}} : f \mapsto u \quad \text{mit} \quad u(x) = \tfrac{1}{2}\big[f(x) - f(-x)\big].$$

Projektoren zur direkten Summenzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel L3N: Zerlegung in symmetrisch und antisymmetrisch

Jede Matrix $M \in \mathbb{R}^{n\times n}$ schreibt sich eindeutig als Summe $M = S + A$ einer symmetrischen Matrix $S \in \mathbb{R}^{n\times n}$, also $S^\top = S$, und einer antisymmetrischen Matrix $A \in \mathbb{R}^{n\times n}$, also $A^\top = -A$. Somit:

$$\mathbb{R}^{n\times n} = \mathbb{R}^{n\times n}_{\text{sym}} \oplus \mathbb{R}^{n\times n}_{\text{asym}}$$

Diese Zerlegung folgt aus den $\mathbb{R}$–linearen Projektoren

$$p_1 = p_+ \,:\, \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n} \,:\, M \mapsto S := \tfrac{1}{2}\big[M + M^\top\big],$$

$$p_2 = p_- \,:\, \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n} \,:\, M \mapsto A := \tfrac{1}{2}\big[M - M^\top\big].$$

Projektoren zur direkten Summenzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L3o: Summenzerlegung dank Projektor / Idempotenz

Ein **Projektor** $p : V \to V$ ist eine lineare Abbildung mit $p^2 = p$.
Daraus folgt die Summenzerlegung $V = \mathrm{Im}(p) \oplus \mathrm{Ker}(p)$.

Beweis: Wir zeigen (a) $\mathrm{Im}(p) + \mathrm{Ker}(p) = V$ und (b) $\mathrm{Im}(p) \cap \mathrm{Ker}(p) = \{0\}$.

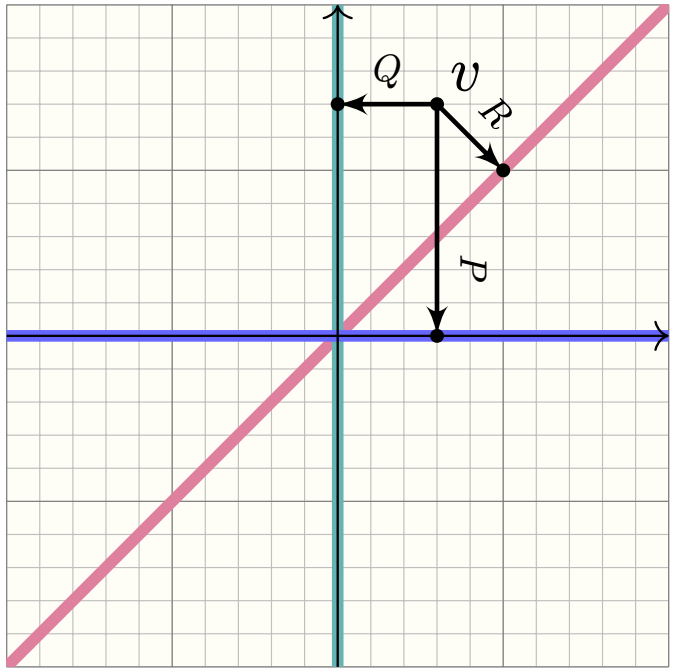
(a) Wir zerlegen $v \in V$ in $v = v_1 + v_2$ mit $v_1 = p(v)$ und $v_2 = v - v_1$.
Es gilt $v_2 \in \mathrm{Ker}(p)$, denn $p(v_2) \overset{\text{Lin}}{=} p(v) - p(v_1) \overset{\text{Def}}{=} p(v) - p^2(v) \overset{\text{Idem}}{=} 0$.

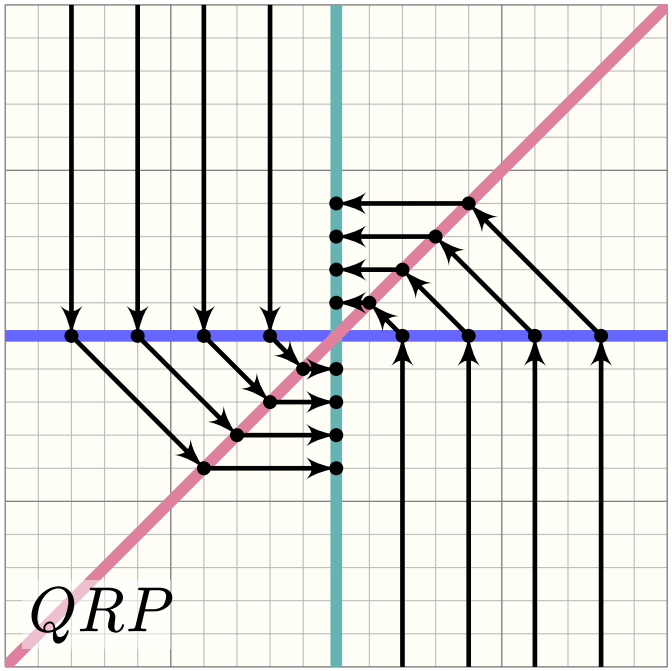
(b) Vorgelegt sei $v \in \mathrm{Im}(p)$, also $v = p(u)$ für ein Urbild $u \in V$.
Gilt zudem $v \in \mathrm{Ker}(p)$, so folgt $0 \overset{\text{Def}}{=} p(v) \overset{\text{Bild}}{=} p^2(u) \overset{\text{Idem}}{=} p(u) \overset{\text{Def}}{=} v$. $\boxed{\text{QED}}$

Projektoren zur direkten Summenzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Aufgabe: Untersuchen Sie $p, q, r : \mathbb{R}^2 \to \mathbb{R}^2$ gegeben durch

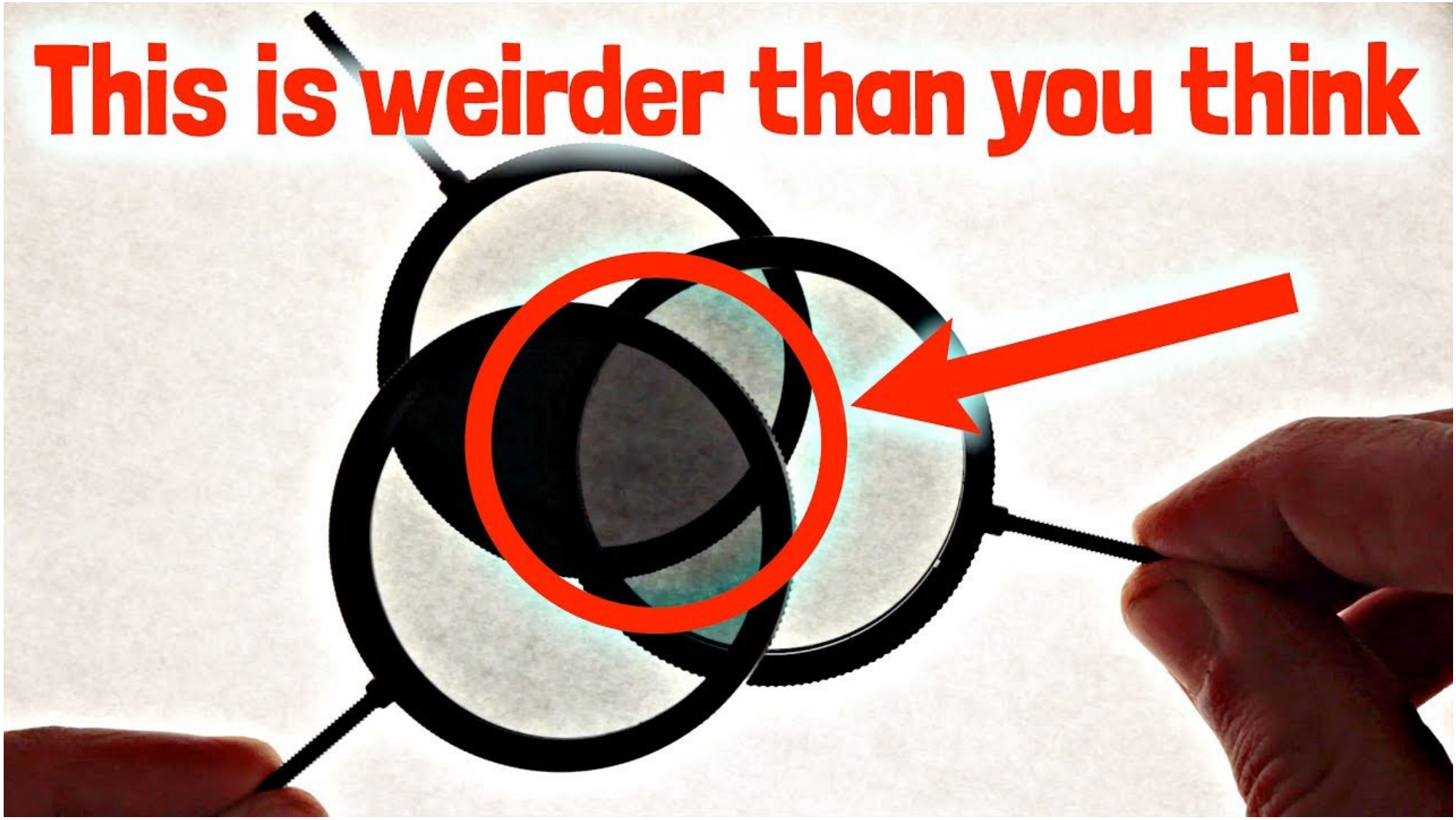
$$P = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad Q = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad R = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Erklären Sie algebraisch und geometrisch $QP = 0 \neq QRP$.

Anwendung: Polarisation des Lichts

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Quantum Venn diagramm paradox. `youtu.be/zcqZHYo7ONs`

Zerlegung der Eins in orthogonale Idempotente

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L3o: Projektoren und Idempotenz

(1) Gegeben sei eine Summenzerlegung $V = \bigoplus_{i \in I}^{\text{int}} V_i$. Für jeden Index $j \in I$ definiert dies den **Projektor** $p_j : V \to V : \sum_{i \in I} v_i \mapsto v_j$ mit $v_i \in V_i$.

($\star$) Wir haben $p_j \in \operatorname{End}_R(V)$ mit $p_j \circ p_i = 0$ für $i \neq j$ und $\sum_{i \in I} p_i = \mathrm{id}_V$.

(2) Allein aus ($\star$) folgt $p_j^2 = p_j$ und $V = \bigoplus_{i \in I}^{\text{int}} V_i$ mit $V_i := \operatorname{Im}(p_i) \leq V$.

Spaltungslemma

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede direkte Summe $V = V_1 \oplus V_2$ definiert Inklusionen und Projektionen:

$$\begin{tikzcd} 0 \arrow[r, shift left] & V_1 \arrow[l, shift left] \arrow[r, hook, shift left, "\iota_1"] & V_1 \oplus V_2 \arrow[l, two heads, shift left, "\pi_1"] \arrow[r, two heads, shift left, "\pi_2"] & V_2 \arrow[l, hook, shift left, "\iota_2"] \arrow[r, shift left] & 0 \arrow[l, shift left] \end{tikzcd}$$

Satz L3P: Spaltungslemma

Gegeben sei eine kurze exakte Sequenz von R–linearen Abbildungen:

$$E: \quad \begin{tikzcd} 0 \arrow[r, "0"] & U \arrow[r, "f"] & V \arrow[l, bend left, dashed, "r"] \arrow[r, "g"] & W \arrow[l, bend left, dashed, "s"] \arrow[r, "0"] & 0 \end{tikzcd}$$

Die folgenden drei Eigenschaften sind untereinander äquivalent:

1. Direkte Summe: Zum Unterraum $U' = f(U)$ in V existiert ein direktes Komplement W' in V so, dass $V = U' \oplus W'$ gilt.
2. Die Sequenz spaltet rechts: Es gibt $s : W \to V$ linear mit $g \circ s = \mathrm{id}_W$.
3. Die Sequenz spaltet links: Es gibt $r : V \to U$ linear mit $r \circ f = \mathrm{id}_U$.

Spaltungslemma

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: „(1) $\Rightarrow$ (2)“: Die Einschränkung $g|_{W'} : W' \to W$ ist bijektiv: Zu jedem $w \in W$ existiert ein Urbild $v \in V$ mit $g(v) = w$. Wir zerlegen $v = u' + w'$ eindeutig in $u' \in U'$ und $w' \in W'$. Dank $U' = \operatorname{Ker}(g)$ gilt $g^{-1}(\{w\}) = U' + w'$, somit $g|_{W'}^{-1}(\{w\}) = \{w'\}$. Da $g|_{W'}$ linear ist, gilt dies auch für $s = \operatorname{inc}_{W'}^{V} \circ g|_{W'}^{-1} : W \to W'$ (L1J). Nach Konstruktion $g \circ s = \operatorname{id}_W$.

„(2) $\Rightarrow$ (1)“: Die Komposition $p = s \circ g : V \to V$ ist idempotent, denn es gilt $p^2 = (s \circ g) \circ (s \circ g) = s \circ (g \circ s) \circ g = s \circ g = p$. Dank L30 erhalten wir $V = \operatorname{Ker} p \oplus \operatorname{Im} p$ mit $\operatorname{Ker} p = \operatorname{Ker} g = \operatorname{Im} f = U'$ und $\operatorname{Im} p = \operatorname{Im} s =: W'$.

Exakte Sequenzen und Spaltung zur direkten Summe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L3Q: exakte Sequenz

Jede Zerlegung $I = K \sqcup J$ definiert eine exakte Sequenz:

$$0 \xrightarrow{0} R^K \xhookrightarrow[u \mapsto u \sqcup 0_J]{\mathrm{inc}_K} R^I \xrightarrow[v \mapsto v|_J]{\mathrm{res}_J} R^J \xrightarrow{0} 0$$

Diese spaltet und beweist so $R^I = \mathrm{inc}_K(R^K) \oplus \mathrm{inc}_J(R^J)$:

$$0 \longrightarrow R^K \underset{\mathrm{res}_K}{\overset{\mathrm{inc}_K}{\rightleftarrows}} R^I \underset{\mathrm{inc}_J}{\overset{\mathrm{res}_J}{\rightleftarrows}} R^J \xrightarrow{0} 0$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel L

Bonusmaterial

There is a substantial body of linear algebra which can be formalized systematically, and constitutes what Steenrod called abstract nonsense, but which provides a well-oiled machinery applicable to many domains.

Serge Lang (1927–2005), *Algebra* (2002)

The introduction of the cipher 0 or the group concept was general nonsense, too, and for a thousand years or two mathematics was more or less stagnating, because nobody was around to make such childish steps.

Alexander Grothendieck (1928–2014)

Inhalt dieses Kapitels L

5 Das Fünferlemma – mit großem Halali!

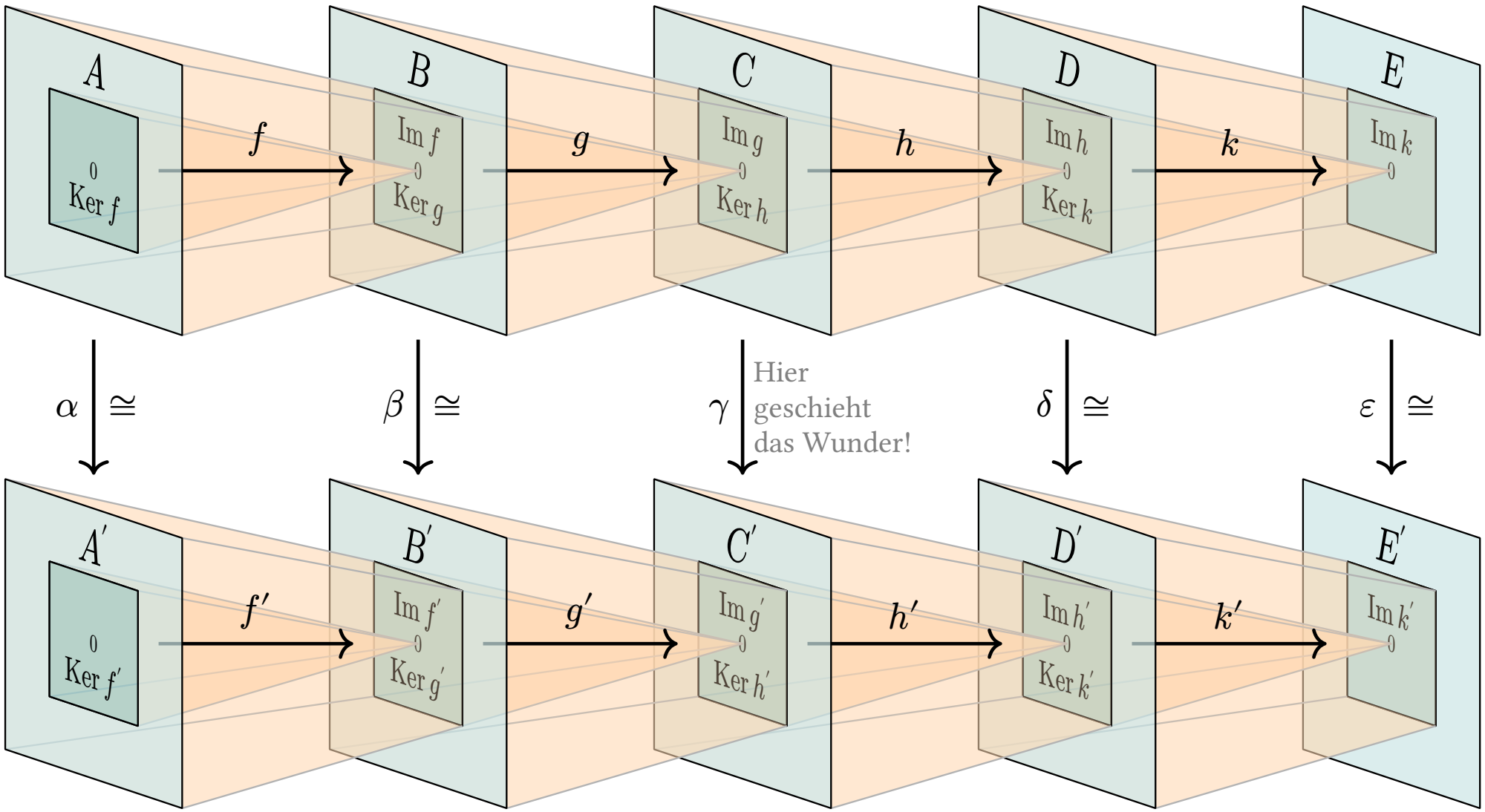
6 Treppenfunktionen und ihr Integral

7 Der chinesische Restsatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Das Fünferlemma – als Kunstwerk



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Das Fünferlemma

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz L5A: Fünferlemma

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"'] \arrow[dr, phantom, "①"] & B \arrow[r, "g"] \arrow[d, "\beta"'] \arrow[dr, phantom, "②"] & C \arrow[r, "h"] \arrow[d, "\gamma"'] \arrow[dr, phantom, "③"] & D \arrow[r, "k"] \arrow[d, "\delta"'] \arrow[dr, phantom, "④"] & E \arrow[d, "\varepsilon"'] \\
A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D' \arrow[r, "k'"] & E'
\end{tikzcd}$$

Gegeben sei das obige kommutative Diagramm mit exakten Zeilen (f, g, h, k) und (f', g', h', k'). Sind $\alpha, \beta, \delta, \varepsilon$ Isomorphismen, so auch γ.

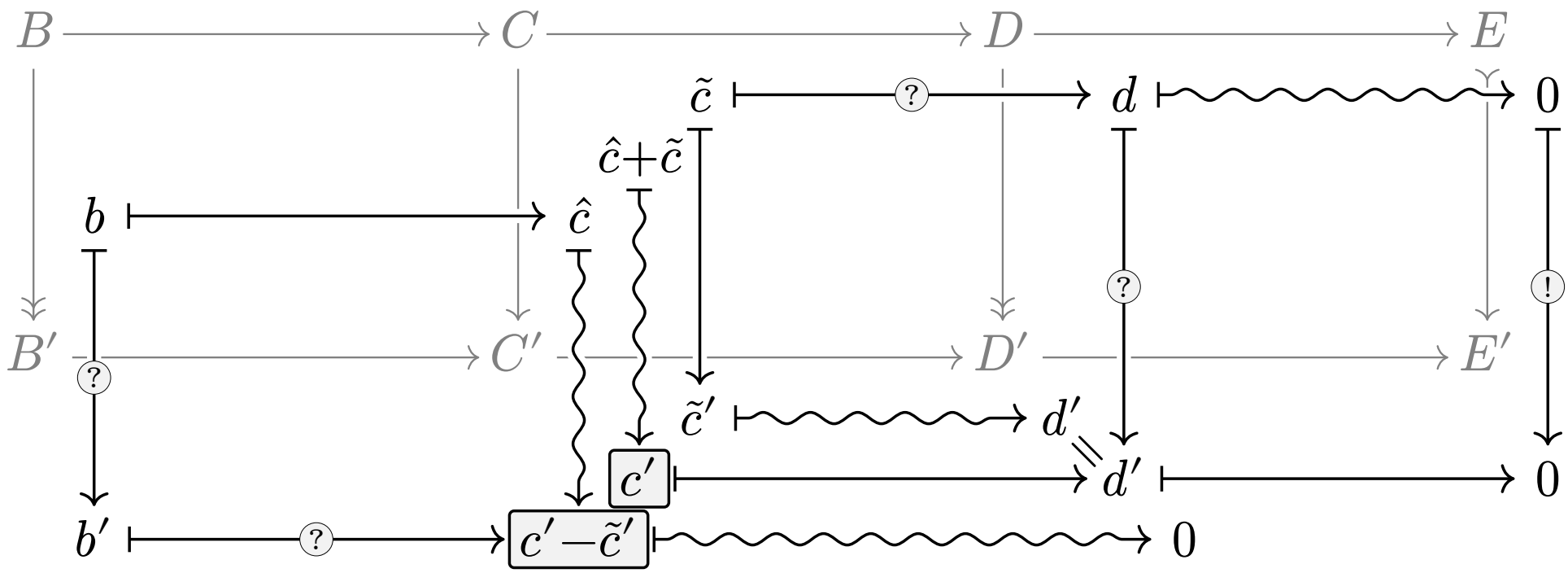
Diagrammjagd als graphische Kunst – ohne Worte

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{tikzcd}
A \arrow[rr] \arrow[dd, two heads] & & B \arrow[rr] & & C \arrow[rr] & & D \arrow[dd, two heads] & \\
& a \arrow[rr, mapsto, squiggly] \arrow[dd, mapsto, "?"] & & b \arrow[rr, mapsto, "?"] \arrow[dd, mapsto] & & c \arrow[rr, mapsto, squiggly] \arrow[dd, mapsto, "?"] & & 0 \arrow[dd, mapsto, "!"] \\
A' \arrow[rr] & & B' \arrow[rr] & & C' \arrow[rr] & & D' & \\
& a' \arrow[rr, mapsto, "?"] & & b' \arrow[rr, mapsto, squiggly] & & \boxed{0} \arrow[rr, mapsto] & & 0
\end{tikzcd}
$$

Diagrammjagd als graphische Kunst – ohne Worte



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel M

Basis und Dimension

$$\begin{tikzcd} & V \arrow[dl, "\Phi_{\mathcal{A}}"'] \arrow[dr, "\Phi_{\mathcal{B}}"] & \\ R^p \arrow[rr, shift left, "\cong"] & & R^q \arrow[ll, shift left] \end{tikzcd}$$

Good general theory does not
search for the maximum generality,
but for the right generality.

Saunders Mac Lane (1909–2005)

Inhalt dieses Kapitels M

Dies ist nur die Saalversion ohne Erläuterungen.

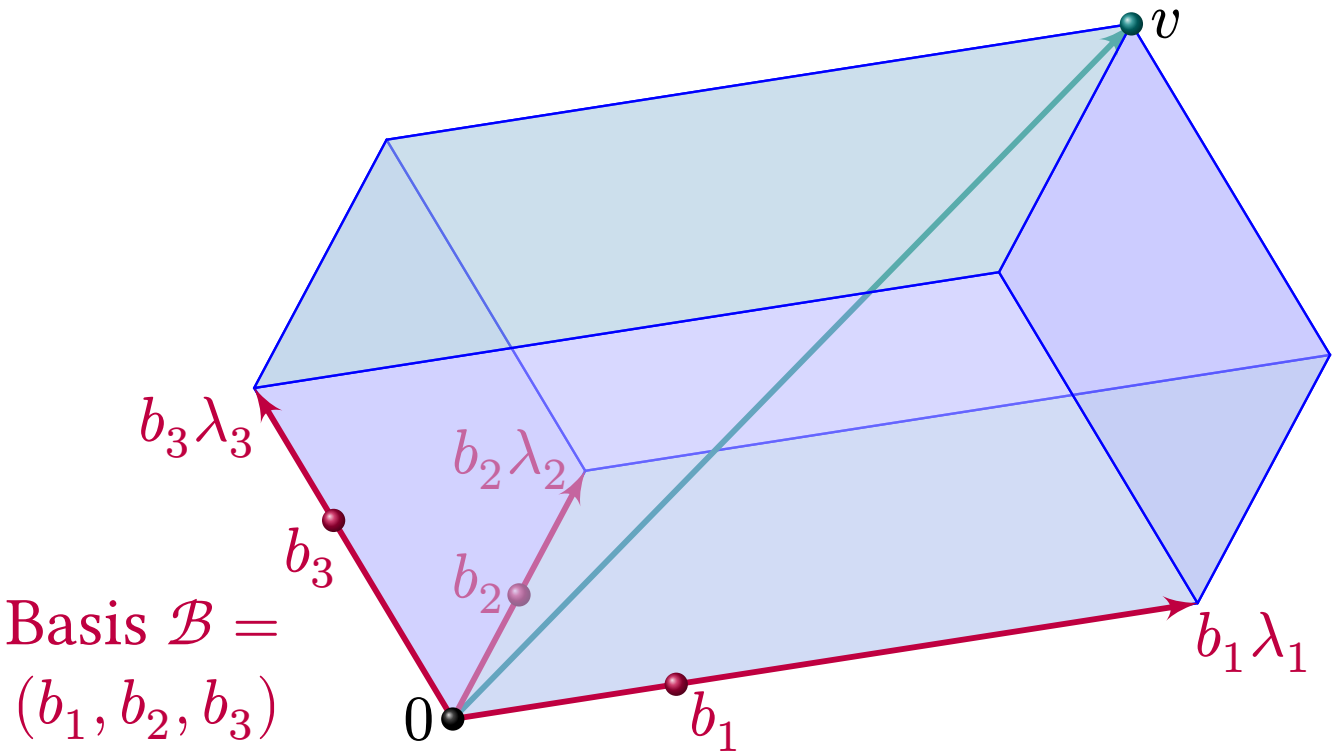
Ausführliche Erläuterungen bietet die Vollversion.

1. Basis: erzeugend und frei!
2. Dimension: Freiheit für alle Vektorräume!
3. Gauß–Algorithmus und Matrixdualität

Basis und Dimension

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Wann ist $\mathcal{B} = (b_i)_{i\in I}$ eine Basis des Raums V? Jeder beliebige Vektor $v \in V$ schreibt sich eindeutig als Linearkombination $v = \sum_{i\in I} b_i\lambda_i$ mit $\lambda \in \mathbb{R}^{(I)}$.

Basis: erzeugend und frei!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition M1A: Basis: erzeugend und frei!

Sei $(V, +, \cdot)$ ein rechtslinearer Raum über dem Ring $(R, +, \cdot)$.
Jede Familie $\mathcal{B} = (b_i)_{i \in I}$ in V definiert ein lineares Koordinatensystem

$$\Phi_{\mathcal{B}} \;:\; R^{(I)} \to V \;:\; \lambda = (\lambda_i)_{i \in I} \;\mapsto\; v = \textstyle\sum_{i \in I} b_i \lambda_i .$$

Wir nennen die Familie $\mathcal{B}$
(1) eine **Basis** des linearen Raums V über R, falls $\Phi_{\mathcal{B}}$ bijektiv ist,
(2) eine **erzeugende Familie** von V über R, falls $\Phi_{\mathcal{B}}$ surjektiv ist,
(3) und **linear unabhängig** / **frei** in V über R, falls $\Phi_{\mathcal{B}}$ injektiv ist.

Der lineare Raum V über R heißt **frei**, falls eine Basis $\mathcal{B}$ in V existiert.

Erzeugende Familien von V über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Speziell für $I = \{1, \dots, n\}$ haben wir $\mathcal{B} = (b_1, \dots, b_n)$ in V und somit $\Phi_{\mathcal{B}} : R^n \to V : \lambda = (\lambda_1, \dots, \lambda_n) \mapsto v = b_1\lambda_1 + \cdots + b_n\lambda_n$.

Das Bild von $\Phi_{\mathcal{B}}$ ist der von $\mathcal{B}$ in V **erzeugte Unterraum** (L2G):

$$\operatorname{Im}(\Phi_{\mathcal{B}}) = \left\{ \sum_{i \in I} b_i \lambda_i \,\middle|\, \lambda \in R^{(I)} \right\} = \langle b_i \mid i \in I \rangle_R = \langle \mathcal{B} \rangle_R$$

Äquivalent sind:

1. Die Abbildung $\Phi_{\mathcal{B}} : R^{(I)} \to V$ ist surjektiv.
2. Die Familie $\mathcal{B}$ erzeugt den ganzen Raum V über R, kurz $\langle \mathcal{B} \rangle_R = V$.
3. Jeder Vektor $v \in V$ erlaubt **mindestens** eine Linearkombination von $\mathcal{B}$.

Linear unabhängige Familien in V über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Der Kern der Abbildung $\Phi_{\mathcal{B}} : R^{(I)} \to V$ ist der Unterraum der Relationen:

$$\operatorname{Ker}(\Phi_{\mathcal{B}}) = \left\{ \lambda \in R^{(I)} \,\middle|\, \sum_{i \in I} b_i \lambda_i = 0 \right\}.$$

Äquivalent sind:

1. Die Abbildung $\Phi_{\mathcal{B}} : R^{(I)} \to V$ ist injektiv.
2. Die Familie $\mathcal{B}$ ist linear unabhängig in V über R.
3. Jeder Vektor $v \in V$ erlaubt **höchstens** eine Linearkombination von $\mathcal{B}$. Koeffizientenvergleich: Aus $v = \sum_{i \in I} b_i \lambda_i = \sum_{i \in I} b_i \mu_i$ folgt $\lambda = \mu$.
4. Es gilt $\operatorname{Ker}(\Phi_{\mathcal{B}}) = \{0\}$.
5. LGS: Der Nullvektor $0 \in V$ schreibt sich nur auf eine **einzige** Weise als R–Linearkombination: Aus $\lambda \in R^{(I)}$ und $0 = \sum_{i \in I} b_i \lambda_i$ folgt $\lambda = 0$.

Basen eines linearen Raumes V über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Äquivalent sind:

1. Die Abbildung $\Phi_{\mathcal{B}} : R^{(I)} \to V$ ist bijektiv.
2. Die Familie $\mathcal{B}$ ist eine Basis des Raums V über R.
3. Es gilt $\mathrm{Ker}(\Phi_{\mathcal{B}}) = \{0\}$ und $\mathrm{Im}(\Phi_{\mathcal{B}}) = V$.
4. Die Familie $\mathcal{B}$ ist linear unabhängig und erzeugt V über R.
5. Jeder Vektor $v \in V$ schreibt sich auf **genau** eine Weise als R–Linearkombination $v = \sum_{i \in I} b_i \lambda_i$ mit $\lambda \in R^{(I)}$.

Als bequeme Abkürzung schreiben wir hierfür:

$$\boxed{V = \langle \mathcal{B} \rangle_R^!}$$

Erste Beispiele: der Koordinatenraum $R^{(I)}$ über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M1B: der Koordinatenraum $R^{(I)}$ über R — Satz L2D

Sei R ein Ring und I eine Menge. Dies definiert den **Koordinatenraum**

$$R^{(I)} = \{\, \lambda : I \to R \,|\, \sharp\,\mathrm{supp}(\lambda) < \infty \,\} \leq R^I.$$

Der Raum $R^{(I)}$ über R ist frei dank der **Standardbasis** $\mathcal{E} = (e_i)_{i \in I}$, mit

$$e_i : I \to R : j \mapsto e_i(j) = \delta_{ij} := \begin{cases} 1 & \text{falls } j = i, \\ 0 & \text{falls } j \neq i. \end{cases}$$

Jeder Vektor $\lambda \in R^{(I)}$ schreibt sich eindeutig als Linearkombination

$$\lambda = \textstyle\sum_{i \in I} e_i \lambda_i.$$

Erste Beispiele: die Räume $\{0\}$ und R über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Der Nullraum $\{0\}$ ist frei über R mit leerer Basis $\mathcal{B} = ()$.

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:

$$\Phi_b : R \xrightarrow{\sim} R : \lambda \mapsto b\lambda \text{ bijektiv} \quad \Longleftrightarrow \quad b \in R^\times \text{ invertierbar}$$

Erste Beispiele: die Räume $\mathbb{Z}$ und $\mathbb{Z}/n$ und $\mathbb{Q}$ über $\mathbb{Z}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Der $\mathbb{Z}$–lineare Raum $\mathbb{Z}$ ist frei; mögliche Basen sind 1 und -1.

Beispiel M1D: die Räume $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Q}$ über $\mathbb{Z}$

(1) Über $\mathbb{Z}$ ist $\mathbb{Z}/n\mathbb{Z}$ nicht frei für $n \in \mathbb{N}_{\geq 2}$.
(2) Über $\mathbb{Z}$ ist $\mathbb{Q}$ nicht frei.

Beweis: (1) Wir zeigen $(\mathbb{Z}/n\mathbb{Z}, +) \not\cong (\mathbb{Z}^{(I)}, +)$ für jede Menge I.
Jedes $v \neq 0$ in $\mathbb{Z}^{(I)}$ hat Ordnung ∞, nicht jedoch $[1]$ in $\mathbb{Z}/n\mathbb{Z}$.

(2) Wir zeigen $(\mathbb{Q}, +) \not\cong (\mathbb{Z}^{(I)}, +)$. Zunächst gilt $\mathbb{Q} \not\cong \{0\} = \mathbb{Z}^{\emptyset}$.
Jedes Element a in $\mathbb{Q}$ ist durch 2 teilbar, nicht jedoch e_i in $\mathbb{Z}^{(I)}$. $\boxed{\text{QED}}$

Erste Beispiele: der Raum $\mathbb{C}^n$ über $\mathbb{C}$ und über $\mathbb{R}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Der lineare Raum $\mathbb{C}^1$ über $\mathbb{C}$ ist frei, die Standardbasis ist 1.
Ebenso ist der Raum $\mathbb{C}^1$ frei über $\mathbb{R} < \mathbb{C}$, die Standardbasis ist $(1, \mathrm{i})$:

$$z = 1x + \mathrm{i}y \quad \text{mit} \quad (x, y) \in \mathbb{R}^2.$$

Beispiel M1F: 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 $\mathbb{R}$.

Erste Beispiele: der Polynomring $\mathbb{K}[X]$ über $\mathbb{K}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Der Polynomring $\mathbb{K}[X]$ über $\mathbb{K}$ hat die **Monombasis** $(X^n)_{n\in\mathbb{N}}$.
Im Falle $\mathbb{Q} \leq \mathbb{K}$ hat $\mathbb{K}[X]$ zudem die **faktorielle Basis** $(X^n/n!)_{n\in\mathbb{N}}$.

Beispiel M1G: gestufte Polynombasis

Sei $(P_n)_{n\in\mathbb{N}}$ eine Familie von Polynomen $P_n \in \mathbb{K}[X]_n^\times$.
Dann ist $(P_n)_{n\in\mathbb{N}}$ eine Basis von $\mathbb{K}[X]$ über $\mathbb{K}$.

Lineare Un/Abhängigkeit von Funktionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M1ı: Monomfunktionen

Sei $(p_n)_{n\in\mathbb{N}}$ die Familie der Monomfunktionen $p_n : \mathbb{R} \to \mathbb{R} : x \mapsto x^n$.
Ist sie im Vektorraum $\mathscr{C}^\infty(\mathbb{R},\mathbb{R}) \leq \mathrm{Fun}(\mathbb{R},\mathbb{R})$ über $\mathbb{R}$ linear unabhängig?

Beweis: Wir betrachten $a_0, \dots, a_n \in \mathbb{R}$ und $f = a_0 p_0 + \dots + a_n p_n$, also

$$f(x) = a_0 + a_1 x + \dots + a_k x^k + \cdots + a_n x^n.$$

$$\Downarrow$$

$$(\partial^k f)(x) = k!\, a_k + x\, r_k(x)$$

$$\Downarrow$$

$$a_k = (\partial^k f)(0)/k!$$

Aus $f = 0$ folgt $a_k = 0$ für alle k. Also ist $(p_n)_{n\in\mathbb{N}}$ linear unabhängig. $\boxed{\text{QED}}$

Lineare Un/Abhängigkeit von Funktionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M1J: Exponentialfunktionen

Sei $(e_\lambda)_{\lambda\in\mathbb{R}}$ die Familie der Exponentialfunktionen $e_\lambda : \mathbb{R} \to \mathbb{R} : t \mapsto \mathrm{e}^{\lambda t}$. Ist sie im Vektorraum $\mathscr{C}^\infty(\mathbb{R},\mathbb{R}) \leq \mathrm{Fun}(\mathbb{R},\mathbb{R})$ über $\mathbb{R}$ linear unabhängig?

Beweis: Zu $\lambda_1 < \ldots < \lambda_n$ und $a_1, \ldots, a_n \neq 0$ in $\mathbb{R}$ erhalten wir:

$$\begin{aligned} f &= \textstyle\sum_{k=1}^n a_k e_{\lambda_k} : \mathbb{R} \to \mathbb{R} \\ f(t)\,\mathrm{e}^{-\lambda_n t} &= \textstyle\sum_{k=1}^{n-1} a_k\,\mathrm{e}^{(\lambda_k-\lambda_n)t} + a_n \\ f(t)\,\mathrm{e}^{-\lambda_n t} &\to a_n \quad \text{für } t \to \infty, \text{ also } f \neq 0. \end{aligned}$$

Lineare Un/Abhängigkeit in $\mathbb{R}$ über $\mathbb{Q}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M1L: eine $\mathbb{Q}$–linear unabhängige Familie in $\mathbb{R}$

Sei $\mathbb{P} = \{2, 3, 5, 7, \dots\}$ die Menge aller Primzahlen in $(\mathbb{N}, \cdot, 1)$.
Ist die Familie $\mathcal{B} = (\ln p)_{p \in \mathbb{P}}$ in $\mathbb{R}$ über $\mathbb{Q}$ linear unabhängig?

Beweis: Angenommen, es besteht eine $\mathbb{Q}$–lineare Relation:

$$\frac{a_1}{b_1} \ln p_1 + \dots + \frac{a_n}{b_n} \ln p_n = 0$$

mit $p_1 < \dots < p_n$ in $\mathbb{P}$ sowie $a_i \in \mathbb{Z}$ und $b_i \in \mathbb{Z}_{>0}$. Wir multiplizieren mit $b = \mathrm{kgV}(b_1, \dots, b_n) \in \mathbb{Z}_{>0}$ und erhalten Koeffizienten $c_i = a_i b / b_i \in \mathbb{Z}$:

$$c_1 \ln p_1 + \dots + c_n \ln p_n = 0$$

Wir nutzen den Gruppenisomorphismus $(\exp, \ln) : (\mathbb{R}, +, 0) \cong (\mathbb{R}_{>0}, \cdot, 1)$:

$$p_1^{c_1} \cdots p_n^{c_n} = 1$$

Dank Fundamentalsatz der Arithmetik B3J folgt $c_1 = \dots = c_n = 0$.

Lineare Un/Abhängigkeit in $\mathbb{R}$ über $\mathbb{Q}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vorgelegt sei $\alpha \in \mathbb{R}$. Erfüllen die Potenzen α^n eine $\mathbb{Q}$–lineare Relation?

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n \overset{?}{=} 0 \quad \text{mit} \quad (a_0, a_1, \dots, a_n) \neq 0$$

Satz M1M: Die eulersche Zahl e ist transzendent. (Hermite 1873)

Die Potenzen $(\mathrm{e}^n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ sind linear unabhängig über $\mathbb{Q}$.

Satz M1N: Die Kreiszahl π ist transzendent. (Lindemann 1882)

Die Potenzen $(\pi^n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ sind linear unabhängig über $\mathbb{Q}$.
Die Quadratur des Kreises mit Zirkel und Lineal ist unmöglich.

Teilfamilien und Oberfamilien

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Bemerkung M1Q: Ober- und Teilfamilien

$$\begin{tikzcd} R^{(K)} \arrow[rr, hook, "\mathrm{inc}", "\lambda \mapsto \lambda \sqcup 0"'] \arrow[dr, "\Phi_{\mathcal{A}}"'] & & R^{(I)} \arrow[dl, "\Phi_{\mathcal{B}}"] \\ & V & \end{tikzcd}$$

Gegeben sei ein linearer Raum V über R,
eine Familie $\mathcal{B} = (v_i)_{i \in I}$ von Vektoren $v_i \in V$
und $\mathcal{A} = (v_i)_{i \in K}$ mit $K \subsetneq I$ eine echte Teilfamilie.

1. Ist $\mathcal{A}$ erzeugend für V, so auch $\mathcal{B}$.
2. Ist $\mathcal{B}$ frei in V, so auch $\mathcal{A}$.

Familien unter linearen Abbildungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Bemerkung M1R: Familie unter linearer Abbildung

$$\begin{tikzcd} & R^{(I)} \arrow[dl, "\Phi_{\mathcal{A}}"'] \arrow[dr, "\Phi_{\mathcal{B}}"] & \\ V \arrow[rr, "f"] & & W \end{tikzcd}$$

Gegeben sei eine R–lineare Abbildung $f : V \to W$,
eine Familie $\mathcal{A} = (v_i)_{i \in I}$ von Vektoren $v_i \in V$
und die Bildfamilie $\mathcal{B} = (w_i = f(v_i))_{i \in I}$.

1. Ist f surjektiv und $\mathcal{A}$ erzeugt V, dann erzeugt $\mathcal{B}$ ganz W.
2. Ist f injektiv und $\mathcal{A}$ in V frei, dann ist auch $\mathcal{B}$ in W frei.
3. Ist f bijektiv und $\mathcal{A}$ eine Basis von V, so ist $\mathcal{B}$ eine Basis von W.

Basen des linearen Raums R^n über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Bemerkung M1s: Gauß für Vektoren im Raum R^n

Jede Familie $\mathcal{B} = (b_1, \dots, b_k)$ von Spaltenvektoren $b_1, \dots, b_k \in R^n$ können wir zur Matrix $B = (b_1, \dots, b_k) \in R^{n \times k}$ zusammensetzen:

$$B = \begin{bmatrix} | & & | \\ b_1 & \cdots & b_k \\ | & & | \end{bmatrix}, \quad \Phi_{\mathcal{B}} : R^k \to R^n : \lambda \mapsto b_1\lambda_1 + \cdots + b_k\lambda_k = B\lambda$$

(1) Damit können wir **Kern** und **Bild** von $\Phi_{\mathcal{B}}$ berechnen:

$$\begin{aligned} \operatorname{Ker}(\Phi_{\mathcal{B}}) = \operatorname{Ker}(B) &:= \{\, \lambda \in R^k \mid B\lambda = 0 \,\} &\leq R^k, \\ \operatorname{Im}(\Phi_{\mathcal{B}}) = \operatorname{Im}(B) &:= \{\, B\lambda \in R^n \mid \lambda \in R^k \,\} &\leq R^n. \end{aligned}$$

(2) Genau dann ist $\mathcal{B}$ eine **Basis**, wenn B **invertierbar** ist:

$$\text{Löse } B\lambda = v \text{ eindeutig durch } \lambda = B^{-1}v!$$

Die Standardbasis des linearen Raums R^n über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M1T: die Standardbasis von R^n über R

Der R–lineare Raum R^n ist frei, seine **Standardbasis** ist

$$\mathcal{E}: \quad e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \ldots, \quad e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

Gestufte Basen des linearen Raums R^n über R

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M1T: eine gestufte Basis von R^n über R

Eine **gestufte Basis** des Raums R^n über R ist von der Form

$$\mathcal{B}: \quad b_1 = \begin{bmatrix} \blacksquare \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} * \\ \blacksquare \\ \vdots \\ 0 \end{bmatrix}, \quad \ldots, \quad b_n = \begin{bmatrix} * \\ * \\ \vdots \\ \blacksquare \end{bmatrix}.$$

Bild und Kern einer Matrix in reduzierter Zeilenstufenform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\left[\begin{array}{ccccc|c|c} 1 & -2 & 0 & 3 & 0 & -1 & 0 \\ 0 & 0 & 1 & 7 & 0 & 4 & 5 \\ 0 & 0 & 0 & 0 & 1 & 9 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{array}\right] \xrightarrow[\text{Merkregel D223}]{\text{graphische}} \begin{array}{c} \left[\begin{array}{cccccc} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 9 \end{array}\right] \\ \begin{array}{cccccc} & v_2 & & v_4 & & w \end{array} \end{array}$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{A} \quad b \quad b'$$

Aufgabe: Gegeben ist $A \in \mathbb{R}^{4\times 5}$ in reduzierter Zeilenstufenform.
(1) Explizieren Sie Basen für das Bild $\operatorname{Im}(A)$ und den Kern $\operatorname{Ker}(A)$.
(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:

$$\operatorname{Im}(A) = \langle e_1, e_2, e_3 \rangle_{\mathbb{R}}^{!} \leq \mathbb{R}^4 \quad \text{und} \quad \operatorname{Ker}(A) = \langle v_2, v_4 \rangle_{\mathbb{R}}^{!} \leq \mathbb{R}^5$$

(2) Es gilt $b = Aw \in \operatorname{Im}(A)$, also $L(A,b) = w + \operatorname{Ker}(A) = w + v_2\mathbb{R} + v_4\mathbb{R}$.

Bild und Kern einer Matrix in reduzierter Zeilenstufenform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{array}{cc}
 & \begin{array}{cccccccccc} s = (& 2, & 3, & & 5, & & & 8 & &) \end{array} \\
A = & \begin{bmatrix}
0 & 1 & 0 & * & 0 & * & * & 0 & * & * \\
0 & 0 & 1 & * & 0 & * & * & 0 & * & * \\
0 & 0 & 0 & 0 & 1 & * & * & 0 & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\end{array}
$$

Aufgabe: Gegeben sei $A \in R^{m \times n}$ in reduzierter Zeilenstufenform mit Stufen $J = \{ s_1 < \ldots < s_r \}$. Explizieren Sie eine Basis für Bild und Kern.

Lösung: (1) Die Pivotspalten J sind eine Basis des Bildraums:

$$\mathrm{Im}(A) \;=\; \langle Ae_j \,|\, j \in J \rangle_R^! \overset{\text{RZSF}}{=} \langle e_1, \ldots, e_r \rangle_R^! \;\leq\; R^m$$

(2) Die freien Spalten $K = \{1, \ldots, n\} \setminus J$ definieren eine Basis des Kerns:

$$\mathrm{Ker}(A) \;=\; \langle v_k := \textstyle\sum_{i=1}^r e_{s_i} a_{ik} - e_k \,|\, k \in K \rangle_R^! \;\leq\; R^n$$

Bild und Kern einer Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Algo M1v: Bild und Kern einer Matrix

Eingabe: $B \in R^{m \times n}$ über dem Divisionsring R
Ausgabe: Basen für $\operatorname{Im}(B) \leq R^m$ und $\operatorname{Ker}(B) \leq R^n$

Satz M1v: Bild und Kern einer Matrix

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 $J = \{ s_1 < \ldots < s_r \}$.

(1) Die Pivotspalten J sind eine Basis des Bildraums:

$$\begin{aligned} \operatorname{Im}(A) &= \langle Ae_j \mid j \in J \rangle_R^! \overset{\text{RZSF}}{=} \langle e_1, \ldots, e_r \rangle_R^! && \leq R^m \\ \operatorname{Im}(B) &= \langle Be_j \mid j \in J \rangle_R^! = \langle S^{-1}e_1, \ldots, S^{-1}e_r \rangle_R^! && \leq R^m \end{aligned}$$

(2) Die freien Spalten $K = \{1, \ldots, n\} \setminus J$ definieren eine Basis des Kerns:

$$\operatorname{Ker}(A) = \operatorname{Ker}(B) = \langle v_k := \textstyle\sum_{i=1}^r e_{s_i} a_{ik} - e_k \mid k \in K \rangle_R^! \leq R^n$$

Anwendungsbeispiel zur linearen Un/Abhängigkeit

Ausprobieren mit Gaël!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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 die Familie $\mathcal{B}$ linear unabhängig?
(2) Welche Teilfamilien sind linear unabhängig?

Lösung: Wir lösen $B\lambda = 0$ mit dem Gauß–Algorithmus (D2H/D2F):

$$B = \begin{bmatrix} 1 & 1 & 3 \\ 1 & 2 & 4 \\ 2 & 3 & 7 \end{bmatrix} \quad \xrightarrow[SB=B']{\text{RZSF}} \quad B' = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \lambda = \begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}.$$

(1) Die Familie (b_1, b_2, b_3) ist linear abhängig, da $b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3 = 0$.

(2) Die Familien (b_1, b_2) und (b_1, b_3) und (b_2, b_3) sind linear unabhängig, zudem alle Teilfamilien, (b_1) und (b_2) und (b_3) sowie $()$.

Anwendungsbeispiel zu erzeugenden Familien

Ausprobieren mit Gaël!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: In $\mathbb{R}^3$ über $\mathbb{R}$ betrachten wir die Familie

$$\mathcal{B}: \quad b_1 = \begin{bmatrix} 5 \\ 1 \\ 4 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \quad b_3 = \begin{bmatrix} 9 \\ 3 \\ 8 \end{bmatrix}, \quad b_4 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \quad b_5 = \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix}.$$

Welche Teilfamilien von $\mathcal{B}$ erzeugen $\mathbb{R}^3$? welche sind frei? welche Basen?

Lösung: Wir lösen $B\lambda = v$ mit dem Gauß–Algorithmus (D2H/D2F):

$$\left[\begin{array}{ccccc|ccc} 5 & 2 & 9 & 1 & 3 & 1 & 0 & 0 \\ 1 & 1 & 3 & 0 & 1 & 0 & 1 & 0 \\ 4 & 2 & 8 & 1 & 3 & 0 & 0 & 1 \end{array}\right] \xrightarrow[\text{Gauß}]{\text{RZSF}} \left[\begin{array}{ccccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 2 & 0 & 1 & -1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & -2 & -2 & 3 \end{array}\right]$$

Minimale erzeugende Familien / maximale unabhängige Familien / Basen:

$\{\mathbf{1}, \mathbf{2}, \mathbf{4}\}$, $\{1, 3, 4\}$, $\{2, 3, 4\}$, $\{1, 2, 5\}$, $\{1, 3, 5\}$, $\{2, 3, 5\}$, $\{1, 4, 5\}$, $\{3, 4, 5\}$

Zusammenfügen von Basen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$F = \begin{bmatrix} 5 & 2 & 9 & 1 & 3 \\ 1 & 1 & 3 & 0 & 1 \\ 4 & 2 & 8 & 1 & 3 \end{bmatrix} \xrightarrow[\text{Gauß M167}]{\text{RZSF}} \cdots \xrightarrow[\text{Merkregel D223}]{\text{graphische}} \begin{array}{c} \left[\begin{array}{ccccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 2 & 0 & 1 & -1 & 1 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & -2 & -2 & 3 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{array}\right] \\ \begin{array}{ccccccccc} & & v_4 & & v_5 & v_1 & v_2 & v_3 \end{array} \end{array}$$

$$\Longrightarrow \quad G = (v_4, v_5) \in \mathbb{R}^{5\times 2}$$

Wie berechnet gilt $\mathrm{Im}(F) = \mathbb{R}^3$ und $\mathrm{Ker}(F) = \mathrm{Im}(G)$ und $\mathrm{Ker}(G) = \{0\}$.

$$0 \xrightarrow{\;0\;} \mathbb{R}^2 \xrightarrow{\;G\;} \mathbb{R}^5 \xrightarrow{\;F\;} \mathbb{R}^3 \xrightarrow{\;0\;} 0$$

$$v_1, v_2, v_3 \longmapsto e_1, e_2, e_3$$

$$e_1, e_2 \longmapsto v_4, v_5$$

Ist die fusionierte Familie $(v_1, v_2, v_3, v_4, v_5)$ in $\mathbb{R}^5$ ebenfalls eine Basis?

Zusammenfügen von Basen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $(0, g, f, 0)$ eine exakte Sequenz über dem Ring R:

$$\begin{tikzcd}
0 \arrow[r, "0"] & U \arrow[r, "g"] & V \arrow[r, "f"] & W \arrow[r, "0"] & 0 \\
 & (k \in K) & v_j \arrow[r, mapsto] & w_j & \\
 & u_k \arrow[r, mapsto] & v_k & (j \in J) &
\end{tikzcd}$$

Zur Menge $I = J \sqcup K$ seien drei Familien gegeben: $\mathcal{V} = (v_i)_{i \in I}$ in V sowie $\mathcal{W} = (w_j)_{j \in J}$ in W mit $f(v_j) = w_j$ und $\mathcal{U} = (u_k)_{k \in K}$ in U mit $g(u_k) = v_k$.

Satz M1x: freie exakte Sequenz

Sind zwei der drei Familien $\mathcal{U}, \mathcal{V}, \mathcal{W}$ Basen, so auch die dritte.

Zusammenfügen von Basen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & R^{(K)} \arrow[r, "\mathrm{inc}", "\mu\mapsto\mu\sqcup 0_J"'] \arrow[d, "\Phi_{\mathcal{U}}"] & R^{(K\sqcup J)} \arrow[r, "\mathrm{res}", "\lambda\mapsto\lambda|_J"'] \arrow[d, "\Phi_{\mathcal{V}}"] & R^{(J)} \arrow[r] \arrow[d, "\Phi_{\mathcal{W}}"] & 0 \arrow[r] \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & 0 \arrow[r] & U \arrow[r, "g"] & V \arrow[r, "f"] & W \arrow[r] & 0 \arrow[r] & 0
\end{tikzcd}$$

Beweis: Die Daten stiften ein kommutatives Diagramm exakter Zeilen.

(1) Sind $\Phi_{\mathcal{U}}$ und $\Phi_{\mathcal{W}}$ Isomorphismen, so auch $\Phi_{\mathcal{V}}$.
(2) Sind $\Phi_{\mathcal{U}}$ und $\Phi_{\mathcal{V}}$ Isomorphismen, so auch $\Phi_{\mathcal{W}}$.
(3) Sind $\Phi_{\mathcal{V}}$ und $\Phi_{\mathcal{W}}$ Isomorphismen, so auch $\Phi_{\mathcal{U}}$. $\boxed{\text{QED}}$

Dimension: Was wollen wir?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dem Koordinatenraum R^n über R wollen wir seine **Dimension** zuordnen:

$$\dim_R(R^n) = n$$

Was tun wir mit einem beliebigen R–linearen Raum V? etwa $V \leq R^N$?

1. Wir suchen eine Basis $\mathcal{B} = (b_i)_{i \in I}$ von V über R. ? **Existenz?**

Diese stiftet einen R–linearen Isomorphismus $\Phi_{\mathcal{B}} : R^{(I)} \xrightarrow{\sim} V$.

2. Damit definieren wir $\dim_R(V) := |I|$. ? **Eindeutigkeit?**

Dimension: Was kann schiefgehen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sei R ein beliebiger Ring.
(1) Gibt es R–lineare Räume V ohne jede Basis?
(2) Gibt es Isomorphismen $R^p \cong R^q$ mit $p \neq q$?
(3) Gibt es invertierbare Matrizen $A \in R^{p \times q}$?

Lösung: (1) Ja, klar, über $\mathbb{Z}$ sind $\mathbb{Z}/2$ und $\mathbb{Q}$ nicht frei, siehe M1D.
(2) Ja, klar, für den Nullring $R = \{0\}$ gilt $R^p = \{(0, \dots, 0)\} \cong R^q$.
(3) Ja, klar, über $R = \{0\}$ ist jede Matrix $A \in R^{p \times q}$ invertierbar!

Gruseliges Gegenbeispiel: ein Ring R mit $R^p \cong R^q$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M2A: $R^p \cong R^q$ dank Reißverschluss über $R = \mathrm{End}_K(K[X])$.

Sei K ein Körper, etwa $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \dots$, und hierüber $V = K^{(\mathbb{N})} = K[X]$.

(a) Im Ring $R = (\mathrm{End}_K(V), +, \circ)$ seien $a, b, c, d : V \to V$ gegeben durch

$$a(x) = (x_0, 0, x_1, 0, x_2, 0, \dots), \qquad c(x) = (x_0, x_2, x_4, x_6, x_8, \dots),$$
$$b(x) = (0, x_0, 0, x_1, 0, x_2, \dots), \qquad d(x) = (x_1, x_3, x_5, x_7, x_9, \dots).$$

Reißverschluss:

$$\begin{bmatrix} c \\ d \end{bmatrix} \begin{bmatrix} a & b \end{bmatrix} = \begin{bmatrix} ca & cb \\ da & db \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{und} \quad \begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = ac + bd = 1.$$

(b) Die Matrizen $\left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right]$ und $\left[\begin{smallmatrix} a & b \end{smallmatrix}\right]$ stiften einen Isomorphismus $R^1 \cong R^2$.

(c) Per Induktion folgt $R^1 \cong R^p$ und somit $R^p \cong R^q$ für alle $p, q \in \mathbb{N}_{\geq 1}$.

Invarianz der Basislänge über Divisionsringen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$B = \begin{bmatrix} | & & | \\ b_1 & \cdots & b_k \\ | & & | \end{bmatrix}, \quad \Phi_{\mathcal{B}} : R^k \to R^n : \lambda \mapsto B\lambda = b_1\lambda_1 + \cdots + b_k\lambda_k$$

Gauß–Algorithmus: Ist R ein Divisionsring, so können wir jede Matrix $B \in R^{n\times k}$ mit dem Gauß–Algorithmus D2H in Zeilenstufenform $A = SB$ bringen mit $S \in \mathrm{GL}_n R$ und ihren Rang r ablesen.

1. $\Phi_{\mathcal{B}}$ bijektiv $\iff r = k = n$.
2. $\Phi_{\mathcal{B}}$ surjektiv $\iff r = n \leq k$.
3. $\Phi_{\mathcal{B}}$ injektiv $\iff r = k \leq n$.

Satz M2B: Invarianz der Basislänge

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$.

1. Ist $\mathcal{B} = (b_1, \dots, b_k)$ eine Basis von R^n über R, so gilt $k = n$.
2. Ist $\mathcal{B} = (b_1, \dots, b_k)$ erzeugend für R^n über R, so gilt $k \geq n$.
3. Ist $\mathcal{B} = (b_1, \dots, b_k)$ unabhängig in R^n über R, so gilt $k \leq n$.

Invarianz der Dimension über Divisionsringen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Als Analogie erinnern wir uns an den Zählsatz H1H:

1. Ist $f : \{1, \dots, k\} \xrightarrow{\sim} \{1, \dots, n\}$ bijektiv, so gilt $k = n$.
2. Ist $f : \{1, \dots, k\} \twoheadrightarrow \{1, \dots, n\}$ surjektiv, so gilt $k \geq n$.
3. Ist $f : \{1, \dots, k\} \hookrightarrow \{1, \dots, n\}$ injektiv, so gilt $k \leq n$.

Satz M2c: Invarianz der Dimension

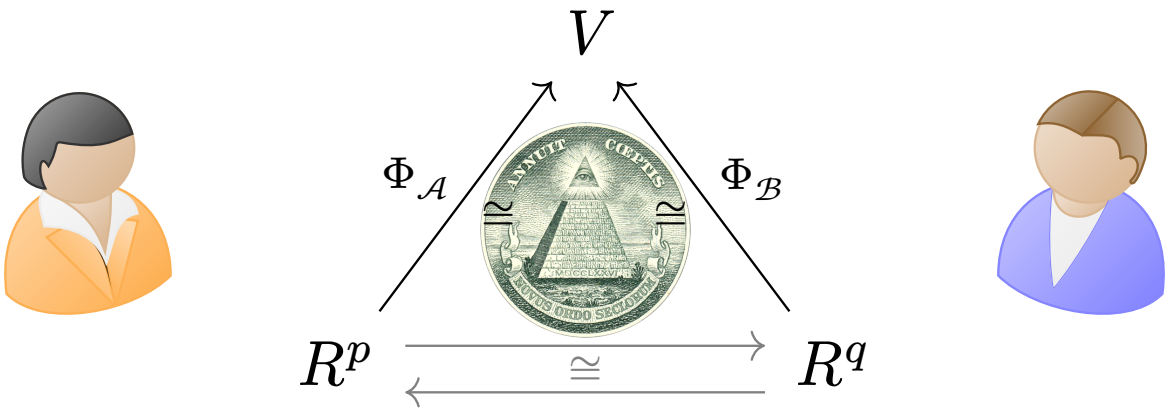
Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$.

1. Ist $f : R^k \xrightarrow{\sim} R^n$ eine R–lineare Bijektion, so gilt $k = n$.
2. Ist $f : R^k \twoheadrightarrow R^n$ eine R–lineare Surjektion, so gilt $k \geq n$.
3. Ist $f : R^k \hookrightarrow R^n$ eine R–lineare Injektion, so gilt $k \leq n$.

Wie definieren wir die „Größe“ eines Raumes V über R?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Definition M2G: Dimension eines linearen Raumes

(1) Ein Ring R erfüllt **Invarianz der Dimension**, falls für alle $p, q \in \mathbb{N}$ gilt: Aus R–linearer Isomorphie $R^p \cong R^q$ folgt die Gleichheit $p = q$.

(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 $|I|$.

In diesem Falle definieren wir die **Dimension** $\dim_R(V) := |I|$.

- ☺ Dies gilt für jeden endlichen Ring $R \neq \{0\}$ dank Zählsatz (H1H),
- ☺ ebenso für jeden Divisionsring dank Gauß–Algorithmus (D2M),
- ☺ zudem für jeden kommutativen Ring dank Determinante (O3A).
- ☹ Über $R = \{0\}$ und $\mathrm{End}_K(K[X])$ gilt $R^p \cong R^q$ für $p, q \in \mathbb{N}_{\geq 1}$ (M2A).

Erste Beispiele zur Dimension

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M2H: erste Beispiele zur Dimension

(1) Sei R ein Körper, DRing oder CRing. Dann gilt

$$\dim_R(R^n) = n.$$

(2) Der Polynomring $R[X]$ ist frei über R, dank Monombasis $(X^n)_{n\in\mathbb{N}}$:

$$\dim_R(R[X]) = |\mathbb{N}|$$

(3) Für den Vektorraum $\mathbb{C}^n$ über $\mathbb{C} > \mathbb{R}$ gilt

$$\dim_{\mathbb{C}}(\mathbb{C}^n) = n \quad \text{und} \quad \dim_{\mathbb{R}}(\mathbb{C}^n) = 2n.$$

Erzeuger auswählen und frei ergänzen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; v_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; v_3 = \begin{bmatrix} 2 \\ 3 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; v_4 = \begin{bmatrix} 5 \\ 2 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \; v_5 = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 0 \\ 0 \end{bmatrix}, \; v_6 = \begin{bmatrix} 7 \\ 4 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; v_7 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Aufgabe: Wählen Sie systematisch eine Basis von $V = \langle v_1, \dots, v_7 \rangle < \mathbb{R}^5$.

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; v_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; \cancel{v_3 = \begin{bmatrix} 2 \\ 3 \\ 0 \\ 0 \\ 0 \end{bmatrix}}, \; v_4 = \begin{bmatrix} 5 \\ 2 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \; \cancel{v_5 = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 0 \\ 0 \end{bmatrix}}, \; \cancel{v_6 = \begin{bmatrix} 7 \\ 4 \\ 0 \\ 0 \\ 0 \end{bmatrix}}, \; v_7 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Erzeuger auswählen und frei ergänzen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma M21: Freistellen und Ergänzen

Sei $(v_j)_{j\in J}$ eine Familie im Vektorraum V über dem Divisionsring R.

0 Sei $\sum_{j\in J} v_j\lambda_j = 0$ mit $\lambda \in R^{(J)}$. Aus $\lambda_k \neq 0$ folgt durch Freistellen $v_k = -\sum_{i\in I} v_i\lambda_i\lambda_k^{-1}$ mit $I = J \smallsetminus \{k\}$, somit $v_k \in \langle v_i \mid i \in I\rangle_R$.

Sei $J = I \sqcup \{k\}$. Die folgenden beiden Aussagen sind äquivalent:

1 Die Teilfamilie $(v_i)_{i\in I}$ ist linear unabhängig und $v_k \notin \langle v_i \mid i \in I\rangle_R$.

2 Die gesamte Familie $(v_j)_{j\in J}$ ist linear unabhängig.

Beweis: „(1) $\Rightarrow$ (2)“: Sei $\sum_{j\in J} v_j\lambda_j = 0$ mit $\lambda \in R^{(J)}$. Dann folgt $\lambda_k = 0$ nach (0) und (1b). Es bleibt $\sum_{i\in I} v_i\lambda_i = 0$, also gilt $\lambda = 0$ nach (1a).

„(1) $\Leftarrow$ (2)“: Ist $(v_j)_{j\in J}$ unabhängig, so auch $(v_i)_{i\in I}$.
Wäre $v_k \in \langle v_i \mid i \in I\rangle_R$, also $v_k = \sum_{i\in I} v_i\lambda_i$ mit $\lambda \in R^{(I)}$, dann gilt die Relation $\sum_{i\in I} v_i\lambda_i - v_k = 0$ für $(v_j)_{j\in J}$ im Widerspruch zu (2). QED

Extremale Charakterisierung von Basen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M2J: extremale Charakterisierung einer Basis

Sei V ein Vektorraum über dem Divisionsring R. Hierin sei $(v_i)_{i\in K}$ ein Erzeugendensystem und $I \subseteq K$ eine Teilmenge. Dann sind äquivalent:

1. Die Familie $\mathcal{B} = (v_i)_{i\in I}$ ist eine Basis von V:
   Sie erzeugt V über R und ist linear unabhängig.
2. Die Familie $\mathcal{B} = (v_i)_{i\in I}$ ist minimal erzeugend: Sie erzeugt V, doch keine echte Teilfamilie $(v_i)_{i\in J}$ mit $J \subsetneq I$ erzeugt V.
3. Die Familie $\mathcal{B} = (v_i)_{i\in I}$ ist maximal unabhängig: Sie ist unabhängig, doch jede echte Oberfamilie $(v_i)_{i\in J}$ mit $I \subsetneq J \subseteq K$ ist abhängig.

Basisauswahl-und-Ergänzungssatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M2κ: Basisauswahl-und-Ergänzungssatz aka Hauptsatz

Sei V ein Vektorraum über dem Divisionsring R.

0 **Basissatz:** Es existiert eine Basis $(v_j)_{j\in J}$ von V über R.

1 **Basisauswahlsatz:** Jedes Erzeugendensystem $(v_k)_{k\in K}$ enthält eine Basis $(v_j)_{j\in J}$ als Teilfamilie mit $J \subseteq K$.

2 **Basisergänzungssatz:** Jede linear unabhängige Familie $(v_i)_{i\in I}$ mit $I \subseteq K$ lässt sich ergänzen zu einer Basis $(v_j)_{j\in J}$ mit $I \subseteq J \subseteq K$.

Basisauswahl-und-Ergänzungssatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Im endlichen Fall sei $I = \{1, \dots, m\} \subseteq \{1, \dots, n\} = K$.
Allgemein sei die Indexmenge $(K, \leq)$ wohlgeordnet und $I < K \smallsetminus I$.

Algo M2L: Basisauswahl-und-Ergänzung über dem Divisionsring R

Eingabe: ein wohlgeordnetes Erzeugendensystem $(v_k)_{k \in K}$ von V über R, angefangen mit $(v_i)_{i \in I}$ linear unabhängig, notfalls $I = \emptyset$

Ausgabe: eine Basis $(v_j)_{j \in J}$ von V über R mit $I \subseteq J \subseteq K$

1: Wähle $J := \{ j \in K \mid v_j \notin \langle v_k \mid k < j \rangle_R \}$

Basisauswahl-und-Ergänzungssatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: (a) Dank Ergänzungslemma M21 gilt $I \subseteq J$.

(b) Lineare Unabhängigkeit: Sei $\sum_{j \in J} v_j \lambda_j = 0$ mit $\lambda \in R^{(J)}$ und $\lambda \neq 0$. Hierzu sei $k = \max \operatorname{supp}(\lambda) \in J$ der maximale Index $k \in J$ mit $\lambda_k \neq 0$. Freistellen M21 ergibt $v_k \in \langle v_i \mid i < k \rangle$, also $k \notin J$, ein Widerspruch.

(c) Gäbe es $k \in K$ mit $v_k \notin \langle v_j \mid j \in J \rangle$, so betrachten wir das minimale. Für alle $i < k$ gilt dann $v_i \in \langle v_j \mid j \in J \rangle$, also $\langle v_i \mid i < k \rangle \leq \langle v_j \mid j \in J \rangle$. Das bedeutet $v_k \notin \langle v_i \mid i < k \rangle$, also $k \in J$, ein Widerspruch.

(d) Erzeugung: Wir haben $V \overset{\text{Vor}}{=} \langle v_k \mid k \in K \rangle \overset{\text{(c)}}{\leq} \langle v_j \mid j \in J \rangle \leq V$. $\boxed{\text{QED}}$

Anwendung: die Dimension von Vektorräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar M2N: Die Dimension ist wohldefiniert.

(1) Jeder Vektorraum V über R erlaubt eine Basis $\mathcal{B} = (b_i)_{i \in I}$ dank M2K.
(2) Jede weitere Basis von V hat selbe Mächtigkeit dank M2C, M2E, M2M.
Damit können wir die **Dimension** von V über R wie erhofft definieren:

$$\boxed{\dim_R(V) := |I|}$$

Basis und Dimension von $\mathbb{R}$ über $\mathbb{Q}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel M2P: Basis von $\mathbb{R}$ über $\mathbb{Q}$, Hamel 1905

Zum Vektorraum $\mathbb{R}$ über $\mathbb{Q}$ existiert eine Basis $\mathcal{B} = (b_i)_{i \in I}$.
Wir erhalten den $\mathbb{Q}$–Isomorphismus $\Phi_{\mathcal{B}} : \mathbb{Q}^{(I)} \xrightarrow{\sim} \mathbb{R}$ und

$$\boxed{\dim_{\mathbb{Q}}(\mathbb{R}) = |\mathbb{R}|.}$$

Basen und Dimension einer direkten Summe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M2τ: Zusammenfügen von Basen in einer direkten Summe

(1) Sei $V = \bigoplus_{k \in K} V_k$ über R. Ist zu jedem $k \in K$ die Familie $(v_i)_{i \in I_k}$ in V_k (a) erzeugend, (b) frei, (c) eine Basis, so auch $(v_i)_{i \in I}$ in V mit $I = \bigsqcup_{k \in K} I_k$.

(2) Die Dimension der direkten Summe ist die Summe der Dimensionen:

$$\boxed{\dim_R(\bigoplus_{k \in K} V_k) = \sum_{k \in K} \dim_R(V_k)}$$

Basen und Dimension für exakte Sequenzen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M2u: kurze exakte Sequenz von Vektorraumhomomorphismen

Sei $(0, g, f, 0)$ eine exakte Sequenz über dem Ring R.

$$\begin{tikzcd}
0 \arrow[r, "0"] & U \arrow[r, "g"] & V \arrow[r, "f"] & W \arrow[r, "0"] & 0 \\
 & u_k \arrow[r, mapsto, "k\in K"] & v_k & & \\
 & & v_j \arrow[r, mapsto, "j\in J"'] & w_j &
\end{tikzcd}$$

(1) Ist R ein Divisionsring, so folgt daraus die **Dimensionsformel**:

$$\boxed{\dim_R(V) = \dim_R(U) + \dim_R(W)}$$

Jede lineare Abbildung $f : V \to W$ definiert ihre kurze exakte Sequenz:

$$0 \xrightarrow{0} \operatorname{Ker}(f) \xhookrightarrow{\text{inc}} V \overset{\hat{f}}{\twoheadrightarrow} \operatorname{Im}(f) \xrightarrow{0} 0$$

(2) Ist R ein Divisionsring, so folgt daraus erneut der **Rangsatz** M1v:

$$\boxed{\dim_R(V) = \dim_R \operatorname{Ker}(f) + \dim_R \operatorname{Im}(f)}$$

Schnitt und Summe von Untervektorräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M2v: Schnitt und Summe von Untervektorräumen

(1) Je zwei Unterräume $V_1, V_2 \leq W$ definieren eine exakte Sequenz:

$$V_1 \cap V_2 \xhookrightarrow[u \mapsto (u,-u)]{g} V_1 \oplus V_2 \xrightarrow[(v_1,v_2) \mapsto v_1+v_2]{f} V_1 + V_2$$

(2) Ist R ein Divisionsring, so folgt daraus die **Dimensionsformel**:

$$\boxed{\dim(V_1 + V_2) + \dim(V_1 \cap V_2) = \dim V_1 + \dim V_2}$$

Analogie beim Zählen: $|X \cup Y| + |X \cap Y| = |X| + |Y|$.

Schnitt und Summe von Untervektorräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M2v: Schnitt und Summe von Untervektorräumen

Wann ist die Summe $V = V_1 + \ldots + V_n$ von Unterräumen direkt?

$$V = V_1 \oplus \cdots \oplus V_n \quad \Longleftrightarrow \quad \forall k : V_k \cap \textstyle\sum_{j \neq k} V_j = \{0\}$$

(3) Ist R ein Divisionsring, so gilt die Schranke $\dim V \leq \sum_{k=1}^{n} \dim V_k$.

(4) Zudem sei $\dim V < \infty$. Die direkte Summe maximiert die Dimension:

$$\boxed{V = V_1 \oplus \cdots \oplus V_n \quad \Longleftrightarrow \quad \dim V = \textstyle\sum_{k=1}^{n} \dim V_k}$$

Beweis: (3) Wir wählen eine Basis $\mathcal{B}_k$ von V_k. Dann wird V erzeugt von $\mathcal{B}_1, \ldots, \mathcal{B}_n$. Daraus wählen wir eine Basis und erhalten die Ungleichung.

(4) Satz M2T zeigt „$\Rightarrow$“. Für „$\Leftarrow$“ untersuchen wir $V = V_k + \sum_{j \neq k} V_j$:

$$\begin{aligned} \dim V + \dim(V_k \cap \textstyle\sum_{j \neq k} V_j) &\overset{(2)}{=} \dim V_k + \dim \textstyle\sum_{j \neq k} V_j \\ &\overset{(3)}{\leq} \dim V_k + \textstyle\sum_{j \neq k} \dim V_j \overset{\text{Vor}}{=} \dim V \end{aligned}$$

Daraus folgt $\dim(V_k \cap \sum_{j \neq k} V_j) = 0$, also $V_k \cap \sum_{j \neq k} V_j = \{0\}$. $\boxed{\text{QED}}$

Klassifikation aller Vektorräume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M2w: Klassifikation aller Vektorräume über einem DRing R

(0) Zu jeder Kardinalzahl $N = |I|$ existieren R–Vektorräume dieser Dimension; das Standardmodell ist der Koordinatenraum $R^{(N)}$ über R.

(1) Genau dann sind Vektorräume V und U über R isomorph, $V \cong U$, wenn sie dieselbe Dimension haben, kurz $\dim_R(V) = \dim_R(U)$.

Beweis: (1) Nach Wahl von Basen (dank Basissatz M2K) haben wir:

$$\begin{tikzcd}
V \arrow[d, dashed, "f"', "\cong"] & R^{(N)} \arrow[l, "\Phi_{\mathcal{V}}"', "\cong"] \arrow[d, dashed, "g"', "\cong"] & N \arrow[d, dashed, "h"', "\cong"] \\
U & R^{(M)} \arrow[l, "\Phi_{\mathcal{U}}"', "\cong"] & M
\end{tikzcd}$$

Komposition $\Longleftrightarrow$ Invarianz $\Longleftrightarrow$ M2C, M2E, M2M

Klassifikation aller Vektorräume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Die endlich-dimensionalen R–Vektorräume sind isomorph zu

$$R^0, R^1, R^2, R^3, \ldots \quad \text{also } R^n \text{ für } n \in \mathbb{N}.$$

Übung: Über $\mathbb{R}$ gilt $\mathbb{R}[X] \cong \mathbb{C}[X]$, aber $\mathbb{R}[X] \ncong \mathscr{C}^\infty(\mathbb{R}, \mathbb{R}) \ncong \mathrm{Fun}(\mathbb{R}, \mathbb{R})$.

Übung: Sind die Gruppen $(\mathbb{Q}^\mathbb{N}, +)$ und $(\mathbb{R}, +)$ isomorph?

Klassifikation aller Vektorraumhomomorphismen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{tikzcd}
 & R^{(J)} \oplus R^{(K)} \arrow[r, "g", "\begin{bmatrix}1&0\\0&0\end{bmatrix}"'] \arrow[d, "\Phi_{\mathcal{V}}", "\cong"'] & R^{(J)} \oplus R^{(L)} \arrow[d, "\Phi_{\mathcal{U}}", "\cong"'] & \\
\mathrm{Ker}(f) \arrow[r, hook, "\mathrm{inc}"] & V \arrow[r, "f"] & U \arrow[r, two heads, "\mathrm{quo}"] & \mathrm{Coker}(f) \\
v_k \arrow[r, mapsto, "(k\in K)"] & v_k & v_j \arrow[r, mapsto, "(j\in J)"'] & u_j \\
 & & u_\ell \arrow[r, mapsto, "(\ell\in L)"] & {[u_\ell]}
\end{tikzcd}
$$

Jede lineare Abbildung $f : V \to U$ definiert vier zugehörige Räume:

Kern	$\mathrm{Ker}(f) \leq V$,	**Cokern**	$\mathrm{Coker}(f) := U/\mathrm{Im}(f)$,
Bild	$\mathrm{Im}(f) \leq U$,	**Cobild**	$\mathrm{Coim}(f) := V/\mathrm{Ker}(f)$.

Dank M2K wählen wir eine Basis $(v_k)_{k\in K}$ von $\mathrm{Ker}(f)$ und ergänzen zu einer Basis $\mathcal{V} = (v_j)_{j\in J\sqcup K}$ von V. Dank M1X ist $(u_j = f(v_j))_{j\in J}$ eine Basis von $\mathrm{Im}(f)$. Wir ergänzen zu einer Basis $\mathcal{U} = (u_j)_{j\in J\sqcup L}$ von U. Dank M1X ist $([u_\ell])_{\ell\in L}$ eine Basis von $\mathrm{Coker}(f)$.

Klassifikation aller Vektorraumhomomorphismen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M2x: Klassifikation aller Vektorraumhomomorphismen

(0) Je drei Mengen (J, K, L) definieren die R–lineare Modellabbildung

$$g : R^{(J \sqcup K)} \to R^{(J \sqcup L)} : \lambda \mapsto \lambda|_J \sqcup 0|_L .$$

$$\begin{tikzcd} V \arrow[r, "f"'] & U \\ R^{(J \sqcup K)} \arrow[u, "\Phi_{\mathcal{V}}", "\cong"'] \arrow[r, "g"] & R^{(J \sqcup L)} \arrow[u, "\Phi_{\mathcal{U}}"', "\cong"] \end{tikzcd}$$

(1) Jeder R–Vektorraumhomomorphismus $f : V \to U$ ist äquivalent zu (genau) einer Modellabbildung g.

(2) Die Kardinalitäten von (J, K, L) sind durch f eindeutig bestimmt:

Rang	$\operatorname{rang}(f)$	$:= \dim_R \operatorname{Im}(f)$	$= \lvert J \rvert$
Defekt	$\operatorname{def}(f)$	$:= \dim_R \operatorname{Ker}(f)$	$= \lvert K \rvert$
Kodefekt	$\operatorname{codef}(f)$	$:= \dim_R \operatorname{Coker}(f)$	$= \lvert L \rvert$

(3) Aus Basen (1) und Dimensionen (2) folgt erneut der **Rangsatz** M1v:

$$\boxed{\begin{aligned} \dim_R(V) &= \dim_R \operatorname{Im}(f) + \dim_R \operatorname{Ker}(f) \\ \dim_R(U) &= \dim_R \operatorname{Im}(f) + \dim_R \operatorname{Coker}(f) \end{aligned}}$$

Dimension unter Sur/In/Bijektionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar M2Y: Dimension unter Sur/In/Bijektionen

Für jeden R–Vektorraumhomomorphismus $f : V \to U$ gilt:

1. Ist $f : V \xrightarrow{\sim} U$ bijektiv, so folgt $\dim V = \dim U$.
2. Ist $f : V \twoheadrightarrow U$ surjektiv, so folgt $\dim V \geq \dim U$.
   Gilt zudem $\dim V \leq \dim U < \infty$, so ist f bijektiv.
3. Ist $f : V \hookrightarrow U$ injektiv, so folgt $\dim V \leq \dim U$.
   Gilt zudem $\infty > \dim V \geq \dim U$, so ist f bijektiv.

$$\begin{tikzcd}
V \arrow[r, "f"'] & U \\
R^{(J \sqcup K)} \arrow[u, "\Phi_{\mathcal{V}}", "\cong"'] \arrow[r, "g"] & R^{(J \sqcup L)} \arrow[u, "\Phi_{\mathcal{U}}"', "\cong"]
\end{tikzcd}$$

Die Modellmatrix $D^r_{m\times n}$ der Größe $m \times n$ vom Rang r

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$D = D^r_{m\times n} := \begin{bmatrix} 1_{r\times r} & 0_{r\times k} \\ 0_{\ell\times r} & 0_{\ell\times k} \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix} \in R^{m\times n}.$$

$$f_D : R^n \to R^m : (x_1, \dots, x_r, \dots, x_n) \mapsto (x_1, \dots, x_r, 0, \dots, 0).$$

$$\begin{aligned} \operatorname{Im}(D) &= \langle e_1, \dots, e_r \rangle^!_R \leq R^m \quad \Longrightarrow \quad \operatorname{rang}(D) = r \\ \operatorname{Ker}(D) &= \langle e_{r+1}, \dots, e_n \rangle^!_R \leq R^n \quad \Longrightarrow \quad \operatorname{def}(D) = n - r \end{aligned}$$

Gauß–Algorithmus beidseitig zur Normalform

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$A \in R^{m\times n} \qquad\qquad B = S^{-1}A$$

$$\begin{bmatrix} 3 & 6 & -6 & -6 & -1 \\ -2 & -4 & 3 & 1 & 5 \\ -1 & -2 & 3 & 5 & -4 \\ 1 & 2 & 1 & 7 & 1 \end{bmatrix} \xleftrightarrow[\text{operationen}]{\text{Zeilen-}} \begin{bmatrix} 1 & 2 & 0 & 4 & 0 \\ 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\text{Spalten-} \updownarrow \text{operationen} \qquad\qquad \text{Spalten-} \updownarrow \text{operationen}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \xleftrightarrow[\text{operationen}]{\text{Zeilen-}} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$D = S^{-1}AT$$

An $SD = AT$ mit $S \in \mathrm{GL}_m\, R$ und $T \in \mathrm{GL}_n\, R$ lesen wir Bild und Kern ab:

$$\operatorname{Im} D = \langle e_1, \dots, e_r \rangle_R^! , \qquad \operatorname{Ker} D = \langle e_{r+1}, \dots, e_n \rangle_R^! ,$$

$$\operatorname{Im} A = \langle Se_1, \dots, Se_r \rangle_R^! , \qquad \operatorname{Ker} A = \langle Te_{r+1}, \dots, Te_n \rangle_R^! .$$

Zeilenraum und Spaltenraum

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$A = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix} = \begin{bmatrix} \text{—} & u_1 & \text{—} \\ & \cdots & \\ \text{—} & u_m & \text{—} \end{bmatrix} \in R^{m \times n}$$

Spaltenraum: $\mathrm{SR}(A) := v_1 \cdot R + \cdots + v_n \cdot R = A \cdot R^{n \times 1} \leq R^{m \times 1}$

Zeilenraum: $\mathrm{ZR}(A) := R \cdot u_1 + \cdots + R \cdot u_m = R^{1 \times m} \cdot A \leq R^{1 \times n}$

Spaltenrang: $\mathrm{sr}(A) := \dim_R \mathrm{SR}(A)$

Zeilenrang: $\mathrm{zr}(A) := \dim_R \mathrm{ZR}(A)$

$$\boxed{\text{Zeilenrang} \overset{?}{=} \text{Spaltenrang}}$$

Zeilenraum und Spaltenraum

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma M31: Zeilenoperationen vs Spaltenoperationen

(1a) Zeilenoperation durch $S \in \mathrm{GL}_m$ R ändert nicht den Zeilenraum:

$$\mathrm{ZR}(SA) \overset{\text{Def}}{=} R^{1\times m} \cdot (S \cdot A) \overset{\text{Ass}}{=} (R^{1\times m} \cdot S) \cdot A \overset{\text{GL}}{=} R^{1\times m} \cdot A \overset{\text{Def}}{=} \mathrm{ZR}(A)$$

(2b) Die Spaltenräume sind i.A. verschieden, doch immer isomorph:

$$\mathrm{SR}(SA) \overset{\text{Def}}{=} (S \cdot A) \cdot R^{n\times 1} \overset{\text{Ass}}{=} S \cdot (A \cdot R^{n\times 1}) \overset{\text{GL}}{\cong} A \cdot R^{n\times 1} \overset{\text{Def}}{=} \mathrm{SR}(A)$$

(2a) Spaltenoperation durch $T \in \mathrm{GL}_n$ R ändert nicht den Spaltenraum:

$$\mathrm{SR}(AT) \overset{\text{Def}}{=} (A \cdot T) \cdot R^{n\times 1} \overset{\text{Ass}}{=} A \cdot (T \cdot R^{n\times 1}) \overset{\text{GL}}{=} A \cdot R^{n\times 1} \overset{\text{Def}}{=} \mathrm{SR}(A)$$

(1b) Die Zeilenräume sind i.A. verschieden, doch immer isomorph:

$$\mathrm{ZR}(AT) \overset{\text{Def}}{=} R^{1\times m} \cdot (A \cdot T) \overset{\text{Ass}}{=} (R^{1\times m} \cdot A) \cdot T \overset{\text{GL}}{\cong} R^{1\times m} \cdot A \overset{\text{Def}}{=} \mathrm{ZR}(A)$$

Zeilenrang gleich Spaltenrang

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M31: Zeilenrang und Spaltenrang sind gleich.

Sei R ein Divisionsring. Für jede Matrix $A \in R^{m \times n}$ über R gilt dann:

$$\boxed{\text{Zeilenrang} \;=\; \text{Spaltenrang}}$$

Beweis: Für alle $S \in \mathrm{GL}_m\, R$ und $T \in \mathrm{GL}_n\, R$ gilt:

$$\mathrm{ZR}(A) \overset{(1)}{\cong} \mathrm{ZR}(S^{-1}AT) \quad \text{und} \quad \mathrm{SR}(A) \overset{(2)}{\cong} \mathrm{SR}(S^{-1}AT)$$

Der Gauß–Algorithmus liefert $S^{-1}AT = D^r_{m \times n}$. Daraus lesen wir ab:

$$\begin{aligned} \mathrm{zr}(A) &\overset{(1)}{=} \mathrm{zr}(S^{-1}AT) \overset{\text{Gauß}}{=} \mathrm{zr}(D^r_{m \times n}) = r \\ \mathrm{sr}(A) &\overset{(2)}{=} \mathrm{sr}(S^{-1}AT) \overset{\text{Gauß}}{=} \mathrm{sr}(D^r_{m \times n}) = r \end{aligned}$$

Anwendungsbeispiel zu Zeilenrang gleich Spaltenrang

Ausprobieren mit Gaël!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sind die Spalten der folgenden Matrix linear unabhängig?

$$A = \begin{bmatrix} 1 & 9 & 3 & 4 & 0 \\ 5 & 1 & 7 & 6 & 2 \\ 4 & 3 & 0 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 9 & 3 & 4 & 0 \\ 5 & 1 & 7 & 6 & 2 \\ 4 & 3 & 0 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 9 & 3 & 4 & 0 \\ 5 & 1 & 7 & 6 & 2 \\ 4 & 3 & 0 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 6 & 8 \end{bmatrix}$$

Lösung: Zwischen den Zeilen besteht eine *offensichtliche* Relation!

⚠ Die Relationen zwischen den Spalten sind *nicht* offensichtlich!
Hier gilt $\operatorname{Ker}(A) = \operatorname{Ker}(B) = \operatorname{Ker}(C) = (119, 52, 15, -158, 98)^\intercal \cdot \mathbb{R}$.

Illustration zum Rangsatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$A = \begin{bmatrix} * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} * & * & * & * & * & * & * & 1 & 0 \\ * & * & * & * & * & * & * & 2 & 0 \\ * & * & * & * & * & * & * & 3 & 3 \\ * & * & * & * & * & * & * & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{bmatrix} \in \mathbb{R}^{5\times 9}$$

Aufgabe: Was können Sie hier über Rang und Defekt aussagen?

Lösung: (1) Hier gilt $0 \leq \dim_{\mathbb{R}} \operatorname{Im}(A) \leq 4$, also $5 \leq \dim_{\mathbb{R}} \operatorname{Ker}(A) \leq 9$.
(2) Hier gilt $2 \leq \dim_{\mathbb{R}} \operatorname{Im}(A) \leq 5$ und somit $4 \leq \dim_{\mathbb{R}} \operatorname{Ker}(A) \leq 7$.

Illustration zum Rangsatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Welche Dimension hat der Kern?

$$f : \mathbb{R}^{100} \to \mathbb{R}^{1} \quad : (x_1, \dots, x_{100}) \mapsto x_1 + \dots + x_{100}$$
$$g : \mathbb{R}^{100} \to \mathbb{R}^{42} \quad : (x_1, \dots, x_{100}) \mapsto (f(x), 0, \dots, 0)$$

Lösung: (1) Offensichtlich gilt $\dim_{\mathbb{R}} \operatorname{Im}(f) = 1$, also $\dim_{\mathbb{R}} \operatorname{Ker}(f) = 99$.
(2) Ebenso gilt $\dim_{\mathbb{R}} \operatorname{Im}(g) = 1$, daraus folgt sofort $\dim_{\mathbb{R}} \operatorname{Ker}(g) = 99$.

Ordnung endlicher Vektorräume und endlicher Körper

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M3J: Ordnung endlicher Vektorräume

Jeder endliche Vektorraum V über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ erfüllt $\sharp V = p^d$ mit $d \in \mathbb{N}$.
Möglich sind also die Ordnungen $1, 2, 3, 4, 5, \cancel{6}, 7, 8, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \ldots$.

Beweis: Dank Basissatz M2K hat V eine Basis $(b_i)_{i \in I}$, somit $\Phi_{\mathcal{B}} : \mathbb{F}_p^{(I)} \xrightarrow{\sim} V$.
Im endlichen Fall folgt $\sharp V = \sharp \mathbb{F}_p^d = p^d$ mit $d = \dim V = \sharp I \in \mathbb{N}$. QED

Satz M3K: Ordnung endlicher Körper

Jeder endliche Körper E erfüllt $\sharp E = p^d$ mit $p \in \mathbb{N}_{\geq 2}$ prim und $d \in \mathbb{N}_{\geq 1}$.
Es gibt Körper der Ordnung $\cancel{1}, 2, 3, 4, 5, \cancel{6}, 7, 8, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, 16, \ldots$.

Beweis: Der Körper E enthält seinen charakteristischen Unterkörper $\mathrm{Char}(E) \cong \mathbb{F}_p$ (K1Q). Hierüber ist E ein Vektorraum (L1D). QED

Ordnung der Gruppe $\mathrm{GL}_3\,\mathbb{F}_2$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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 (D2M).

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 noch $2^3 - 2 = 6$ Möglichkeiten.
3. Für $a_3 \in \mathbb{F}_2^3 \smallsetminus \langle a_1, a_2 \rangle$ bleiben nur $2^3 - 2^2 = 4$ 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 $\mathrm{GL}_n\,\mathbb{F}_q$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sei V ein linearer Raum über $\mathbb{F}_q$ mit $\dim(V) = n$.
(0) Wie viele Familien $(a_1, \dots, a_k) \in V^k$ gibt es? (1) linear unabhängig?
(2) Welche Ordnung hat die allgemeine lineare Gruppe $\mathrm{Aut}(V) \cong \mathrm{GL}_n\,\mathbb{F}_q$?
(4) Wie viele Unterräume $U \leq V$ mit $\dim(U) = k$ gibt es demnach?

Lösung: (0) Wir haben $V \cong \mathbb{F}_q^n$, also $\sharp V = q^n$ und $\sharp V^k = q^{nk}$. (1) Sei

$$\begin{aligned} B_q(n,k) &:= \{\,(a_1, \dots, a_k) \in V^k \text{ linear unabhängig}\,\} \\ &\overset{\text{M21}}{=} \{\,(a_1, \dots, a_k) \in V^k \mid \forall i : a_i \in V \smallsetminus \langle a_1, \dots, a_{i-1} \rangle^!_{\mathbb{F}_q}\,\}. \end{aligned}$$

(1) Für die Elementezahl $b_q(n,k) := \sharp B_q(n,k)$ folgt:

$$b_q(n,k) \;=\; (q^n - 1)(q^n - q) \dots (q^n - q^{k-1}) \;=\; \textstyle\prod_{i=0}^{k-1} (q^n - q^i)$$

(2) Die Gruppe $\mathrm{Aut}(V) \cong \mathrm{GL}_n\,\mathbb{F}_q$ hat demnach Ordnung $b_q(n,n)$.

(3) Die Anzahl der linear unabhängigen Familien $(a_1, \dots, a_k)$ ist $b_q(n,k)$.
Jede erzeugt einen Unterraum $U = \langle a_1, \dots, a_k \rangle^!_{\mathbb{F}_q} \leq V$ der Dimension k.
Umgekehrt wird U von genau $b_q(k,k)$ dieser Familien / Basen erzeugt.

Ordnung der Gruppe $\mathrm{GL}_n\,\mathbb{F}_q$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M3L: Ordnung der Gruppe $\mathrm{GL}_n\,\mathbb{F}_q$

(1) Die Anzahl der linear unabhängigen Familien $(a_1, \dots, a_k)$ in $\mathbb{F}_q^n$ ist

$$b_q(n,k) \;=\; \prod_{i=0}^{k-1}(q^n - q^i) \;=\; (q^n-1)(q^n-q)\cdots(q^n-q^{k-1}).$$

(2) Die Ordnung der Gruppe $\mathrm{GL}_n\,\mathbb{F}_q \cong \mathrm{Aut}(\mathbb{F}_q^n)$ ist demnach $b_q(n,n)$:

$$\sharp\,\mathrm{GL}_n\,\mathbb{F}_q \;=\; \prod_{k=0}^{n-1}(q^n - q^k) \;=\; (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}).$$

(3) Die Anzahl der k–dimensionalen Unterräume $U \leq \mathbb{F}_q^n$ ist

$$\binom{n}{k}_q \;:=\; \frac{b_q(n,k)}{b_q(k,k)} \;=\; \prod_{i=0}^{k-1}\frac{q^n-q^i}{q^k-q^i} \;=\; \prod_{i=0}^{k-1}\frac{q^{n-i}-1}{q^{k-i}-1}.$$

Lineare Abbildungen mit vorgegebenem Rang

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M3M: Anzahl linearer Abbildungen mit vorgegebenem Rang

Seien V, W Vektorräume über $\mathbb{F}_q$ mit $\dim(V) = k$ und $\dim(W) = n$ und

$$\begin{aligned} \operatorname{Hom}_{\mathbb{F}_q}(V, W)_r &:= \left\{ f : V \to W \,\middle|\, \operatorname{rang}(f) = r \right\} \\ &\cong \left\{ (U, \bar{f}, B) \,\middle|\, U \leq V,\ \bar{f} : V/U \xrightarrow{\sim} B,\ B \leq V,\ \dim B = r \right\}. \end{aligned}$$

Für jeden Rang $r \in \mathbb{N}$ gilt demnach:

$$\sharp \operatorname{Hom}_{\mathbb{F}_q}(V, W)_r = \binom{k}{r}_q \cdot \sharp \operatorname{GL}_r \mathbb{F}_q \cdot \binom{n}{r}_q$$

Dimensionskriterium für Basen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Korollar M3N: Schrankenlemma und Dimensionskriterium für Basen

Sei R ein Divisionsring und V ein R–Vektorraum mit $\dim_R(V) = n \in \mathbb{N}$.

1. Sei $\mathcal{B} = (v_1, \dots, v_\ell)$ in V erzeugend. Dann gilt $\ell \geq n$.
2. Sei $\mathcal{B} = (v_1, \dots, v_\ell)$ linear unabhängig. Dann gilt $\ell \leq n$.
3. Gilt (1) oder (2) und zudem $\ell = n$, so ist $\mathcal{B}$ eine Basis.

Beweis: (1) Dank Basisauswahlsatz (M2K) können wir $v_1, \dots, v_\ell$ verkürzen zu einer Basis; diese hat Länge n dank Invarianz der Dimension (M2C).

(2) Dank Basisergänzungsatz (M2K) können wir $v_1, \dots, v_\ell$ ergänzen zu einer Basis; diese hat Länge n dank Invarianz der Dimension (M2C). QED

Dimension von Untervektorräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz M3o: Dimension von Untervektorräumen

Jeder Untervektorraum $U \leq V$ hat ein Komplement U', d.h. $V = U \oplus U'$.
(1) Es folgt $\dim U \leq \dim V$. (2) Gilt $\dim U = \dim V < \infty$, so folgt $U = V$.

Beweis: (0) Dank Satz M2K wählen wir eine Basis $(v_j)_{j \in J}$ von U.
Diese ergänzen wir zu einer Basis $(v_i)_{i \in I}$ von V, wobei $I = J \sqcup K$.
Damit gilt $V = U \oplus U'$ mit $U = \langle v_j \mid j \in J \rangle_R^!$ und $U' = \langle v_k \mid k \in K \rangle_R^!$.

(1) Daraus folgt $\dim U = |J| \leq |I| = \dim V$ dank H2B.
(2) Im Falle $|J| = |I| < \infty$ folgt $J = I$ dank H2B. QED

Wie prüfen wir Exaktheit? Geschickt dank Dimension!

$$R^k \xrightarrow[\operatorname{Im} B \subseteq]{B} R^n \xrightarrow[\supseteq \operatorname{Ker} A]{A} R^m$$

Die Inklusion $\operatorname{Im} B \subseteq \operatorname{Ker} A$ ist äquivalent zu $AB = 0$.

Satz M3P: Kriterium für Exaktheit

Genau dann ist (B, A) exakt, wenn $AB = 0$ gilt und $\operatorname{rang} B = \operatorname{def} A$.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wie ergänzen wir exakt? Dank Gauß–Algorithmus!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$0 \longrightarrow R^k \xrightarrow[\begin{bmatrix} 0_{r\times k} \\ 1_{k\times k}\end{bmatrix}]{E} R^n \xrightarrow[\begin{bmatrix} 1_{r\times r} & 0_{r\times k} \\ 0_{\ell\times r} & 0_{\ell\times k}\end{bmatrix}]{F} R^m \xrightarrow[\begin{bmatrix} 0_{\ell\times r} & 1_{\ell\times \ell}\end{bmatrix}]{G} R^\ell \longrightarrow 0$$

Modell:

Algo M3Q: exakte Ergänzung

Eingabe: eine Matrix $F \in R^{m\times n}$ über dem Divisionsring R

Ausgabe: $E \in R^{n\times k}$ und $G \in R^{\ell\times m}$ mit $(0, E, F, G, 0)$ exakt

1: Bringe $(F, 1_{m\times m})$ in red. Zeilenstufenform (SF, S) mit $S \in \mathrm{GL}_m R$

2: Lies Rang r und Defekt k ab sowie eine Basis $\operatorname{Ker} F = \langle v_1, \dots, v_k \rangle_R^!$

3: Wähle $E = (v_1, \dots, v_k)$ und $G = (s_{r+1}; \dots; s_n)$ die letzten Zeilen von S

Wie rechnen wir mit Unterräumen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Eine Ebene $U \subseteq \mathbb{R}^3$ können wir auf zwei Weisen beschreiben:
(1) **Parameterform:** $U = \langle u_1, u_2 \rangle_{\mathbb{R}}^! = \operatorname{Im}(E)^!$ mit Basis $u_1, u_2 \in \mathbb{R}^3$ von U.
(2) **Normalform:** $U = \operatorname{Ker}(G)^!$ mit einem Normalenvektor $G \in \mathbb{R}^{3\times 1}$.

$$\begin{tikzcd}
0 \arrow[r] & R^k \arrow[r, "E"] & R^n \arrow[r, "G"] & R^\ell \arrow[r] & 0 \\
& & \vee\!| & & \\
& & \operatorname{Im}(E)^! = U = \operatorname{Ker}(G)^! & &
\end{tikzcd}$$

Wie beschreiben wir einen Unterraum $U \leq R^n$, bequem und effizient?

(1) Als Bildraum $U = \operatorname{Im} E$ eines Erzeugendensystems, $E \in R^{n\times k}$.
Minimal, frei, mit linear unabhängigen Spalten gilt $\operatorname{rang} E = k$: **Basis!**

(2) Als Lösungsraum $U = \operatorname{Ker} G$ eines Gleichungssystems, $G \in R^{\ell\times n}$.
Minimal, frei, mit linear unabhängigen Zeilen gilt $\operatorname{rang} G = \ell$: **Kobasis!**

Wie rechnen wir mit Unterräumen?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Anwendung: Liegt ein vorgegebener Vektor $v \in R^n$ in $U \leq R^n$?

(1) Für $U = \mathrm{Im}(E)$: 😐 Löse $E\lambda = v$.

(2) Für $U = \mathrm{Ker}(G)$: 🙂 Prüfe $Gv = 0$.

Anwendung: Finde einen Vektor / alle Vektoren v in $U \leq R^n$!

(2) Für $U = \mathrm{Ker}(G)$: 😐 Löse $Gv = 0$ als Basis von $\mathrm{Ker}(G)$.

(1) Für $U = \mathrm{Im}(E)$: 🙂 Hier genügt $v = E\lambda$ mit $\lambda \in R^k$.

Wechsel der Darstellung: Kern vs Bild

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Algo M3R: von Kern zu Bild

Eingabe: $A \in R^{\ell \times n}$ mit $U = \mathrm{Ker}(A)$
Ausgabe: $B \in R^{n \times k}$ mit $U = \mathrm{Im}(B)^!$

1: Bringe A in RZSF A'
2: Erhalte $B = (b_1, \dots, b_k)$ als Basis von $\mathrm{Ker}\, A' = \mathrm{Ker}\, A$ dank M1v

Algo M3R: von Bild zu Kern

Eingabe: $B \in R^{n \times k}$ mit $U = \mathrm{Im}(B)$
Ausgabe: $A \in R^{\ell \times n}$ mit $U = \mathrm{Ker}(A)^!$

1: Bringe B in RSSF B'
2: Erhalte $A = (a_1; \dots; a_\ell)$ als Basis von $\mathrm{Ann}\, B' = \mathrm{Ann}\, B$ dank M1v

Inklusion und Gleichheit von Unterräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Algo M3T: Inklusion von Unterräumen

Eingabe: Unterräume $U = \mathrm{Im}(B)$ und $V = \mathrm{Ker}(A)$ in R^n

Ausgabe: Gilt die Inklusion $U \subseteq V$?

1: Es gilt $U \subseteq V$ gdw $AB = 0$.

2: Gilt zudem $\dim U = \dim V$, so folgt Gleichheit $U = V$.

Summe und Schnitt von Unterräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Algo M3u: Summe von Unterräumen

Eingabe: $U_1, \dots, U_k \leq R^n$
Ausgabe: $V = U_1 + \dots + U_k$

1: Stelle $U_i = \mathrm{Im}(B_i)$ als Bild dar
2: Erhalte $V = \mathrm{Im}(B_1, \dots, B_k)$ als Bild

Algo M3u: Schnitt von Unterräumen

Eingabe: $U_1, \dots, U_\ell \leq R^n$
Ausgabe: $V = U_1 \cap \dots \cap U_\ell$

1: Stelle $U_i = \mathrm{Ker}(A_i)$ als Kern dar
2: Erhalte $V = \mathrm{Ker}(A_1; \dots; A_\ell)$ als Kern

Bild und Urbild von Unterräumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Matrix $F \in R^{m \times n}$ stiftet die lineare Abbildung $f : R^n \to R^m : v \mapsto Fv$.

Algo M3v: Bild eines Unterraums

Eingabe: $U \leq R^n$
Ausgabe: $V = f(U) \leq R^m$

1: Stelle $U = \mathrm{Im}(E)$ als Bild dar
2: Erhalte $V = \mathrm{Im}(FE)$ als Bild

Algo M3v: Urbild eines Unterraums

Eingabe: $V \leq R^m$
Ausgabe: $U = f^{-1}(V) \leq R^n$

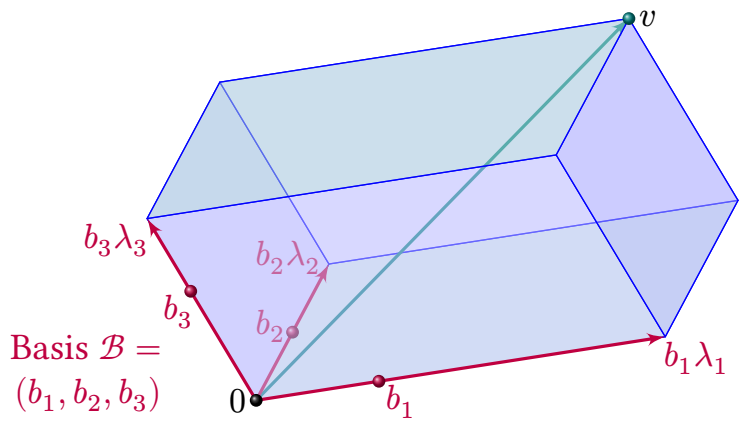
1: Stelle $V = \mathrm{Ker}(G)$ als Kern dar
2: Erhalte $U = \mathrm{Ker}(GF)$ als Kern

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel M

Bonusmaterial



Evolution has ensured that our brains just aren't equipped to visualise 11 dimensions directly. However, from a purely mathematical point of view, it's just as easy to think in 11 dimensions, as it is to think in three or four.

Stephen Hawking (1942–2018)

Inhalt dieses Kapitels M

5 Jeder endliche Divisionsring ist ein Körper!

6 Basis und Dimension: Ergänzungen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dimension des Schnitts, nach Lewis Carroll

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Der $\mathbb{R}$–Vektorraum $V = \mathbb{R}^{100}$ enthält Unterräume $E \cong \mathbb{R}^{70}$, $F \cong \mathbb{R}^{75}$, $G \cong \mathbb{R}^{80}$, $H \cong \mathbb{R}^{85}$. Wie groß ist $U := E \cap F \cap G \cap H \leq V$ (1) höchstens? (2) mindestens?

Lösung: (1) Offensichtlich gilt $U \leq E$, also $\dim(U) \leq \dim(E) = 70$.

(2) Wir nutzen $\dim(E + F) = \dim(E) + \dim(F) - \dim(E \cap F)$. Damit gilt:

$$\begin{aligned}
\dim(E \cap F) &= \dim(E) + \dim(F) - \dim(E + F) \\
&\geq 70 + 75 - 100 = 45 \\
\dim(E \cap F \cap G) &= \dim(E \cap F) + \dim(G) - \dim((E \cap F) + G) \\
&\geq 45 + 80 - 100 = 25 \\
\dim(E \cap F \cap G \cap H) &= \dim(E \cap F \cap G) + \dim(H) - \dim((E \cap F \cap G) + H) \\
&\geq 25 + 85 - 100 = 10
\end{aligned}$$

Alternativ: Wir beschreiben $E, F, G, H \leq \mathbb{R}^{100}$ durch $30, 25, 20, 15$ lineare Gleichungen. Somit ist U Lösung von 90 Gleichungen, also $\dim U \geq 10$.

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel N

Matrixdarstellung und Minimalpolynom

$$\frac{1}{4}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & \mathrm{i} & -1 & -\mathrm{i}\\ 1 & -1 & 1 & -1\\ 1 & -\mathrm{i} & -1 & \mathrm{i}\end{bmatrix}\begin{bmatrix}0 & 3 & 2 & 1\\ 1 & 0 & 3 & 2\\ 2 & 1 & 0 & 3\\ 3 & 2 & 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -\mathrm{i} & -1 & \mathrm{i}\\ 1 & -1 & 1 & -1\\ 1 & \mathrm{i} & -1 & -\mathrm{i}\end{bmatrix} = \begin{bmatrix}\lambda_0 & 0 & 0 & 0\\ 0 & \lambda_1 & 0 & 0\\ 0 & 0 & \lambda_2 & 0\\ 0 & 0 & 0 & \lambda_3\end{bmatrix}$$

The introduction of numbers as coordinates [...] is an act of violence whose only practical vindication is the special calculatory manageability.
Hermann Weyl (1885–1955), *Philosophy of Mathematics and Natural Science*

Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels N

1 Lineare Abbildungen und Matrizen

2 Basiswechsel und Koordinatentransformation

3 Diagonalisierung dank Minimalpolynom

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Vergleich von Homomorphismen auf Erzeugern

$$\begin{tikzcd} V \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] \arrow[r, phantom, "\overset{?}{\underset{i}{=}}"] & W \end{tikzcd}$$

Lemma N1A: Vergleichslemma für Homomorphismen

Seien $f, g : V \to W$ rechtslinear über R und $f(v_i) = g(v_i)$ für $i \in I$.
(1) Daraus folgt $f(v) = g(v)$ für alle $v \in \langle v_i \mid i \in I \rangle_R$.
(2) Erzeugt $(v_i)_{i \in I}$ ganz V, so folgt $f = g$.

Beweis: (1) Für $v = \sum_{i \in I} v_i \lambda_i$ mit $\lambda = (\lambda_i)_{i \in I} \in R^{(I)}$ gilt:

$$\begin{aligned} f(v) &\overset{\text{Def}}{=} f\left(\textstyle\sum_{i \in I} v_i \lambda_i\right) \overset{\text{Lin}}{=} \textstyle\sum_{i \in I} f(v_i)\lambda_i \\ &\overset{\text{Vor}}{=} \textstyle\sum_{i \in I} g(v_i)\lambda_i \overset{\text{Lin}}{=} g\left(\textstyle\sum_{i \in I} v_i \lambda_i\right) \overset{\text{Def}}{=} g(v) \end{aligned}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Konstruktion dank Prinzip der linearen Fortsetzung

$$\begin{tikzcd} V \arrow[rr, dashed, "\exists! f", "v_i \mapsto w_i"'] & & W \\ & I \arrow[ul, "\mathcal{B}", "v_i \leftarrow\!\shortmid i"'] \arrow[ur, "\mathcal{C}"', "i \mapsto w_i"] & \end{tikzcd} \qquad \begin{tikzcd} V \arrow[rr, dashed, "\exists! f", "v_i \mapsto w_i"'] & & W \\ & R^{(I)} \arrow[ul, "\Phi_{\mathcal{B}}", "\cong"', "v_i \leftarrow\!\shortmid e_i"'] \arrow[ur, "\Phi_{\mathcal{C}}"', "e_i \mapsto w_i"] & \end{tikzcd}$$

Satz N1B: das Prinzip der linearen Fortsetzung, PLF

Gegeben sei ein R–linearer Raum V mit Basis $\mathcal{B} = (v_i)_{i \in I}$ sowie als Ziel eine Familie $\mathcal{C} = (w_i)_{i \in I}$ in einem R–linearen Raum W. Dann existiert genau eine R–lineare Abbildung $f : V \to W$ mit $v_i \mapsto w_i$ für alle $i \in I$.

Explizit gilt $f = \Phi_{\mathcal{C}} \circ \Phi_{\mathcal{B}}^{-1}$, also

$$\boxed{f : v = \textstyle\sum_{i \in I} v_i \lambda_i \;\mapsto\; \lambda \;\mapsto\; w = \textstyle\sum_{i \in I} w_i \lambda_i \quad \text{für alle } \lambda \in R^{(I)}.}$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Anwendungsbeispiel: formale Ableitung von Polynomen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel N1c: formale Ableitung von Polynomen

Sei $K[X]$ der Polynomring über dem kommutativen Ring K.

(1) Wir definieren die **Ableitung** als die K–lineare Abbildung

$$D = \partial_X \,:\, K[X] \to K[X] \,:\, X^n \mapsto nX^{n-1} \quad \text{für alle } n \in \mathbb{N}.$$

☺ Dank PLF N1B bedeutet das $F = \sum_n a_n X^n \;\mapsto\; f = \sum_n n a_n X^{n-1}$.

(2) Im Falle $\mathbb{Q} \leq K$ definieren wir ebenso das **Integral**:

$$I = \int_X \,:\, K[X] \to K[X] \,:\, X^n \mapsto \tfrac{1}{n+1} X^{n+1}$$

☺ Dank PLF N1B bedeutet das $f = \sum_n a_n X^n \;\mapsto\; F = \sum_n \frac{a_n}{n+1} X^{n+1}$.

(3) Damit gilt der **HDI** for Polynome:

$$(D \circ I)(f) = f \quad \text{und} \quad (I \circ D)(F) = F - F(0)$$

☺ Dank Vergleichslemma N1A genügt es, dies auf $(X^n)_{n\in\mathbb{N}}$ zu prüfen.

Darstellung einer linearen Abbildung durch eine Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Zu jeder Matrix $A \in R^{m\times n}$ gehört ihre R–lineare Abbildung $f_A = \mathrm{L}(A)$:

$$A = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix} \quad \Longrightarrow \quad f_A : R^n \to R^m : x \mapsto y = Ax = \sum_{j=1}^{n} v_j x_j$$

In der j-ten Spalte stehen die Koordinaten des j-ten Basisbildes, $e_j \mapsto v_j$.

♦ Satz D1J: Bijektion zwischen Matrizen und linearen Abbildungen

(0) Zu $A \in R^{m\times n}$ ist $\mathrm{L}(A) := f_A : R^n \to R^m : x \mapsto Ax$ linear. Umgekehrt:
(1) Für $f : R^n \to R^m$ linear gilt $f = f_A$ mit $A = \mathrm{M}(f) := (f(e_1), \dots, f(e_n))$.

$$\boxed{(\mathrm{L}, \mathrm{M}) : R^{m\times n} \cong \mathrm{Hom}_R(R^n, R^m) : A \leftrightarrows f}$$

Darstellung einer linearen Abbildung durch eine Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$f : \mathbb{R}^3 \to \mathbb{R}^2 : \begin{bmatrix} x \\ y \\ z \end{bmatrix} \mapsto \begin{bmatrix} 4z + 3y \\ 5x + 2z \end{bmatrix}.$$

Aufgabe: Stellen Sie f durch eine Matrix A dar, sodass $f = f_A$.

Lösung: Wir schreiben jedes Basisbild $f(e_j)_{j=1}^3$ in der Zielbasis $(e_i)_{i=1}^2$:

$$f(e_1) = \begin{bmatrix} 0 \\ 5 \end{bmatrix} = \begin{cases} +e_1 \cdot 0 \\ +e_2 \cdot 5, \end{cases} \quad f(e_2) = \begin{bmatrix} 3 \\ 0 \end{bmatrix} = \begin{cases} +e_1 \cdot 3 \\ +e_2 \cdot 0, \end{cases} \quad f(e_3) = \begin{bmatrix} 4 \\ 2 \end{bmatrix} = \begin{cases} +e_1 \cdot 4 \\ +e_2 \cdot 2. \end{cases}$$

Wir erhalten:

$$\mathrm{M}(f) = A = \begin{bmatrix} 0 & 3 & 4 \\ 5 & 0 & 2 \end{bmatrix} \in \mathbb{R}^{2\times 3}$$

Probe:

$$f_A : \begin{bmatrix} x \\ y \\ z \end{bmatrix} \mapsto \begin{bmatrix} 0 & 3 & 4 \\ 5 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0x + 3y + 4z \\ 5x + 0y + 2z \end{bmatrix}.$$

Darstellung einer linearen Abbildung durch eine Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{tikzcd}
R^n \arrow[r, "x \mapsto Ax", "f_A"'] \arrow[d, "\Phi_{\mathcal{B}}"', "\cong"] & R^m \arrow[d, "\Phi_{\mathcal{C}}"', "\cong"] \\
V \arrow[r, "f"] & W
\end{tikzcd}
$$

$$
\boxed{
\begin{aligned}
f &= \mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A) := \Phi_{\mathcal{C}} \circ \mathrm{L}(A) \circ \Phi_{\mathcal{B}}^{-1} \\
A &= \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f) := \mathrm{M}(\Phi_{\mathcal{C}}^{-1} \circ f \circ \Phi_{\mathcal{B}})
\end{aligned}
}
$$

Darstellung einer linearen Abbildung durch eine Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz N1G: Bijektion zwischen Matrizen und linearen Abbildungen

Gegeben sei eine Basis $\mathcal{B} = (b_j)_{j=1}^n$ von V und $\mathcal{C} = (c_i)_{i=1}^m$ von W über R.

(1) Jede Matrix $A \in R^{m\times n}$ definiert die zugehörige R–lineare Abbildung

$$f = \mathrm{L}_{\mathcal{B}}^{\mathcal{C}}(A) : V \to W : v = \sum_{j=1}^n b_j\lambda_j \mapsto w = \sum_{i=1}^m c_i\mu_i, \quad \mu_i = \sum_{j=1}^n a_{ij}\lambda_j.$$

(2) Jede R–lineare Abbildung $f : V \to W$ lässt sich eindeutig so darstellen.

$$f : b_j \mapsto f(b_j) = \textstyle\sum_{i=1}^m c_i a_{ij} \quad \Longrightarrow \quad \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f) := A = (a_{ij}) \in R^{m\times n}$$

(3) Dies stiftet eine Bijektion zwischen Matrizen und Homomorphismen:

$$\boxed{(\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}) : R^{m\times n} \cong \mathrm{Hom}_R(V, W) : A \leftrightarrows f}$$

Anwendungsbeispiel: darstellende Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Stellen Sie die Ableitung $\partial : \mathbb{R}[X]_{\leq 3} \to \mathbb{R}[X]_{\leq 2}$ über $\mathbb{R}$ dar als Matrix $A := \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\partial)$ bezüglich der Monombasen. **Lösung:** Wir betrachten

$$\begin{array}{llll} \text{den Startraum} & V = \mathbb{R}[X]_{\leq 3} & \text{mit der Basis} & \mathcal{B} = (X^j)_{j=0}^{3}, \\ \text{den Zielraum} & W = \mathbb{R}[X]_{\leq 2} & \text{mit der Basis} & \mathcal{C} = (X^i)_{i=0}^{2}. \end{array}$$

Wir schreiben jedes Basisbild $\partial(X^j) = \sum_{i=0}^{2} X^i a_{ij}$ in Zielkoordinaten:

$$\begin{array}{lllll} X^0 & \mapsto & \partial X^0 = 0 & = & X^0 \cdot \mathbf{0} + X^1 \cdot \mathbf{0} + X^2 \cdot \mathbf{0} \\ X^1 & \mapsto & \partial X^1 = 1 & = & X^0 \cdot \mathbf{1} + X^1 \cdot \mathbf{0} + X^2 \cdot \mathbf{0} \\ X^2 & \mapsto & \partial X^2 = 2X & = & X^0 \cdot \mathbf{0} + X^1 \cdot \mathbf{2} + X^2 \cdot \mathbf{0} \\ X^3 & \mapsto & \partial X^3 = 3X^2 & = & X^0 \cdot \mathbf{0} + X^1 \cdot \mathbf{0} + X^2 \cdot \mathbf{3} \end{array}$$

In der j-ten Spalte von A stehen die Koordinaten des j-ten Basisbildes:

$$A = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\partial) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

Anwendungsbeispiel: darstellende Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Stellen Sie die Ableitung $\partial : \mathbb{R}[X]_{\leq 3} \to \mathbb{R}[X]_{\leq 2}$ dar als Matrix $A' := \mathrm{M}^{\mathcal{C}'}_{\mathcal{B}'}(\partial)$ bezüglich der faktoriellen Basen. **Lösung:** Wir betrachten

$$\begin{array}{llll} \text{den Startraum} & V = \mathbb{R}[X]_{\leq 3} & \text{mit der Basis} & \mathcal{B}' = (X^j/j!)_{j=0}^{3}, \\ \text{den Zielraum} & W = \mathbb{R}[X]_{\leq 2} & \text{mit der Basis} & \mathcal{C}' = (X^i/i!)_{i=0}^{2}. \end{array}$$

Wir schreiben jedes Basisbild $\partial(X^j/j!) = \sum_{i=0}^{2} (X^i/i!)\, a'_{ij}$:

$$\begin{array}{lllll} X^0/0! & \overset{\partial}{\mapsto} & 0 & = & X^0/0! \cdot \mathbf{0} + X^1/1! \cdot \mathbf{0} + X^2/2! \cdot \mathbf{0} \\ X^1/1! & \mapsto & X^0/0! & = & X^0/0! \cdot \mathbf{1} + X^1/1! \cdot \mathbf{0} + X^2/2! \cdot \mathbf{0} \\ X^2/2! & \mapsto & X^1/1! & = & X^0/0! \cdot \mathbf{0} + X^1/1! \cdot \mathbf{1} + X^2/2! \cdot \mathbf{0} \\ X^3/3! & \mapsto & X^2/2! & = & X^0/0! \cdot \mathbf{0} + X^1/1! \cdot \mathbf{0} + X^2/2! \cdot \mathbf{1} \end{array}$$

In der j-ten Spalte von A' stehen die Koordinaten des j-ten Basisbildes:

$$A' = \mathrm{M}^{\mathcal{C}'}_{\mathcal{B}'}(\partial) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Zusammenfassung: darstellende Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Ziel:

$$\begin{tikzcd}
R^n \arrow[r, "x \mapsto Ax", "A"'] \arrow[d, "\Phi_{\mathcal{B}}"', "\cong"] & R^m \arrow[d, "\Phi_{\mathcal{C}}"', "\cong"] \\
V \arrow[r, "f"] \arrow[u, leftrightarrow, "\mathrm{M}_{\mathcal{B}}^{\mathcal{C}}", "\mathrm{L}_{\mathcal{B}}^{\mathcal{C}}"'] & W
\end{tikzcd}$$

$$A = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f) = \mathrm{M}(\Phi_{\mathcal{C}}^{-1} \circ f \circ \Phi_{\mathcal{B}})$$

Weg:

$$\begin{array}{c|cccc}
 & b_1 & b_2 & \dots & b_n \\
 & \overset{f}{\downarrow} & \downarrow & & \downarrow \\
\hline
c_1 & a_{11} & a_{12} & \dots & a_{1n} \\
c_2 & a_{21} & a_{22} & \dots & a_{2n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
c_m & a_{m1} & a_{m2} & \dots & a_{mn}
\end{array}$$

$$f(b_j) = \sum_{i=1}^{m} c_i a_{ij}$$

Darstellende Matrizen und Addition / zentrale Skalierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz N1H: Verträglichkeit mit Addition und Skalierung

Gegeben sei eine Basis $\mathcal{V} = (v_i)_{i=1}^n$ von V und $\mathcal{W} = (w_i)_{i=1}^m$ von W.

(1) Das oben konstruierte Bijektionspaar

$$(\mathrm{L}_{\mathcal{V}}^{\mathcal{W}}, \mathrm{M}_{\mathcal{V}}^{\mathcal{W}}) : (R^{m\times n}, +, \cdot) \cong (\mathrm{Hom}_R(V, W), +, \cdot)$$

ist ein Isomorphismus linearer Räume über dem Zentrum $Z(R) \leq R$.

(2) Ist der Ring R kommutativ, also $Z(R) = R$, so gilt demnach

$$\dim_R \mathrm{Hom}_R(V, W) = \dim_R(R^{m\times n}) = mn.$$

Darstellende Matrizen und Komposition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{tikzcd}
R^q \arrow[r, "A"'] \arrow[rr, bend left, "B\cdot A"] \arrow[d, "\Phi_{\mathcal{U}}"', "\cong"] & R^p \arrow[r, "B"'] \arrow[d, "\Phi_{\mathcal{V}}"', "\cong"] & R^n \arrow[d, "\Phi_{\mathcal{W}}"', "\cong"] \\
U \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & V \arrow[r, "g"] & W
\end{tikzcd}
$$

$$\mathrm{M}_{\mathcal{U}}^{\mathcal{W}}(g \circ f) = \mathrm{M}_{\mathcal{V}}^{\mathcal{W}}(g) \cdot \mathrm{M}_{\mathcal{U}}^{\mathcal{V}}(f)$$

$$\mathrm{L}_{\mathcal{U}}^{\mathcal{W}}(B \cdot A) = \mathrm{L}_{\mathcal{V}}^{\mathcal{W}}(B) \circ \mathrm{L}_{\mathcal{U}}^{\mathcal{V}}(A)$$

Darstellende Matrizen und Komposition

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Stellen Sie die Ableitung $\partial : \mathbb{R}[X]_{\leq 3} \to \mathbb{R}[X]_{\leq 2}$ als Matrix D dar, ebenso das Integral $\int : \mathbb{R}[X]_{\leq 2} \to \mathbb{R}[X]_{\leq 3}$ als Matrix I, bezüglich der Monombasen. Was erwarten Sie für die Produkte $D \cdot I$ und $I \cdot D$?

Lösung: Wir finden

$$D = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\partial) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \quad I = \mathrm{M}_{\mathcal{C}}^{\mathcal{B}}(\textstyle\int) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/3 \end{bmatrix}.$$

Für die Produkte gilt

$$D \cdot I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad I \cdot D = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Darstellung von Endomorphismen und Automorphismen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd} R^n \arrow[r, "f_A"] \arrow[d, "\Phi_{\mathcal{B}}"', "\cong"] & R^n \arrow[d, "\Phi_{\mathcal{B}}"', "\cong"] \\ V \arrow[r, "f"] & V \end{tikzcd}$$

Korollar N1J: Endomorphismenring und Automorphismengruppe

Sei V ein rechtslinearer Raum über R mit Basis $\mathcal{B} = (b_i)_{i=1}^n$.

(1) Das obige Bijektionspaar ist ein Isomorphismus von Ringen:

$$(\mathrm{L}_{\mathcal{B}}^{\mathcal{B}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}) : (R^{n\times n}, +, 0_{n\times n}, \cdot, 1_{n\times n}) \cong (\mathrm{End}_R(V), +, 0, \circ, \mathrm{id}_V)$$

(2) Insbesondere ist dies ein Isomorphismus von Gruppen:

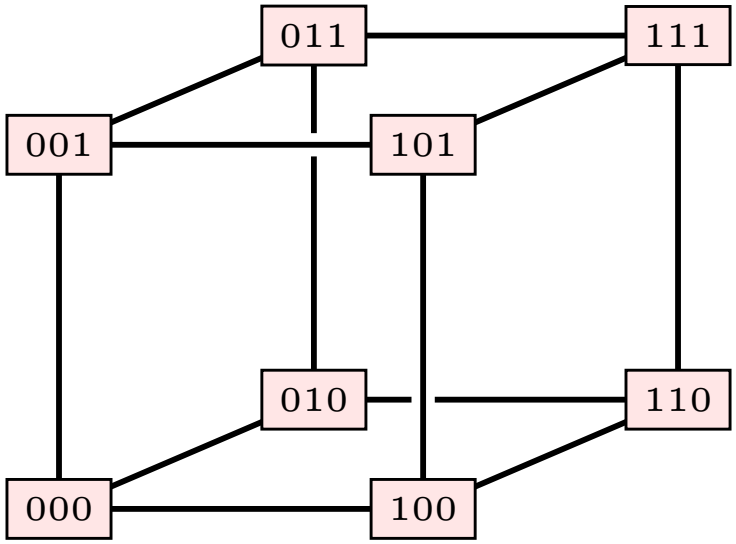
$$(\mathrm{L}_{\mathcal{B}}^{\mathcal{B}}, \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}) : (\mathrm{GL}_n R, \cdot, 1_{n\times n}) \cong (\mathrm{Aut}_R(V), \circ, \mathrm{id}_V)$$

Darstellung von Endomorphismen und Automorphismen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir betrachten $(\mathbb{F}_2^3, +)$:



Aufgabe: Wie viele Elemente haben $\mathrm{End}(\mathbb{F}_2^3, +)$ und $\mathrm{Aut}(\mathbb{F}_2^3, +)$? **Lösung:**

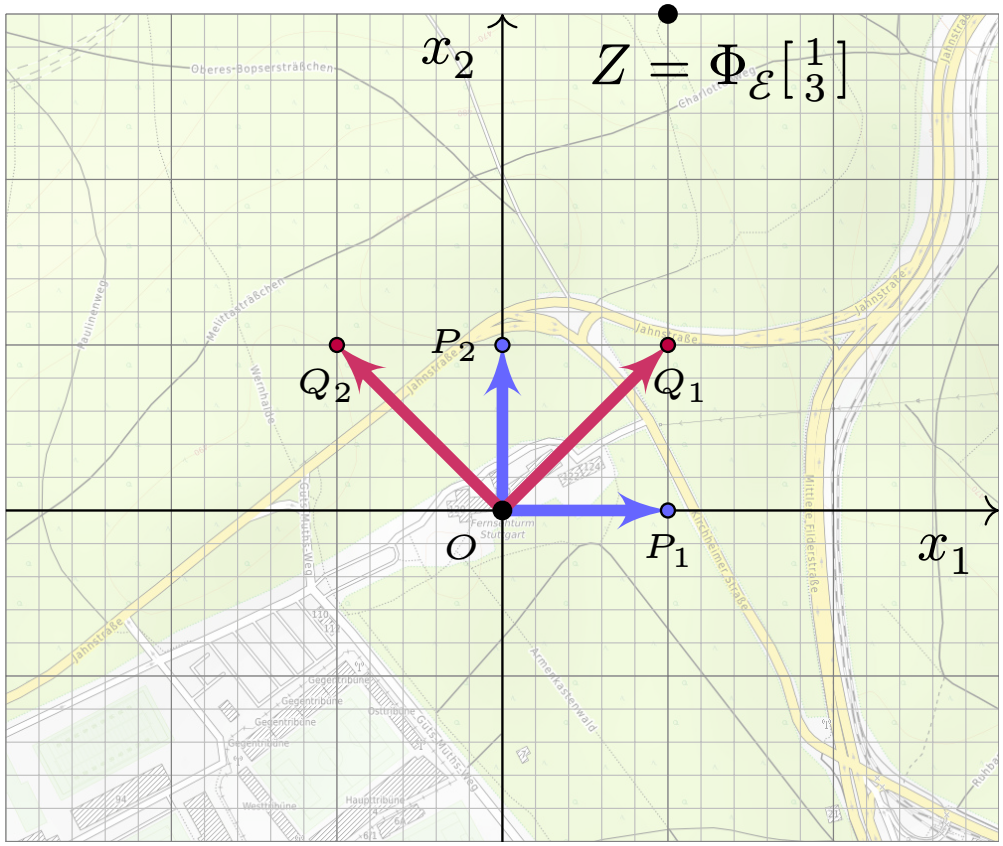
$$\mathrm{End}_{\mathbb{F}_2}(\mathbb{F}_2^3, +) \overset{\text{N1J}}{\cong} \mathbb{F}_2^{3\times 3} \quad \Longrightarrow \quad \sharp\,\mathrm{End}_{\mathbb{F}_2}(\mathbb{F}_2^3, +) \;=\; 2^9 = 512$$

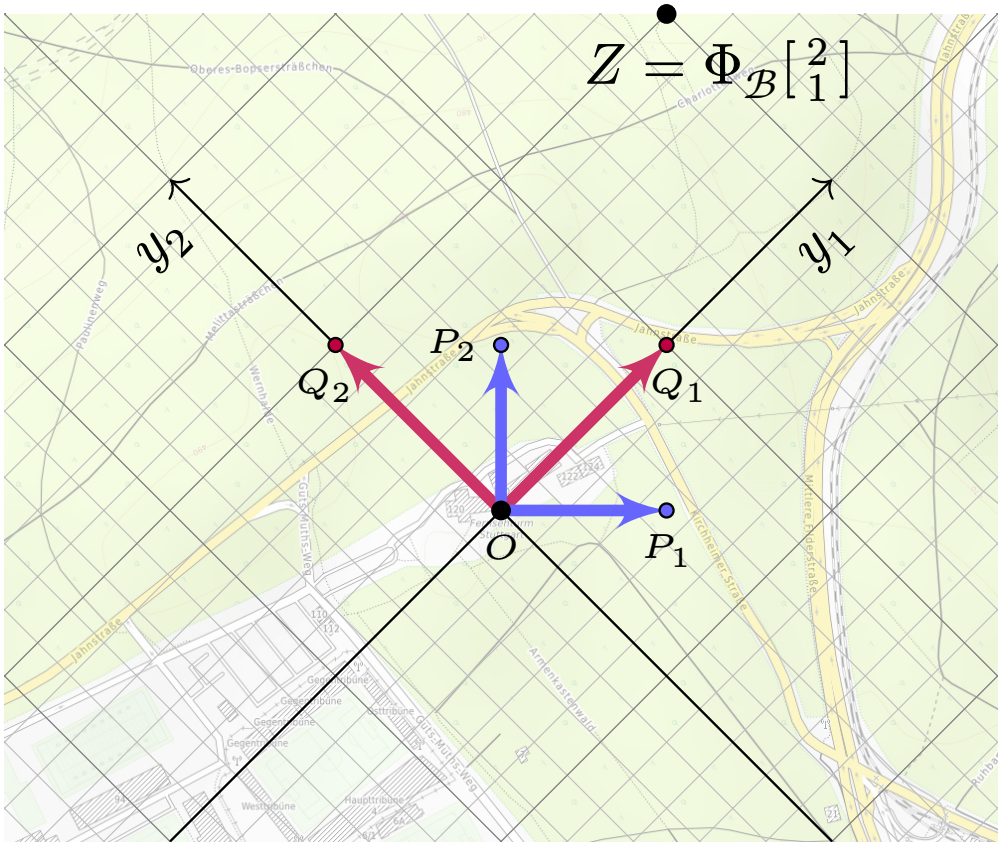
$$\mathrm{Aut}_{\mathbb{F}_2}(\mathbb{F}_2^3, +) \overset{\text{N1J}}{\cong} \mathrm{GL}_3\,\mathbb{F}_2 \quad \Longrightarrow \quad \sharp\,\mathrm{Aut}_{\mathbb{F}_2}(\mathbb{F}_2^3, +) \overset{\text{M342}}{=} 7 \cdot 6 \cdot 4 \;=\; 168$$

Basiswechsel und Koordinatentransformation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Aufgabe: Wir betrachten den linearen Raum $\mathbb{R}^2$ über $\mathbb{R}$ 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 $v = e_1 x_1 + e_2 x_2$ mit $x \in \mathbb{R}^2$ und ebenso $v = b_1 y_1 + b_2 y_2$ mit $y \in \mathbb{R}^2$. Wie rechnen Sie x und y um?

Basiswechsel und Koordinatentransformation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd} R^n \arrow[rr, shift left, "\mathrm{T}_{\mathcal{B}}^{\mathcal{C}}"] \arrow[dr, shift left, "\cong"] & & R^n \arrow[ll, shift left, "\mathrm{T}_{\mathcal{C}}^{\mathcal{B}}"] \arrow[dl, shift left, "\cong"] \\ & V \arrow[ul, shift left, "\Phi_{\mathcal{B}}"] \arrow[ur, shift left, "\Phi_{\mathcal{C}}"] & \end{tikzcd}$$

$$\begin{tikzcd} x \arrow[rr, shift left, mapsto, "y=Tx"] \arrow[dr, shift left] & & y \arrow[ll, shift left, mapsto, "x=T^{-1}y"] \arrow[dl, shift left] \\ & v & \end{tikzcd}$$

Die Umrechnung von $\mathcal{B}$ nach $\mathcal{C}$ leistet die **Basiswechselmatrix**

$$\mathrm{T}_{\mathcal{B}}^{\mathcal{C}} := \mathrm{M}(\Phi_{\mathcal{C}}^{-1} \circ \mathrm{id}_V \circ \Phi_{\mathcal{B}}) = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(\mathrm{id}_V).$$

Zur Berechnung schreiben wir die Startbasis $\mathcal{B}$ in der Zielbasis $\mathcal{C}$:

$$\mathrm{id}_V(b_j) = \sum_{i=1}^{n} c_i t_{ij} \quad \Longrightarrow \quad T = \mathrm{T}_{\mathcal{B}}^{\mathcal{C}} = (t_{ij}) \in \mathrm{GL}_n\, R$$

Basiswechsel und Koordinatentransformation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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:

$$\left.\begin{aligned} b_1 &= 1e_1 + 1e_2 \\ b_2 &= -1e_1 + 1e_2 \end{aligned}\right\} \quad \Longrightarrow \quad \mathrm{T}_{\mathcal{B}}^{\mathcal{E}} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

Für $\mathrm{T}_{\mathcal{E}}^{\mathcal{B}}$ schreiben wir die Startbasis $\mathcal{E}$ in der Zielbasis $\mathcal{B}$ (LGS / Gauß):

$$\left.\begin{aligned} e_1 &= \tfrac{1}{2}b_1 - \tfrac{1}{2}b_2 \\ e_2 &= \tfrac{1}{2}b_1 + \tfrac{1}{2}b_2 \end{aligned}\right\} \quad \Longrightarrow \quad \mathrm{T}_{\mathcal{E}}^{\mathcal{B}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

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!

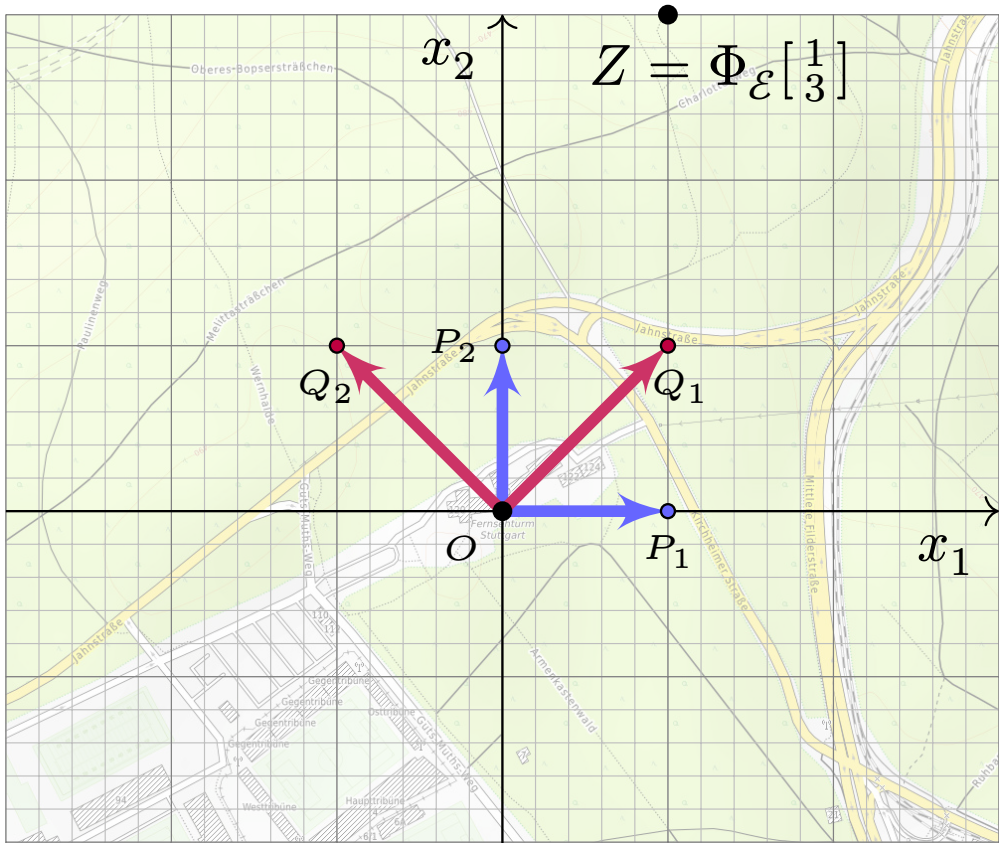
Beispiel:

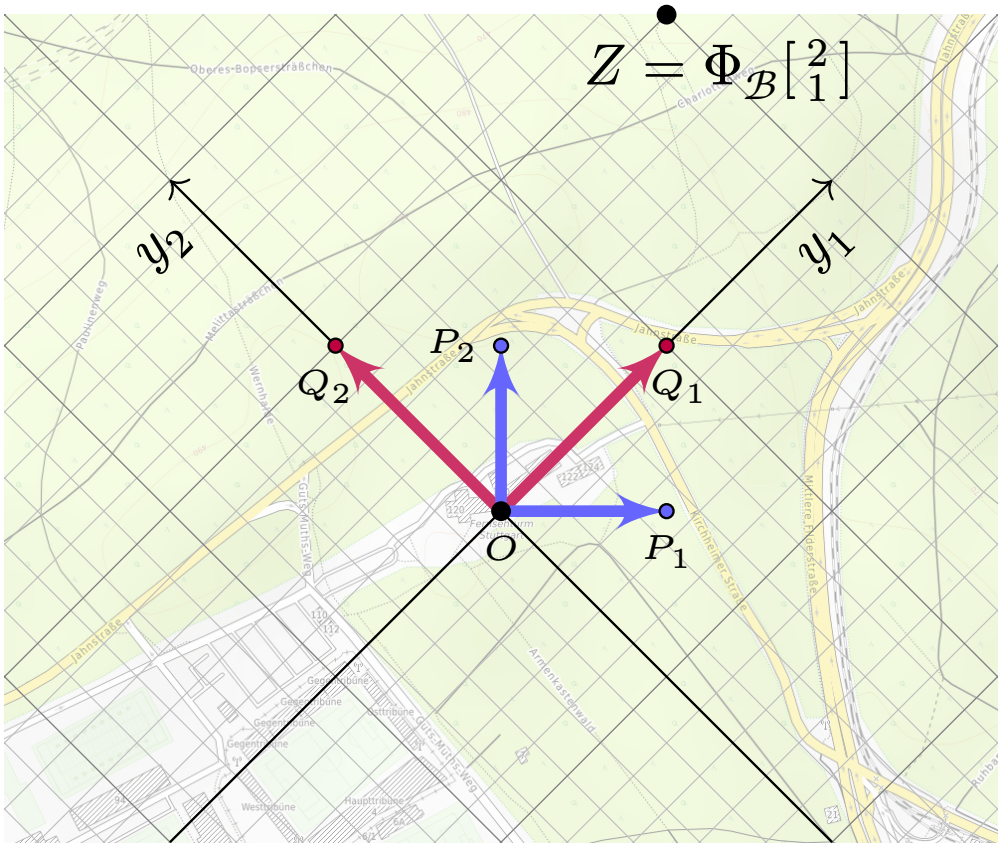
$$\mathrm{T}_{\mathcal{E}}^{\mathcal{B}} \cdot \Phi_{\mathcal{E}}^{-1}(Z) = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \Phi_{\mathcal{B}}^{-1}(Z)$$

Basiswechsel und Koordinatentransformation

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





Jeder Vektor $v \in \mathbb{R}^2$ schreibt sich eindeutig als $v = e_1 x_1 + e_2 x_2$ mit $x \in \mathbb{R}^2$ und ebenso $v = b_1 y_1 + b_2 y_2$ mit $y \in \mathbb{R}^2$. 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 Transformationsformel

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{tikzcd}
R^n \arrow[rrr, "A = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f)"] \arrow[dr, "\Phi_{\mathcal{B}}", "\cong"'] \arrow[dd, shift right, "\mathrm{T}_{\mathcal{B}}^{\mathcal{B}'}", "\cong"'] & & & R^m \arrow[dl, "\Phi_{\mathcal{C}}", "\cong"'] \arrow[dd, shift right, "\mathrm{T}_{\mathcal{C}}^{\mathcal{C}'}", "\cong"'] \\
& V \arrow[r, "f"] & W & \\
R^n \arrow[ur, "\Phi_{\mathcal{B}'}", "\cong"'] \arrow[uu, shift right, "\mathrm{T}_{\mathcal{B}'}^{\mathcal{B}}", "\cong"'] \arrow[rrr, "A' = \mathrm{M}_{\mathcal{B}'}^{\mathcal{C}'}(f)"'] & & & R^m \arrow[ul, "\Phi_{\mathcal{C}'}", "\cong"'] \arrow[uu, shift right, "\mathrm{T}_{\mathcal{C}'}^{\mathcal{C}}", "\cong"']
\end{tikzcd}
$$

$$\boxed{\mathrm{M}_{\mathcal{B}'}^{\mathcal{C}'}(f) = \mathrm{T}_{\mathcal{C}}^{\mathcal{C}'} \cdot \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f) \cdot \mathrm{T}_{\mathcal{B}'}^{\mathcal{B}}}$$

Matrixumformung als Basiswechsel

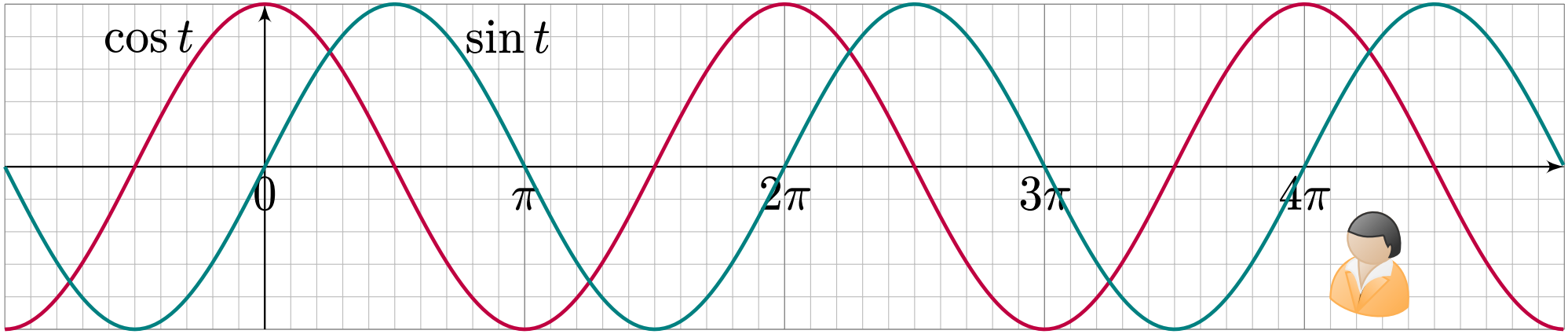
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

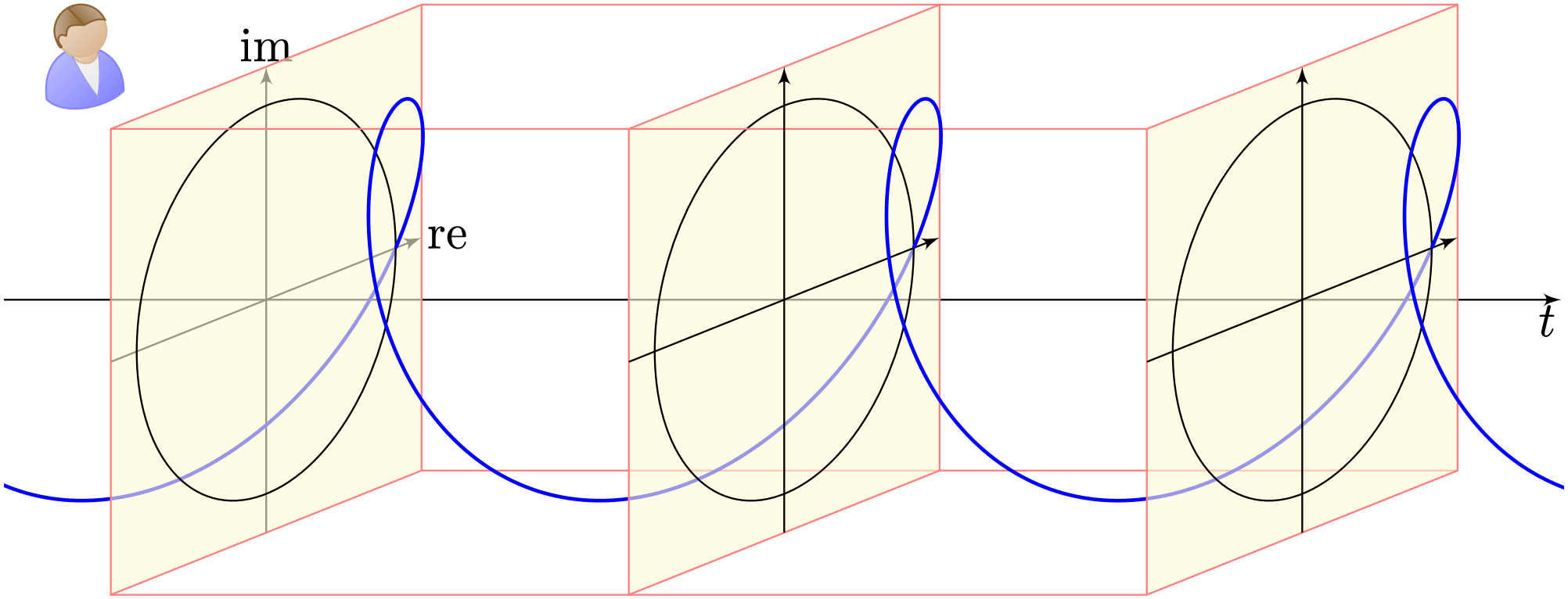
$$
\begin{tikzcd}
R^n \arrow[rr, "A = \mathrm{M}_{\mathcal{B}}^{\mathcal{C}}(f)"'] \arrow[dr, "\Phi_{\mathcal{B}}", "\cong"'] \arrow[dd, shift right, "T^{-1}", "\cong"'] & & R^m \arrow[dl, "\Phi_{\mathcal{C}}"', "\cong"] \arrow[dd, shift right, "S^{-1}", "\cong"'] \\
& V \arrow[r, "f"] & W \\
R^n \arrow[rr, "A' = S^{-1}AT"] \arrow[ur, shift right, "T", "\cong"'] \arrow[ur, "\Phi_{\mathcal{B}'}", "\cong"'] & & R^m \arrow[ul, shift right, "S", "\cong"'] \arrow[ul, "\Phi_{\mathcal{C}'}", "\cong"']
\end{tikzcd}
$$

$$A \cong A' = S^{-1}AT \quad \text{mit} \quad \mathcal{B}' = \mathcal{B}T \quad \text{und} \quad \mathcal{C}' = \mathcal{C}S$$

Erinnerung: die komplexe Exponentialfunktion



$$g : \mathbb{R} \to \mathbb{C} : t \mapsto \mathrm{e}^{\mathrm{i}t} = \cos t + \mathrm{i} \sin t$$



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Basiswechsel zur Diagonalisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{aligned} V &= \langle \cos, \sin \rangle_{\mathbb{C}}^{!} &&= \{ f : \mathbb{R} \to \mathbb{C} : t \mapsto a_1 \cos(t) + a_2 \sin(t) \mid a_1, a_2 \in \mathbb{C} \} \\ &= \langle g, \overline{g} \rangle_{\mathbb{C}}^{!} &&= \{ f : \mathbb{R} \to \mathbb{C} : t \mapsto c_1 \, \mathrm{e}^{\mathrm{i}t} + c_2 \, \mathrm{e}^{-\mathrm{i}t} \mid c_1, c_2 \in \mathbb{C} \} \end{aligned}$$

Aufgabe: (1) Stellen Sie die Ableitung $\partial : V \to V$ in diesen Basen dar. (2) Berechnen Sie die Basiswechselmatrizen. (3) Machen Sie die Probe.

Lösung: (1) Wir nutzen die Basen $\mathcal{A} = (\cos, \sin)$ und $\mathcal{B} = (g, \overline{g})$ von V.
(1a) Wir finden $\cos' = -\sin$ und $\sin' = \cos$. Die darstellende Matrix ist:

$$A = \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

(1b) Wir finden $g' = \mathrm{i}g$ und $\overline{g}' = -\mathrm{i}\overline{g}$. Die darstellende Matrix ist also:

$$B = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix}$$

Basiswechsel zur Diagonalisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(2a) Für $\mathrm{T}_{\mathcal{B}}^{\mathcal{A}}$ schreiben wir die Startbasis $\mathcal{B}$ in der Zielbasis $\mathcal{A}$:

$$\left.\begin{aligned} g(t) &= 1\cos(t) + \mathrm{i}\sin(t) \\ \overline{g}(t) &= 1\cos(t) - \mathrm{i}\sin(t) \end{aligned}\right\} \quad \Longrightarrow \quad \mathrm{T}_{\mathcal{B}}^{\mathcal{A}} = \begin{bmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{bmatrix} = T$$

(2b) Für $\mathrm{T}_{\mathcal{A}}^{\mathcal{B}}$ schreiben wir die Startbasis $\mathcal{A}$ in der Zielbasis $\mathcal{B}$:

$$\left.\begin{aligned} \cos(t) &= \tfrac{1}{2}g(t) + \tfrac{1}{2}\overline{g}(t) \\ \sin(t) &= \tfrac{1}{2\mathrm{i}}g(t) - \tfrac{1}{2\mathrm{i}}\overline{g}(t) \end{aligned}\right\} \quad \Longrightarrow \quad \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2\mathrm{i}} \\ \frac{1}{2} & \frac{-1}{2\mathrm{i}} \end{bmatrix} = T^{-1}$$

(3) Probe! (3a) Gilt $\mathrm{T}_{\mathcal{B}}^{\mathcal{A}} \cdot \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} \overset{?!}{=} 1_{2\times 2}$? und $\mathrm{T}_{\mathcal{A}}^{\mathcal{B}} \cdot \mathrm{T}_{\mathcal{B}}^{\mathcal{A}} \overset{?!}{=} 1_{2\times 2}$?

(3b) Einsetzen in die Transformationsformel $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \mathrm{T}_{\mathcal{A}}^{\mathcal{B}} \cdot \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) \cdot \mathrm{T}_{\mathcal{B}}^{\mathcal{A}}$:

$$\begin{bmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix} \overset{?!}{=} \begin{bmatrix} \frac{1}{2} & \frac{1}{2\mathrm{i}} \\ \frac{1}{2} & \frac{-1}{2\mathrm{i}} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{bmatrix}$$

Basiswechsel zur Diagonalisierung

$$
\begin{tikzcd}
R^n \arrow[rr, "A=\mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f)"'] \arrow[dr, "\Phi_{\mathcal{A}}", "\cong"'] \arrow[dd, shift left, "T=\mathrm{T}_{\mathcal{B}}^{\mathcal{A}}"', "\cong"] & & R^n \arrow[dl, "\Phi_{\mathcal{A}}"', "\cong"] \arrow[dd, shift right, "\mathrm{T}_{\mathcal{B}}^{\mathcal{A}}"', "\cong"] \\
& V \arrow[r, "f"] & V \\
R^n \arrow[rr, "B=\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f)"'] \arrow[ur, "\Phi_{\mathcal{B}}"', "\cong"] \arrow[uu, shift left, "\mathrm{T}_{\mathcal{A}}^{\mathcal{B}}"', "\cong"] & & R^n \arrow[ul, "\Phi_{\mathcal{B}}"', "\cong"] \arrow[uu, shift right, "\mathrm{T}_{\mathcal{A}}^{\mathcal{B}}=T^{-1}"', "\cong"]
\end{tikzcd}
$$

$$B = T^{-1}AT$$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Diagonalisierung eines Endomorphismus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition N3A: Diagonalisierung eines Endomorphismus

(1) Sei $f : V \to V$ linear über R. Eine **diagonalisierende Basis** zu f ist eine Basis $\mathcal{B} = (b_i)_{i=1}^n$ von V, für die die darstellende Matrix von f diagonal ist:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \operatorname{diag}(\lambda_1, \dots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}$$

Das bedeutet:

$$f(b_i) = b_i \lambda_i$$

Eine solche Basis $\mathcal{B} = (b_i)_{i \in I}$ von V über R nennen wir **Eigenbasis** zu f. Existiert zu f eine Eigenbasis $\mathcal{B}$ von V, so nennen wir f **diagonalisierbar**.

Diagonalisierung einer Matrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition N3A: Diagonalisierung einer Matrix

(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:

$$T^{-1}AT = \mathrm{diag}(\lambda_1, \dots, \lambda_n) = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}$$

D.h. die Spalten der Matrix $T = (v_1, \dots, v_n)$ sind eine Eigenbasis von f_A.

Eigenvektoren – Eigenwerte – Eigenräume

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition N3B: Eigenvektoren, Eigenwerte, Eigenräume

(1) Sei $f : V \to V$ linear über R. Ein **Eigenpaar** (v, λ) von f besteht aus einem Vektor $v \in V \setminus \{0\}$ und einem Skalar $\lambda \in R$, die $f(v) = v\lambda$ erfüllen. Wir nennen dann $v \neq 0$ einen **Eigenvektor** und λ einen **Eigenwert** von f.

(2) Zu jedem Skalar $\lambda \in R$ definieren wir den zugehörigen **Eigenraum**

$$\mathrm{E}(\lambda) \;=\; \mathrm{Eig}(f, \lambda) \;:=\; \{v \in V \mid f(v) = v\lambda\} \;\overset{!}{=}\; \mathrm{Ker}(f - \mathrm{id}_V \lambda).$$

Genau dann ist $\lambda \in R$ ein Eigenwert von f, wenn $\mathrm{E}(\lambda) \neq \{0\}$ gilt.

Immer gilt $0 \in \mathrm{E}(\lambda)$. Für jeden Vektor $v \in V$ gilt folgende Äquivalenz:

$$f(v) = v\lambda \quad \Longleftrightarrow \quad f(v) - \mathrm{id}_V(v)\lambda = 0 \quad \Longleftrightarrow \quad (f - \mathrm{id}_V \lambda)(v) = 0$$

Für alle Vektoren $u, v \in \mathrm{E}(\lambda)$ und zentralen Skalare $\rho \in Z(R) \leq R$ gilt:

$$f(u+v) \overset{\text{Add}}{=} f(u) + f(v) \overset{\text{Eig}}{=} u\lambda + v\lambda \overset{\text{Dst}}{=} (u+v)\lambda \implies u + v \in \mathrm{E}(\lambda)$$
$$f(v \cdot \rho) \overset{\text{Lin}}{=} f(v) \cdot \rho \overset{\text{Eig}}{=} v\lambda \cdot \rho \overset{\text{Znt}}{=} (v \cdot \rho)\lambda \implies v \cdot \rho \in \mathrm{E}(\lambda)$$

Somit ist $\mathrm{E}(\lambda) \leq V$ ein linearer Unterraum über dem Zentrum $Z(R) \leq R$.

Warum wir hier über einem Körper K arbeiten sollten...

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

? Über welchen Ringen können wir effizient diagonalisieren?

- Wir benötigen einen Divisionsring R für Gauß, Basis, Dimension, etc.
- Wir benötigen Kommutativität, daher das Zentrum $K := Z(R) \leq R$.

Vereinbarung: Für den Rest des Kapitels sei K ein Körper und

$$\boxed{\lambda \cdot v = v \cdot \lambda \text{ für } v \in V \text{ und } \lambda \in K.}$$

Diagonalisierung – Eigenbasis – Eigenraumzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele:
Für $\lambda = 0$ ist $\operatorname{Eig}(f, 0) = \operatorname{Ker}(f)$ der Kern der Abbildung $f : V \to V$.
Für $\lambda = 1$ ist $\operatorname{Eig}(f, 1) = \operatorname{fix}(f)$ die Fixpunktmenge von $f : V \to V$.

Satz N3c: Diagonalisierung, Eigenbasis, Eigenraumzerlegung

Sei $f : V \to V$ linear über dem Körper K. Äquivalent sind:

1. Der Endomorphismus $f \in \operatorname{End}_K(V)$ ist **diagonalisierbar**.
2. Es existert eine Basis aus Eigenvektoren, kurz **Eigenbasis**.
3. Der Raum $V \overset{!}{=} \bigoplus_{\lambda \in K} \operatorname{Eig}(f, \lambda)$ ist Summe der **Eigenräume**.

Beweis: Die Äquivalenz „(1) $\Leftrightarrow$ (2)“ ist klar nach Definition N3A.
„(3) $\Rightarrow$ (2)“: Wähle je eine (Eigen)Basis $\mathcal{B}_\lambda$ von $\mathrm{E}(\lambda) \leq V$ dank M2K und erhalte daraus die Eigenbasis $\mathcal{B} = \bigsqcup_{\lambda \in K} \mathcal{B}_\lambda$ von V dank M2T.
„(2) $\Rightarrow$ (3)“: Umgekehrt, sortiere die Eigenbasis $\mathcal{B} \overset{!}{=} \bigsqcup_{\lambda \in K} \mathcal{B}_\lambda$. QED

Eigenvektor oder nicht?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Welche Vektoren $v_1, \dots, v_5$ sind Eigenvektoren der Matrix A?

$$A = \begin{bmatrix} -9 & 27 & -22 \\ -2 & 6 & -4 \\ 2 & -6 & 6 \end{bmatrix} \in \mathbb{R}^{3\times 3}, \qquad \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Lösung: Gemäß Definition N3B prüfen wir, ob $Av \overset{?}{=} \lambda v$ gilt:

$$A \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 9 \\ 2 \\ -2 \end{bmatrix}, \quad \text{also kein EV.} \qquad A \begin{bmatrix} 3 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \quad \text{EV zu } \lambda = 0.$$

$$A \begin{bmatrix} 2 \\ 0 \\ -1 \end{bmatrix} = \begin{bmatrix} 4 \\ 0 \\ -2 \end{bmatrix}, \quad \text{EV zu } \lambda = 2. \qquad A \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, \quad \text{EV zu } \lambda = 1.$$

Damit finden wir eine Eigenbasis und diagonalisierenden Basiswechsel:

$$T = \begin{bmatrix} 3 & 2 & 1 \\ 1 & 0 & 2 \\ 0 & -1 & 2 \end{bmatrix}, \quad T^{-1} = \begin{bmatrix} 2 & -5 & 4 \\ -2 & 6 & -5 \\ -1 & 3 & -2 \end{bmatrix}, \quad T^{-1}AT = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Geometrisches Beispiel: Basiswechsel zur Diagonalisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Sei $V = \mathbb{R}^2$. Zum Spaltenvektor $v = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right] \in \mathbb{R}^2$ betrachten wir

$$f : \mathbb{R}^2 \to \mathbb{R}^2 : x \mapsto x - v \cdot v^\top \cdot x.$$

(1a) Ist diese Abbildung $f : V \to V$ linear über $\mathbb{R}$?
(1b) Schreiben Sie f als Matrix A bezüglich der Standardbasis.

(2) Finden Sie eine / die minimale Relation zwischen $f^0, f^1, f^2, f^3, \ldots$.

Zu $f : \mathbb{R}^2 \to \mathbb{R}^2$ und $\lambda \in \mathbb{R}$ untersuchen wir den **Eigenraum**

$$\boxed{\mathrm{E}(\lambda) := \left\{ x \in \mathbb{R}^2 \;\middle|\; f(x) = \lambda x \right\}.}$$

(3) Bestimmen Sie Basen für $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$.

(4a) Erhalten Sie so eine direkte Summe $\mathrm{E}(+1) \oplus \mathrm{E}(-1) = \mathbb{R}^2$?
(4b) Setzen Sie die Basen aus (3) zu einer Basis $\mathcal{B}$ von $\mathbb{R}^2$ zusammen.
(4c) Schreiben Sie f als Matrix bezüglich dieser Eigenbasis $\mathcal{B}$.

(5a) Zeichnen Sie $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$ in der Ebene $\mathbb{R}^2$.
(5b) Erklären Sie die Wirkung von f geometrisch.

Geometrisches Beispiel: Basiswechsel zur Diagonalisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lösung: Zum Spaltenvektor $v = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right]$ betrachten wir

$$f : \mathbb{R}^2 \to \mathbb{R}^2 : x \mapsto x - v \cdot v^\intercal \cdot x.$$

(1a) Ja, die Abbildung f ist linear, wie wir direkt nachrechnen:

$$f(x\lambda + y\mu) = \cdots\ldots = f(x)\lambda + f(y)\mu \quad \text{für alle } x, y \in \mathbb{R}^2 \text{ und } \lambda, \mu \in \mathbb{R}.$$

(1b) Wir berechnen die Bilder der Basisvektoren:

$$\left.\begin{aligned} f(e_1) &= \cdots\ldots = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = 0 \cdot e_1 + 1 \cdot e_2 \\ f(e_2) &= \cdots\ldots = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = 1 \cdot e_1 + 0 \cdot e_2 \end{aligned}\right\} \implies A = \mathrm{M}_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Geometrisches Beispiel: Basiswechsel zur Diagonalisierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(2) Statt $f^0, f^1, f^2, \ldots \in \mathrm{End}_{\mathbb{R}}(V)$ untersuchen wir $A^0, A^1, A^2, \ldots \in \mathbb{R}^{2\times 2}$:

$$A^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad A^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1 \cdot A^0 + 0 \cdot A^1$$

Demnach gilt $A^2 - A^0 = 0$ in $\mathbb{R}^{2\times 2}$, also $f^2 - f^0 = 0$ in $\mathrm{End}_{\mathbb{R}}(V)$, (Minimal)Polynom $P = \mu_f := X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$.

(3) Wir bestimmen die Unterräume $\mathrm{E}(+1)$ und $\mathrm{E}(-1)$ wie folgt:

$$\mathrm{E}(+1) = \mathrm{Ker}(f - \mathrm{id}) = \mathrm{Ker} \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} = \mathbb{R}\, b_1 \quad \text{mit} \quad b_1 := \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\mathrm{E}(-1) = \mathrm{Ker}(f + \mathrm{id}) = \mathrm{Ker} \begin{bmatrix} +1 & 1 \\ 1 & +1 \end{bmatrix} = \mathbb{R}\, b_2 \quad \text{mit} \quad b_2 := \begin{bmatrix} -1 \\ 1 \end{bmatrix}$$

(4) Wir erhalten so zu f die Eigenbasis $\mathcal{B} = (b_1, b_2)$ von $\mathbb{R}^2$.
Nach Konstruktion gilt $f(b_1) = +1 \cdot b_1$ und $f(b_2) = -1 \cdot b_2$, also

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Geometrisches Beispiel: Basiswechsel zur Diagonalisierung

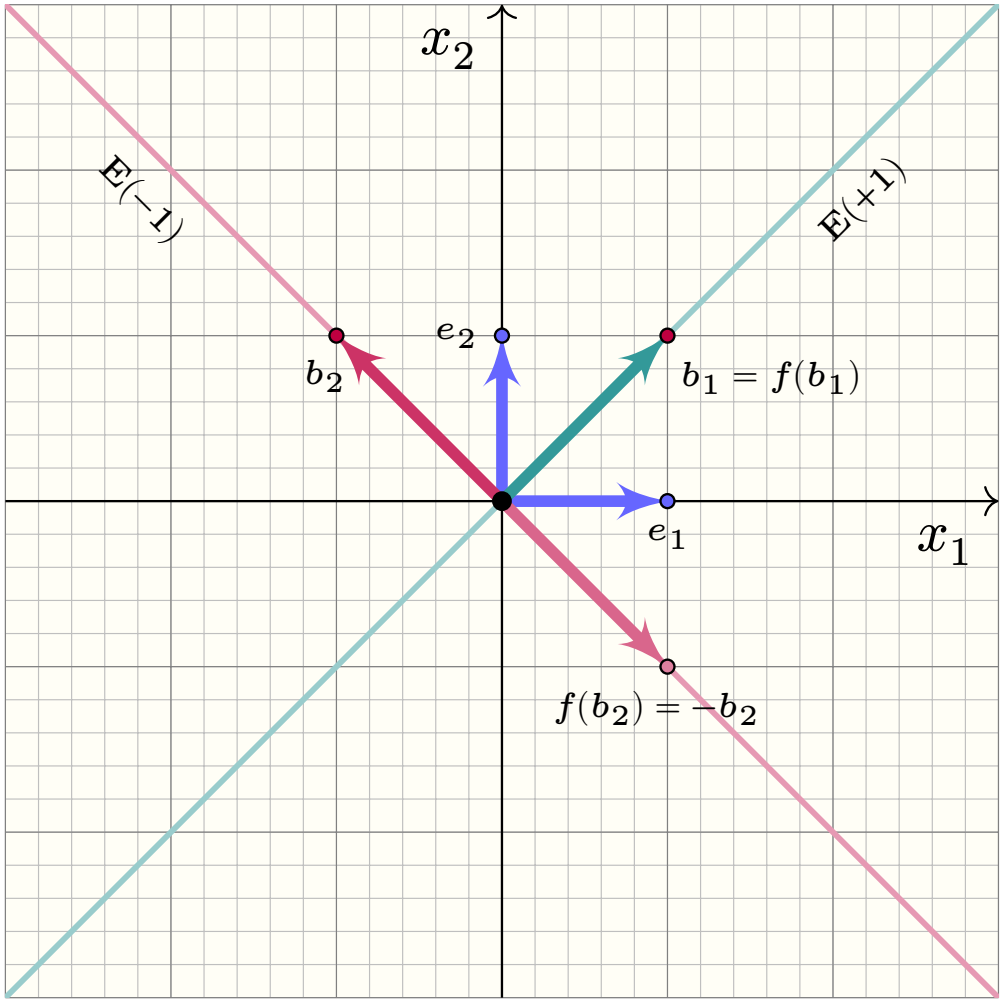
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(5) In der Eigenbasis $\mathcal{B} = (b_1, b_2)$ können wir die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$ einfach darstellen und besser verstehen… dank Eigenraumzerlegung!

$$\mathrm{M}_{\mathcal{E}}^{\mathcal{E}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$ ist die Spiegelung an der Hauptdiagonalen.

Polynome von Endomorphismen und Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Weiterhin sei K ein Körper. Wir betrachten ein Polynom

$$P = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \in K[X].$$

Für X können wir jeden Endomorphismus $f \in \mathrm{End}_K(V)$ einsetzen:

$$P(f) = a_0 \,\mathrm{id}_V + a_1 f + a_2 f^2 + \ldots + a_n f^n \in \mathrm{End}_K(V)$$

Das Polynom P **annulliert** f in $v \in V$, falls $P(f)(v) = 0$ gilt.
Das Polynom P **annulliert** f auf ganz V, falls $P(f) = 0$ gilt.

Beispiele: Im Ring $(\mathrm{End}_K(V), +, \circ)$ betrachten wir:

$$f^2 = f \iff f^2 - f = 0 \iff f \circ (f - \mathrm{id}_V) = 0$$

Das bedeutet, $P = X^2 - X = X(X-1)$ annulliert f, kurz $P(f) = 0$.

$$f^2 = \mathrm{id}_V \iff f^2 - \mathrm{id}_V = 0 \iff (f - \mathrm{id}_V) \circ (f + \mathrm{id}_V) = 0$$

Das bedeutet, $Q = X^2 - 1 = (X-1)(X+1)$ annulliert f, kurz $Q(f) = 0$.

Das lokale Minimalpolynom μ_f^v

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition N3D: das lokale Minimalpolynom $\mu_f^v = \mathrm{MiPo}_f^v$

Sei K ein Körper und $f \in \mathrm{End}_K(V)$, etwa $V = K^n$ und $f(x) = Ax$ mit $A \in K^{n\times n}$. Jeder Vektor $v \in V$ erzeugt seinen **f–zyklischen Unterraum**

$$Z = Z(v) := \langle f^n(v) \,|\, n \in \mathbb{N} \rangle_K \leq V,$$
$$\dim_K(Z) = m := \sup\{ n \in \mathbb{N} \,|\, f^0(v), \dots, f^{n-1}(v) \text{ linear unabhängig} \}.$$

(0) Im Falle $m = \infty$ ist $(f^n(v))_{n\in\mathbb{N}}$ eine Basis von Z. Wir setzen $\mu_f^v := 0$.

(1) Im Falle $m \in \mathbb{N}$ ist $(f^n(v))_{n<m}$ eine Basis von Z. Wir erhalten daraus

$$a_0 f^0(v) + \dots + a_{m-1} f^{m-1}(v) + f^m(v) = 0$$

mit eindeutigen Koeffizienten $a_0, \dots, a_{m-1} \in K$. Damit definieren wir

$$\mu_f^v := a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m \in K[X]_m^1$$

als das **lokale Minimalpolynom** von $f \in \mathrm{End}_K(V)$ bezüglich $v \in V$.

Das (globale) Minimalpolynom μ_f

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition N3E: das (globale) Minimalpolynom $\mu_f = \mathrm{MiPo}_f$

Zu $f \in \mathrm{End}_K(V)$ erzeugen die Potenzen $f^0, f^1, f^2, \ldots$ den Unterraum

$$Z := \langle f^n \mid n \in \mathbb{N} \rangle_K \leq \mathrm{End}_K(V),$$
$$\dim_K(Z) = m := \sup\{n \in \mathbb{N} \mid f^0, \ldots, f^{n-1} \text{ linear unabhängig}\}.$$

(0) Im Falle $m = \infty$ ist $(f^n)_{n\in\mathbb{N}}$ eine Basis von Z. Wir setzen $\mu_f := 0$.

(1) Im Falle $m \in \mathbb{N}$ ist $(f^n)_{n<m}$ eine Basis von Z. Wir erhalten daraus

$$a_0 f^0 + \ldots + a_{m-1} f^{m-1} + f^m = 0$$

mit eindeutigen Koeffizienten $a_0, \ldots, a_{m-1} \in K$. Damit definieren wir

$$\mu_f := a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m \in K[X]^1_m$$

als das (globale) **Minimalpolynom** des Endomorphismus $f \in \mathrm{End}_K(V)$.

Das Minimalpolynom teilt jedes annullierende Polynom.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Minimalität: Sei $P \in K[X]$ mit $P(f) = 0$. Polynomdivision $P = Q\mu_f + R$ ergibt $Q, R \in K[X]$ mit $\deg R < \deg \mu_f$. Auch $R = P - Q\mu_f$ annulliert f, denn $R(f) = 0$. Da $\deg \mu_f$ minimal ist, bleibt nur $R = 0$, also $P = Q\mu_f$.

Satz N3F: Das Minimalpolynom teilt jedes annullierende Polynom.

(1) Lokal sei $I := \{\, P \in K[X] \mid P(f)(v) = 0 \,\}$. Dann gilt $I = \mu_f^v K[X]$.

(2) Global sei $J := \{\, P \in K[X] \mid P(f) \quad = 0 \,\}$. Dann gilt $J = \mu_f K[X]$.

(3) Dank (1) gilt $\mu_f^v \mid \mu_f$. Dank (2) folgt $\mu_f = \mathrm{kgV}(\, \mu_f^v \,;\, v \in V)$.

Kernzerlegung: ein wirkmächtiger Satz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz N3G: Kernzerlegung

Sei $f : V \to V$ linear über dem Körper K, kurz $f \in \operatorname{End}_K(V)$.

(0) Für $P = (X - \lambda_1) \cdots (X - \lambda_n) \in K[X]$ mit $\{\lambda_1, \dots, \lambda_n\}^! \subseteq K$ gilt

$$\operatorname{Ker} P(f) = \operatorname{Ker}(f - \lambda_1) \oplus \dots \oplus \operatorname{Ker}(f - \lambda_n).$$

(1) In $K[X]$ sei $P = P_1 \cdots P_n$ mit $\operatorname{ggT}(P_i, P_j) = 1$ für alle $i \neq j$. Dann folgt

$$\operatorname{Ker} P(f) = \operatorname{Ker} P_1(f) \oplus \dots \oplus \operatorname{Ker} P_n(f).$$

(2) Wenn P zudem f annulliert, $P(f) = 0$, so folgt $\operatorname{Ker} P(f) = V$.
Wenn P dabei einfach zerfällt wie in (0), so ist f diagonalisierbar.

Beispiele: Jeder Projektor $f = f^2$ ist diagonalisierbar, dank Zerlegung

$$P = X^2 - X = X(X - 1) \quad \text{und} \quad V = \mathrm{E}(0) \oplus \mathrm{E}(1) \overset{\text{L3O}}{=} \operatorname{Ker} f \oplus \operatorname{Im} f.$$

Gilt $f^2 = \mathrm{id}_V$ und $\operatorname{char} K \neq 2$, so ist f diagonalisierbar, dank Zerlegung

$$P = X^2 - 1 = (X - 1)(X + 1) \quad \text{und} \quad V = \mathrm{E}(+1) \oplus \mathrm{E}(-1).$$

Kernzerlegung: ein eleganter Beweis

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: Für $U := \operatorname{Ker} P(f)$ gilt $f(U) \subseteq U$; für $v \in U$ gilt $f(v) \in U$, denn

$$P(f)(f(v)) = (PX)(f)(v) = (XP)(f)(v) = f(P(f)(v)) = f(0) = 0.$$

Für P_i und seinen Cofaktor $Q_i := \prod_{j \neq i} P_j$ gilt $P = Q_i P_i = P_i Q_i$, also $\operatorname{Ker} P_i(f) \leq \operatorname{Ker} P(f)$ und $\operatorname{Ker} Q_i(f) \leq \operatorname{Ker} P(f)$. Dank $\operatorname{ggT}(P_i, Q_i) = 1$ und Bézout C3E existieren $P_i^*, Q_i^* \in K[X]$ mit $P_i^* P_i + Q_i^* Q_i = 1$.

Auf $U = \operatorname{Ker} P(f)$ definieren wir $\sigma_i, \pi_i : U \to U$ durch $\sigma_i = P_i^*(f) P_i(f)$ und $\pi_i = Q_i^*(f) Q_i(f)$. Es gilt $\sigma_i + \pi_i = \mathrm{id}_U$ sowie $\sigma_i \circ \pi_i = \pi_i \circ \sigma_i = 0$.

Dank L3O ist U direkte Summe von $\operatorname{Ker} \sigma_i = \operatorname{Im} \pi_i$ und $\operatorname{Ker} \pi_i = \operatorname{Im} \sigma_i$.

$$\begin{array}{ccccccc} \operatorname{Ker} P_i(f) & \leq & \operatorname{Ker} \sigma_i & \overset{\text{L3O}}{=} & \operatorname{Im} \pi_i & \leq & \operatorname{Ker} P_i(f) \\ \operatorname{Ker} Q_i(f) & \leq & \operatorname{Ker} \pi_i & \overset{\text{L3O}}{=} & \operatorname{Im} \sigma_i & \leq & \operatorname{Ker} Q_i(f) \end{array}$$

Daraus folgt die Zerlegung $\operatorname{Ker} P(f) = \operatorname{Ker} P_i(f) \oplus \operatorname{Ker} Q_i(f)$.

Per Induktion folgt $\operatorname{Ker} P(f) = \operatorname{Ker} P_1(f) \oplus \ldots \oplus \operatorname{Ker} P_n(f)$. $\boxed{\text{QED}}$

Lokales Minimalpolynom und Eigenvektorzerlegung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz N3H: lokales Minimalpolynom und Eigenvektorzerlegung

Sei $f : V \to V$ linear über K. Für jeden Vektor $v \in V$ sind äquivalent:

1. Unser Vektor v ist eine Summe von Eigenvektoren:
   $v = v_1 + \ldots + v_n$ mit $f(v_i) = \lambda_i v_i$ und $\{\lambda_1, \ldots, \lambda_n\}^! \subseteq K$.
2. Das Minimalpolynom $\mu_f^v \in K[X]$ zerfällt einfach über K:
   $\mu_f^v \mid P = (X - \lambda_1) \cdots (X - \lambda_n)$ mit $\{\lambda_1, \ldots, \lambda_n\}^! \subseteq K$.

Beweis: „$\Rightarrow$“: P annulliert f in $v_1, \ldots, v_n$, also in v. Dank N3F folgt $\mu_f^v \mid P$.
„$\Leftarrow$“: Das folgt aus der Kernzerlegung N3G für $\operatorname{Ker} P(f) \ni v$. QED

Genau dann ist $f \in \operatorname{End}_K(V)$ diagonalisierbar, also $V = \bigoplus_{\lambda \in K} \operatorname{Eig}(f, \lambda)$, wenn das MiPo $\mu_f^v \in K[X]$ über K einfach zerfällt für jeden Vektor $v \in V$.

Minimalpolynom und Diagonalisierungsverfahren

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz N3H: Minimalpolynom als Diagonalisierungskriterium

Sei K ein Körper und V ein K–Vektorraum endlicher Dimension. Genau dann ist $f \in \mathrm{End}_K(V)$ diagonalisierbar, wenn $\mu_f \in K[X]$ einfach zerfällt.

MiPo-Verfahren N3H: (0) Berechne $\mu_f \in K[X]$, etwa dank Gauß.
(1) Zerfällt $\mu_f = (X - \lambda_1) \cdots (X - \lambda_n)$ mit $\{\lambda_1, \dots, \lambda_n\}^! \subseteq K$, so folgt

$$V = \mathrm{Ker}(f - \lambda_1) \oplus \cdots \oplus \mathrm{Ker}(f - \lambda_n).$$

(2) Wähle darin jeweils Basen und erhalte eine Eigenbasis von V zu f.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel N31: Diagonalisierung in $\mathbb{K}^{2\times 2}$ über $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Berechnen Sie Minimalpolynom und Diagonalisierung soweit möglich:

$$A = \begin{bmatrix} -2 & 6 \\ -2 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$$

Lösung: (A) Wir finden $\mu_A = 2 - 3X + X^2$ dank Gauß–Verfahren (N3D):

$$A^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A^1 = \begin{bmatrix} -2 & 6 \\ -2 & 5 \end{bmatrix}, \quad A^2 = \begin{bmatrix} -8 & 18 \\ -6 & 13 \end{bmatrix}, \quad \begin{bmatrix} 1 & -2 & -8 \\ 0 & -2 & -6 \\ 0 & 6 & 18 \\ 1 & 5 & 13 \end{bmatrix} \xrightarrow{\text{RZSF}} \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Über $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ zerfällt $X^2 - 3X + 2 = (X-1)(X-2)$. Eigenräume:

$$\operatorname{Ker}(A-1) = \operatorname{Ker}\begin{bmatrix} -3 & 6 \\ -2 & 4 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}\mathbb{K}, \quad \operatorname{Ker}(A-2) = \operatorname{Ker}\begin{bmatrix} -4 & 6 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}\mathbb{K},$$

Basiswechsel: $$T = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}, \quad T^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}, \quad T^{-1}AT = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Dies ist nur die Saalversion ohne Erläuterungen.

Kapitel N

Bonusmaterial

$$
\begin{tikzcd}
R^n \arrow[rr, "A=\mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(f)"] \arrow[dr, "\Phi_{\mathcal{A}}", "\cong"'] \arrow[d, shift left, "T=\mathrm{T}_{\mathcal{B}}^{\mathcal{A}}", "\cong"'] & & R^n \arrow[dl, "\Phi_{\mathcal{A}}"', "\cong"] \arrow[d, shift right, "\mathrm{T}_{\mathcal{B}}^{\mathcal{A}}"', "\cong"] \\
V \arrow[u, shift left, "\mathrm{T}_{\mathcal{A}}^{\mathcal{B}}"] \arrow[rr, "f"] & & V \arrow[u, shift right, "\mathrm{T}_{\mathcal{A}}^{\mathcal{B}}=T^{-1}"'] \\
R^n \arrow[ur, "\Phi_{\mathcal{B}}", "\cong"'] \arrow[rr, "B=\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f)"'] & & R^n \arrow[ul, "\Phi_{\mathcal{B}}"', "\cong"]
\end{tikzcd}
$$

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

Ausführliche Erläuterungen bietet die Vollversion.

Inhalt dieses Kapitels N

5 Übungsaufgaben und Anwendungsbeispiele

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel O

Signatur und Determinante

$$\operatorname{sign}(\sigma) = \prod_{\{i \neq j\}} \frac{\sigma(i)-\sigma(j)}{i-j} \in \{\pm 1, 0\}$$

$$\det(A) = \sum_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot \prod_{j=1}^{n} a_{\sigma(j),j}$$

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 O

1 Die Signatur einer endlichen Selbstabbildung

2 Die Determinante einer quadratischen Matrix

3 Geometrische Anwendungen der Determinante

4 Rückblick und Ausblick

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Motivation und Überblick

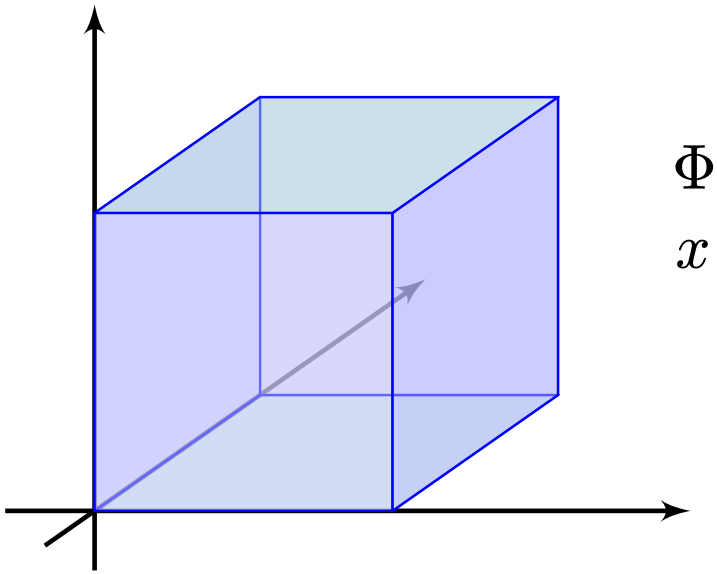
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

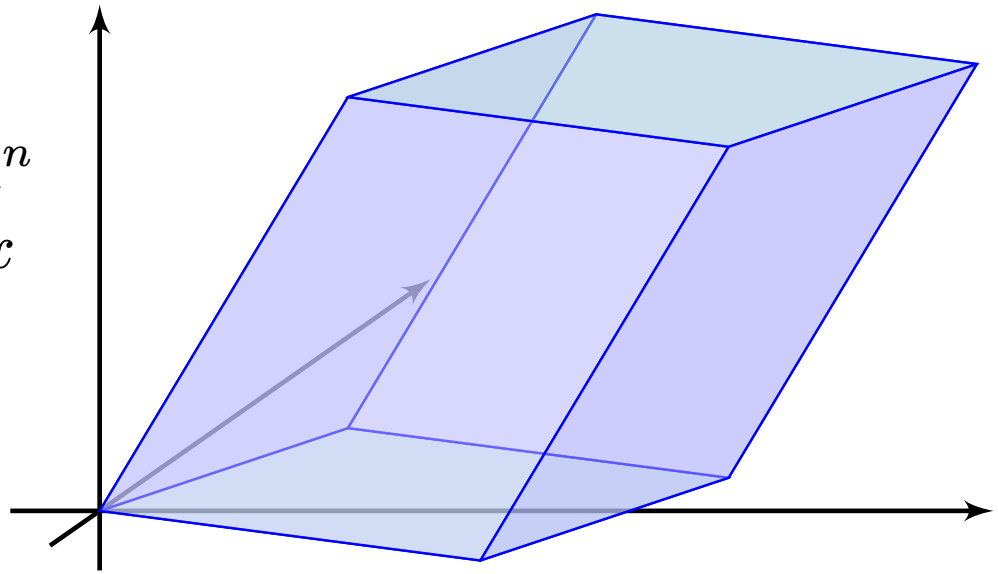
☺ Für 2×2–Matrizen kennen Sie Determinante und Inversion (D1N):

$$\det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = ad - bc, \qquad \begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$

? Gibt es eine ähnliche Formel zur Inversion von Matrizen $A \in \mathbb{K}^{n \times n}$?

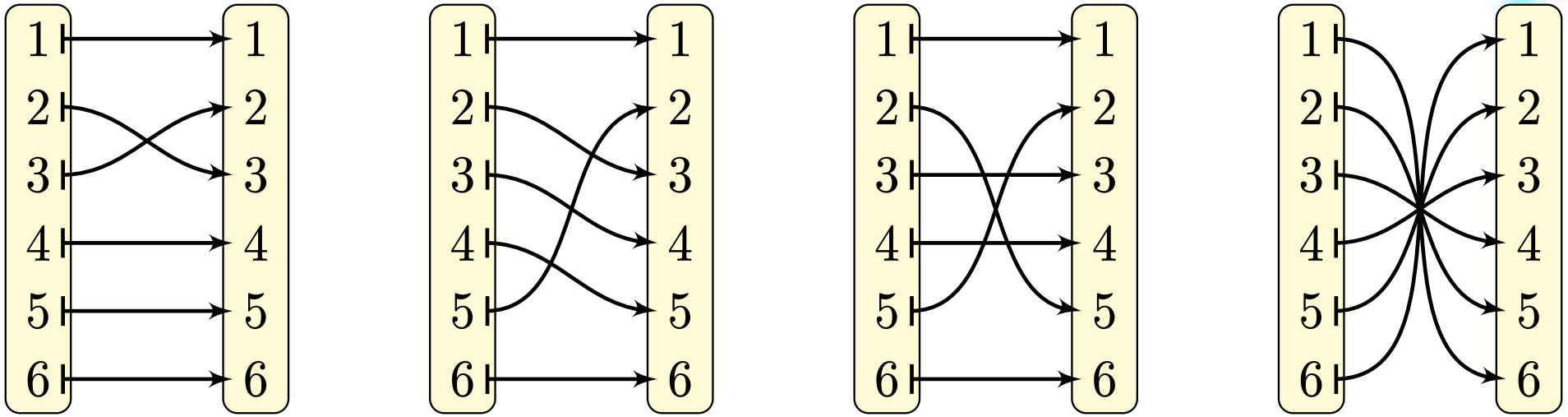


$$\Phi : \mathbb{R}^n \to \mathbb{R}^n$$
$$x \mapsto y = Ax$$



? Wie berechnen wir das n–dimensionale Volumen eines Parallelotops?
Elegante Lösung: die Determinante $\det A = \sum_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot \prod_{j=1}^{n} a_{\sigma(j),j}$.

Anschauliches Beispiel: ein Kartrennen



$\mathrm{inv} = 1$ $\quad$ $\mathrm{inv} = 3$ $\quad$ $\mathrm{inv} = 5$ $\quad$ $\mathrm{inv} = \frac{n(n-1)}{2}$

Aufgabe: Für jeden Kart kennen wir die Startposition $i \in X = \{1, \dots, n\}$ und nach dem Rennen auch die Zielposition $\sigma(i) \in X$, zusammen $\sigma \in \mathrm{S}_n$. (1) Wie viele Überholmanöver gab es mindestens? (2) und tatsächlich?

Lösung: Wir betrachten die Menge der **Inversionen** aka **Fehlstände**:

$$\mathrm{Inv}(\sigma) := \left\{ \{i, j\} \subseteq X \,\middle|\, i < j \wedge \sigma(i) > \sigma(j) \right\}$$

(1) Die Anzahl der Überholmanöver ist mindestens $\mathrm{inv}(\sigma) := \sharp\,\mathrm{Inv}(\sigma)$.
(2) Die tatsächliche Anzahl ist eventuell größer, um eine gerade Zahl!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Anschauliches Beispiel: ein Kartrennen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma O1A: Transpositionen und Inversionen – Prozess und Ergebnis

(1) Es gilt $\quad \sharp\,\text{Überholmanöver} = \sharp\,\mathrm{Inv}(\sigma) + 2n \quad$ mit $n \in \mathbb{N}$.

(2) Es folgt $\quad \mathrm{inv}(\sigma) + \mathrm{inv}(\tau) \equiv \mathrm{inv}(\sigma \bullet \tau) \quad$ modulo 2.

Beweis: (1) Doppeltes Abzählen! Wir betrachten jedes Paar $\{i < j\}$:
(1a) Für $\sigma(i) < \sigma(j)$ gab es $0 + 2n_{ij}$ Überholmanöver, wobei $n_{ij} \in \mathbb{N}$.
(1b) Für $\sigma(i) > \sigma(j)$ gab es $1 + 2n_{ij}$ Überholmanöver, wobei $n_{ij} \in \mathbb{N}$.
Die Gesamtzahl ist somit $\sharp\,\mathrm{Inv}(\sigma) + 2n$ mit $n = \sum_{i<j} n_{ij} \in \mathbb{N}$. QED

Mathematisches Extrakt: Inversionen und Parität

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

„Ein kurioses Rennen! Die Reihenfolge aller sechs Wagen hat sich vom Start zum Ziel komplett umgekehrt. Dennoch war der Verlauf des Rennens eher langweilig, mit insgesamt nur 13 Überholmanövern.“ – „Nein, es waren 30.“

Aufgabe: Ist das möglich? **Lösung:** Nein, denn $\operatorname{inv}(\sigma) = \binom{6}{2} = \frac{6\cdot 5}{2} = 15$. Möglich wären $15, 17, 19, 21, 23, \ldots$ Überholmanöver, niemals 13 oder 30.

Definition O1B: Inversionen und Parität einer Permutation

Zu jeder Permutation $\sigma \in \mathrm{S}_n$ definieren wir ihre **Parität**

$$\varepsilon : \mathrm{S}_n \to \mathbb{Z}_2 = \{0, 1\} : \sigma \mapsto \operatorname{inv}(\sigma) \bmod 2.$$

Dank obiger Zählung gilt $\varepsilon(\sigma \bullet \tau) = \varepsilon(\sigma) + \varepsilon(\tau) \bmod 2$ für alle $\sigma, \tau \in \mathrm{S}_n$, und somit ist $\varepsilon : (\mathrm{S}_n, \bullet, \mathrm{id}_n) \to (\mathbb{Z}_2, +_2, 0)$ ein Gruppenhomomorphismus.

Eine Permutation $\sigma \in \mathrm{S}_n$ heißt **un/gerade**, falls $\operatorname{inv}(\sigma)$ un/gerade ist. Die geraden bilden die **alternierende Gruppe** $\mathrm{A}_n = \operatorname{Ker} \varepsilon \trianglelefteq \mathrm{S}_n$.

Optimale Erzeugung durch Fundamentaltranspositionen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\mathrm{S}_n = \langle\ \tau_1 = (1,2),\ \ \tau_2 = (2,3),\ \ \tau_2 = (3,4),\ \ \ldots,\ \ \tau_{n-1} = (n-1,1)\ \rangle$$

Satz O1E: optimale Erzeugung durch Fundamentaltranspositionen

(1) Sei $\sigma \in \mathrm{S}_n$ eine Permutation. Es gilt

$$\mathrm{inv}(\sigma \circ \tau_i) = \mathrm{inv}(\sigma) \pm 1 \quad \text{und} \quad \mathrm{inv}(\tau_j \circ \sigma) = \mathrm{inv}(\sigma) \pm 1.$$

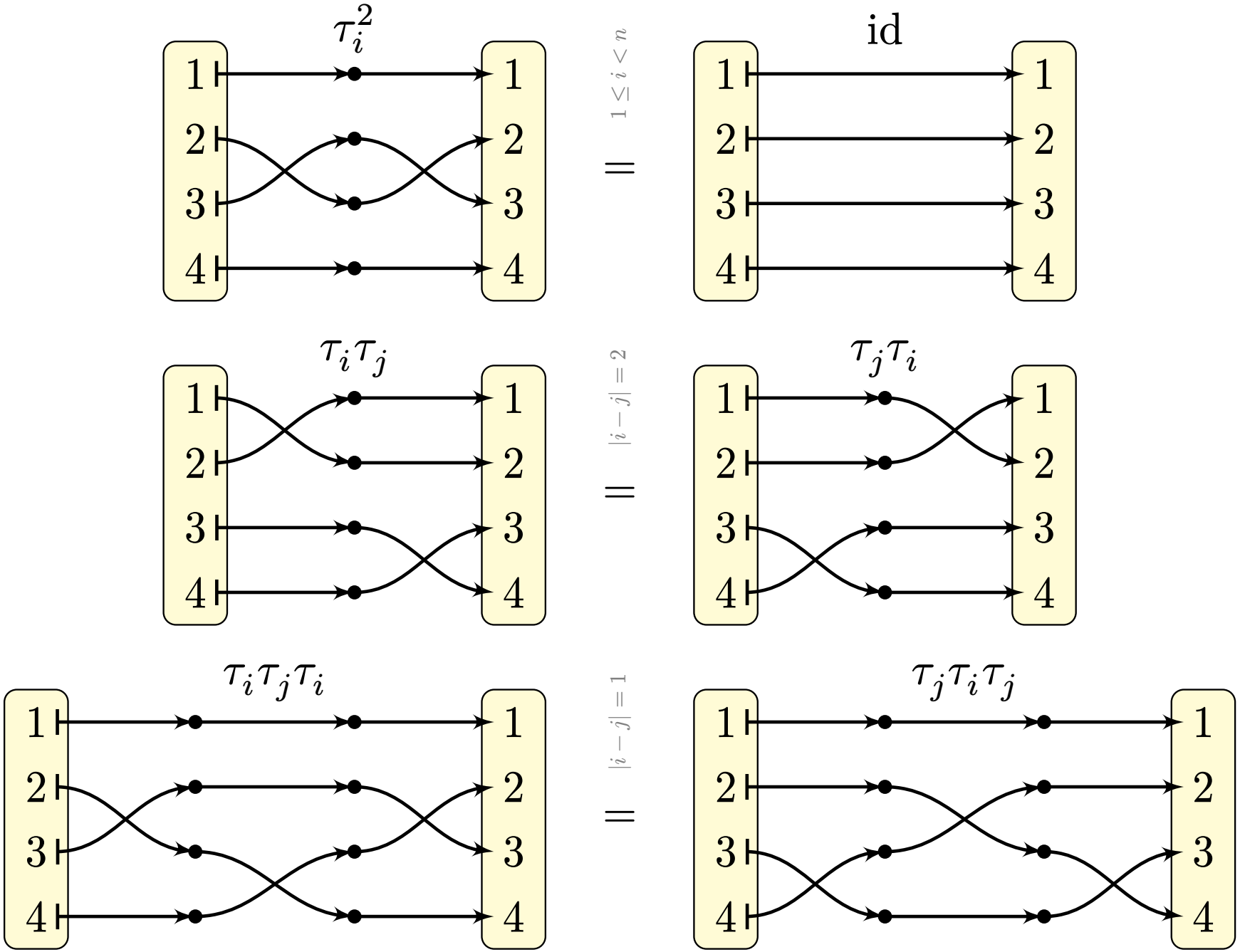
(2) Im Falle $\mathrm{inv}(\sigma) > 0$ existieren $i, j \in \{1, \ldots, n-1\}$ mit

$$\mathrm{inv}(\sigma \circ \tau_i) = \mathrm{inv}(\sigma) - 1 \quad \text{und} \quad \mathrm{inv}(\tau_j \circ \sigma) = \mathrm{inv}(\sigma) - 1.$$

(3) Jede Permutation $\sigma \in \mathrm{S}_n$ ist ein Produkt der Form $\sigma = \tau_{i_1} \tau_{i_2} \cdots \tau_{i_\ell}$.
(a) Die minimale Länge ist $\ell = \mathrm{inv}(\sigma)$. (b) Allgemein gilt $\ell \in \mathrm{inv}(\sigma) + 2\mathbb{N}$.

Die fundamentalen Transpositionen und ihre Relationen

Dies ist nur die Saalversion ohne Erläuterungen.



Ausführliche Erläuterungen bietet die Vollversion.

Die Signatur einer Selbstabbildung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{tikzcd}
(\mathrm{T}_X, \circ, \mathrm{id}_X) \arrow[r, "\mathrm{sign}_X"'] \arrow[d, phantom, "\cup"] & (\{\pm 1, 0\}, \cdot, 1) \arrow[d, phantom, "\cup"] \\
(\mathrm{S}_X, \circ, \mathrm{id}_X) \arrow[r, "f \mapsto \mathrm{sign}(f)"] & (\{\pm 1\}, \cdot, 1)
\end{tikzcd}$$

Satz O1H: die Signatur einer Selbstabbildung

Zu $n \in \mathbb{N}$ betrachten wir die endliche Menge $X = \{1 < \ldots < n\} \subset \mathbb{Q}$.

(0) Zu jeder Selbstabbildung $f : X \to X$ definieren wir die **Signatur**

$$\mathrm{sign}_X(f) := \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \overset{!}{\in} \{\pm 1, 0\}.$$

(1) Die Signatur ist multiplikativ, das heißt $\mathrm{sign}(g \circ f) = \mathrm{sign}(g) \cdot \mathrm{sign}(f)$.

Die Signatur einer Selbstabbildung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: (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 (H2J):

$$f_2 : \binom{X}{2} \xrightarrow{\sim} \binom{X}{2} : \{i \neq j\} \mapsto \{k \neq \ell\} = \{f(i) \neq f(j)\}$$

Daraus folgt:

$$\big|\operatorname{sign}(f)\big| \overset{\text{Def}}{=} \prod_{\{i \neq j\}} \frac{|f(i) - f(j)|}{|i - j|} \overset{\text{Bij}}{=} \frac{\prod_{\{k \neq \ell\}} |k - \ell|}{\prod_{\{i \neq j\}} |i - j|} = 1$$

Die Signatur einer Selbstabbildung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

(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 dank (0b):

$$\begin{aligned}
\operatorname{sign}(g \circ f) &\overset{\text{Def}}{=} \prod_{\{i \neq j\}} \frac{g(f(i)) - g(f(j))}{i - j} \\
&\overset{\mathbb{Q}}{=} \prod_{\{i \neq j\}} \frac{g(f(i)) - g(f(j))}{f(i) - f(j)} \cdot \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \\
&\overset{\text{Bij}}{=} \prod_{\{k \neq \ell\}} \frac{g(k) - g(\ell)}{k - \ell} \cdot \prod_{\{i \neq j\}} \frac{f(i) - f(j)}{i - j} \overset{\text{Def}}{=} \operatorname{sign}(g) \cdot \operatorname{sign}(f)
\end{aligned}$$

Effiziente Berechnung der Signatur

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O1J: effiziente Berechnung der Signatur dank Zykelregel

(0) Für jede Permutation $\sigma \in \mathrm{S}_X$ gilt $\operatorname{sign}(\sigma) = (-1)^{\operatorname{inv}(\sigma)} = (-1)^{\varepsilon(\sigma)}$.

(1) Für jede Transposition $\tau = (a, b) \in \mathrm{S}_X$ gilt somit $\operatorname{sign}(\tau) = -1$.

(2) Für jeden ℓ–Zykel $\sigma = (a_1, a_2, \dots, a_\ell) \in \mathrm{S}_X$ gilt $\operatorname{sign}(\sigma) = (-1)^{\ell-1}$.

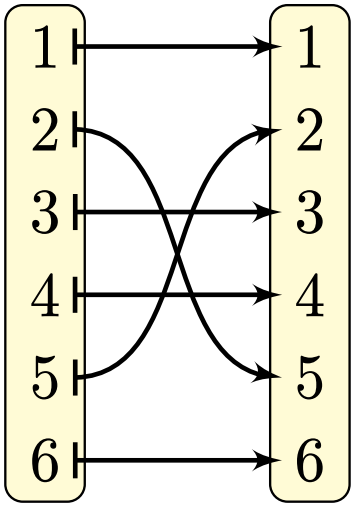
$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 7 & 4 & 6 & 2 & 3 & 8 \end{bmatrix} = \underset{+}{(1)}\ \underset{-}{(2,5,4,7)}\ \underset{+}{(6)}\ \underset{+}{(3,9,8)}$$

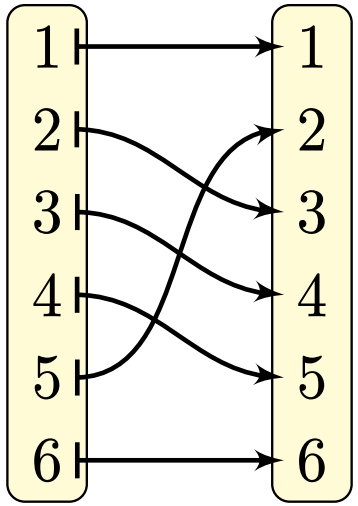
Effiziente Berechnung der Signatur

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele:





Beweis: (0) Für $\sigma \in \mathrm{S}_n$ wissen wir bereits $\operatorname{sign}(\sigma) \in \{\pm 1\}$, genauer gilt:

$$\operatorname{sign}(\sigma) \overset{\text{Def}}{=} \prod_{\{i \neq j\}} \underbrace{\frac{\sigma(i) - \sigma(j)}{i - j}}_{< 0 \text{ gdw } \{i,j\} \in \operatorname{Inv}(\sigma)} = (-1)^{\operatorname{inv}(\sigma)}$$

(1) Für $\tau = (a, b)$ gilt $\operatorname{inv}(\tau) = 2\,|a - b| - 1$. Dank (0) folgt

$$\operatorname{sign}(\tau) = (-1)^{\operatorname{inv}(\tau)} = -1.$$

(2) Es gilt $\sigma = (a_1, a_2, \ldots, a_\ell) = (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{\ell-1}, a_\ell)$. $\boxed{\text{QED}}$

Invarianz der Signatur: Umnummerierung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei $X = \{1 < \ldots < n\}$ und Y mit $\sharp Y = n$ eine beliebige Menge.

$$
\begin{tikzcd}
X \arrow[rrr, "f = \nu^{-1} \circ g \circ \nu"'] \arrow[dr, "\nu", "\cong"'] & & & X \\
& Y \arrow[r, "g"] & Y & \\
X \arrow[uu, shift left, "\tau", "\cong"'] \arrow[uu, shift right, "\tau^{-1}"] \arrow[ur, "\nu'", "\cong"'] \arrow[rrr, "f' = \nu'^{-1} \circ g \circ \nu'"'] & & & X \arrow[ul, "\nu", "\cong"'] \arrow[ul, "\nu'", "\cong"'] \arrow[uu, shift left, "\tau", "\cong"'] \arrow[uu, shift right, "\tau^{-1}"]
\end{tikzcd}
$$

$$\mathrm{sign}_X(f') \overset{\text{O1H}}{=} \mathrm{sign}_X(\tau)^{-1} \cdot \mathrm{sign}_X(f) \cdot \mathrm{sign}_X(\tau) \overset{\text{Com}}{=} \mathrm{sign}_X(f)$$

Somit ist die Signatur $\mathrm{sign}_Y(g) := \mathrm{sign}_X(f) = \mathrm{sign}_X(f')$ wohldefiniert.

Die alternierende Gruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Sei X eine beliebige endliche Menge, nicht unbedingt $X = \{1 < \ldots < n\}$. Ist $f : X \to X$ nicht bijektiv, so gilt $\operatorname{sign}(f) = 0$. Für $\sigma \in \mathrm{S}_X$ berechnen wir $\operatorname{sign}(\sigma)$ dank Zykelregel O1J(2). Beispiel $\operatorname{sign}((🍎, 🍐, 🍋)(🍅, 🍓)) = -1$.

Definition O1O: die alternierende Gruppe $A_X \trianglelefteq S_X$

Die geraden Permutationen bilden die **alternierende Gruppe**

$$\mathrm{A}_X = \operatorname{Alt}(X) := \operatorname{Ker}(\operatorname{sign}_X) = \{\sigma \in \mathrm{S}_X \mid \operatorname{sign}(\sigma) = +1\} \trianglelefteq \mathrm{S}_X .$$

Die alternierende Gruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele: Für $X = \{1\}$ haben wir:

$$\begin{aligned} \mathrm{S}_1 &= \mathrm{Sym}(X) = \{\mathrm{id}_X\} \\ \mathrm{A}_1 &= \mathrm{Alt}(X) \ \ = \{\mathrm{id}_X\} \end{aligned}$$

Für $X = \{1, 2\}$ haben wir:

$$\begin{aligned} \mathrm{S}_2 &= \mathrm{Sym}(X) = \{\mathrm{id}_X,\ (1,2)\} \\ \mathrm{A}_2 &= \mathrm{Alt}(X) \ \ = \{\mathrm{id}_X\} \end{aligned}$$

Für $X = \{1, 2, 3\}$ haben wir:

$$\begin{aligned} \mathrm{S}_3 &= \mathrm{Sym}(X) = \{\mathrm{id}_X,\ (1,2,3),\ (1,3,2),\ (1,2),\ (1,3),\ (2,3)\} \\ \mathrm{A}_3 &= \mathrm{Alt}(X) \ \ = \{\mathrm{id}_X,\ (1,2,3),\ (1,3,2)\} \end{aligned}$$

Die alternierende Gruppe

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O1P: Ordnung der alternierenden Gruppe

Sei X eine endliche Menge mit Elementezahl $n = \sharp X \geq 2$.

$$\mathrm{A}_X \xhookrightarrow{\text{inc}} \mathrm{S}_X \xrightarrow{\text{sign}_X} \{\pm 1\}$$

(1) Somit gilt $\mathrm{S}_X = \mathrm{S}_X^+ \sqcup \mathrm{S}_X^-$ mit $\mathrm{S}_X^+ = \text{sign}_X^{-1}(\{1\}) = \mathrm{A}_X \trianglelefteq \mathrm{S}_X$ und

$$\mathrm{S}_X^- = \text{sign}_X^{-1}(\{-1\}) = \tau \circ \mathrm{A}_X = \mathrm{A}_X \circ \tau \quad \text{für} \quad \tau \in \mathrm{S}_X^- .$$

(2) Für die Gruppenordnung (Elementezahl) gilt:

$$\sharp\, \mathrm{S}_X = n! \quad \text{und} \quad \sharp\, \mathrm{A}_X = n!/2$$

Spektakuläre Anwendung: das 15-Puzzle

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

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: Wie / Kommen Sie von B zurück zu A? Und von C zu A?

A :

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

$\sigma(1)$	$\sigma(2)$	$\sigma(3)$	$\sigma(4)$
$\sigma(5)$	$\sigma(6)$	$\sigma(7)$	$\sigma(8)$
$\sigma(9)$	$\sigma(10)$	$\sigma(11)$	$\sigma(12)$
$\sigma(13)$	$\sigma(14)$	$\sigma(15)$	$\sigma(16)$

$+ \quad - \quad + \quad -$

Das freie Feld $\sigma^{-1}(16)$

$- \quad + \quad - \quad +$

zeigt das Vorzeichen $s(\sigma)$

$+ \quad - \quad + \quad -$

gemäß Schachbrettmuster.

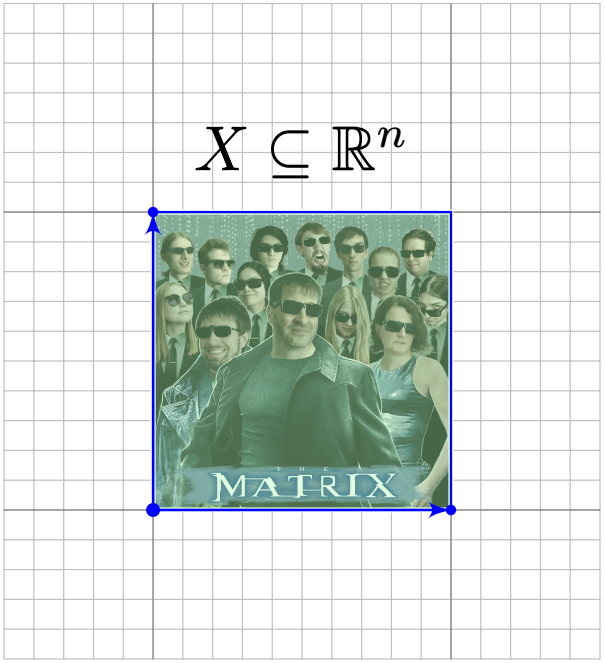
$- \quad + \quad - \quad +$

Invariante: Das Produkt $I(\sigma) := s(\sigma) \cdot \operatorname{sign}(\sigma)$ ist konstant, mit $I(\alpha) = 1$. Das Puzzle B mit $I(\beta) = 1$ können Sie lösen, aber C mit $I(\gamma) = -1$ nicht!

Geometrische Motivation: Volumen und Determinante

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



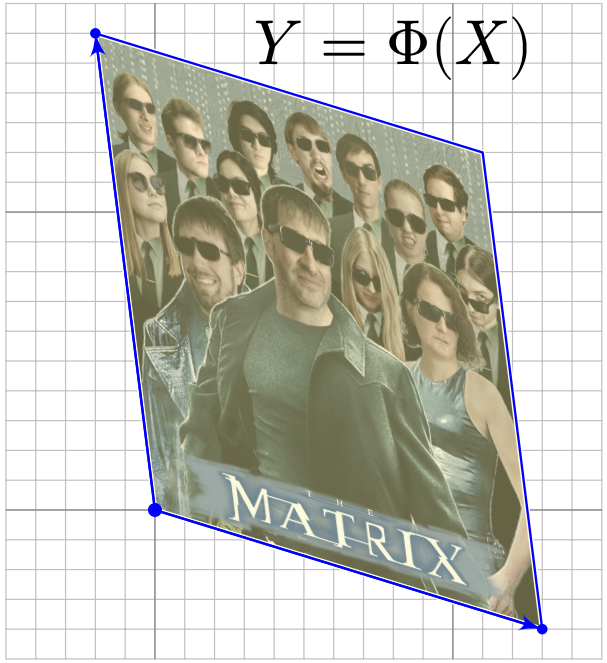
lineare Abbildung

$$\Phi : \mathbb{R}^n \to \mathbb{R}^n$$

$$x \mapsto y = Ax$$

Zahlenbeispiel:

$$A = \begin{bmatrix} 1.3 & -0.2 \\ -0.4 & 1.6 \end{bmatrix}$$

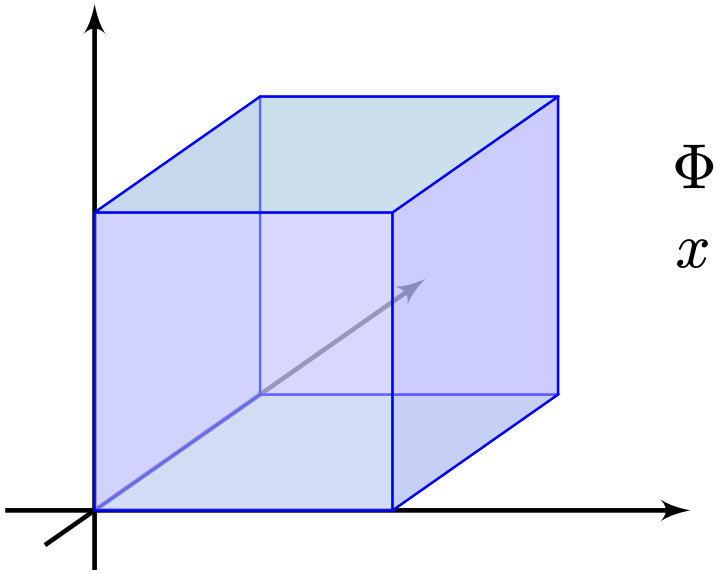


$$\boxed{\mathrm{vol}_n(Y) = \mathrm{vol}_n(X) \cdot |\det(A)|}$$

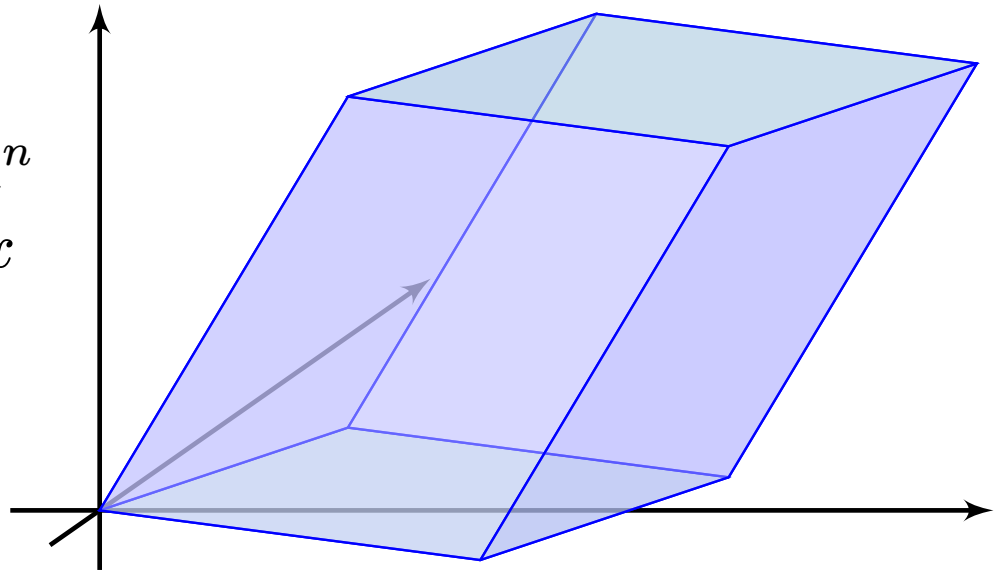
Geometrische Motivation: Volumen und Determinante

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



$$\Phi : \mathbb{R}^n \to \mathbb{R}^n$$
$$x \mapsto y = Ax$$



Je n Vektoren $\mathcal{A} = (a_1, \dots, a_n)$ im $\mathbb{R}^n$ spannen ein **Parallelotop** auf:

$$P = \{\, a_1 x_1 + \cdots + a_n x_n \mid x_1, \dots, x_n \in [0,1] \,\} = A \cdot [0,1]^n$$

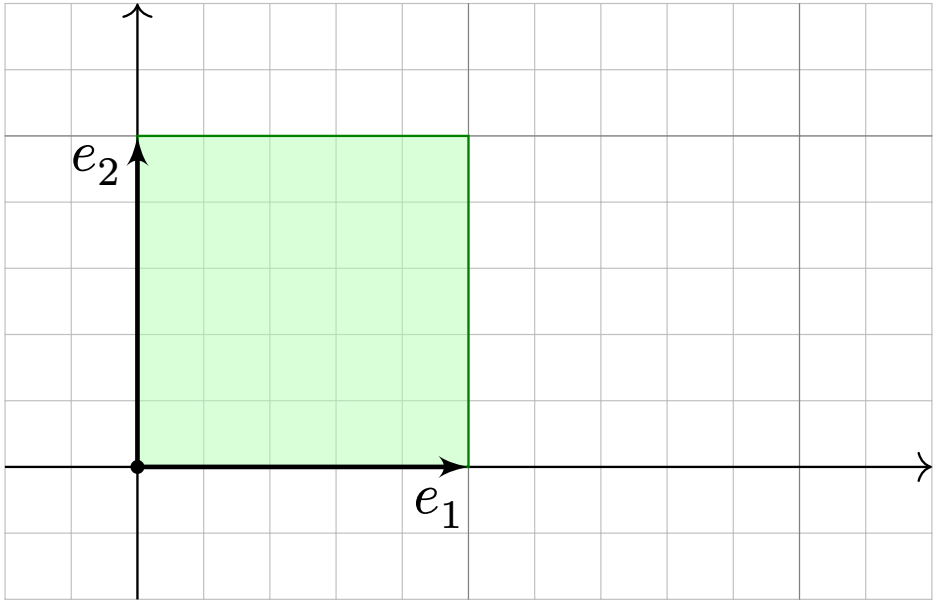
Wir untersuchen nun das **orientierte Volumen**

$$v : \mathbb{R}^{n \times n} \to \mathbb{R} : A \mapsto v(A) \quad \text{sodass} \quad \mathrm{vol}_n(P) = |v(A)|.$$

Determinante als orientiertes Volumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



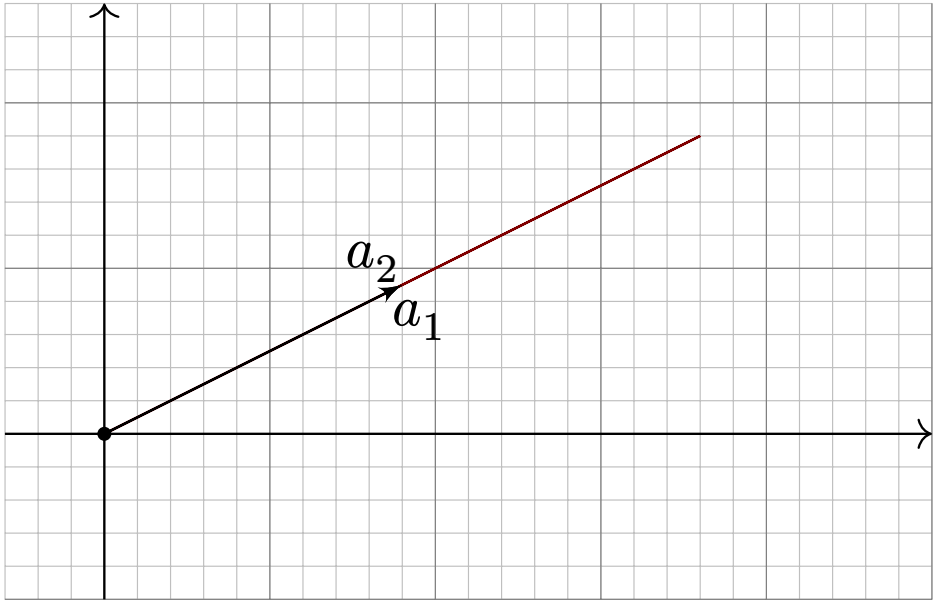
1. Normierung:

$$\boxed{v(e_1, \dots, e_n) = 1.}$$

Determinante als orientiertes Volumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



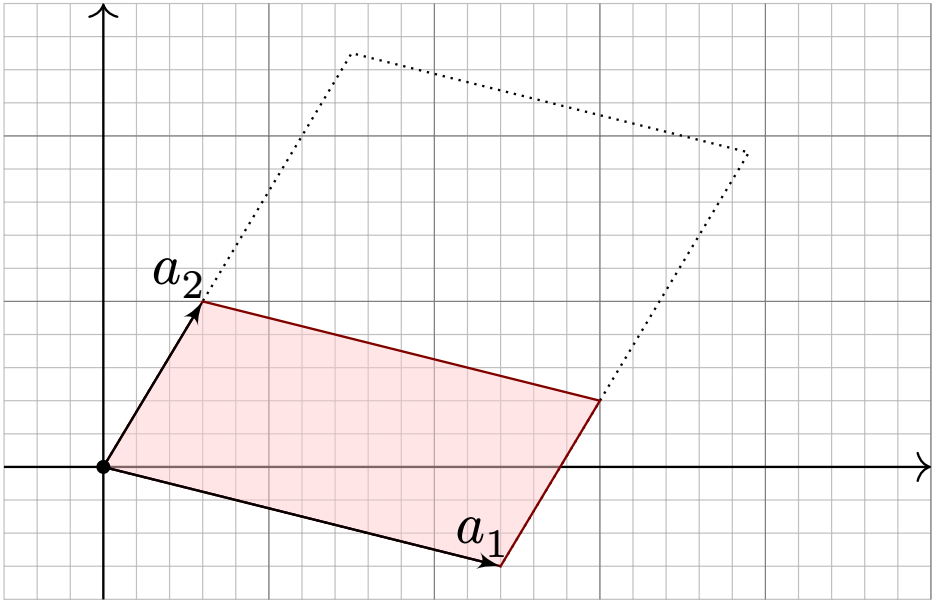
2. Degenerierung:

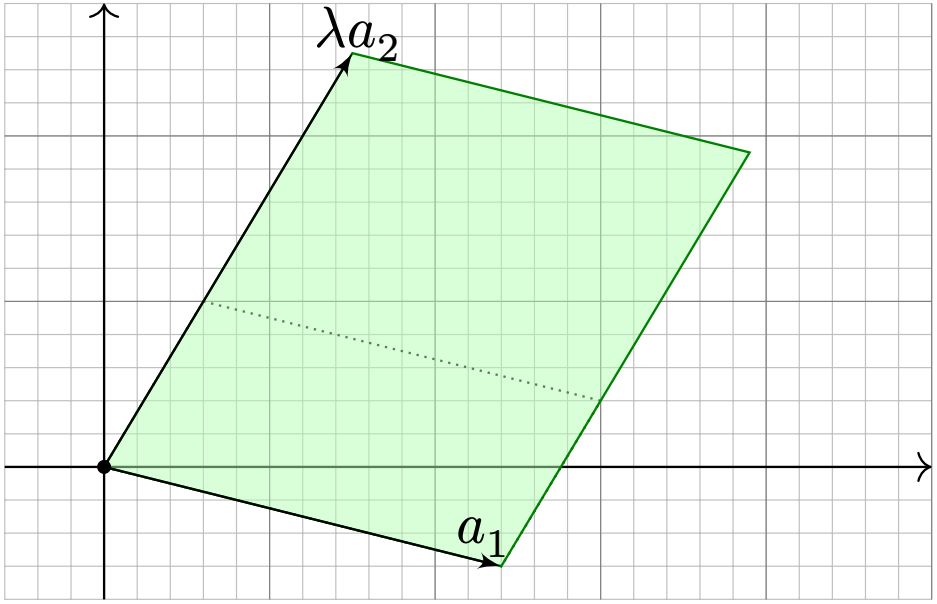
$$\boxed{v(a_1, \dots, a_i, \dots, a_i, \dots, a_n) = 0.}$$

Determinante als orientiertes Volumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





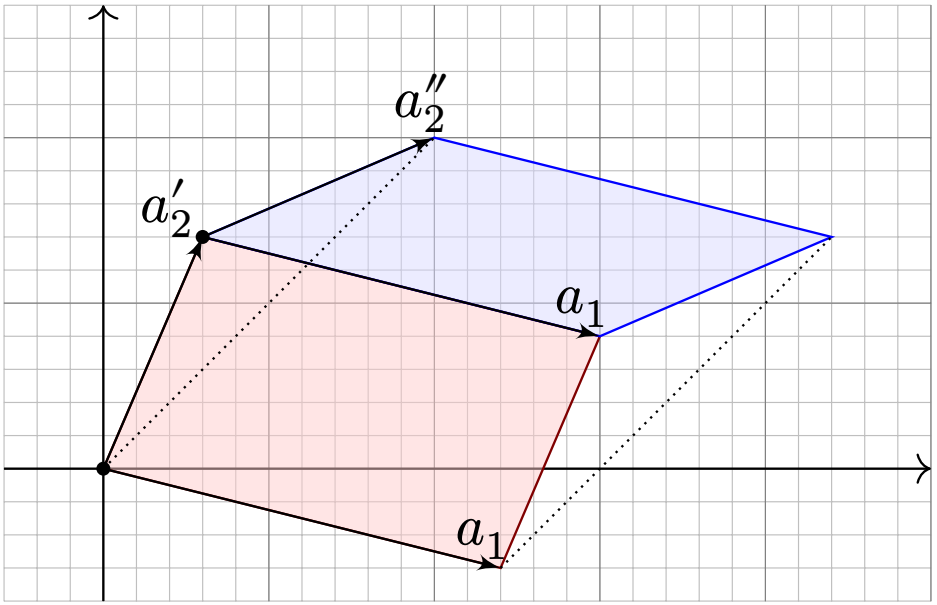
3. Skalierung:

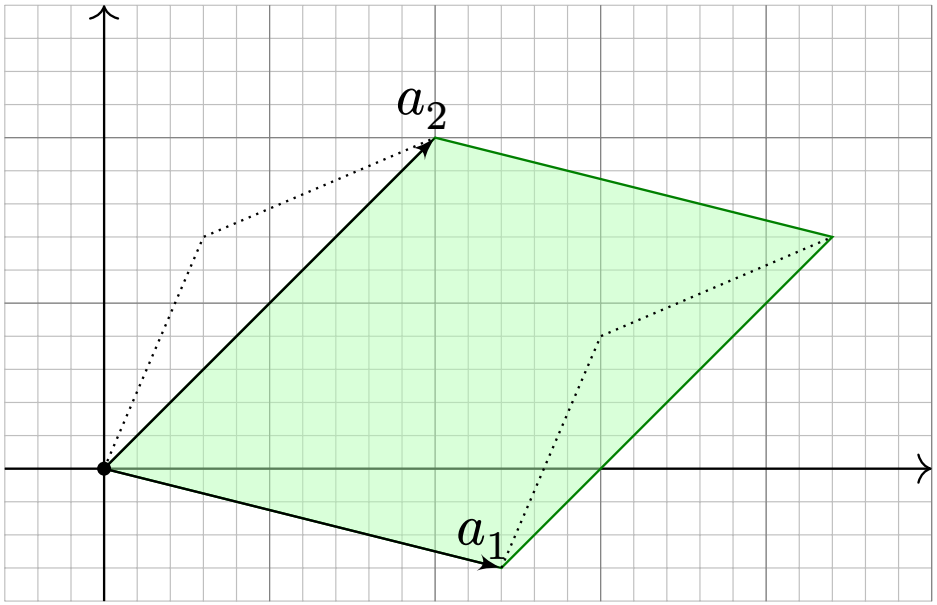
$$\boxed{v(a_1, \dots, \lambda a_i, \dots, a_n) = \lambda v(a_1, \dots, a_i, \dots, a_n).}$$

Determinante als orientiertes Volumen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.





4. Additivität:

$$v(a_1, \dots, a_i' + a_i'', \dots, a_n) = v(a_1, \dots, a_i', \dots, a_n) + v(a_1, \dots, a_i'', \dots, a_n)$$

Multilinear, alternierend, normiert

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition O2A: multilinear, alternierend, normiert

Sei K ein kommutativer Ring. Wir betrachten eine Abbildung

$$v : K^{n\times\ell} \to K : (a_1, \dots, a_i, \dots, a_\ell) \mapsto v(a_1, \dots, a_i, \dots, a_\ell).$$

(1) Wir nennen v **multilinear** über K, falls v linear in jeder Spalte i ist:

$$\begin{aligned} v(a_1, \dots, a_i' + a_i'', \dots, a_\ell) &= v(a_1, \dots, a_i', \dots, a_\ell) + v(a_1, \dots, a_i'', \dots, a_\ell), \\ v(a_1, \dots, \lambda \cdot a_i, \dots, a_\ell) &= \lambda \cdot v(a_1, \dots, a_i, \dots, a_\ell) \end{aligned}$$

(2) Wir nennen v **alternierend**, falls $v(a_1, \dots, a_i, \dots, a_i, \dots, a_\ell) = 0$, und **antisymmetrisch**, falls $v(\dots, a_i, \dots, a_j, \dots) = -v(\dots, a_j, \dots, a_i, \dots)$.

(3) Wir nennen v **normiert**, falls $n = \ell$ und $v(e_1, \dots, e_n) = 1$ gilt.

Einmal Null, immer Null

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Bemerkung O2B: einmal Null, immer Null

Dank Additivität in Spalte i folgt aus $a_i = 0$ bereits $v(A) = 0_K$, denn

$$v(\dots, a_i', \dots) \;=\; v(\dots, a_i' + 0, \dots) \;=\; v(\dots, a_i', \dots) + v(\dots, 0, \dots).$$

Transvektion ändert nichts.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma O2c: Transvektion ändert nichts.

Ist $v : K^{n\times\ell} \to K$ multilinear und alternierend, so gilt

$$v(\dots, a_i, \dots, a_j + \lambda a_i, \dots) \;=\; v(\dots, a_i, \dots, a_j, \dots) + \lambda\, \cancel{v(\dots, a_i, \dots, a_i, \dots)}$$

Aus alternierend folgt antisymmetrisch.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Lemma O2D: Aus alternierend folgt antisymmetrisch.

Sei v multilinear. (1) Ist v alternierend, so auch antisymmetrisch.
(2) Die Umkehrung gilt, falls 2 in unserem Grundring K kürzbar ist.

Beweis: (1) Wir nutzen die Additivität in den beiden Spalten $i \neq j$:

$$\begin{aligned}
0 &\overset{\text{alt}}{=} v(\dots, a_i + a_j, \dots, a_i + a_j, \dots) \\
&\overset{\text{add}}{=} v(\dots, a_i, \dots, a_i + a_j, \dots) + v(\dots, a_j, \dots, a_i + a_j, \dots) \\
&\overset{\text{add}}{=} + \cancel{v(\dots, a_i, \dots, a_i, \dots)} + v(\dots, a_i, \dots, a_j, \dots) \\
&\quad + v(\dots, a_j, \dots, a_i, \dots) + \cancel{v(\dots, a_j, \dots, a_j, \dots)}
\end{aligned}$$

(2) Aus Antisymmetrie und $a_i = a_j$ folgt $2v(\dots, a_i, \dots, a_j, \dots) = 0$.

Die Permutationsmatrix P_σ

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Jede Abbildung $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ definiert ihre zugehörige Matrix

$$P_\sigma := (e_{\sigma(1)}, \dots, e_{\sigma(n)}) \in K^{n \times n},$$

also $P_\sigma e_i = e_{\sigma(i)}$. Beispiele:

$$\sigma = (1,2,3) = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right] \in \mathrm{S}_3 \quad \Longrightarrow \quad P_\sigma = (e_2, e_3, e_1) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \in K^{3\times 3}$$

$$\tau = (2,3) = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right] \in \mathrm{S}_3 \quad \Longrightarrow \quad P_\tau = (e_1, e_3, e_2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \in K^{3\times 3}$$

Lemma O2F: Permutationsmatrix P_σ

Ist $v : K^{n\times n} \to K$ multilinear und alternierend, so gilt

$$v(P_\sigma) = \operatorname{sign}(\sigma) \cdot v(E).$$

Beweis: Für σ nicht injektiv gilt $v(P_\sigma) = 0$ (O2A) und $\operatorname{sign}(\sigma) = 0$ (O1H). Jede Permutation $\sigma \in \mathrm{S}_n$ ist Produkt $\sigma = \tau_1 \cdots \tau_\ell$ von Transpositionen (O1E), also $\operatorname{sign}(\sigma) = (-1)^\ell$ (O1J) und $v(P_\sigma) = (-1)^\ell \cdot v(E)$ (O2D). QED

Der Hauptsatz zu Determinanten

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2G: Existenz, Eindeutigkeit, Eigenschaften der Determinante

Sei K ein kommutativer Ring und $n \in \mathbb{N}$. Unter allen Abbildungen $K^{n\times n} \to K$ gibt es genau eine multilineare, alternierende, normierte. Diese Abbildung nennen wir die **Determinante** und schreiben hierfür

$$\det_K^n : K^{n\times n} \to K : A \mapsto \det(A) =: |A|.$$

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.

Zu $A = (a_1, \dots, a_n)$ definieren wir die **adjunkte Matrix** $A' = \operatorname{adj}(A)$ durch die **transponierten Cofaktoren** $a'_{ij} := \det(\dots, a_{i-1}, e_j, a_{i+1}, \dots)$.

5. Es gilt $AA' = A'A = \det(A)E$, also $A^{-1} = \det(A)^{-1}A'$. (Cramer)

Dimension $n = 2$: Inversion von 2×2–Matrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel O2H: Determinante und Inversion von 2×2–Matrizen

$$\det_K^2 : K^{2\times 2} \to K : A = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \mapsto \det A = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc.$$

$$\operatorname{adj} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}, \qquad \begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$$

Dimension $n = 3$: Sarrus–Regel aka Jägerzaun

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel O21: Determinante und Inversion von 3×3–Matrizen

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \Rightarrow \det A = \begin{cases} \text{Diagonalen minus Gegendiagonalen} \\ + a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} \end{cases}$$

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} a_{22}a_{33} - a_{23}a_{32} & a_{13}a_{32} - a_{12}a_{33} & a_{12}a_{23} - a_{13}a_{22} \\ a_{23}a_{31} - a_{21}a_{33} & a_{11}a_{33} - a_{13}a_{31} & a_{13}a_{21} - a_{11}a_{23} \\ a_{21}a_{32} - a_{22}a_{31} & a_{12}a_{31} - a_{11}a_{32} & a_{11}a_{22} - a_{12}a_{21} \end{bmatrix}$$

Anwendungsbeispiel zur Invertierbarkeit

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$A(\lambda) = \begin{bmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{bmatrix} \in \mathbb{R}^{3\times 3}$$

Aufgabe: Für welche $\lambda \in \mathbb{R}$ ist die Matrix $A(\lambda)$ invertierbar? **Lösung:**

$$\det A(\lambda) = \begin{vmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{vmatrix} = \cdots \ldots = 60 - 12\lambda$$

Für $\lambda = 5$ ist die Matrix singulär, für $\lambda \neq 5$ ist sie regulär / invertierbar.

Rekursion: die Streichungsmatrix A_{ij}

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aus $A \in K^{n\times n}$ bilden wir die **Streichungsmatrix** $A_{ij} \in K^{(n-1)\times(n-1)}$:

$$A_{ij} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i,1} & \cdots & a_{i,j-1} & a_{i,j} & a_{i,j+1} & \cdots & a_{i,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & a_{n,j} & a_{n,j+1} & \cdots & a_{n,n} \end{bmatrix}$$

Zur Stelle (i,j) mit **Faktor** a_{ij} erhalten wir so den **Cofaktor**:

$$\boxed{\tilde{a}_{ij} \;:=\; (-1)^{i+j} \det A_{ij}}$$

Rekursion: die Spalten-Ersetzungsmatrix $A_{ij}^{|}$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: In der Matrix $A \in K^{n\times n}$ ersetzen wir die j-te Spalte durch e_i:

$$A_{ij}^{|} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & \cdots & \vdots & 0 & \vdots & \cdots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i,1} & \cdots & a_{i,j-1} & 1 & a_{i,j+1} & \cdots & a_{i,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \cdots & \vdots & 0 & \vdots & \cdots & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & 0 & a_{n,j+1} & \cdots & a_{n,n} \end{bmatrix}$$

Wir tauschen (i,j) nach (n,n) und erhalten dank Leibniz–Formel:

$$\boxed{\det A_{ij}^{|} \overset{\text{O2G}}{=} (-1)^{i+j} \det A_{ij}}$$

Die rekursive Laplace–Entwicklung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2J: Entwicklungssatz von Laplace

Entwicklung nach der j-ten Spalte: $\det A = \sum_{i=1}^{n} a_{ij}\,(-1)^{i+j} \det A_{ij}$,

Entwicklung nach der i-ten Zeile: $\det A = \sum_{j=1}^{n} a_{ij}\,(-1)^{i+j} \det A_{ij}$.

Beweis:

$$\begin{aligned}
\det(a_1, \dots, a_n) &= \det(a_1, \dots, a_{j-1}, \textstyle\sum_{i=1}^{n} e_i a_{ij}, a_{j+1}, \dots, a_n) \\
&\overset{\text{Lin}}{=} \textstyle\sum_{i=1}^{n} a_{ij} \det(a_1, \dots, a_{j-1}, e_i, a_{j+1}, \dots, a_n) \\
&\overset{\text{O2G}}{=} \textstyle\sum_{i=1}^{n} a_{ij}\,(-1)^{i+j} \det A_{ij}
\end{aligned}$$

Die rekursive Laplace–Entwicklung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$((-1)^{i+j})_{ij} = \begin{bmatrix} + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \\ + & - & + & - & + & - & + & - \\ - & + & - & + & - & + & - & + \end{bmatrix}$$

Die rekursive Laplace–Entwicklung

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Berechnen 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:

$$\begin{vmatrix} 7 & 3 & 0 \\ 2 & 1 & 5 \\ 4 & 2 & 0 \end{vmatrix} = +0 \begin{vmatrix} 2 & 1 \\ 4 & 2 \end{vmatrix} - 5 \begin{vmatrix} 7 & 3 \\ 4 & 2 \end{vmatrix} + 0 \begin{vmatrix} 7 & 3 \\ 2 & 1 \end{vmatrix} = (-5) \cdot 2 = -10$$

(2) Wir entwickeln $\det(B)$ nach der zweiten Zeile:

$$\begin{vmatrix} 3 & 1 & 2 & 2 \\ 4 & 0 & 0 & 2 \\ 7 & 2 & 1 & 0 \\ 0 & 5 & 8 & 3 \end{vmatrix} = -4 \begin{vmatrix} 1 & 2 & 2 \\ 2 & 1 & 0 \\ 5 & 8 & 3 \end{vmatrix} + 0 \begin{vmatrix} 3 & 2 & 2 \\ 7 & 1 & 0 \\ 0 & 8 & 3 \end{vmatrix} + 0 \begin{vmatrix} 3 & 1 & 2 \\ 7 & 2 & 0 \\ 0 & 5 & 3 \end{vmatrix} + 2 \begin{vmatrix} 3 & 1 & 2 \\ 7 & 2 & 1 \\ 0 & 5 & 8 \end{vmatrix}$$

$$= \cdots \ldots = -4 \cdot [2 \cdot 11 + 3 \cdot (-3)] + 2 \cdot [3 \cdot 11 - 7 \cdot (-2)] = 42$$

Wie konstruieren wir die Determinante?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition O2κ: Konstruktion der Determinante

Wir konstruieren $\det_K^n : K^{n\times n} \to K$ durch die **Leibniz–Formel**

$$\det(A) = \sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot \prod_{j=1}^n a_{\sigma(j),j}$$

Die Determinante ist invariant unter Transposition.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2L: Invarianz unter Transposition

Die Determinante ist invariant unter Transposition: $\det(A^\intercal) = \det(A)$.

Beweis: Wir nutzen die Kommutativität in K und sortieren die Faktoren:

$$a_{\sigma(1),1} \cdots a_{\sigma(n),n} \overset{\text{Com}}{=} a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)}$$

Wir erhalten:

$$\begin{aligned}
\det(A^\intercal) &\overset{\text{Def}}{=} \textstyle\sum_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a^\intercal_{\sigma(1),1} \cdots a^\intercal_{\sigma(n),n} \\
&\overset{\text{Def}}{=} \textstyle\sum_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \\
&\overset{\text{Inv}}{=} \textstyle\sum_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma^{-1}) \cdot a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)} \\
&\overset{\text{Sort}}{=} \textstyle\sum_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n} \overset{\text{Def}}{=} \det(A)
\end{aligned}$$

Die Determinante tut, was eine Determinante tun muss.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2M: Die Determinante erfüllt die drei Weierstraß–Axiome.

Die Determinante $\det_K^n$ ist multilinear, alternierend, normiert.

Beweis: (1) Die Determinante $A \mapsto \det(A)$ ist linear in jeder Spalte:

$$\begin{aligned}
&\det(a_1, \dots, a'_i + \lambda a''_i, \dots, a_n) \\
&= \textstyle\sum_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdots (a'_{\sigma(i),i} + \lambda a''_{\sigma(i),i}) \cdots a_{\sigma(n),n} \\
&= \cdots \cdots = \det(a_1, \dots, a'_i, \dots, a_n) + \lambda \det(a_1, \dots, a''_i, \dots, a_n)
\end{aligned}$$

(2) Sei $a_i = a_j$ für ein Paar $i \neq j$. Für $\sigma \in \mathrm{A}_n$ und $\sigma' = \sigma \circ (i, j)$ gilt:

$$a_{\sigma(1),1} \cdots a_{\sigma(i),i} \cdots a_{\sigma(j),j} \cdots a_{\sigma(n),n} = a_{\sigma'(1),1} \cdots a_{\sigma'(i),i} \cdots a_{\sigma'(j),j} \cdots a_{\sigma'(n),n}$$

In der Leibniz–Formel löschen sich so alle Terme paarweise aus.

(3) Für die Einheitsmatrix $E = 1_{n \times n}$ und jede Permutation $\sigma \in \mathrm{S}_n$ gilt

$$\operatorname{sign}(\sigma) \cdot e_{\sigma(1),1} \cdots e_{\sigma(n),n} = \begin{cases} 1 & \text{für } \sigma = \mathrm{id}, \\ 0 & \text{für } \sigma \neq \mathrm{id}. \end{cases}$$

Der Eindeutigkeitssatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2N: Eindeutigkeitssatz für die Determinante

Ist $v : K^{n\times n} \to K$ multilinear und alternierend, so gilt

$$\boxed{v(A) = v(E)\cdot \det(A)}$$

Beweis:

$$\begin{aligned} v(a_1,\dots,a_n) &= v\Big(\textstyle\sum_{\sigma_1=1}^n e_{\sigma_1} a_{\sigma_1,1},\ \dots,\ \sum_{\sigma_n=1}^n e_{\sigma_n} a_{\sigma_n,n}\Big) \\ &\overset{(1)}{=} \textstyle\sum_{\sigma_1=1}^n \cdots \sum_{\sigma_n=1}^n a_{\sigma_1,1}\cdots a_{\sigma_n,n}\, v(e_{\sigma_1},\dots,e_{\sigma_n}) \\ &\overset{(2)}{=} \textstyle\sum_{\sigma\in \mathrm{T}_n} a_{\sigma(1),1}\cdots a_{\sigma(n),n}\ \mathrm{sign}(\sigma)\, v(E) \ = \ v(E)\det(A) \end{aligned}$$

Der Multiplikationssatz

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2o: Die Determinante ist multiplikativ.

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

Beweis: (1) Wir halten $A \in K^{n \times n}$ fest und betrachten die Abbildung

$$v : K^{n \times n} \to K : B \mapsto v(B) := \det(A \cdot B) = \det(Ab_1, \dots, Ab_n).$$

Dank Eindeutigkeitssatz O2N wissen wir $v(B) = v(E) \cdot \det(B)$, also

$$\det(A \cdot B) \overset{\text{Def}}{=} v(B) \overset{\text{O2N}}{=} v(E) \cdot \det(B) \overset{\text{Def}}{=} \det(A) \cdot \det(B).$$

Die Determinante ist nicht additiv!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Bemerkung O2P: Warnung, die Determinante ist nicht additiv!

(1) Nur in Dimension $n = 1$ haben wir $\det_K^1 : (K^{1\times 1}, +, \cdot) \xrightarrow{\sim} (K, +, \cdot)$.

(2) In Dimension $n \geq 2$ ist die Determinante

$$\det_K^n : (K^{n\times n}, \cdot, 1_{n\times n}) \to (K, \cdot, 1)$$

multiplikativ, aber **nicht additiv!** Gegenbeispiel:

$$\det \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0 \quad \text{und} \quad \det \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = 0 \quad \text{aber} \quad \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1.$$

(3) Die Determinante $\det_K^n$ ist insgesamt **K–homogen vom Grad n**:

$$\det(\lambda A) = \lambda^n \det(A)$$

Insbesondere gilt $\det(-A) = (-1)^n \det(A)$.

Die Cramersche Regel und das Determinantenverfahren

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2Q: Cramersche Regel / Determinantenverfahren für LGS

Vorgelegt 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 $j \in \{1, \dots, n\}$:

$$\boxed{\det(\dots, a_{j-1}, b, a_{j+1}, \dots) = \det(A) \cdot x_j}$$

(2) Ist $\det(A)$ in K invertierbar, so wird $Ax = b$ eindeutig gelöst 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 (O2M):

$$\det(\dots, a_{j-1}, b, a_{j+1}, \dots) \;=\; \sum_{i=1}^{n} \det(\dots, a_{j-1}, a_i, a_{j+1}, \dots) \cdot x_i$$

Alle Terme mit $i \neq j$ verschwinden, es bleibt nur $\det(A) \cdot x_j$. QED

Anwendungsbeispiel zum Determinantenverfahren

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Lösen Sie zu jedem Parameter $\lambda \in \mathbb{R}$ das Gleichungssystem

$$A(\lambda)\,x = e_1 \quad \text{mit} \quad A(\lambda) = \begin{bmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{bmatrix} \in \mathbb{R}^{3\times 3}.$$

Lösung: Wir wissen bereits $\det A(\lambda) = 60 - 12\lambda$, siehe O223.
Für $\lambda \neq 5$ können wir das Determinantenverfahren O2Q nutzen.

$$\begin{vmatrix} \mathbf{1} & 2 & 3 \\ \mathbf{0} & \lambda & 6 \\ \mathbf{0} & 8 & 9 \end{vmatrix} \overset{\text{O2I}}{=} 9\lambda - 48, \qquad \begin{vmatrix} 1 & \mathbf{1} & 3 \\ 4 & \mathbf{0} & 6 \\ 7 & \mathbf{0} & 9 \end{vmatrix} \overset{\text{O2I}}{=} 6, \qquad \begin{vmatrix} 1 & 2 & \mathbf{1} \\ 4 & \lambda & \mathbf{0} \\ 7 & 8 & \mathbf{0} \end{vmatrix} \overset{\text{O2I}}{=} 32 - 7\lambda.$$

Zu jedem Parameter $\lambda \in \mathbb{R} \setminus \{5\}$ finden wir so die einzige Lösung:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \overset{\text{O2Q}}{=} \frac{1}{\det A} \begin{bmatrix} \det(b, a_2, a_3) \\ \det(a_1, b, a_3) \\ \det(a_1, a_2, b) \end{bmatrix} \overset{\text{O2I}}{=} \frac{1}{60 - 12\lambda} \begin{bmatrix} 9\lambda - 48 \\ 6 \\ 32 - 7\lambda \end{bmatrix}$$

Adjunkte und Inversionsformel

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Wir wenden die Cramersche Regel auf die Gleichung $AX = 1_{n\times n}$ an.

Satz O2R: Adjunkte und Inversionsformel

(0) Zur Matrix $A = (a_1, \dots, a_n) \in K^{n\times n}$ definieren wir ihre **adjunkte Matrix** $A' = \operatorname{adj}(A) \in K^{n\times n}$ durch die (transponierten!) Cofaktoren

$$a'_{ij} := \det(a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n).$$

(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

$$\boxed{A^{-1} = \det(A)^{-1} \operatorname{adj}(A).}$$

Adjunkte und Inversionsformel

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beweis: (1a) Wir berechnen $D = A' \cdot A$ koeffizientenweise:

$$\begin{aligned} d_{ik} &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{n} a'_{ij} a_{jk} \\ &\overset{\text{Def}}{=} \textstyle\sum_{j=1}^{n} \det(a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n) a_{jk} \\ &\overset{\text{Lin}}{=} \det(a_1, \dots, a_{i-1}, \textstyle\sum_{j=1}^{n} e_j a_{jk}, a_{i+1}, \dots, a_n) \\ &\overset{\text{Def}}{=} \det(a_1, \dots, a_{i-1}, a_k, a_{i+1}, \dots, a_n) \overset{\text{Alt}}{=} \delta_{ik} \det(A) \end{aligned}$$

Das zeigt $A' \cdot A = \det(A) \cdot 1_{n \times n}$. Ebenso zeigen Sie $A \cdot A' = \det(A) \cdot 1_{n \times n}$.

Die allgemeine lineare Gruppe $\mathrm{GL}_n\, K$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2R: die allgemeine lineare Gruppe über einem kommutativen Ring

(3) Genau dann ist A in $K^{n\times n}$ invertierbar, wenn $\det(A)$ in K dies ist:

$$\mathrm{GL}_n(K) \overset{(2)}{=} \left\{ A \in K^{n\times n} \,\middle|\, \det(A) \in K^\times \right\}$$

Die spezielle lineare Gruppe $\mathrm{SL}_n\, K$

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2R: die spezielle lineare Gruppe über einem kommutativen Ring

(4) Die Matrizen mit Determinante 1 bilden die **spezielle lineare Gruppe**

$$\mathrm{SL}_n(K) := \left\{ A \in K^{n\times n} \,\middle|\, \det(A) = 1 \right\} = \mathrm{Ker}(\det{}_K^n) \overset{(3)}{\trianglelefteq} \mathrm{GL}_n(K).$$

Beispiele: Über K haben wir $\mathrm{GL}_1(K) = K^\times$ und $\mathrm{SL}_1(K) = \{1\}$ sowie

$$\mathrm{GL}_2(K) = \left\{ \left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right] \,\middle|\, ad - bc \in K^\times \right\}, \qquad \begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$

$$\mathrm{SL}_2(K) = \left\{ \left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right] \,\middle|\, ad - bc = 1 \right\},$$

Determinante von Dreiecksmatrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Berechnen Sie die Determinante jeder oberen Dreiecksmatrix:

$$A = \begin{bmatrix} \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{bmatrix}$$

$$\det(A) \overset{\text{Def}}{=} \sum_{\sigma \in \mathrm{S}_n} \operatorname{sign}(\sigma) \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n} \overset{\square}{=} \lambda_1 \cdots \lambda_n$$

Determinante von Dreiecksmatrizen

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O2w: Determinante einer Dreiecksmatrix

(1) Sei $A \in K^{n\times n}$ eine 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 O2K.

(2) Entsprechendes gilt für jede Block-Dreiecksmatrix:

$$A = \begin{bmatrix} B_{11} & * & * & * \\ 0 & B_{22} & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & B_{\ell\ell} \end{bmatrix} \quad \text{oder} \quad \begin{bmatrix} B_{11} & 0 & 0 & 0 \\ * & B_{22} & 0 & 0 \\ * & * & \ddots & 0 \\ * & * & * & B_{\ell\ell} \end{bmatrix}$$

In diesem Fall gilt $\det(A) = \det(B_{11})\cdot\det(B_{22})\cdots\det(B_{\ell\ell})$ dank O2K.

Beispiel: eine Block-Dreiecksmatrix

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$A = \begin{bmatrix} 1 & 2 & * & * & * & * & * & * & * \\ 3 & 4 & * & * & * & * & * & * & * \\ 0 & 0 & 2 & * & * & * & * & * & * \\ 0 & 0 & 0 & 3 & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 4 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 5 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & \lambda & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 7 & 8 & 9 \end{bmatrix} \in \mathbb{R}^{9\times 9}$$

$$\det(A) = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \begin{vmatrix} 1 & 2 & 3 \\ 4 & \lambda & 6 \\ 7 & 8 & 9 \end{vmatrix} = (-2) \cdot 120 \cdot (60 - 12\lambda)$$

$$= -2880 \cdot (5 - \lambda)$$

Berechnung der Determinante dank Gauß–Verfahren

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Bemerkung O2x: Spalten- und Zeilenoperationen

1. Transvektion $T_{ij}(\lambda)$ ändert nichts (O2C), $\det(T_{ij}(\lambda)) = 1$.
2. Skalierung $S_i(\mu)$ multipliziert mit μ (O2M), $\det(S_i(\mu)) = \mu$.
3. Vertauschung P_{ij} multipliziert mit -1 (O2F), $\det(P_\sigma) = \operatorname{sign}(\sigma)$.

Algo O2Y: effiziente 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 dank Gauß D2H
2: return $\det(A) = \det(S)^{-1}\det(B)$ dank O2X und O2W

Rechenaufwand: Gauß–Verfahren vs 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	Zeit bei
7	343	35 280	10^{12} op/s
8	512	322 560	GPU/CPU:
9	729	3 265 920	
10	1000	36 288 000 😐	< 1 ms
15	3375	$\approx 2 \cdot 10^{13}$ ☹	≈ 20 s
20	8000	$\approx 5 \cdot 10^{19}$ ☹	$\gtrapprox 1.5$ a
25	15625	$\approx 2 \cdot 10^{25}$ ☹	$\gtrapprox 10^7$ a
100	10^6	$\approx 9 \cdot 10^{157}$ ☹	kosmisch

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Rückblick: Was sagt uns die Determinante?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\det_K^n : K^{n\times n} \to K : A \mapsto \det A \overset{\text{Def}}{=} \sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \prod_{j=1}^n a_{\sigma(j),j}$$

Algebraisch: Genau dann ist A im Matrixring $K^{n\times n}$ invertierbar / regulär, wenn $\det A$ im Ring K dies ist.

Geometrisch über den reellen Zahlen $\mathbb{R}$: Die Determinante $\det A$ misst die Volumenverzerrung der linearen Abbildung $f_A : \mathbb{R}^n \to \mathbb{R}^n : x \mapsto Ax$.

Überblick: Fast alle Matrizen $A \in \mathbb{R}^{n\times n}$ sind regulär, singuläre haben Wkt 0 (dünn), singuläre werden regulär durch beliebig kleine Störung (dicht), reguläre bleiben regulär bei hinreichend kleiner Störung (offen).

Rückblick: Wie berechnen wir die Determinante?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

0. Leibniz–Formel $K^{n\times n} \to K : A \mapsto \det A = \sum_{\sigma\in \mathrm{S}_n} \operatorname{sign}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j}$.
1. Rekursive Laplace–Entwicklung nach einer Zeile oder einer Spalte.
2. Multiplikativität $\det(AB) = \det(A)\det(B)$, damit Gauß–Verfahren!

Ist jede invertierbare Matrix quadratisch?

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \overset{!}{=} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\boxed{A} \cdot \boxed{B} \overset{?}{=} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

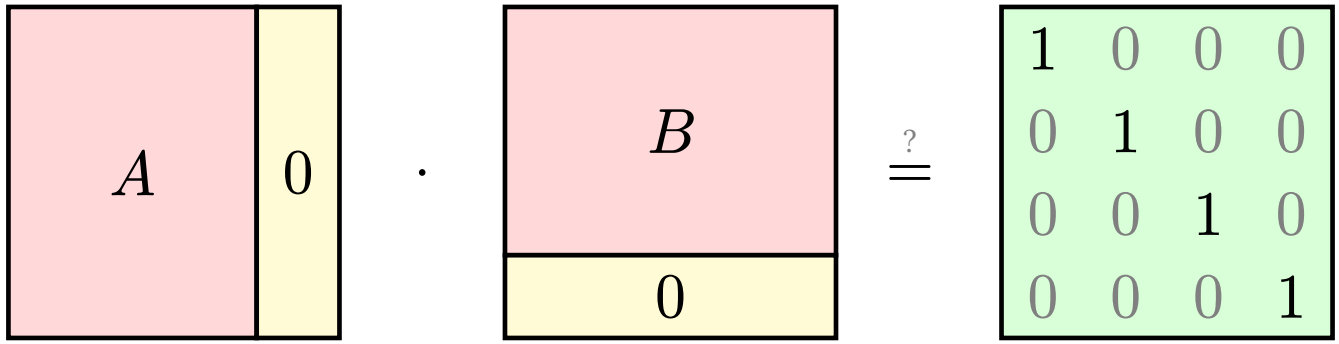
Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Invertierbare Matrizen über einem kommutativen Ring

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.



Satz O3A: Invertierbare Matrizen sind quadratisch.

Sei $(K, +, 0, \cdot, 1)$ ein kommutativer Ring mit $0 \neq 1$ sowie $m, n \in \mathbb{N}$.
(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 jede Matrix $A \in K^{n \times m}$ gilt: Ist A invertierbar, so folgt $n = m$.

Beweis: (1) Wäre $m < n$, so ergänzen wir durch Nullen zu $A', B' \in K^{n \times n}$. Somit gilt $\det(A') = \det(B') = 0$ (O2B), andererseits $A' \cdot B' = 1_{n \times n}$, also:

$$0 \overset{\text{Vor}}{=} \det(A') \cdot \det(B') \overset{\text{O2O}}{=} \det(A' \cdot B') \overset{\text{Vor}}{=} \det(1_{n \times n}) \overset{\text{Def}}{=} 1 \quad ↯$$

Die Determinante eines Endomorphismus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Können sich Alice und Bob auf „die Determinante“ einigen?

$$
\begin{tikzcd}
K^n \arrow[rrr, "A = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(f)"] \arrow[dr, "\Phi_{\mathcal{B}}", "\cong"'] \arrow[d, shift right, "\mathrm{T}_{\mathcal{B}}^{\mathcal{B}'}", "\cong"'] & & & K^n \arrow[dl, "\Phi_{\mathcal{B}}"', "\cong"] \arrow[d, shift right, "\mathrm{T}_{\mathcal{B}}^{\mathcal{B}'}"', "\cong"] \\
K^n \arrow[u, shift right, "\mathrm{T}_{\mathcal{B}'}^{\mathcal{B}}", "\cong"'] \arrow[r, "\Phi_{\mathcal{B}'}", "\cong"'] & V \arrow[rr, "f"] & & V \arrow[l, "\Phi_{\mathcal{B}'}"', "\cong"] \\
K^n \arrow[rrr, "A' = \mathrm{M}_{\mathcal{B}'}^{\mathcal{B}'}(f)"'] & & & K^n \arrow[u, shift right, "\mathrm{T}_{\mathcal{B}'}^{\mathcal{B}}", "\cong"']
\end{tikzcd}
$$

In $K^{n\times n}$ haben wir $A' = T^{-1} \cdot A \cdot T$ mit $T = \mathrm{T}_{\mathcal{B}'}^{\mathcal{B}}$ und $T^{-1} = \mathrm{T}_{\mathcal{B}}^{\mathcal{B}'}$. Also:

$$\det(A') \overset{\text{O2o}}{=} \det(T)^{-1} \cdot \det(A) \cdot \det(T) \overset{\text{Com}}{=} \det(A)$$

Somit ist die Determinante $\det_V(f) := \det(A) = \det(A')$ wohldefiniert.

Die Determinante eines Endomorphismus

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiel: Wir betrachten die Ableitung ∂ auf dem $\mathbb{C}$–Vektorraum

$$\begin{aligned} V &= \langle \cos(2t), \sin(2t), \cos(3t), \sin(3t) \rangle_{\mathbb{C}}^{!} \\ &= \langle \mathrm{e}^{2\mathrm{i}t}, \mathrm{e}^{-2\mathrm{i}t}, \mathrm{e}^{3\mathrm{i}t}, \mathrm{e}^{-3\mathrm{i}t} \rangle_{\mathbb{C}}^{!} \quad \leq \quad \mathbb{C}^{\mathbb{R}}. \end{aligned}$$

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:

$$\mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) = \begin{bmatrix} 0 & 2 & 0 & 0 \\ -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & -3 & 0 \end{bmatrix}, \qquad \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} 2\mathrm{i} & 0 & 0 & 0 \\ 0 & -2\mathrm{i} & 0 & 0 \\ 0 & 0 & 3\mathrm{i} & 0 \\ 0 & 0 & 0 & -3\mathrm{i} \end{bmatrix}$$

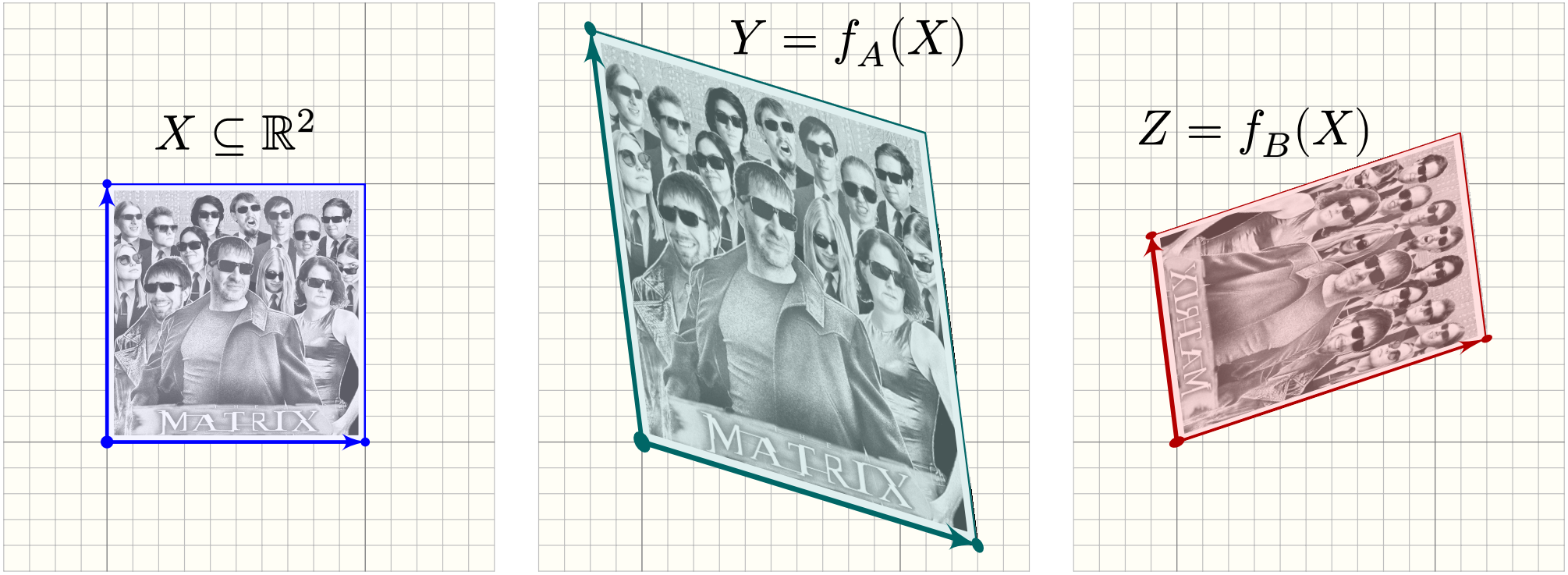
$$\det_V(\partial) \overset{\text{O3D}}{=} \det \mathrm{M}_{\mathcal{A}}^{\mathcal{A}}(\partial) \overset{\text{O3D}}{=} \det \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) \overset{\text{O2W}}{=} 36$$

Die Determinante misst Volumen und Orientierung.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$A = \begin{bmatrix} 1.3 & -0.2 \\ -0.4 & 1.6 \end{bmatrix} \quad \text{vs} \quad B = \begin{bmatrix} -0.1 & 1.2 \\ 0.8 & 0.4 \end{bmatrix}$$



Wir finden hier $\det(A) = +2$ und $\det(B) = -1$.

Die Determinante misst Volumen und Orientierung.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Die Volumenverzerrung wird gemessen durch den Betrag

$$v : (\mathbb{R}^{n\times n}, \cdot, 1_{n\times n}) \xrightarrow{\det} (\mathbb{R}, \cdot, 1) \xrightarrow{\mathrm{abs}} (\mathbb{R}_{\geq 0}, \cdot, 1) : A \mapsto |\det(A)|,$$

$$(\mathrm{GL}_n\,\mathbb{R}, \cdot, 1_{n\times n}) \xrightarrow{\det} (\mathbb{R}^\times, \cdot, 1) \xrightarrow{\mathrm{abs}} (\mathbb{R}_{>0}, \cdot, 1).$$

Das Orientierungsverhalten wird gemessen durch das Vorzeichen

$$\varepsilon : (\mathbb{R}^{n\times n}, \cdot, 1_{n\times n}) \xrightarrow{\det} (\mathbb{R}, \cdot, 1) \xrightarrow{\mathrm{sign}} (\{\pm 1, 0\}, \cdot, 1),$$

$$(\mathrm{GL}_n\,\mathbb{R}, \cdot, 1_{n\times n}) \xrightarrow{\det} (\mathbb{R}^\times, \cdot, 1) \xrightarrow{\mathrm{sign}} (\{\pm 1\}, \cdot, 1).$$

Wie orientieren wir einen $\mathbb{R}$–Vektorraum?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Definition O3E: die beiden Orientierungen eines $\mathbb{R}$–Vektorraums

Sei V ein $\mathbb{R}$–Vektorraum endlicher Dimension $\dim_{\mathbb{R}}(V) = n \in \mathbb{N}$.

(1) Eine **Orientierung** von V ist eine Zuordnung $\alpha : \{\text{Basen}\} \to \{\pm 1\}$ mit $\alpha(\mathcal{C}) = \alpha(\mathcal{B}) \cdot \varepsilon(\mathrm{T}_{\mathcal{B}}^{\mathcal{C}})$ für je zwei Basen $\mathcal{B}$ und $\mathcal{C}$ von V über $\mathbb{R}$.

(2) Als **Standardorientierung** auf $\mathbb{R}^n$ definieren wir $\varepsilon : \mathcal{B} \mapsto \operatorname{sign}\det(\mathcal{B})$. Jeder $\mathbb{R}$–Vektorraum V hat genau zwei Orientierungen, nämlich $\pm\alpha$.

(3) Ein Isomorphismus $h : (V, \alpha) \xrightarrow{\sim} (V', \alpha')$ orientierter $\mathbb{R}$–Vektorräume heißt **orientierungserhaltend/umkehrend**, falls $\alpha' \circ h = +\alpha$ bzw. $= -\alpha$.

Wie orientieren wir einen $\mathbb{R}$–Vektorraum?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beispiele: (0) Auf $\mathbb{R}^0 = \{0\}$ ist die Standardorientierung $\varepsilon : () \mapsto +1$.
(1) Die Gerade $\mathbb{R}^1$ teilt $\varepsilon = \operatorname{sign} : \mathbb{R}^\times \to \{\mp 1\}$ in „links“ und „rechts“.
(2) Auch in der Ebene $\mathbb{R}^2$ sagt $\varepsilon(b_1, b_2) = \mp 1$ ob „links“ oder „rechts“.

Jede Basis $\mathcal{B}$ von V definiert eine Orientierung $[\mathcal{B}]$ auf V mit $[\mathcal{B}](\mathcal{B}) = +1$.
Die Orientierung $[\mathcal{B}]$ ist demnach explizit gegeben durch $[\mathcal{B}](\mathcal{C}) := \varepsilon(\mathrm{T}_{\mathcal{B}}^{\mathcal{C}})$.
Die Standardbasis von $\mathbb{R}^n$ ergibt die Standardorientierung $\varepsilon = [e_1, \dots, e_n]$.

Wie orientieren wir einen $\mathbb{R}$–Vektorraum?

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Wie orientieren Sie folgende Vektorräume?

$$\begin{aligned} &(1) \quad U = \{\, x \in \mathbb{R}^4 \mid x_1 + x_2 + x_3 + x_4 = 0 \,\} && \leq \mathbb{R}^4 \\ &(2) \quad V = \langle 1, \cos, \sin \rangle_{\mathbb{R}}^{!} && \leq \mathbb{R}^{\mathbb{R}} \end{aligned}$$

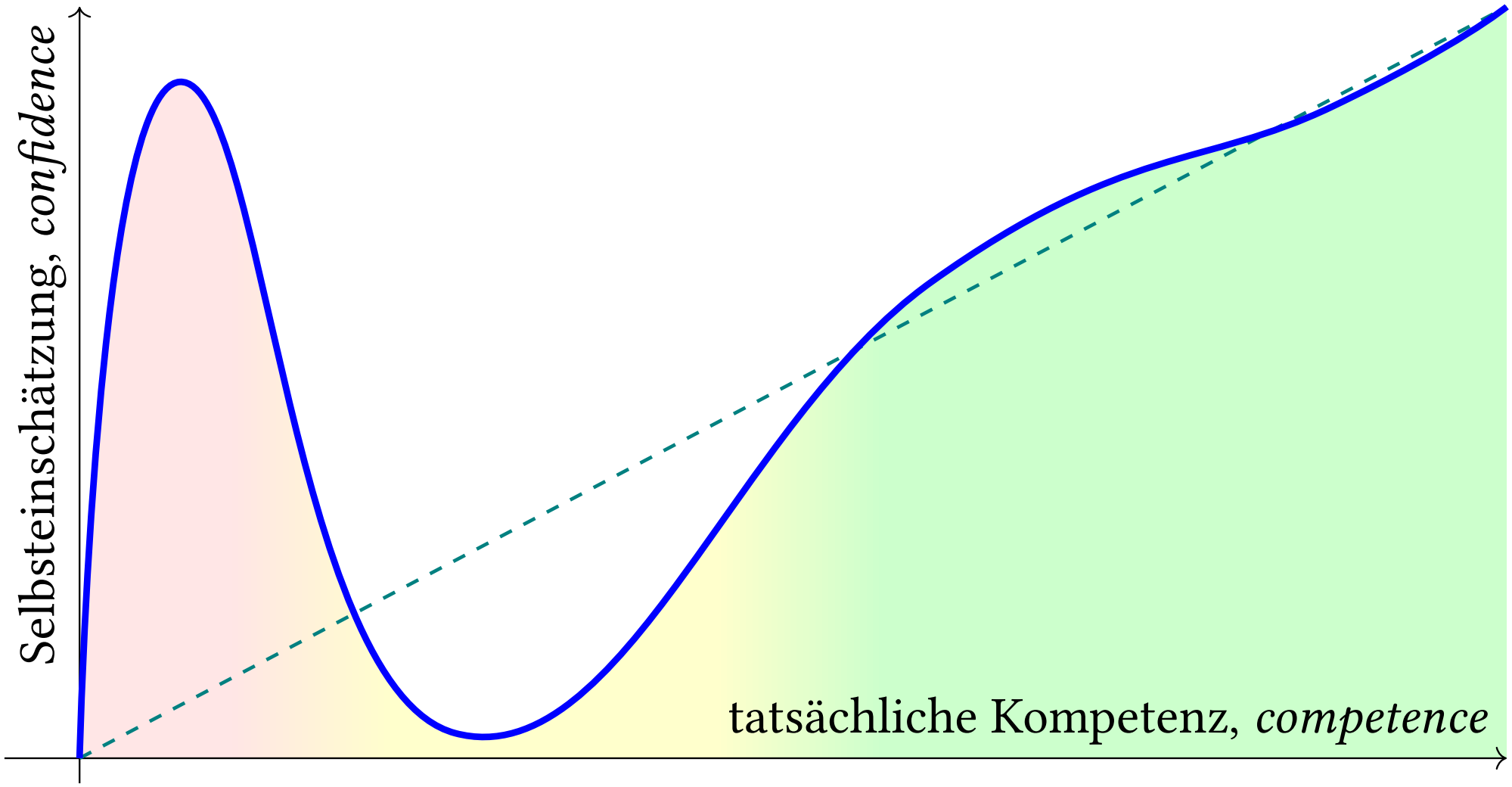
Aufgabe: Welches Orientierungsverhalten hat ∂ auf $W = \langle \cos, \sin \rangle_{\mathbb{R}}^{!}$?

Lösung: Wir wählen eine *beliebige* Basis von W, etwa $\mathcal{B} = (\cos, \sin)$.

$$A = \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\partial) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \Longrightarrow \quad \det_W(\partial) \overset{\text{Def}}{=} \det_{\mathbb{R}}^{2}(A) = +1$$

Lernen ist ein mühsamer Prozess, doch er lohnt sich!

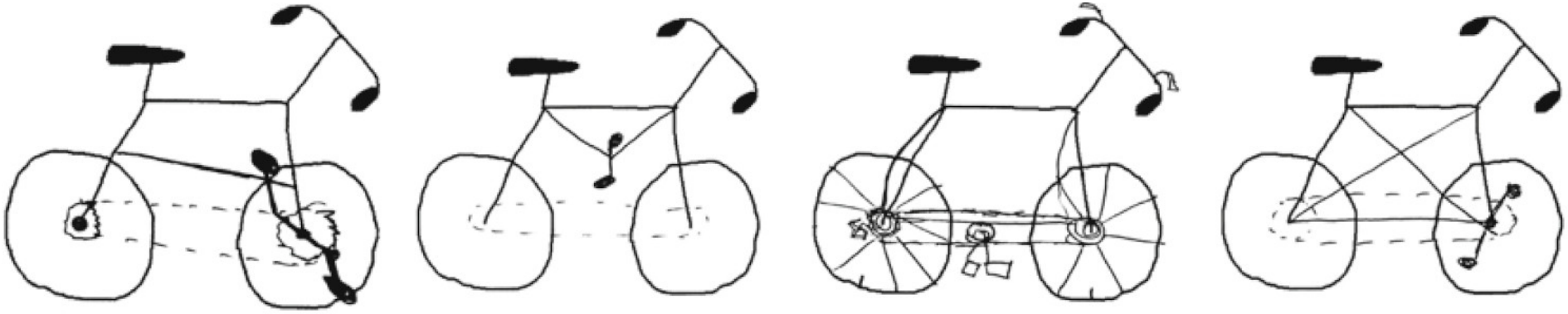
Sie wollen lernen. – Aller Anfang ist schwer. – Wir unterstützen Sie.



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Studium: Sie erarbeiten sich die nötige Erklärtiefe!

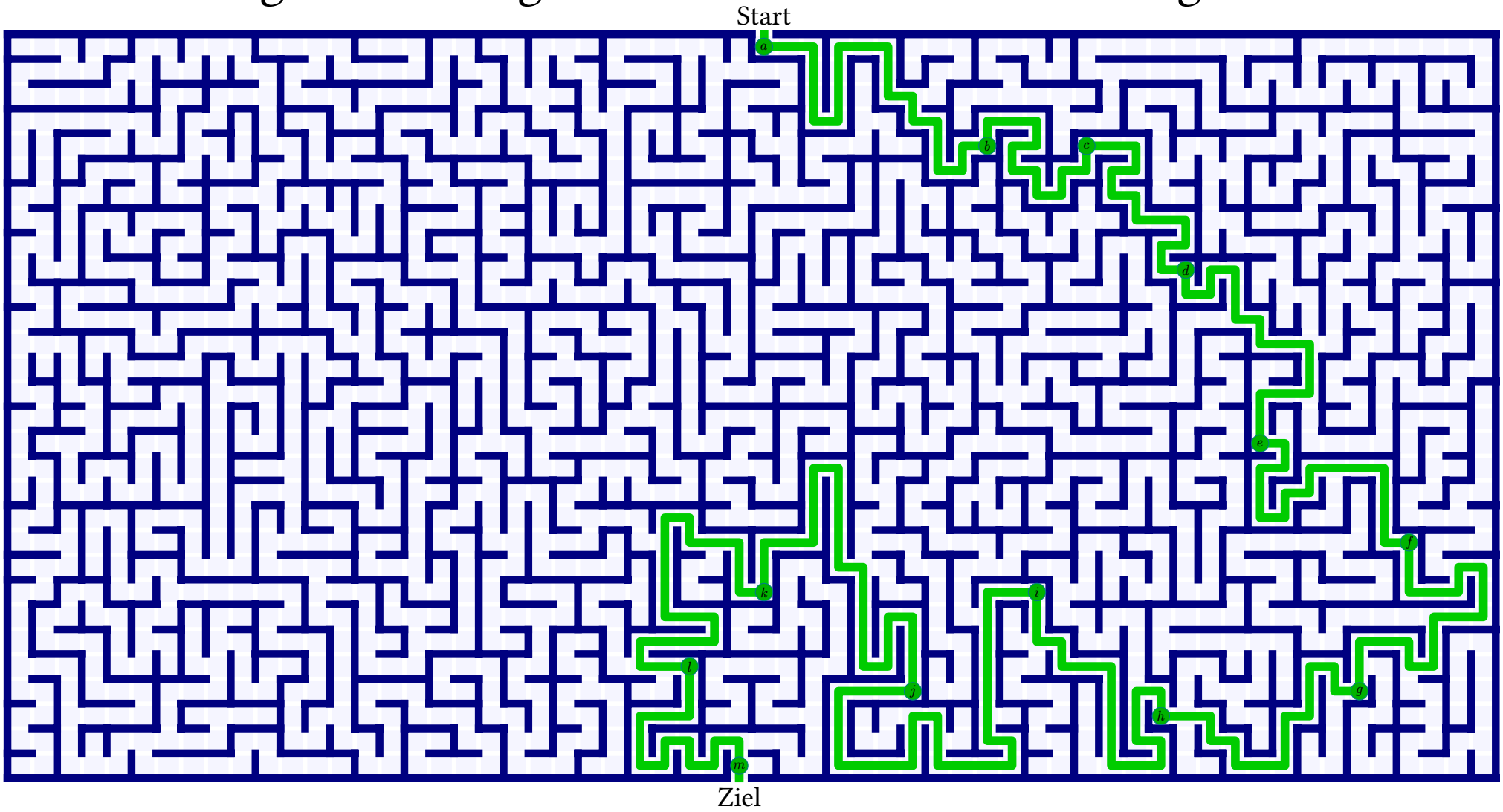


Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Unsere Arbeitsteilung zwischen Lehren und Lernen

Ich führe Argumente sorgsam vor. — Sie arbeiten alles gründlich nach.



Dies ist nur die Saalversion ohne Erläuterungen.

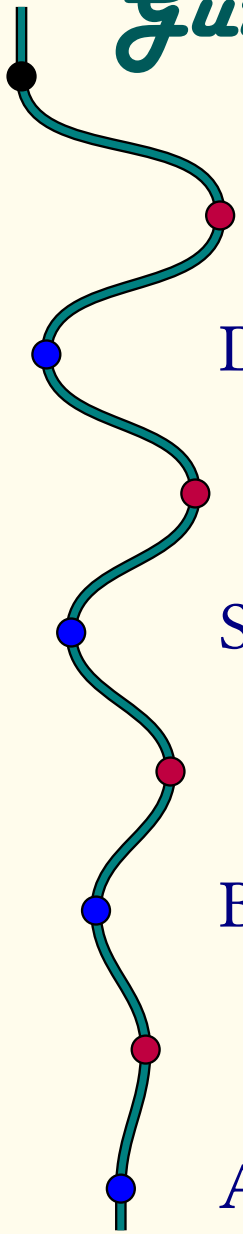
Ausführliche Erläuterungen bietet die Vollversion.

Die Struktur der Mathematik hilft Ihnen!

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Gute mathematische Kommunikation



Motivation — einführende Beispiele

Definition — Vereinbarung, Konvention, Notation

Gegen/Beispiele — Miss/Verständnis

Satz — Feststellung, Rechenregel, Algorithmus

Gegen/Beispiele — Fehl/Anwendung

Beweis — Begründung, Rechenweg, Verfahren

kritischer Rückblick — Feinschliff

Anwendungen, Quiz, Übung, Prüfung, ...

Ihr Ziel ist hehr, der Weg ist lang.

Dies ist nur die Saalversion ohne Erläuterungen.

Linear Algebra 2020/21

WƎLCOME TO

$$\begin{bmatrix} 1 & \bullet \\ \bullet & 1 \end{bmatrix}$$

THE MATRIX!

There is a difference between
knowing the path and walking the path.

Linear Algebra 2020/21

TRANSFORM

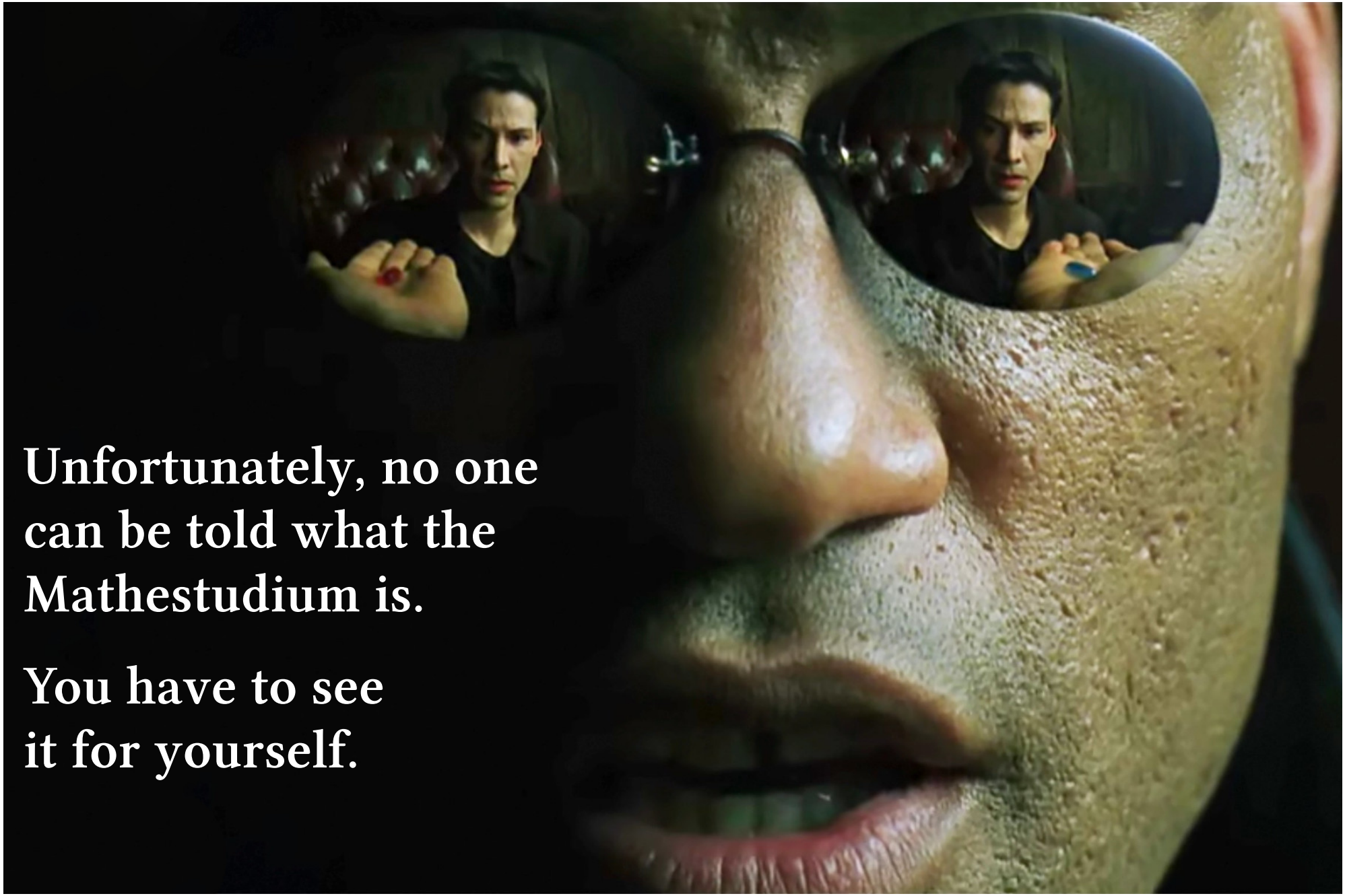
$$\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$$

THƎ MATR1X!

I can only show you the door.
You're the one that has to walk through it.

Ausführliche Erläuterungen bietet die Vollversion.

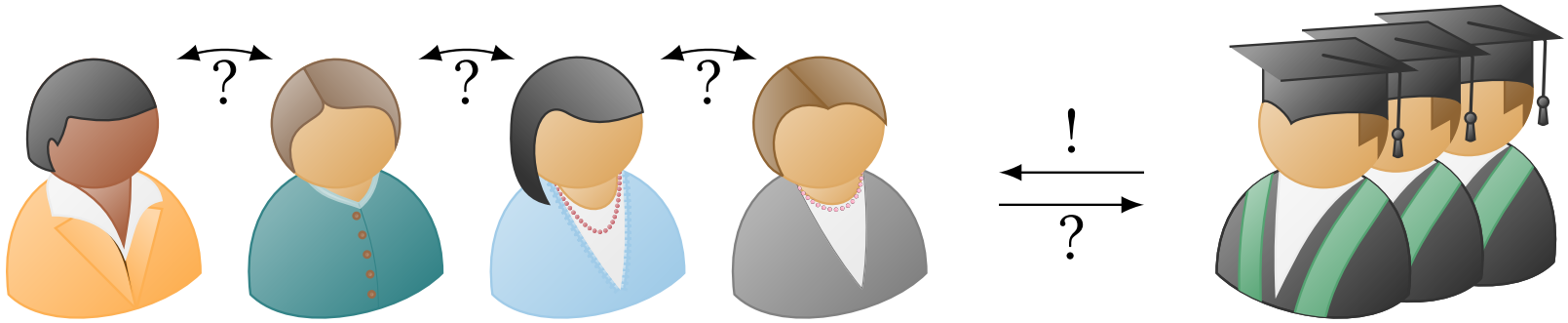
Ihr Ziel ist hehr, der Weg ist lang.



Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Beste Betreuung durch Ihr LinA-Team



Lea Pia Ida Mia … Team LinA

Alles wird gut. Keine Panik!

Your Hitchhiker's Guide to Mathematics

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Schöne Mathematik – gute Vorlesung – faire Klausur

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Kapitel O

Bonusmaterial

You cannot read mathematics the way you read a novel. If you zip through a page in less than an hour, you are probably going too fast. When you encounter the phrase "as you should verify", you should indeed do the verification, which will usually require some writing on your part. When steps are left out, you need to supply the missing pieces. You should ponder and internalize each definition. For each theorem, you should seek examples to show why each hypothesis is necessary. Discussions with other students should help. [...] Mathematics can be learned only by doing.

Sheldon Axler, *Linear Algebra Done Right* (2026)

Inhalt dieses Kapitels O

5 Große Matrizen, doch gut strukturiert

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Eine 10×10–Matrix, doch gut strukturiert

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 & 4 \\ 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 & 3 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix} \overset{(a)}{=} \begin{vmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix}$$

Vorgehen: (a) Von der i-ten Zeile subtrahieren wir die $(i+1)$-te für $i = 1, \dots, 9$ (b) Wir addieren die erste Spalte zu jeder folgenden Spalte $j = 2, \dots, 10$. Wir erhalten:
$\det(A) \;=\; -2^8 \cdot 3^2 \;=\; -2304$

$$\overset{(b)}{=} \begin{vmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & -2 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & -2 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & -2 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & -2 & 0 & 0 \\ * & * & * & * & * & * & * & * & -2 & 0 \\ * & * & * & * & * & * & * & * & * & 9 \end{vmatrix}$$

Vandermonde–Matrix und ihre Determinante

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Aufgabe: Berechnen Sie die Determinante der **Vandermonde–Matrix**

$$V(x_0, \dots, x_n) := (x_i^j)_{i=0,\dots,n}^{j=0,\dots,n} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix} \in K^{(n+1)\times(n+1)}.$$

$$\begin{vmatrix} 1 \end{vmatrix} = 1, \qquad \begin{vmatrix} 1 & x_0 \\ 1 & x_1 \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ 1 & x_1 - x_0 \end{vmatrix} = x_1 - x_0$$

Vandermonde–Matrix und ihre Determinante

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

$$
\begin{aligned}
\begin{vmatrix} 1 & x_0 & x_0^2 \\ 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \end{vmatrix}
&\overset{(a)}{=}
\begin{vmatrix} 1 & 0 & 0 \\ 1 & x_1 - x_0 & (x_1 - x_0)x_1 \\ 1 & x_2 - x_0 & (x_2 - x_0)x_2 \end{vmatrix} \\
&\overset{(b)}{=}
\begin{vmatrix} x_1 - x_0 & (x_1 - x_0)x_1 \\ x_2 - x_0 & (x_2 - x_0)x_2 \end{vmatrix} \\
&\overset{(c)}{=}
(x_1 - x_0)(x_2 - x_0) \begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix}
\end{aligned}
$$

Vandermonde–Matrix und ihre Determinante

Dies ist nur die Saalversion ohne Erläuterungen.

Ausführliche Erläuterungen bietet die Vollversion.

Satz O5A: die Vandermonde–Matrix und ihre Determinante

$$V = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix} \quad \Longrightarrow \quad \det V = \prod_{i<j} (x_j - x_i)$$