

Kapitel J

Basis und Dimension

*Good general theory does not
search for the maximum generality,
but for the right generality.*

Saunders Mac Lane (1909–2005)

Inhalt dieses Kapitels J

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

- 2 Konstruktion von Basen
 - Existenz von Basen
 - Erste Anwendungen
 - Exakte Sequenzen

- 3 Aufgaben und Ergänzungen

In diesem Kapitel erarbeiten wir die Begriffe **Basis** und **Dimension**. Diese schlagen die Brücke von der allgemeinen Theorie der linearen Räume zur Matrizenrechnung, insbesondere zum Gauß–Algorithmus über Divisionsringen (B2c) und seinen zahlreichen Anwendungen.

Damit verbinden wir beides: starke Theorie und effiziente Algorithmen! Das ist der Grund für den anhaltenden Erfolg der Linearen Algebra. Lineare Methoden sind ungemein praktisch und werden überall genutzt, innerhalb der Mathematik und in ihren zahlreichen Anwendungen.

Aller Voraussicht nach wird diese Kombination auch in den nächsten hundert Jahren weiter erfolgreich sein. Gerade aktuell aufstrebende Anwendungen wie Data Science und Quantum Computing benötigen diese Verbindung; aus abstrakter Theorie werden konkrete Methoden.

😊 Mathematische Abstraktion ist etwas Gutes, Sie sollten sie nicht fürchten, sondern nutzen lernen. Im Idealfall bedeutet sie nicht Anwendungsferne, sondern im Gegenteil vielseitige Anwendbarkeit. (Ich muss dies betonen, weil manchmal das Gegenteil behauptet wird.)

Natürlich sind wir mit unseren bescheidenen Grundlagen noch weit entfernt von hochfliegenden Anwendungen, doch wir bauen darauf zu. Der Weg ist zwar weit, doch wir gehen ihn unbeirrt Schritt um Schritt. Sie sind gerüstet, egal, welchen Abzweig Sie später einschlagen.

Lohnt sich die Sorgfalt und die Mühe der Grundlagen? Ich denke ja. Mathematische Erkenntnis und solide wissenschaftliche Arbeit haben einen extrem langen Nutzen. Die Investition lohnt sich!

Im letzten Kapitel haben wir die allgemeinen Begriffe zu linearen Räumen über einem Ring R erklärt. Nun wollen wir etwas spezifischer werden und tieferliegende Techniken erarbeiten. Dazu benötigen wir einen **Divisionsring**, und zwar an zwei ganz wesentlichen Stellen:

- 1 Der Gaußalgorithmus B2c über einem Divisionsring R .
- 2 Der Existenzsatz J2B für Basen über einem Divisionsring R .

Der allgemeine Kontext ist dennoch ein Vorteil: Sie verfügen über ein reichhaltiges Repertoire an illustrativen und relevanten Beispielen! Daran sehen wir insbesondere, was alles schiefgehen kann, und dass unsere Voraussetzungen tatsächlich benötigt werden.

😊 Ein typisches Gegenbeispiel ist der Ring \mathbb{Z} der ganzen Zahlen: Dieser ist natürlich überall wichtig, viele Anwendungen fragen nach ganzzahligen Lösungen. Doch \mathbb{Z} ist leider kein Körper, und oft ist es heilsam, sich einfache Gegenbeispiele über \mathbb{Z} vor Augen zu führen.

😊 Wenn Sie möchten, können Sie sich in diesem gesamten Kapitel R als einen Divisionsring vorstellen, oder besser noch einen Körper. Die meisten Zahlenbeispiele, die ich hier zur Illustration vorstelle, sind ganz konventionell und arbeiten über den Körpern $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(Ich hatte hie und da auch nicht-kommutative Beispiele im Sinn, etwa Hamiltons Quaternionen, doch diese scheinen bei den Studierenden auf wenig Gegenliebe zu treffen. Es bleibt genug anderes Schönes.)

😊 Viele Ergebnisse sind wörtlich genauso über jedem Ring gültig, daher gehe ich behutsam vor und sage jeweils dazu, was benötigt wird. Das entspricht einer gewissen Denkökonomie und Nachhaltigkeit: Wir nehmen nur so viel, wie wir wirklich brauchen.

Der einzige Nachteil ist, dass man sich die nötigen Voraussetzungen merken muss. Das gelingt am besten, indem Sie die Beweise kennen! Ich hoffe, der mögliche Nachteil wandelt sich so in einen Vorteil, da nun transparenter wird, was wie wo genutzt wird.

Matrizen $A \in R^{m \times n}$ operieren von links auf Spaltenvektoren $R^{n \times 1} \cong R^n$. Skalare $\lambda \in R$ sollten dann von rechts operieren. Durch diese einfache Regel sortieren sich all unsere Formeln und Indexkonventionen von selbst, wie durch Zauberhand fügt sich alles an den rechten Platz.

Diese bessere Buchführung der Indizes halte ich für hilfreich.

Viele Lehrbücher zur Linearen Algebra arbeiten ausschließlich über Körpern. Im kommutativen Fall können wir die Skalare von der einen auf die andere Seite umschreiben, daher stehen dann Skalare meist ebenfalls links. Dagegen ist soweit rein gar nichts einzuwenden.

Die Indexkonventionen sehen dann jedoch recht unnatürlich aus!

Ich mache mir daher die Mühe, beide Sichtweisen zu erklären, sodass Sie für jede Situation die jeweils passende Notation anwenden können. In diesem Kapitel bedeutet das: Matrizen links, Skalare rechts.

Matrizenrechnung ist nicht nur, aber auch, Buchhaltung der Indizes. Das erfordert anfangs etwas Gewöhnung, ist aber letztlich nur eine Frage der Sorgfalt. Wenn Sie anschließend programmieren wollen, und das wollen Sie, dann geht es gar nicht anders!

Ich formuliere daher die entscheidenden Algorithmen hier explizit aus, sodass sie im Idealfall sofort genutzt und implementiert werden können. Das ist für mich als Autor zwar etwas mühsam, aber es nützt Ihnen zur Klarheit und zur direkten Anwendbarkeit. Sie werden dies in den Übungen merken, wenn Sie selbst erste Rechnungen anstrengen.

Auf den ersten Blick mögen die so gewonnenen Formeln abschrecken, und manche wünschen sich Beispiele ohne theoretische Grundlagen, doch ich bin überzeugt, Sie benötigen *beides* zu Ihrem Lernerfolg. Vorlesung und Übungen ergänzen sich daher weiterhin ganz wesentlich. Lernen Sie beides zu schätzen und zu nutzen: Theorie und Praxis.

Definition J1A: Basis, erzeugend und linear unabhängig

Sei $(V, +, \cdot)$ ein (rechts)linearer Raum über dem Ring $(R, +, \cdot)$.

Gegeben sei eine Familie $\mathcal{B} = (b_i)_{i \in I}$ von Vektoren $b_i \in V$.

Diese Familie \mathcal{B} definiert die R -lineare Abbildung

$$\Phi_{\mathcal{B}} : R^{(I)} \rightarrow V : \lambda = (\lambda_i)_{i \in I} \mapsto v = \sum_{i \in I} b_i \lambda_i.$$

Wir nennen die Familie \mathcal{B} ...

- 1 eine **Basis** des linearen Raums V über R , wenn $\Phi_{\mathcal{B}}$ bijektiv ist,
- 2 eine **erzeugende Familie** von V über R , wenn $\Phi_{\mathcal{B}}$ surjektiv ist,
- 3 und **linear unabhängig** in V über R , wenn $\Phi_{\mathcal{B}}$ injektiv ist.

Der R -lineare Raum V heißt **frei**, wenn eine Basis \mathcal{B} in V existiert; das Paar (V, \mathcal{B}) heißt dann ein **basierter linearer Raum** über R .

Wir schreiben die Skalare hier rechts, alles gilt sinngemäß ebenso links. Über einem kommutativen Ring ist diese Unterscheidung unnötig.

Basis, erzeugend und linear unabhängig

Eine Familie $\mathcal{B} = (b_i)_{i \in I}$ in V ist eine Abbildung $\mathcal{B} : I \rightarrow V : i \mapsto b_i$.

Das bedeutet, jedem Index $i \in I$ wird ein Element $b_i \in V$ zugeordnet.

Im Falle $I = \{1, \dots, n\}$ schreiben wir dies auch bequem als Aufzählung

$$\mathcal{B} = (b_i)_{i=1}^n = (b_1, b_2, \dots, b_n).$$


Wir erlauben ebenso unendliche Indexmengen, etwa $I = \mathbb{N}$:

$$\mathcal{B} = (b_i)_{i \in \mathbb{N}} = (b_0, b_1, b_2, \dots).$$

In Definition J1A ist die Indexmenge I zunächst beliebig.

Auch $I = \emptyset$ ist erlaubt; hierbei ist $R^\emptyset = \{0\}$ der Nullraum.

Die Elementezahl $\#I$ nennen wir die **Länge** der Familie \mathcal{B} , oder auch die **Mächtigkeit** oder **Kardinalität** von I bzw. \mathcal{B} .

 Auch wenn die Indexmenge I unendlich ist, so sind doch unsere Linearkombinationen $\sum_{i \in I} b_i \lambda_i$ immer endlich. Dies stellen wir sicher, indem wir nur I -Tupel $\lambda \in R^{(I)}$ mit endlichem Träger zulassen (I1Q).

Das Bild von $\Phi_{\mathcal{B}}$ ist der von \mathcal{B} in V **erzeugte Unterraum** ($\langle \mathcal{B} \rangle$):

$$\text{im}(\Phi_{\mathcal{B}}) = \langle \mathcal{B} \rangle_R = \langle b_i \mid i \in I \rangle_R = \left\{ \sum_{i \in I} b_i \lambda_i \mid \lambda \in R^{(I)} \right\}$$

Jedes I -Tupel $\lambda \in R^{(I)}$ über R mit endlichem Träger (!) definiert die zugehörige **Linearkombination** $\Phi_{\mathcal{B}}(\lambda) = \sum_{i \in I} b_i \lambda_i$ der Familie \mathcal{B} in V .

Äquivalent sind:

- 1 Die Familie \mathcal{B} erzeugt den Raum V über R , kurz $\langle \mathcal{B} \rangle_R = V$.
- 2 Die Abbildung $\Phi_{\mathcal{B}}$ ist surjektiv: siehe Definition J1A(2).
- 3 Jeder Vektor $v \in V$ schreibt sich auf **mindestens** eine Weise als eine Linearkombination $v = \sum_{i \in I} b_i \lambda_i$ mit $\lambda \in R^{(I)}$.

Wir nennen \mathcal{B} dann eine **erzeugende Familie** von V über R , oder ein **R -Erzeugendensystem**, kurz **Erzeugendensystem**.

Die Menge aller Linearkombinationen von \mathcal{B} in V über R heißt auch das **Erzeugnis** oder der **Aufspann** von \mathcal{B} über R .

Die Schreibweise $\langle \mathcal{B} \rangle_R$ betont den hier verwendeten Grundring R . Wenn dieser aus dem Kontext klar ist, so schreiben wir auch kurz $\langle \mathcal{B} \rangle$.

Im Falle einer endlichen Familie $\mathcal{B} = (b_1, \dots, b_n)$ schreiben wir auch

$$\begin{aligned} \langle \mathcal{B} \rangle &= \langle v_i \mid i = 1, \dots, n \rangle = \langle b_1, \dots, b_n \rangle \\ &= \langle b_1, \dots, b_n \rangle_R = b_1 R + \dots + b_n R \leq V. \end{aligned}$$

Je nach Situation ist die eine oder die andere Schreibweise bequemer. All diese Notationen beschreiben das Bild von $\Phi_{\mathcal{B}} : R^{(I)} \rightarrow V$.

Es erweist sich im Folgenden meist als besser, nicht nur die Bildmenge $\text{im}(\Phi_{\mathcal{B}}) = \langle \mathcal{B} \rangle \subseteq V$ zu nutzen, sondern explizit auch die Abbildung $\Phi_{\mathcal{B}}$.

Der Kern der Abbildung $\Phi_{\mathcal{B}} : R^{(I)} \rightarrow V$ ist

$$\ker(\Phi_{\mathcal{B}}) = \left\{ \lambda \in R^{(I)} \mid \sum_{i \in I} b_i \lambda_i = 0 \right\}.$$

Jedes Element $\lambda \in \ker(\Phi_{\mathcal{B}})$ heißt eine **Relation** zwischen den Vektoren $(b_i)_{i \in I}$ in V , im Falle $\lambda \neq 0$ nennen wir dies eine **nicht-triviale Relation** und die Familie \mathcal{B} ist **linear abhängig**. Äquivalent sind:

- 1 Die Familie \mathcal{B} ist linear unabhängig in V über R .
- 2 Die Abbildung $\Phi_{\mathcal{B}}$ ist injektiv: siehe Definition J1A(3).
- 3 Jeder Vektor $v \in V$ schreibt sich auf **höchstens** eine Weise als eine R -Linearkombination $v = \sum_{i \in I} b_i \lambda_i$ mit $\lambda \in R^{(I)}$.
- 4 Es gilt $\ker(\Phi_{\mathcal{B}}) = \{0\}$: Der Kern von $\Phi_{\mathcal{B}}$ ist trivial, siehe I1R.
- 5 Der Nullvektor $0 \in V$ schreibt sich nur auf **genau** eine Weise als R -Linearkombination: Aus $\lambda \in R^{(I)}$ und $0 = \sum_{i \in I} b_i \lambda_i$ folgt $\lambda = 0$.

Wir nennen \mathcal{B} dann eine **linear unabhängige Familie** in V über R , oder einfach **R -linear unabhängig**, kurz **linear unabhängig**.

Das unscheinbare Injektivitätskriterium (4) ist überaus praktisch und wird sich im Folgenden immer wieder als hilfreich erweisen.

Arbeitersparnis: Für die Injektivität von $\Phi_{\mathcal{B}} : R^{(I)} \rightarrow V$ brauchen wir nur eine einzige Faser zu überprüfen, nämlich $\ker(\Phi_{\mathcal{B}}) = \Phi_{\mathcal{B}}^{-1}(\{0\})$.

😊 Die explizite Umformulierung (5) ist daher meist ein effizienter Ansatz, um lineare Un/Abhängigkeit zu prüfen. Konkret heißt das:

Zum Nachweis der **linearen Abhängigkeit** genügt ein Gegenbeispiel, also eine nicht-triviale Relation $\lambda \in R^{(I)}$, das heißt $\lambda \neq 0$ mit

$$\sum_{i \in I} b_i \lambda_i = 0.$$

Zum Nachweis der **linearen Unabhängigkeit** setzen wir umgekehrt die Gleichung $\sum_{i \in I} b_i \lambda_i = 0$ für $\lambda \in R^{(I)}$ an und müssen dann zeigen, dass $\lambda = 0$ die einzige Lösung ist.

⚠ Das klingt zunächst ganz einfach, und das ist es im Prinzip auch, doch diese Technik erfordert einige Übung und vor allem Sorgfalt!

Die Lineare Unabhängigkeit und die Erzeugung von V fassen wir zum Begriff der Basis zusammen, wie in Definition J1A vereinbart.

Äquivalent sind:

- 1 Die Familie \mathcal{B} ist eine Basis des Raums V über R .
- 2 Die Abbildung $\Phi_{\mathcal{B}} : R^{(I)} \rightarrow V$ ist ein Isomorphismus.
- 3 Es gilt $\ker(\Phi_{\mathcal{B}}) = \{0\}$ und $\text{im}(\Phi_{\mathcal{B}}) = V$.
- 4 Die Familie \mathcal{B} ist linear unabhängig und erzeugt V über R .
Wir schreiben hierfür abkürzend $V = \langle \mathcal{B} \rangle_R^!$.
- 5 Jeder Vektor $v \in V$ schreibt sich auf **genau** eine Weise als eine R -Linearkombination $v = \sum_{i \in I} b_i \lambda_i$ mit $\lambda \in R^{(I)}$.

Wir nennen $\Phi_{\mathcal{B}} : R^{(I)} \rightarrow V$ das **Koordinatensystem** von V zur Basis \mathcal{B} und $\lambda = (\lambda_i)_{i \in I} = \Phi_{\mathcal{B}}^{-1}(v)$ den **Koordinatenvektor** von v bezüglich \mathcal{B} .

Zur Notation $V = \langle \mathcal{B} \rangle_R^!$ sagen wir, V wird **frei erzeugt** von \mathcal{B} über R . Das beinhaltet zwei Aussagen: V wird von \mathcal{B} erzeugt, also $V = \langle \mathcal{B} \rangle_R$, und \mathcal{B} ist frei, also ohne Relationen, das heißt R -linear unabhängig. Das ist eine bequeme Formel für „ \mathcal{B} ist eine Basis von V über R “.

Jede Basis $\mathcal{B} = (b_i)_{i \in I}$ von V über R stiftet einen Isomorphismus

$$\Phi_{\mathcal{B}} : R^{(I)} \xrightarrow{\sim} V : \lambda = (\lambda_i)_{i \in I} \mapsto v = \sum_{i \in I} b_i \lambda_i.$$

Wir erhalten eine Zerlegung von V als direkte Summe $V = \bigoplus_{i \in I} V_i$ der Teilräume $V_i = b_i R$ mit Isomorphismen $\varphi_i : R \xrightarrow{\sim} V_i : \lambda_i \mapsto b_i \lambda_i$.

Demnach gilt: Ein linearer Raum V über R ist genau dann frei, wenn V die direkte Summe isomorpher Kopien des Raums R ist.

Gilt nämlich umgekehrt $V = \bigoplus_{i \in I} V_i$ mit Isomorphismen $\varphi_i : R \xrightarrow{\sim} V_i$, so erhalten wir daraus die Basis $\mathcal{B} = (b_i)_{i \in I}$ mit $b_i = \varphi_i(1)$.

Erste Beispiele: $\{0\}$ und R über R

Beispiel: Der Nullraum $\{0\}$ ist frei über R mit leerer Basis $\mathcal{B} = ()$.

Ausführlich: Die Indexmenge $I = \emptyset$ ist hier die leere Menge.

Demnach gilt $R^{(\emptyset)} = R^\emptyset = \{0\}$ mit $0: \emptyset \rightarrow \mathbb{Z}$, siehe D302.

Somit ist $\Phi_{\mathcal{B}}: R^\emptyset \rightarrow \{0\}$ tatsächlich ein Isomorphismus.

😊 Auch dieser „triviale“ Sonderfall fügt sich nahtlos ein.

Beispiel: Der R -lineare Raum R ist frei, die Standardbasis ist 1 .

Genau dann ist $b \in R$ eine R -Basis, wenn b in R invertierbar ist:

$$\Phi_b : R \xrightarrow{\sim} R : \lambda \mapsto b\lambda \text{ bijektiv} \iff b \in R^\times \text{ invertierbar}$$

Beweis: Die Implikation „ \Leftarrow “ ist klar dank $\Phi_b^{-1} = \Phi_{b^{-1}}$. Die Umkehrung „ \Rightarrow “ ist noch interessanter: Da Φ_b surjektiv ist, existiert $c \in R$ mit $bc = 1$, also ist b rechtsinvertierbar durch c . Zudem ist Φ_b injektiv: Wir haben $b1 = b = 1b = (bc)b = b(cb)$, nach Kürzen also $1 = cb$. □

😊 Das entspricht Satz B2D, hier im Spezialfall von 1×1 -Matrizen. Die folgenden Beispiele illustrieren dies für die Ringe \mathbb{Z} und \mathbb{Z}/n .

Erste Beispiele: \mathbb{Z} und \mathbb{Z}/n über \mathbb{Z}

Beispiel: Der \mathbb{Z} -lineare Raum \mathbb{Z} ist frei; mögliche Basen sind 1 und -1 .

Jedes $b \in \mathbb{Z} \setminus \{0, \pm 1\}$ ist \mathbb{Z} -linear unabhängig, erzeugt aber nicht \mathbb{Z} .

Ausführlich: Hier ist $\Phi_b: \mathbb{Z} \xrightarrow{\sim} b\mathbb{Z} \subsetneq \mathbb{Z}$ injektiv, aber nicht surjektiv.

Beispiel: Der \mathbb{Z}/n -lineare Raum ist \mathbb{Z}/n frei, die Standardbasis ist 1 .

Weitere Basen sind $b \in (\mathbb{Z}/n)^\times = \{ [a] \mid a \in \mathbb{Z} \wedge \text{ggT}(a, n) = 1 \}$; dies sind die invertierbaren Elemente des Rings \mathbb{Z}/n (A20).

Beispiel J1B: der Raum $\mathbb{Z}/n\mathbb{Z}$ ist nicht frei über \mathbb{Z} .

Der \mathbb{Z} -lineare Raum \mathbb{Z}/n mit $n \in \mathbb{N}_{\geq 2}$ ist nicht frei über \mathbb{Z} .

Nur für $n \in \{0, 1\}$ sind $\mathbb{Z}/0 \cong \mathbb{Z}$ und $\mathbb{Z}/1 = \{0\}$ frei über \mathbb{Z} .

Beweis: Das folgt aus $\mathbb{Z}^{(I)} \not\cong \mathbb{Z}/n$ für jede Menge I . Ausführlich:

Jede abelsche Gruppe V ist ein \mathbb{Z} -linearer Raum (I1K). Für $1 < \#V < \infty$ ist V nicht frei über \mathbb{Z} . Zum Beweis sei $\mathcal{B} = (b_i)_{i \in I}$ eine Familie in V .

Im Falle $I = \emptyset$ ist $\mathbb{Z}^{(I)} = \{0\}$ und $\Phi_{\mathcal{B}}: \mathbb{Z}^{(I)} \rightarrow V$ nicht surjektiv.

Im Falle $I \neq \emptyset$ ist $\mathbb{Z}^{(I)}$ unendlich, also $\Phi_{\mathcal{B}}$ nicht injektiv. □

Beispiel J1C: der Koordinatenraum $R^{(I)}$ über R

Sei R ein Ring und I eine Menge. Der **Koordinatenraum**

$$R^{(I)} = \{ \lambda : I \rightarrow R \mid \#\text{supp}(\lambda) < \infty \} \leq R^I$$

ist frei bezüglich der **Standardbasis** $\mathcal{E} = (e_i)_{i \in I}$, wobei

$$e_i : I \rightarrow R : j \mapsto e_i(j) = \begin{cases} 1 & \text{falls } j = i, \\ 0 & \text{falls } j \neq i. \end{cases}$$

Jedes Element $\lambda \in R^{(I)}$ schreibt sich eindeutig als Linearkombination

$$\lambda = \sum_{i \in I} e_i \lambda_i.$$

Hier ist demnach $\Phi_{\mathcal{E}} = \text{id} : R^{(I)} \xrightarrow{\sim} R^{(I)}$ die identische Abbildung.

Beispiel: Für die Indexmenge $I = \{1, \dots, m\} \times \{1, \dots, n\}$ erhalten wir den R -linearen Raum $R^{m \times n}$ der $m \times n$ -Matrizen mit der Standardbasis $\mathcal{E} = (E_{ij})_{ij}$. Die Matrix $E_{ij} \in R^{m \times n}$ hat an der Stelle (i, j) den Eintrag 1 und sonst überall 0. Wie gesehen: Diese Matrizen bilden eine Basis!

😊 Dieser vertraute Koordinatenraum $R^{(I)}$ ist unser Modell, er dient uns als Standardraum. Hierin können wir besonders gut „in Koordinaten“ rechnen, hierzu haben wir insbesondere die Standardbasis $(e_i)_{i \in I}$.

Jede Familie $\mathcal{B} = (b_i)_{i \in I}$ in V definiert die R -lineare Abbildung

$$\Phi_{\mathcal{B}} : R^{(I)} \rightarrow V : \lambda = (\lambda_i)_{i \in I} \mapsto v = \sum_{i \in I} b_i \lambda_i.$$

Dabei gilt $e_i \mapsto b_i$ für jeden Index $i \in I$. Wenn \mathcal{B} zudem eine Basis ist, so ist $\Phi_{\mathcal{B}}$ ein Isomorphismus: Er übersetzt verlustfrei den Modellraum $R^{(I)}$ mit der Standardbasis $(e_i)_{i \in I}$ in den Raum V mit der Basis $(b_i)_{i \in I}$ und zurück. Jeder basierte Raum $(V, (b_i)_{i \in I})$ sieht demnach genau aus wie der Standardraum $(R^{(I)}, (e_i)_{i \in I})$, bis auf den Isomorphismus $\Phi_{\mathcal{B}}$.

Erste Beispiele: \mathbb{C} über \mathbb{C} und über \mathbb{R}

Beispiel: Der \mathbb{C} -lineare Raum \mathbb{C} ist frei, die Standardbasis ist 1. Allgemein ist jedes Element $b \in \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ eine \mathbb{C} -Basis von \mathbb{C} .

Ebenso ist der Raum \mathbb{C} frei über $\mathbb{R} \leq \mathbb{C}$, die Standardbasis ist $(1, i)$: Jede komplexe Zahl $z \in \mathbb{C}$ schreibt sich eindeutig als Linearkombination

$$z = 1x + iy \quad \text{mit Koeffizienten} \quad (x, y) \in \mathbb{R}^2.$$

Auch $(1, -i)$ ist eine \mathbb{R} -Basis von \mathbb{C} . (Es gibt unendlich viele weitere.)

! Die Familie (1) erzeugt den Raum \mathbb{C} über \mathbb{C} , aber nicht über \mathbb{R} . Die Familie $(1, i)$ ist linear unabhängig über \mathbb{R} , aber abhängig über \mathbb{C} .

Beispiel J1D: Basis von \mathbb{C}^n , komplex vs reell

Ist $\mathcal{B}_{\mathbb{C}} = (b_1, \dots, b_n)$ eine Basis der Länge n von \mathbb{C}^n über \mathbb{C} , dann ist $\mathcal{B}_{\mathbb{R}} = (b_1, b_1i, \dots, b_n, b_ni)$ eine Basis der Länge $2n$ von \mathbb{C}^n über \mathbb{R} .

! Diese Eigenschaften hängen demnach sensibel vom Grundring ab. Aus dem Kontext muss hervorgehen, über welchem Ring wir arbeiten.

Erste Beispiele: der Raum \mathbb{C}^n über \mathbb{C} und über \mathbb{R}

Aufgabe: Beweisen Sie die Behauptung dieses Beispiels!

Lösung: (1) Die Familie $\mathcal{B}_{\mathbb{R}}$ erzeugt \mathbb{C}^n über \mathbb{R} : Vorgelegt sei $v \in \mathbb{C}^n$. Da $\mathcal{B}_{\mathbb{C}}$ eine Basis über \mathbb{C} ist, existieren Koeffizienten $z \in \mathbb{C}^n$ mit

$$v = \sum_{k=1}^n b_k z_k = \sum_{k=1}^n b_k \operatorname{Re}(z_k) + b_k i \operatorname{Im}(z_k).$$

Dies stellt v als \mathbb{R} -Linearkombination von $\mathcal{B}_{\mathbb{R}}$ dar.

(2) Zudem ist $\mathcal{B}_{\mathbb{R}}$ in \mathbb{C}^n linear unabhängig über \mathbb{R} : Vorgelegt seien reelle Koeffizienten $x_1, y_1, \dots, x_n, y_n \in \mathbb{R}$. Aus der Linearkombination

$$0 = \sum_{k=1}^n b_k x_k + b_k i y_k = \sum_{k=1}^n b_k (x_k + i y_k)$$

folgt $x_k + i y_k = 0$, da $\mathcal{B}_{\mathbb{C}}$ linear unabhängig über \mathbb{C} ist.

Das bedeutet $x_k = y_k = 0$ für alle $k = 1, \dots, n$.

Beispiel: Sei K ein kommutativer Ring und $K[X]$ der Polynomring.

Dann ist $K[X]$ frei über K bezüglich der **Monombasis** $(X^n)_{n \in \mathbb{N}}$.

Das ist geradezu die Definition G3A des Polynomrings $K[X]$ über K . Daraus folgt insbesondere die Gleichheit durch Koeffizientenvergleich und daraus anschließend alle weiteren Rechenregeln!

Im Falle $\mathbb{Q} \leq K$ hat $K[X]$ zudem die **faktorielle Basis** $(\frac{1}{n!} X^n)_{n \in \mathbb{N}}$.

Beispiel J1E: gestufte Polynombasis

Sei $(P_n)_{n \in \mathbb{N}}$ eine **gestufte Familie** von Polynomen $P_n \in K[X]$, mit den Eigenschaften $\deg(P_n) = n$ und $\text{lc}(P_n) \in K^\times$ für alle $n \in \mathbb{N}$.

Dann ist $(P_n)_{n \in \mathbb{N}}$ eine Basis von $K[X]$ über K .

Aufgabe: Ist $K[X]$ ein linearer Raum über dem Ring $K[X^2]$? Ist er frei? Ist allgemein $K[X]$ frei über $K[X^n]$? Falls ja, nennen Sie eine Basis.

Lösung: Ja, $K[X]$ ist frei über $K[X^2]$ bezüglich der Basis $1, X$. (I2M)
Für $n \in \mathbb{N}_{\geq 1}$ ist $K[X]$ frei über $K[X^n]$ mit Basis $1, X, X^2, \dots, X^{n-1}$.

Aufgabe: Beweisen Sie die Behauptung des Beispiels J1E! Genauer:

$$K[X] = \langle P_n \mid n \in \mathbb{N} \rangle_K,$$

$$K[X]_{\leq d} = \langle P_n \mid n \leq d \rangle_K.$$

Lösung: (1) Wir zeigen die Inklusion „ \subseteq “ per Induktion über d :
Für $K[X]_{<0} = \{0\}$ ist die Aussage klar. Für $P \in K[X]_{\leq d}$ gilt

$$Q = P - \text{lc}(P) \text{lc}(P_n)^{-1} P_n \in K[X]_{<d} = \langle P_n \mid n < d \rangle.$$

Somit gilt $P \in \langle P_n \mid n \leq d \rangle$, wie behauptet.

(2) Zudem ist $(P_n)_{n \in \mathbb{N}}$ in $K[X]$ linear unabhängig über K .

Wir betrachten eine K -Linearkombination zu Null:

$$P = \lambda_0 P_0 + \lambda_1 P_1 + \dots + \lambda_n P_n$$

Im Falle $\lambda_n \neq 0$ gilt $\deg(P) = n$. Aus $P = 0$ folgt also $\lambda_n = 0$.

Per Induktion schließen wir aus $P = 0$ somit $\lambda_k = 0$ für alle k .

Beispiel: Der R -lineare Raum R^n ist frei, die **Standardbasis** ist

$$\mathcal{E} : e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, e_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \dots, e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

Beweis: (1) Jeder Vektor $x \in R^n$ schreibt sich als Linearkombination

$$x = \sum_{i=1}^n e_i x_i.$$

(2) Eindeutigkeit: Sind zwei solche Darstellungen gegeben,

$$\sum_{i=1}^n e_i \lambda_i = \sum_{i=1}^n e_i \mu_i,$$

so folgt $\lambda_i = \mu_i$ für alle $i = 1, \dots, n$.

Basen des linearen Raums R^n über R

Alternativ zu (2): Jede Relation zwischen e_1, \dots, e_n ist trivial, denn aus $\sum_{i=1}^n e_i \lambda_i = 0$ folgt $\lambda_i = 0$ für alle $i = 1, \dots, n$.

😊 Die Basiseigenschaft ist für die Familie \mathcal{E} offensichtlich. Wir haben $R^n = R^I = R^{(I)}$ für $I = \{1, \dots, n\}$, siehe Beispiel J1c.

😊 Dabei stellen wir erfreut fest: Zu jedem Vektor $x \in R^n$ sind die vertrauten kartesischen Koordinaten (x_1, \dots, x_n) zugleich die Koordinaten bezüglich der Standardbasis $\mathcal{E} = (e_1, \dots, e_n)$.

Wir nennen \mathcal{E} die **Standardbasis**, manche Autoren sagen hierzu auch die **kanonische Basis**, die **übliche Basis**, oder ähnliches.

😞 Bitte sagen Sie zu \mathcal{E} nicht „die Basis“ des R^n , das ist verkehrt. Es gibt zu R^n viele weitere Basen, wie wir gleich sehen werden, die Standardbasis ist besonders einfach. Je nach Problemstellung sind andere Basen eventuell noch nützlicher. Dazu später mehr.

Basen des linearen Raums R^n über R

Für jede Familie $\mathcal{B} = (b_1, \dots, b_k)$ mit $b_1, \dots, b_k \in R^n$ gilt:

$$\Phi_{\mathcal{B}} : R^k \xrightarrow{\sim} R^n : \lambda \mapsto b_1\lambda_1 + \dots + b_k\lambda_k = B\lambda$$

Wir identifizieren R^n hier mit Spaltenvektoren $R^{n \times 1}$ und betrachten die Vektoren $b_1, \dots, b_k \in R^n$ als die Spalten der Matrix $B \in R^{n \times k}$.

1 Der **Kern** von $\Phi_{\mathcal{B}}$ ist der **Lösungsraum**

$$\ker(\Phi_{\mathcal{B}}) = \ker(B) := \{ \lambda \in R^k \mid B\lambda = 0 \} \leq R^k.$$

Jede Lösung $\lambda \in R^k$ zu $B\lambda = 0$ ist eine Relation der Familie \mathcal{B} . Genau dann ist \mathcal{B} linear unabhängig, wenn $\ker(B) = \{0\}$ gilt.

2 Das **Bild** von $\Phi_{\mathcal{B}}$ ist der **Spaltenraum**

$$\text{im}(\Phi_{\mathcal{B}}) = \text{im}(B) := \langle b_1, \dots, b_k \rangle_R \leq R^n.$$

Genau dann ist \mathcal{B} erzeugend für R^n , wenn $\text{im}(B) = R^n$ gilt.

3 Genau dann ist die Familie \mathcal{B} eine **Basis** von R^n über R , wenn die Matrix B invertierbar ist, siehe Satz B2D zu $B\lambda = v$.

Gestufte Basen des linearen Raums R^n über R

Beispiel J1F: eine gestufte Basis

Eine **gestufte Basis** des Raums R^n über R ist von der Form

$$b_1 = \begin{bmatrix} \blacksquare \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} * \\ \blacksquare \\ \vdots \\ 0 \end{bmatrix}, \quad \dots, \quad b_n = \begin{bmatrix} * \\ * \\ \vdots \\ \blacksquare \end{bmatrix}$$

mit $b_{ij} = 0$ für alle $j > i$ und invertierbarem Leitkoeffizienten $b_{ii} \in R^\times$. Jede Teilfamilie ist linear unabhängig, jede Oberfamilie ist erzeugend.

Übung: Erklären Sie, warum (b_1, \dots, b_n) tatsächlich eine Basis ist.

Was können Sie über die zugehörige Matrix B sagen?

Wie bringen Sie B in (reduzierte) Zeilenstufenform?

Wie lösen Sie damit die Gleichung $B\lambda = v$?

😊 Das ist ein schönes und wichtiges Beispiel. Hier freuen Sie sich, dass Sie bereits seit Satz B2D über passendes Werkzeug verfügen!

Aufgabe: In \mathbb{R}^3 über \mathbb{R} betrachten wir die Familie

$$\mathcal{B} : b_1 = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}, b_2 = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, b_3 = \begin{bmatrix} 3 \\ 4 \\ 7 \end{bmatrix}.$$

- (1) Ist \mathcal{B} linear unabhängig? Nennen Sie alle Relationen!
 (2) Welche Teilfamilien von \mathcal{B} sind linear unabhängig?

Lösung: Wir lösen $B\lambda = v$ mit dem Gauß-Algorithmus (B2c/B2B):

$$B = \begin{bmatrix} 1 & 1 & 3 \\ 1 & 2 & 4 \\ 2 & 3 & 7 \end{bmatrix} \xrightarrow[\substack{\text{RZSF} \\ SB=B'}]{} B' = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \lambda = \begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}.$$

- (1) Die Familie $\mathcal{B} = (b_1, b_2, b_3)$ ist linear abhängig: Nicht-triviale Relationen sind λ , denn $b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3 = 0$, und alle Vielfachen.
 (2) Die Familien (b_1, b_2) und (b_1, b_3) und (b_2, b_3) sind linear unabhängig, zudem offensichtlich auch (b_1) und (b_2) und (b_3) sowie $()$.

Die hier betrachtete Familie $\mathcal{B} = (b_1, b_2, b_3)$ ist linear abhängig, doch die Relation λ ist nicht offensichtlich: Wir müssen rechnen.

Dank Gauß finden wir die Zeilenstufenform $B' = SB$. Die invertierbare Matrix $S \in GL_3 \mathbb{R}$ codiert die Zeilenoperationen, somit gilt $B = S^{-1}B'$. Daraus folgt insbesondere $\ker(B) = \ker(B')$, denn $B\lambda = 0 \Leftrightarrow B'\lambda = 0$.

In der Matrix B' sieht man sehr leicht, dank reduzierter Zeilenstufenform, dass die Familie der drei Spalten $(B'e_1, B'e_2, B'e_3)$ linear abhängig ist. Dasselbe gilt dann auch für die Familie (Be_1, Be_2, Be_3) .

Ebenso sehen wir, dass $(B'e_1, B'e_2)$ und $(B'e_1, B'e_3)$ und $(B'e_2, B'e_3)$ jeweils linear unabhängig sind. Dasselbe gilt dann auch für die Familien (Be_1, Be_2) und (Be_1, Be_3) und (Be_2, Be_3) von Spalten der Matrix B .

😊 Jede Teilfamilie ist dann ebenfalls linear unabhängig (J1G).

😊 Satz J1P erklärt Ihnen allgemein einen Algorithmus, mit dem Sie zu jeder Matrix den Bildraum und den Kern bestimmen können.

Aufgabe: In \mathbb{R}^3 über \mathbb{R} betrachten wir die Familie

$$\mathcal{B} : b_1 = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}, b_2 = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, b_3 = \begin{bmatrix} 3 \\ 4 \\ 7 \end{bmatrix}, b_4 = \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}.$$

- (1) Ist \mathcal{B} erzeugend? linear unabhängig? eine Basis von \mathbb{R}^3 ?
 (2) Welche Teilfamilien von \mathcal{B} sind Basen von \mathbb{R}^3 ?

Lösung: Wir lösen $B\lambda = v$ mit dem Gauß-Algorithmus (B2C/B2B):

$$B = \begin{bmatrix} 1 & 1 & 3 & 3 \\ 1 & 2 & 4 & 2 \\ 2 & 3 & 7 & 1 \end{bmatrix} \xrightarrow[\text{SB=B'}]{\text{RZSF}} B' = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \lambda = \begin{bmatrix} 2 \\ 1 \\ -1 \\ 0 \end{bmatrix}.$$

- (1) Die Familie $\mathcal{B} = (b_1, b_2, b_3, b_4)$ ist erzeugend, aber linear abhängig:
 Eine nicht-triviale Relationen ist λ , denn $b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3 + b_4\lambda_4 = 0$.
 (2) Die Familien (b_1, b_2, b_4) und (b_1, b_3, b_4) und (b_2, b_3, b_4) sind Basen.
 Wir sehen dies leicht in B' und übertragen es dann auf B .

Die hier betrachtete Familie $\mathcal{B} = (b_1, b_2, b_3, b_4)$ erzeugt den Raum \mathbb{R}^3 , doch diese Eigenschaft ist nicht offensichtlich: Wir müssen rechnen.

Dank Gauß finden wir die Zeilenstufenform $B' = SB$. Die invertierbare Matrix $S \in GL_3 \mathbb{R}$ codiert die Zeilenoperationen, somit gilt $B = S^{-1}B'$. Daraus folgt insbesondere $\text{im}(B') = S \text{im}(B)$ und $\text{im}(B) = S^{-1} \text{im}(B')$.

In der Matrix B' sieht man sehr leicht, dank reduzierter Zeilenstufenform, dass die Familie $e_1 = B'e_1, e_2 = B'e_2, e_3 = B'e_4$ den Raum \mathbb{R}^3 erzeugt. Dasselbe gilt dann auch für $S^{-1}e_1 = Be_1, S^{-1}e_2 = Be_2, S^{-1}e_3 = Be_4$.

Ebenso sehen wir, dass die Familien Be_1, Be_3, Be_4 und Be_2, Be_3, Be_4 Basen sind: Wir sehen dies leicht in B' und übertragen es dann auf B .

😊 Das ist eine schöne, konkrete Illustration zum Basisauswahlsatz J2B.

😊 Satz J1P erklärt Ihnen allgemein einen Algorithmus, mit dem Sie zu jeder Matrix den Bildraum und den Kern bestimmen können.

Aus diesen ersten Zahlenbeispielen extrahieren wir bereits ein paar hilfreiche Bemerkungen, die Ihnen allgemein nützen werden.

Bemerkung: Sei V ein Vektorraum über dem Divisionsring R . Zwei Vektoren $v_1, v_2 \in V$ sind R -linear abhängig, falls

$$v_1\lambda_1 + v_2\lambda_2 = 0 \quad \text{mit} \quad (\lambda_1, \lambda_2) \neq (0, 0).$$

Nach Ummummerierung sei $\lambda_1 \neq 0$. Dann gilt:

$$v_1 = v_2(-\lambda_2\lambda_1^{-1})$$

😊 Einer der beiden Vektoren ist ein Vielfaches des anderen.

⚠ Diese einfache Anschauung gilt nur für zwei Vektoren!

Beispiel: Die drei Vektoren $v_1 = (0, 1)$, $v_2 = (1, 0)$, $v_3 = (1, 1)$ in R^2 sind als Familie linear abhängig, aber doch paarweise unabhängig.

Übung: Nennen Sie $n + 1$ Vektoren im linearen Raum R^n über R , die linear abhängig sind, aber je n davon sind linear unabhängig.

Sei $(v_i)_{i \in I}$ eine Familie von Vektoren im linearen Raum V über R . Die folgenden **offensichtlichen Kriterien** sind für die lineare Abhängigkeit zwar nicht notwendig, aber doch hinreichend:

- 1 Einer der Vektoren ist gleich Null: $v_i = 0$ für ein $i \in I$.
- 2 Zwei Vektoren sind gleich: $v_i = v_j$ für $i \neq j$ in I .
- 3 Ein Vektor ist ein Vielfaches eines anderen.

Wenn eines dieser Kriterien erfüllt ist, dann ist die Familie $(v_i)_{i \in I}$ offensichtlich linear abhängig. Die Umkehrung gilt jedoch nicht: Lineare Abhängigkeit ist nicht immer offensichtlich!

⚠ Die oben vereinbarte Definition J1A der linearen Un/Abhängigkeit ist mit Bedacht gewählt. Sie lässt sich nicht weiter vereinfachen!

*Alles sollte so einfach wie möglich gemacht werden
— aber nicht noch einfacher.*

Albert Einstein (1879–1955)

Aufgabe: Sei $\mathbb{P} = \{2, 3, 5, 7, \dots\}$ die Menge der Primzahlen. Ist die Familie $\mathcal{B} = (\ln p)_{p \in \mathbb{P}}$ in \mathbb{R} linear unabhängig über \mathbb{Q} ?

Lösung: Wir betrachten eine \mathbb{Q} -Linearkombination zu Null:

$$q_1 \ln p_1 + \dots + q_n \ln p_n = 0$$

mit $p_1 < \dots < p_n$ in \mathbb{P} und $q_1, \dots, q_n \in \mathbb{Q}$, also $q_i = a_i/b_i$, $a_i \in \mathbb{Z}$, $b_i \in \mathbb{Z}^*$.

$$\frac{a_1}{b_1} \ln p_1 + \dots + \frac{a_n}{b_n} \ln p_n = 0$$

Wir multiplizieren mit $b = \text{kgV}(b_1, \dots, b_n) \in \mathbb{Z}^*$ und erhalten $c_i = q_i b \in \mathbb{Z}$:

$$c_1 \ln p_1 + \dots + c_n \ln p_n = 0$$

Dank $(\exp, \ln) : (\mathbb{R}, +, 0) \cong (\mathbb{R}_{>0}, \cdot, 1)$ ist dies äquivalent zu:

$$p_1^{c_1} \cdots p_n^{c_n} = 1$$

Dank Fundamentalsatz der Arithmetik A2J folgt $c_1 = \dots = c_n = 0$, also $q_1 = \dots = q_n = 0$: Jede rationale Relation zwischen $(\ln p)_{p \in \mathbb{P}}$ ist trivial.

Das ist ein schönes und konkretes Beispiel, das zur Abwechslung nicht von Vektoren im \mathbb{R}^n handelt und nicht auf Matrizenrechnung beruht.

Bitte versuchen Sie mit der Definition und diesen Illustrationen, Begriff und Technik der linearen Un/Abhängigkeit richtig zu verstehen. Das ist nicht ganz leicht, aber wesentlich für die Lineare Algebra!

Zum Abschluss stelle ich einige einfache Bemerkungen zusammen, die die Logik der Begriffe beleuchten. Bitte nutzen Sie dies als Prüfstein für Ihr Verständnis: Lesen Sie nochmals gründlich die Definition J1A und versuchen Sie, die Umformulierungen sicher nachzuvollziehen.

Mit diesen Bemerkungen können Sie auch die vorigen Beispiele nochmals durchgehen: Sie werden viele der Argumente in den konkreten Rechnungen wiedererkennen. Es lohnt sich also!

Es ist auch für alle folgenden Argumente und Rechnungen hilfreich, diese grundlegenden Beobachtungen parat zu haben.

Teilfamilien und Oberfamilien

Bemerkung J1G: Teilfamilien und Oberfamilien

Sei V ein linearer Raum über dem Ring R .

- 1 Ist die Familie $\mathcal{B} = (v_i)_{i \in I}$ erzeugend für V ,
so auch jede Oberfamilie $\mathcal{C} = (v_i)_{i \in J}$ mit $J \supseteq I$.
- 2 Ist die Familie $\mathcal{C} = (v_i)_{i \in J}$ nicht erzeugend für V ,
so auch keine Teilfamilie $\mathcal{B} = (v_i)_{i \in I}$ mit $I \subseteq J$.
- 3 Ist die Familie $\mathcal{B} = (v_i)_{i \in I}$ in V linear abhängig,
so auch jede Oberfamilie $\mathcal{C} = (v_i)_{i \in J}$ mit $J \supseteq I$.
- 4 Ist die Familie $\mathcal{C} = (v_i)_{i \in J}$ in V linear unabhängig,
so auch jede Teilfamilie $\mathcal{B} = (v_i)_{i \in I}$ mit $I \subseteq J$.
- 5 Genau dann ist $\mathcal{C} = (v_i)_{i \in J}$ linear abhängig,
wenn eine endliche Teilfamilie $\mathcal{B} = (v_i)_{i \in I}$ linear abhängig ist.
- 6 Genau dann ist $\mathcal{C} = (v_i)_{i \in J}$ linear unabhängig,
wenn jede endliche Teilfamilie $\mathcal{B} = (v_i)_{i \in I}$ linear unabhängig ist.

Teilfamilien und Oberfamilien

J130
Erläuterung

Beweis: Das ist klar nach Definition. QED

Schreiben Sie es zur Übung und als Wiederholung sorgsam aus!
Aussagen (1) und (3) und (5) sind jeweils klar nach Definition.
Aussagen (2) und (4) und (6) folgen daraus durch Kontraposition.

$$\begin{array}{ccc}
 I & \xrightarrow{\text{inc}} & J \\
 \searrow \mathcal{B} & & \swarrow \mathcal{C} \\
 & & V
 \end{array}
 \qquad
 \begin{array}{ccc}
 R^{(I)} & \xrightarrow{\text{inc}} & R^{(J)} \\
 \searrow \Phi_{\mathcal{B}} & & \swarrow \Phi_{\mathcal{C}} \\
 & & V
 \end{array}$$

Für Teilfamilien und Oberfamilien ist folgende Konvention nützlich:

Bemerkung J1H: Ausdehnung / Einschränkung der Indexmenge

Für $I \subseteq J$ betrachten wir $R^I \leq R^J$ und $R^{(I)} \leq R^{(J)}$ als Teilräume.

Ausführlich nutzen wir dazu $(\iota, \rho) : R^I \rightleftarrows R^J$ und $(\iota, \rho) : R^{(I)} \rightleftarrows R^{(J)}$
vermöge $\rho : \mu \mapsto \lambda = \mu|_J$ und $\iota : \lambda \mapsto \mu$ mit $\mu|_I = \lambda$ und $\mu|_{J \setminus I} = 0$.

Bemerkung J11: Familie unter linearer Abbildung

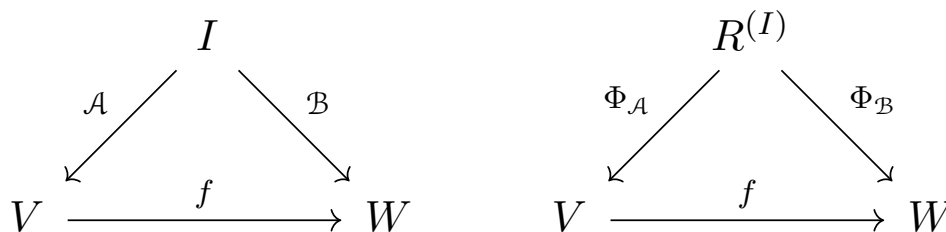
Gegeben sei eine R -lineare Abbildung $f: V \rightarrow W$ und eine Familie $\mathcal{A} = (v_i)_{i \in I}$ von Vektoren $v_i \in V$ mit der Bildfamilie $\mathcal{B} = (f(v_i))_{i \in I}$.

- 1 Ist f bijektiv und die Familie $\mathcal{A} = (v_i)_{i \in I}$ eine Basis von V , so ist auch die Bildfamilie $\mathcal{B} = (f(v_i))_{i \in I}$ eine Basis von W .
- 2 Ist f surjektiv und die Familie $\mathcal{A} = (v_i)_{i \in I}$ erzeugt den Raum V , so erzeugt die Bildfamilie $\mathcal{B} = (f(v_i))_{i \in I}$ den Raum W .
- 3 Ist f injektiv und die Familie $\mathcal{A} = (v_i)_{i \in I}$ in V linear unabhängig, so ist die Bildfamilie $\mathcal{B} = (f(v_i))_{i \in I}$ in W linear unabhängig.
- 4 Ist die Familie $\mathcal{A} = (v_i)_{i \in I}$ linear abhängig in V , so ist die Bildfamilie $\mathcal{B} = (f(v_i))_{i \in I}$ linear abhängig in W .
- 5 Ist die Bildfamilie $\mathcal{B} = (f(v_i))_{i \in I}$ linear unabhängig in W , so ist die Familie $\mathcal{A} = (v_i)_{i \in I}$ linear unabhängig in V .

Familien und lineare Abbildungen

Beweis: Das ist klar nach Definition. □ QED

Schreiben Sie es zur Übung und als Wiederholung sorgsam aus!



Die Aussagen (1–3) beruhen auf folgender allgemeinen Überlegung:

- 1 Die Komposition von zwei Bijektionen ist bijektiv.
- 2 Die Komposition von zwei Surjektionen ist surjektiv.
- 3 Die Komposition von zwei Injektionen ist injektiv.

Aussage (4) ist klar: Jede Relation λ der Familie \mathcal{A} besteht weiter für die Bildfamilie \mathcal{B} . Daraus folgt (5) durch Kontraposition.

Invarianz der Basislänge

Für jede Familie $\mathcal{B} = (b_1, \dots, b_k)$ mit $b_1, \dots, b_k \in R^n$ gilt:

$$\Phi_{\mathcal{B}} : R^k \xrightarrow{\sim} R^n : \lambda \mapsto b_1\lambda_1 + \dots + b_k\lambda_k = B\lambda$$

Ist R ein Divisionsring, so können wir B mit dem Gauß-Algorithmus in Zeilenstufenform überführen und den Rang r ablesen. Satz B2D besagt:

- 1 $\Phi_{\mathcal{B}}$ surjektiv $\iff r = n \leq k$, also Rang gleich Zeilenzahl.
- 2 $\Phi_{\mathcal{B}}$ injektiv $\iff r = k \leq n$, also Rang gleich Spaltenzahl.
- 3 $\Phi_{\mathcal{B}}$ bijektiv $\iff r = k = n$, also B quadratisch mit vollem Rang.

Satz J1J: Invarianz der Basislänge

Sei R ein Divisionsring.

- 1 Ist $\mathcal{B} = (b_1, \dots, b_k)$ ein Erzeugendensystem von R^n , so gilt $k \geq n$.
- 2 Ist $\mathcal{B} = (b_1, \dots, b_k)$ linear unabhängig in R^n , so gilt $k \leq n$.
- 3 Ist $\mathcal{B} = (b_1, \dots, b_k)$ eine Basis von R^n , so gilt $k = n$.

Invarianz der Basislänge

Diese Aussagen scheinen zunächst anschaulich recht plausibel, gemessen an unserer geometrisch-physikalischen Erfahrung: Im Raum \mathbb{R}^3 genügen zwei Vektoren nicht zum Aufspann von \mathbb{R}^3 und je vier Vektoren im \mathbb{R}^3 sind zwangsläufig linear abhängig.

So scheint es zumindest ... und erweist sich nun als wahr, denn wir können es beweisen wie hier in Satz J1J formuliert.

Schon im Raum \mathbb{R}^{100} ist allein mit „Anschauung“ keineswegs klar, warum jede Familie von 101 Vektoren linear abhängig sein sollte, oder eine Familie von 99 Vektoren nicht zum Aufspann genügt. Man möchte dies zwar gerne glauben, aber das hilft nicht weiter.

😊 Über Divisionsringen hilft uns wieder einmal der Gauß-Algorithmus! Intuition und Anschauung sind schön und gut, doch wir brauchen mehr: Für eine tragfähige Theorie benötigen wir präzise Definitionen, nachvollziehbare Argumente und effiziente Werkzeuge.

⚠️ Diese guten Eigenschaften gelten nicht über jedem Ring! Es gibt mahnende Gegenbeispiele, siehe etwa Beispiel J10.

Invarianz der Dimension

Als Analogie erinnern wir uns an den Zählssatz E1G:


- 1 Ist $f : \{1, \dots, k\} \twoheadrightarrow \{1, \dots, n\}$ surjektiv, so gilt $k \geq n$.
- 2 Ist $f : \{1, \dots, k\} \hookrightarrow \{1, \dots, n\}$ injektiv, so gilt $k \leq n$.
- 3 Ist $f : \{1, \dots, k\} \xrightarrow{\sim} \{1, \dots, n\}$ bijektiv, so gilt $k = n$.

Satz J1K: Invarianz der Dimension


Sei R ein Divisionsring. Für alle $k, n \in \mathbb{N}$ gilt:

- 1 Ist $f : R^k \twoheadrightarrow R^n$ eine R -lineare Surjektion, so gilt $k \geq n$.
- 2 Ist $f : R^k \hookrightarrow R^n$ eine R -lineare Injektion, so gilt $k \leq n$.
- 3 Ist $f : R^k \xrightarrow{\sim} R^n$ eine R -lineare Bijektion, so gilt $k = n$.

Beweis: Dies folgt aus Satz J1J und Bemerkung J1I: Die Bildfamilie $(f(e_i))_{i=1}^k$ in R^n ist (1) erzeugend, (2) unabhängig, (3) eine Basis. QED

 In diesem Beweis nutzen wir den Gauß-Algorithmus (B2D), deshalb fordern wir als Voraussetzung, dass R ein Divisionsring ist. Der Satz gilt auch über jedem kommutativen Ring $R \neq \{0\}$, siehe L3c. Über beliebigen Ringen gilt der Satz im Allgemeinen nicht, siehe J1o.

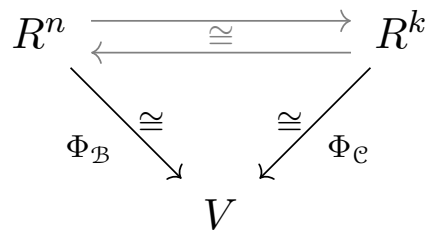
Invarianz der Dimension

 Sätze J1J und J1K sind wichtige Ergebnisse über Divisionsringen. Wir bekommen diese Resultate hier gratis aus dem Gauß-Algorithmus, da wir zuvor in Kapitel B schon gut und gründlich gearbeitet haben. Diese anfängliche Investition zahlt sich hier und überall aus.

Der Aufbau der Theorie muss insgesamt logisch schlüssig sein, doch innerhalb der logischen Anforderungen bleiben noch viele Freiheiten. Die Vorgehensweise der Darstellung, die Anordnung der Begriffe und Argumente ist eine interessante (und knifflige) didaktische Frage.

Viele Lehrbücher zur Linearen Algebra behandeln die Matrizenrechnung und den Gauß-Algorithmus erst später, nach Vektorräumen und Basen. In diesem Falle müssen die ersten Rechenbeispiele zur Erzeugung und linearen Unabhängigkeit aufgeschoben werden, auch die zugehörigen Beweise müssen anders organisiert werden. Das gelingt ebenso.

Ich finde es eleganter, zwei Fliegen mit einer Klappe zu schlagen:
Der Gauß-Algorithmus erlaubt effiziente Rechnungen *und* Beweise!



Definition J1L: Dimension eines linearen Raumes

(1) Ein Ring R erfüllt die **Invarianz der Dimension**, falls für alle $k, n \in \mathbb{N}$ gilt: Aus Isomorphie $R^k \cong R^n$ folgt Gleichheit $k = n$.

(2) Unter der Voraussetzung (1) gilt: Ist V ein R -linearer Raum mit Basis $\mathcal{B} = (b_i)_{i \in I}$, so haben alle Basen von V dieselbe Länge $\#I$.

In diesem Falle definieren wir die **Dimension** $\dim_R(V) := \#I$.

Dies gilt für jeden Divisionsring (J1K), insbesondere für jeden Körper. Dies gilt auch für jeden endlichen Ring $R \neq \{0\}$ dank Zähl­satz E1G. Es gilt ebenso für jedem kommutativen Ring $R \neq \{0\}$, siehe L3c.

⚠ Über dem Nullring $R = \{0\}$ hingegen gilt $R^1 \cong R^n$ für alle $n \in \mathbb{N}$. Für ein nicht-triviales, raffiniertes Gegenbeispiel siehe unten J1O

😊 Damit können wir die „Größe“ des Raums V über R messen.

Bemerkung: Zur Dimension $\dim_R(V)$ benötigen wir zwei Zutaten:

- 1 Der R -lineare Raum V muss frei sein, also mindestens eine Basis haben; das gilt leider nicht immer, siehe J1B. Es gilt für alle Vektorräume, siehe J2B und J2C.
- 2 Der Ring R muss die Invarianz der Dimension erfüllen: Je zwei Basen von V haben dann dieselbe Länge. Dies gilt für Divisionsringe dank J1J und J1K.

⚠ Wenn wir im Folgenden von der Dimension $\dim_R(V)$ sprechen, so müssen diese beiden Voraussetzungen erfüllt sein: Wir müssen sie im allgemeinen Fall fordern und im konkreten Fall nachweisen!

😊 Über jedem Divisionsring sind die Voraussetzungen (1) und (2) immer erfüllt. Das ist die grundlegende Erkenntnis dieses Kapitels.

Über Ringen, die keine Divisionsringe sind, sagen die meisten Autoren vorsichtig **Rang**, ich nenne dies in beiden Fällen einfach **Dimension**.

😊 Vielleicht halten Sie dieses vorsichtige Vorgehen für hasenfüßig. Ist das nicht alles klar? Beispiel J10 schützt Sie vor naivem Irrglauben!

Dem Koordinatenraum R^n sieht man die Zahl n direkt an:

Die Menge R^n besteht aus n -Tupel (x_1, \dots, x_n) über R .

Für einen freien Raum V über R hingegen ist das nicht klar.

Wir können eine Basis $(b_i)_{i \in I}$ wählen, aber es gibt viele Basen, und die Wahl einer Basis ist daher notgedrungen immer willkürlich. Es gibt nicht „die“ Basis von V , sondern nur eine Basis von vielen.

Wenn wir also die Dimension von V über R definieren wollen, so müssen wir zunächst sicherstellen, dass je zwei Basen $(b_i)_{i \in I}$ und $(c_j)_{j \in J}$ von V immer dieselbe Länge haben, also $\#I = \#J$ gilt. Genau das sichert die Voraussetzung der Invarianz der Dimension!

😊 Für viele „vernünftige“ Ringe gilt die Invarianz der Dimension: zunächst für jeden Divisionsring (J1K) und anschließend für jeden kommutativen Ring (L3C). Sie gilt insbesondere für jeden Körper!

Definition J1L gibt uns eine konkrete Berechnungsmethode an die Hand, meist tatsächlich einen expliziten Algorithmus (siehe unten, Satz J1P).

😊 Genau so wird die Dimension $\dim_R(V)$ definiert und in vielen typischen Fällen auch direkt berechnet: Wir finden eine geeignete Familie $(b_i)_{i \in I}$ von V , weisen für $(b_i)_{i \in I}$ lineare Unabhängigkeit und Erzeugung von V nach, und schließen so $\dim_R(V) = \#I$.

😊 Es genügt, dieses Verfahren für *eine* Basis zu durchlaufen: Jede andere Basis ist genauso gut und liefert dasselbe Ergebnis! Nach Alexandre Dumas berühmtem Motto: *Eine für alle, alle für eine*. Das ist nicht nur theoretisch elegant, sondern auch praktisch effizient.

😊 In unseren vorigen Beispielen haben wir Basen explizit angegeben und die Eigenschaften nachgewiesen: Unabhängigkeit und Erzeugung. Wir wissen nun auch, dass alle weiteren Basen dieselbe Länge haben. Zur Wiederholung und Betonung nennen ich die folgenden Beispiele.

Erste Beispiele zur Dimension

Beispiel: Sei R ein Divisionsring oder ein kommutativer Ring. Dann gilt

$$\dim_R(R^n) = n.$$

Dies enthält die Spezialfälle $\dim_R(\{0\}) = 0$ und $\dim_R(R) = 1$.

Siehe hierzu Beispiel J1C: Allgemein gilt $\dim_R(R^I) = \#I$.


Beispiel: Für die komplexen Zahlen \mathbb{C} gilt

$$\dim_{\mathbb{C}}(\mathbb{C}^n) = n \quad \text{und} \quad \dim_{\mathbb{R}}(\mathbb{C}^n) = 2n.$$

Siehe Beispiel J1D: Basis und Dimension hängen vom Grundring ab! Daher die Schreibweise $\dim_R(V)$, abgekürzt $\dim V$ nur falls R klar ist.

Beispiel: Sei K ein kommutativer Ring und $K[X]$ der Polynomring. Dann ist $K[X]$ frei über K bezüglich der Monombasis $(X^n)_{n \in \mathbb{N}}$, also

$$\dim_K(K[X]) = \infty.$$

 Der Raum $K[X]$ kann über K nicht endlich erzeugt werden, denn $\langle P_1, \dots, P_n \rangle_K \leq K[X]_{\leq m}$ mit $m = \max\{\deg P_1, \dots, \deg P_n\}$.

Erste Beispiele zur Dimension

Die Dimension $\dim_{\mathbb{R}}(\mathbb{R}^n) = n$ ist anschaulich plausibel, insbesondere für kleine Werte $n = 1, 2, 3$. Doch schon für einfache Beispiele wie

$$V = \left\{ x \in \mathbb{R}^7 \mid \sum_{i=1}^7 x_i = \sum_{i=1}^7 ix_i = \sum_{i=1}^7 i^2 x_i = 0 \right\}$$

benötigen wir eine präzise Definition des Dimensionsbegriffs!

Nochmal zur Betonung: Die Berechnung der Dimension $\dim_R(V)$ verläuft immer nach demselben Muster: Wir finden eine geeignete Familie $(b_i)_{i \in I}$ von V , weisen für $(b_i)_{i \in I}$ lineare Unabhängigkeit und Erzeugung von V nach, und schließen so $\dim_R(V) = \#I$.

In diesen ersten Beispielen ist diese Berechnung besonders leicht. Die Komplexität der nötigen Rechnungen hängt von der konkret vorliegenden Anwendung ab, doch das Prinzip ist immer dasselbe.

Im Verlauf dieses Kapitels werden wir mehrere Methoden erarbeiten zur Konstruktion von Basen und zur Berechnung der Dimension. Zur Dimension von Bild und Kern einer Matrix siehe Satz J1P.

Die Invarianz der Dimension J1L besagt: Je zwei endliche Basen von V haben dieselbe Länge. Könnte es sein, dass eine Basis endlich ist und eine andere unendlich? Nein! Diese Klärung reichen wir nun nach:

Lemma J1M: einmal unendlich, immer unendlich

Sei R ein beliebiger Ring mit $0 \neq 1$, also $R \neq \{0\}$.

- (1) Ist I unendlich, so ist der Raum $R^{(I)}$ über R nicht endlich erzeugt.
- (2) Hat ein linearer Raum V über R eine unendliche Basis $\mathcal{B} = (b_i)_{i \in I}$, so ist jedes Erzeugendensystem $\mathcal{C} = (c_j)_{j \in J}$ ebenfalls unendlich.

Beweis: (1) Für jede endliche Familie $v_1, \dots, v_n \in R^{(I)}$ ist $E = \bigcup_{k=1}^n \text{supp}(v_k)$ endlich und $\langle v_1, \dots, v_n \rangle \leq R^{(E)} \subsetneq R^{(I)}$.
(Zu dieser Sichtweise $R^{(E)} \leq R^{(I)}$ siehe J1H.)

(2) Wir betrachten die Familie $(v_j)_{j \in J}$ in $R^{(I)}$ mit $v_j = \Phi_{\mathcal{B}}^{-1}(c_j) \in R^{(I)}$. Dank (1) erzeugt $(v_j)_{j \in J}$ nicht $R^{(I)}$, also erzeugt $\mathcal{C} = (c_j)_{j \in J}$ nicht V .
(Zu dieser Schlussweise siehe Bemerkung J1I.) QED

Invarianz der Dimension, auch unendlich

Satz J1N: Invarianz der Dimension, auch unendlich

Sei R ein Divisionsring. Für alle Mengen I, J gilt:

- 1 Ist $f : R^{(I)} \twoheadrightarrow R^{(J)}$ eine lineare Surjektion, so gilt $\#I \geq \#J$.
- 2 Ist $f : R^{(I)} \hookrightarrow R^{(J)}$ eine lineare Injektion, so gilt $\#I \leq \#J$.
- 3 Ist $f : R^{(I)} \xrightarrow{\sim} R^{(J)}$ eine lineare Bijektion, so gilt $\#I = \#J$.

Beweis: Dank Bemerkung J1I wissen wir: Die Bildfamilie $(f(e_i))_{i \in I}$ in $R^{(J)}$ ist (1) erzeugend, (2) unabhängig, (3) eine Basis.

(1) Die endlichen Fälle sind geklärt dank J1K.
Ist J unendlich, so auch I dank Lemma J1M.
Ist I unendlich, so ist die Aussage trivial.

(2) Die endlichen Fälle sind geklärt dank J1K.
Ist I unendlich, so auch J , ebenfalls dank J1K.
Ist J unendlich, so ist die Aussage trivial.

(3) Diese Aussage folgt aus (1) und (2). QED

Ein mahndendes Gegenbeispiel

⚠ Über manchen Ringen hat der Begriff „Dimension“ keinen Sinn!
 Beispiel: Über dem Nullring $R = \{0\}$ gilt $R^1 \cong R^n$ für alle $n \in \mathbb{N}$.

Beispiel J10: ein nicht-trivialer Ring mit $R^1 \cong R^2$

Sei K ein Körper, etwa $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$. Hierüber sei $V = K^{(\mathbb{N})} = K[X]$ der Vektorraum der Folgen $x = (x_0, x_1, x_2, \dots)$ mit endlichem Träger.

Im Ring $R = (\text{End}_K(V), +, \circ)$ seien $a, b, c, d: V \rightarrow V$ gegeben durch

$$\begin{aligned} a(x) &= (x_0, 0, x_1, 0, x_2, 0, \dots), & c(x) &= (x_0, x_2, x_4, x_6, x_8, \dots), \\ b(x) &= (0, x_0, 0, x_1, 0, x_2, \dots), & d(x) &= (x_1, x_3, x_5, x_7, x_9, \dots). \end{aligned}$$

(1) Für Matrizen über dem Ring R gelten dann die Gleichungen

$$\begin{pmatrix} c \\ d \end{pmatrix} \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} ca & cb \\ da & db \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = ac + bd = 1.$$

(2) Die Matrizen $\begin{pmatrix} c \\ d \end{pmatrix}$ und $\begin{pmatrix} a & b \end{pmatrix}$ stiften einen Isomorphismus $R^1 \cong R^2$.

(3) Per Induktion folgt $R^1 \cong R^n$ und somit $R^m \cong R^n$ für alle $m, n \in \mathbb{N}_{\geq 1}$.

Ein mahndendes Gegenbeispiel

Beweis: (1) Diese Gleichungen können Sie direkt nachrechnen!

$$c \circ a : x \mapsto (x_0, 0, x_1, 0, x_2, 0, \dots) \mapsto (x_0, x_1, x_2, \dots)$$

$$c \circ b : x \mapsto (0, x_0, 0, x_1, 0, x_2, \dots) \mapsto (0, 0, 0, \dots)$$

$$d \circ a : x \mapsto (x_0, 0, x_1, 0, x_2, 0, \dots) \mapsto (0, 0, 0, \dots)$$

$$d \circ b : x \mapsto (0, x_0, 0, x_1, 0, x_2, \dots) \mapsto (x_0, x_1, x_2, \dots)$$

$$a \circ c : x \mapsto (x_0, x_2, x_4, \dots) \mapsto (x_0, 0, x_2, 0, x_4, 0, \dots)$$

$$b \circ d : x \mapsto (x_1, x_3, x_5, \dots) \mapsto (0, x_1, 0, x_3, 0, x_5, 0, \dots)$$

Somit gilt $ca = db = \text{id}_V$ und $cb = da = 0$ sowie $ac + bd = \text{id}_V$.

Der Isomorphismus (2) folgt sofort aus (1):

$$f : R^1 \rightarrow R^2 : r \mapsto \begin{pmatrix} cr \\ dr \end{pmatrix}, \quad g : R^2 \rightarrow R^1 : \begin{pmatrix} s \\ t \end{pmatrix} \mapsto as + bt.$$

(3) Für alle $k \in \mathbb{N}$ gilt demnach $R^{1+k} \cong R^1 \times R^k \cong R^2 \times R^k \cong R^{2+k}$.

Dank Transitivität folgt $R^1 \cong R^n$ und $R^m \cong R^n$ für alle $m, n \in \mathbb{N}_{\geq 1}$. **QED**

Dieses Gegenbeispiel ist zunächst erschreckend, doch auch heilsam. Es ist insgesamt nicht so kompliziert wie es auf den ersten Blick scheint, sondern eher sehr konkret und durchsichtig und auch recht natürlich:

😊 Für Polynome gilt $a: P(X) \mapsto P(X^2)$ und $b: P(X) \mapsto XP(X^2)$ sowie $(c, d): P \mapsto (P_0, P_1)$ mit $P = P_0(X^2) + XP_1(X^2)$, siehe I2M: Dies entspricht der Zerlegung in geraden und ungeraden Anteil.

😊 Der Raum $K^{(\mathbb{N})} = K[X]$ der Polynome ist klein und übersichtlich. Die Konstruktion gelingt wörtlich genauso mit dem Folgenraum $K^{\mathbb{N}}$. Alle Formeln und Rechnungen sind für $K^{\mathbb{N}}$ genau dieselben.

Aufgabe: Über einem *kommutativen* Ring R mit $1 \neq 0$ hingegen ist diese Pathologie unmöglich: Hier gilt $R^1 \not\cong R^n$ für alle $n \in \mathbb{N}_{\geq 2}$.

Lösung: Je zwei Elemente $a, b \in R^1$ sind R -linear abhängig gemäß

$$a(-b) + ba = 0.$$

In R^n hingegen gibt es R -linear unabhängige Elemente e_1, e_2, \dots

😊 Wir werden in Kapitel L die Determinante konstruieren und als Werkzeug nutzen lernen. Damit können wir beweisen, dass jeder kommutative Ring $R \neq \{0\}$ die Invarianz der Dimension erfüllt (L3c): Für alle $m \neq n$ in \mathbb{N} gilt $R^m \not\cong R^n$. Die obige Aufgabe zu $R^1 \not\cong R^n$ für $n \geq 2$ ist eine einfache und erhellende Illustration hierzu.

Bild und Kern einer Matrix in reduzierter Zeilenstufenform

$$\left[\begin{array}{ccccc|cc} 1 & -2 & 0 & 3 & 0 & -1 & 0 \\ 0 & 0 & 1 & 7 & 0 & 4 & 5 \\ 0 & 0 & 0 & 0 & 1 & 9 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{array} \right] \xrightarrow{\substack{\text{graphische} \\ \text{Merkregel}}} \left[\begin{array}{cc|cc|c} 1 & -2 & 0 & 3 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 & 0 & 4 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 9 \end{array} \right]$$

$\underbrace{\hspace{10em}}_A \quad \underbrace{\hspace{2em}}_b \quad \underbrace{\hspace{2em}}_{b'}$
 v_2
 v_4
 w

Aufgabe: Gegeben ist $A \in \mathbb{R}^{4 \times 5}$ in reduzierter Zeilenstufenform.

- (1) Explizieren Sie Basen für das Bild $\text{im}(A)$ und den Kern $\text{ker}(A)$.
- (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:

$$\text{im}(A) = \langle e_1, e_2, e_3 \rangle_{\mathbb{R}} \leq \mathbb{R}^4 \quad \text{und} \quad \text{ker}(A) = \langle v_2, v_4 \rangle_{\mathbb{R}} \leq \mathbb{R}^5$$

Die Familie (v_2, v_4) ist gestuft, also linear unabhängig in \mathbb{R}^5 .

- (2) Es gilt $b = Aw \in \text{im}(A)$, also $L(A, b) = w + \text{ker}(A) = w + v_2\mathbb{R} + v_4\mathbb{R}$, siehe Satz I1R. Zum Kontrast: Es gilt $b' \notin \text{im}(A)$, also $L(A, b') = \emptyset$,

Bild und Kern einer Matrix in reduzierter Zeilenstufenform

$$s = (\quad 2, \quad 3, \quad 5, \quad 8 \quad)$$

$$A = \begin{bmatrix} 0 & 1 & 0 & * & 0 & * & 0 & * & * \\ 0 & 0 & 1 & * & 0 & * & * & 0 & * \\ 0 & 0 & 0 & 0 & 1 & * & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Aufgabe: Gegeben sei $A \in \mathbb{R}^{m \times n}$ in reduzierter Zeilenstufenform mit Stufen $s = (s_1 < \dots < s_r)$. Nennen Sie eine Basis für Bild und Kern.

Lösung: (1) Die Pivotspalten sind eine Basis des Bildraums:

$$\text{im}(A) = \langle Ae_j \mid j \in J = \{s_1, \dots, s_r\} \rangle_{\mathbb{R}} = \langle e_1, \dots, e_r \rangle_{\mathbb{R}} \leq \mathbb{R}^m$$

(2) Die verbleibenden freien Spalten induzieren eine Basis des Kerns:

$$\text{ker}(A) = \langle v_j \mid j \in K = \{1, \dots, n\} \setminus \{s_1, \dots, s_r\} \rangle_{\mathbb{R}} \leq \mathbb{R}^n$$

Dabei gilt $v_j := \sum_{i=1}^r e_{s_i} a_{ij} - e_j$, wie im vorigen Beispiel illustriert. Die Familie $(v_j)_{j \in K}$ ist gestuft, also \mathbb{R} -linear unabhängig (J1F).

😊 Das ist ein eleganter und universell einsetzbarer Algorithmus! Über jedem Divisionsring R überführt der Gauß-Algorithmus B2c jede Matrix B in reduzierte Zeilenstufenform A . Daraus lesen wir Basen für Bild $\text{im}(A)$ und Kern $\text{ker}(A)$ ab, wie hier ausgeführt.

Aufgabe: Beweisen Sie, dass die jeweils für Bild und Kern angegebenen Vektoren tatsächlich eine Basis bilden.

Lösung: (1) Die Pivotspalten sind eine Basis des Bildraums:

$$\text{im}(A) = \langle Ae_j \mid j \in J = \{s_1, \dots, s_r\} \rangle_R^! = \langle e_1, \dots, e_r \rangle_R^! \leq R^m$$

(1a) Für jede Zeile $i = 1, \dots, r$ und die zugehörige Pivotspalte $j = s_i$ gilt $e_i = Ae_j \in \text{im}(A)$ dank RZSF. Daraus folgt $\text{im}(A) \supseteq \langle e_1, \dots, e_r \rangle_R$.

(1b) Die umgekehrte Inklusion $\text{im}(A) \subseteq \langle e_1, \dots, e_r \rangle_R$ ist klar, denn alle Spaltenvektoren von A haben Träger in $\{1, \dots, r\}$.

(1c) Die Vektoren $Ae_j = e_i$ in R^m sind R -linear unabhängig (J1F). Somit haben wir tatsächlich eine Basis von $\text{im}(A)$ vorliegen!

(2) Die verbleibenden freien Spalten induzieren eine Basis des Kerns:

$$\text{ker}(A) = \langle v_j \mid j \in K = \{1, \dots, n\} \setminus \{s_1, \dots, s_r\} \rangle_R^! \leq R^n$$

(2a) Zunächst liegt jeder Vektor $v_j := \sum_{i=1}^r e_{s_i} a_{ij} - e_j$ im Kern, denn

$$Av_j = \sum_{i=1}^r Ae_{s_i} a_{ij} - Ae_j = \sum_{i=1}^r e_i a_{ij} - \sum_{i=1}^r e_i a_{ij} = 0.$$

(2b) Sei umgekehrt $\lambda \in \text{ker}(A)$. Dazu betrachten wir $\mu \in \text{ker}(A)$ mit

$$\mu = \lambda + \sum_{j \in K} v_j \lambda_j.$$

Nach Konstruktion gilt $\mu_j = 0$ für alle $j \in K$, also $\mu = \sum_{j \in J} e_j \mu_j$, sowie

$$0 = A\mu = \sum_{j \in J} Ae_j \mu_j = \sum_{i=1}^r e_i \mu_{s_i}.$$

Dank linearer Unabhängigkeit von e_1, \dots, e_r in R^m folgt $\mu_{s_i} = 0$ für alle $i = 1, \dots, r$, also $\mu = 0$. Das bedeutet $\lambda = -\sum_{j \in K} v_j \lambda_j \in \langle v_j \mid j \in K \rangle$.

(2c) Die Familie $(v_j)_{j \in K}$ ist gestuft, also R -linear unabhängig (J1F). Somit haben wir tatsächlich eine Basis von $\text{ker}(A)$ vorliegen!

Bild und Kern und Dimensionsformel

Satz J1P: Bild und Kern und Dimensionsformel

Gegeben sei die Matrix $B \in R^{m \times n}$ und eine Transformation $S \in \text{GL}_m R$ in reduzierte Zeilenstufenform $A = SB$ mit Stufen $s = (s_1 < \dots < s_r)$.

(1) Die Pivotspalten $j = s_1, \dots, s_r$ sind eine Basis des Bildraums:

$$\text{im}(A) = \langle Ae_j \mid j \in J = \{s_1, \dots, s_r\} \rangle_R^! = \langle e_1, \dots, e_r \rangle_R^! \leq R^m$$

$$\text{im}(B) = \langle Be_j \mid j \in J = \{s_1, \dots, s_r\} \rangle_R^! = \langle S^{-1}e_1, \dots, S^{-1}e_r \rangle_R^! \leq R^m$$

(2) Die verbleibenden freien Spalten induzieren eine Basis des Kerns:

$$\ker(A) = \ker(B) = \langle v_j \mid j \in K = \{1, \dots, n\} \setminus \{s_1, \dots, s_r\} \rangle_R^! \leq R^n$$

Dabei gilt $v_j := \sum_{i=1}^r e_{s_i} a_{ij} - e_j$, wie zuvor erklärt.

(3) Insbesondere gilt $\dim_R \text{im}(B) = r$ und $\dim_R \ker(B) = n - r$.

Unabhängig vom Rang r folgt daraus die Dimensionsformel:

$$\dim_R \ker(B) + \dim_R \text{im}(B) = n$$

Bild und Kern und Dimensionsformel

Aufgabe: Beweisen Sie, dass die jeweils für Bild und Kern angegebenen Vektoren tatsächlich eine Basis bilden.

Lösung: Die Basen für $\text{im}(A)$ und $\ker(A)$ haben wir in der vorigen Aufgabe explizit ausgeführt und alle Behauptungen nachgewiesen.

(1) Wir haben $A = SB$, also $B = S^{-1}A$ und $\text{im}(B) = S^{-1} \text{im}(A)$.

Dank $\text{im}(A) = \langle e_1, \dots, e_r \rangle_R^!$ folgt $\text{im}(B) = \langle S^{-1}e_1, \dots, S^{-1}e_r \rangle_R^!$.

Wir setzen $e_i = Ae_{s_i}$ ein und erhalten $\text{im}(B) = \langle Be_{s_1}, \dots, Be_{s_r} \rangle_R^!$.

(2) Die Matrizen $A = SB$ und $B = S^{-1}A$ haben denselben Kern.

(3) Die Dimensionen folgen aus den expliziten Basen in (1) und (2).

😊 Da wir in (3) von Dimension sprechen, setzen wir stillschweigend voraus, dass unser Ring R die Invarianz der Dimension erfüllt (J1L). Dies gilt insb. für alle Divisionsringe und alle kommutativen Ringe.

😊 Über jedem Divisionsring R überführt der Gauß-Algorithmus B2c jede Matrix B in reduzierte Zeilenstufenform A . Daraus lesen wir Basen für Bild $\text{im}(A)$ und Kern $\ker(A)$ ab, wie hier ausgeführt.

Bild und Kern und Dimensionsformel

Aufgabe: Vorgelegt sei eine Matrix $A \in \mathbb{R}^{5 \times 9}$ von folgender Gestalt:

$$\begin{bmatrix} * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & * & * & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Was können Sie über die Dimension von Bild und Kern aussagen?

Lösung: Für jede Matrix $A \in \mathbb{R}^{m \times n}$ gilt die Dimensionsformel

$$\dim_{\mathbb{R}} \ker(A) + \dim_{\mathbb{R}} \operatorname{im}(A) = n.$$

Hier haben wir $0 \leq \dim_{\mathbb{R}} \operatorname{im}(A) \leq 4$ und somit $5 \leq \dim_{\mathbb{R}} \ker(A) \leq 9$.

Alle fünf Möglichkeiten $(0, 9)$, $(1, 8)$, $(2, 7)$, $(3, 6)$, $(4, 5)$ kommen vor:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Bild und Kern und Dimensionsformel

Aufgabe: Vorgelegt sei eine Matrix $A \in \mathbb{R}^{5 \times 9}$ von folgender Gestalt:

$$\begin{bmatrix} * & * & * & * & * & * & * & 1 & 0 \\ * & * & * & * & * & * & * & 2 & 0 \\ * & * & * & * & * & * & * & 3 & 3 \\ * & * & * & * & * & * & * & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

Was können Sie über die Dimension von Bild und Kern aussagen?

Lösung: Hier gilt $2 \leq \dim_{\mathbb{R}} \operatorname{im}(A) \leq 5$ und somit $4 \leq \dim_{\mathbb{R}} \ker(A) \leq 7$.

Alle vier Möglichkeiten $(2, 7)$, $(3, 6)$, $(4, 5)$, $(5, 4)$ treten tatsächlich auf.

Aufgabe: Welche Dimension hat der Kern der \mathbb{R} -linearen Abbildung

$$f : \mathbb{R}^{100} \rightarrow \mathbb{R} : (x_1, \dots, x_{100}) \mapsto x_1 + \dots + x_{100} ?$$

Lösung: Es gilt $\dim_{\mathbb{R}} \operatorname{im}(f) = 1$, also $\dim_{\mathbb{R}} \ker(f) = 99$. Explizit ist die Matrix $A = (1, \dots, 1)$ in RZSF. Eine Basis des Kerns ist $(e_1 - e_j)_{j=2}^{100}$.

Extremale Charakterisierung von Basen

Jeder R -lineare Raum besitzt ein Erzeugendensystem, etwa $(v)_{v \in V}$. Eine Basis existiert jedoch nicht immer, siehe $\mathbb{Z}/2$ über \mathbb{Z} (J1B). Wir wollen nun zeigen: Jeder Vektorraum besitzt eine Basis.


Satz J2A: extremale Charakterisierung einer Basis

Sei V ein Vektorraum über dem Divisionsring R .

Sei $(b_i)_{i \in K}$ ein Erzeugendensystem und $I \subseteq K$.


Dann sind äquivalent:

- 1 Die Familie $\mathcal{B} = (b_i)_{i \in I}$ ist eine Basis von V :
Sie erzeugt V über R und ist linear unabhängig.
- 2 $\mathcal{B} = (b_i)_{i \in I}$ erzeugt V und ist dabei minimal:
Keine echte Teilfamilie $(b_i)_{i \in J}$ mit $J \subsetneq I$ erzeugt V .
- 3 $\mathcal{B} = (b_i)_{i \in I}$ ist linear unabhängig in V und dabei maximal:
Jede echte Oberfamilie $(b_i)_{i \in J}$ mit $I \subsetneq J \subseteq K$ ist linear abhängig.

 Minimal / maximal gilt hier bezüglich Inklusion, nicht Elementezahl. Der Satz ist genau so gemeint, wie er hier sorgsam ausformuliert ist.

Extremale Charakterisierung von Basen

Dieser Satz fordert als Eingabedatum ein Erzeugendensystem von V über R . Meist gibt die konkrete Anwendung ein Erzeugendensystem vor. Wenn uns dazu partout nichts Besseres einfällt, so nehmen wir notfalls die gesamte Menge V als Erzeugendensystem, also die Familie $(v)_{v \in V}$.

 Die Begriffe *minimal* und *maximal* sind hier im Sinne der Inklusion zu verstehen, so wie in geordneten Mengen (Posets) üblich, siehe F11; genau hierzu haben wir Begriffe und Beispiele in Kapitel F vorbereitet.

 Ich weise vorsorglich auf ein verbreitetes Missverständnis hin:

Damit ist nicht gemeint, dass die Elementezahl minimal / maximal wäre! Das spielt in diesem Satz keine Rolle, es hat genau genommen auch gar keinen rechten Sinn, denn die Mengen dürfen unendlich sein.

Um jedes Missverständnis möglichst auszuschließen, habe ich in der zweiten Zeile jeweils explizit ausformuliert, was *minimal* und *maximal* hier für Teilfamilien und Oberfamilien bedeuten. Möge es nützen!

Basis als maximale linear unabhängige Familie

- 1 Die Familie $\mathcal{B} = (b_i)_{i \in I}$ ist eine Basis von V :
Sie erzeugt V über R und ist linear unabhängig.
- 3 $\mathcal{B} = (b_i)_{i \in I}$ ist linear unabhängig in V und dabei maximal:
Jede echte Oberfamilie $(b_i)_{i \in J}$ mit $I \subsetneq J \subseteq K$ ist linear abhängig.

Beweis: „(1) \Rightarrow (3)“: Wir zeigen Maximalität.

Für jeden Index $j \in J \setminus I$ gilt $b_j \in \langle b_i \mid i \in I \rangle_R$, denn \mathcal{B} ist eine Basis. Wir haben also $b_j = \sum_{i \in I} b_i \lambda_i$ mit $\lambda \in R^{(I)}$, und somit liefert $b_j - \sum_{i \in I} b_i \lambda_i = 0$ eine nicht-triviale Relation für $(b_i)_{i \in J}$.

„(3) \Rightarrow (1)“: Aus (3) und $k \in K$ folgern wir $b_k \in \langle b_i \mid i \in I \rangle_R$; daraus folgt sofort $\langle b_i \mid i \in I \rangle_R \supseteq \langle b_k \mid k \in K \rangle_R = V$, also gilt (1).

Gäbe es $b_k \in V \setminus \langle b_i \mid i \in I \rangle_R$, so wäre die Oberfamilie $(b_i)_{i \in J}$ mit $J = I \sqcup \{k\}$ linear unabhängig: Hierzu sei $\lambda \in R^{(J)}$ und $\sum_{i \in J} b_i \lambda_i = 0$. Wäre dabei $\lambda_k \neq 0$, so hätten wir $b_k = \sum_{i \in I} b_i (-\lambda_i \lambda_k^{-1}) \in \langle b_i \mid i \in I \rangle_R$. Somit muss $\lambda_k = 0$ gelten, und das heißt $\sum_{i \in I} b_i \lambda_i = 0$. Aber $\mathcal{B} = (b_i)_{i \in I}$ ist linear unabhängig, also $\lambda = 0$.

Basis als minimales Erzeugendensystem

- 1 Die Familie $\mathcal{B} = (b_i)_{i \in I}$ ist eine Basis von V :
Sie erzeugt V über R und ist linear unabhängig.
- 2 $\mathcal{B} = (b_i)_{i \in I}$ erzeugt V und ist dabei minimal:
Keine echte Teilfamilie $(b_i)_{i \in J}$ mit $J \subsetneq I$ erzeugt V .

Beweis: „(1) \Rightarrow (2)“: Wir zeigen Minimalität;

für jeden Index $k \in I \setminus J$ gilt $b_k \notin \langle b_i \mid i \in J \rangle_R$.

Wäre $b_k \in \langle b_i \mid i \in J \rangle_R$, also $b_k = \sum_{i \in J} b_i \lambda_i$ mit $\lambda \in R^{(J)}$, dann liefert $b_k - \sum_{i \in J} b_i \lambda_i = 0$ eine nicht-triviale Relation für $(b_i)_{i \in I}$. Das widerspricht der linearen Unabhängigkeit der Familie $\mathcal{B} = (b_i)_{i \in I}$.


„(2) \Rightarrow (1)“: Wir zeigen lineare Unabhängigkeit von $\mathcal{B} = (b_i)_{i \in I}$.

Sei $\lambda \in R^{(I)}$ und $\sum_{i \in I} b_i \lambda_i = 0$. Angenommen, $\lambda_k \neq 0$ für ein $k \in I$.

Wir setzen dann $J = I \setminus \{k\}$ und erhalten $b_k = \sum_{i \in J} b_i (-\lambda_i \lambda_k^{-1})$.

In jeder Linearkombination von $(b_i)_{i \in I}$ können wir b_k so ersetzen.

Also erzeugt auch die echte Teilfamilie $(b_i)_{i \in J}$ immer noch V . □

 Für „(2) \Rightarrow (1)“ und „(3) \Rightarrow (1)“ müssen wir $\lambda_k \in R \setminus \{0\}$ invertieren. Daher gelingt dieser Beweis tatsächlich nur über einem Divisionsring R .

Existenz von Basen

Satz J2B: Existenz von Basen

Sei V ein Vektorraum über dem Divisionsring R und erzeugt von $(v_i)_{i \in K}$.

(1) **Basisergänzungssatz:** Jede linear unabhängige Familie $(v_i)_{i \in I}$ mit $I \subseteq K$ lässt sich zu einer Basis $(v_i)_{i \in J}$ von V ergänzen mit $I \subseteq J \subseteq K$.

(2) **Basisauswahlsatz:** Jedes Erzeugendensystem $(v_i)_{i \in K}$ enthält eine Basis $(v_i)_{i \in J}$ von V als Teilfamilie mit $\emptyset \subseteq J \subseteq K$.

(3) **Existenzsatz:** In jedem Vektorraum V existiert eine Basis $(v_i)_{i \in J}$.

 Wir setzen voraus, dass R ein Divisionsring ist. Ohne geht es nicht:

Beispiel: Im \mathbb{Z} -linearen Raum \mathbb{Z} ist $(5, 6)$ erzeugend und minimal, jedoch keine Basis; hieraus lässt sich keine Basis auswählen.

Beispiel: Im \mathbb{Z} -linearen Raum \mathbb{Z} ist (5) linear unabhängig und maximal, jedoch keine Basis; (5) lässt sich nicht zu einer Basis ergänzen.

Beispiel: Der \mathbb{Z} -lineare Raum $\mathbb{Z}/2\mathbb{Z}$ ist nicht frei (J1B):
Es existiert keine \mathbb{Z} -Basis von $\mathbb{Z}/2\mathbb{Z}$.

Existenz von Basen

(1) **Basisergänzungssatz:** Jede linear unabhängige Familie $(v_i)_{i \in I}$ mit $I \subseteq K$ lässt sich zu einer Basis $(v_i)_{i \in J}$ von V ergänzen mit $I \subseteq J \subseteq K$.

Beweis: (1a) Zur Vereinfachung sei K endlich, also V endlich erzeugt. Wir wählen J maximal mit $I \subseteq J \subseteq K$ und $(v_i)_{i \in J}$ linear unabhängig. Dank des vorangegangenen Satzes J2A ist $(v_i)_{i \in J}$ eine Basis von V .

(1b) Falls K unendlich ist, so argumentieren wir entsprechend. Wir betrachten das System aller linear unabhängigen Familien:

$$X = \{ J \mid I \subseteq J \subseteq K \text{ und } (v_i)_{i \in J} \text{ linear unabhängig} \}$$

Die geordnete Menge (X, \subseteq) erfüllt die Voraussetzung des Zornschen Lemmas F1v und besitzt somit mindestens ein maximales Element.

(2) Wir setzen $I = \emptyset$ und wählen J wie in (1).

(3) Zu V existiert ein Erzeugendensystem, notfalls $(v)_{v \in V}$. Daraus können wir dank (2) eine Basis auswählen. **QED**

Die Anwendung des Zornschen Lemmas in (1b) bedarf der Erläuterung. Ganz anschaulich wollen wir linear unabhängige Vektoren hinzufügen, bis wir „schließlich“ eine maximale Familie erreichen. Im endlichen Fall ist das offensichtlich möglich, im unendlichen Fall ist es delikant.

◆ Satz F1v: Lemma von Zorn

Eine geordnete Menge, in der jede Kette eine obere Schranke hat, enthält mindestens ein maximales Element.

Wir wollen dies hier auf die geordnete Menge (X, \subseteq) anwenden. Dazu sei $Y \subseteq X$ eine Kette, das bedeutet, je zwei Elemente $J_1, J_2 \in Y$ sind vergleichbar, es gilt also $J_1 \subseteq J_2$ oder $J_2 \subseteq J_1$. Wir setzen $J := \bigcup Y$. Es gilt $I \subseteq J \subseteq K$ und die Familie $(v_i)_{i \in J}$ ist linear unabhängig:

Hierzu betrachten wir eine Relation, also eine Linearkombination zu Null, $0 = v_{i_1} \lambda_1 + \dots + v_{i_n} \lambda_n$ mit $i_1, \dots, i_n \in J$ und $\lambda_1, \dots, \lambda_n \in R$. Zu jedem Index i_k existiert $J_k \in Y$ mit $i_k \in J_k$. Da Y eine Kette ist, können wir so sortieren, dass $J_1 \subseteq \dots \subseteq J_n$ gilt. Aber die Familie $(v_i)_{i \in J_n}$ ist linear unabhängig! Also folgt $\lambda_1 = \dots = \lambda_n = 0$.

In der geordneten Menge (X, \subseteq) hat demnach jede Kette $Y \subseteq X$ eine obere Schranke $J = \bigcup Y$. Dank Zorns Lemma F1v enthält (X, \subseteq) mindestens ein maximales Element. Genau dies wollten wir zeigen.

☹ Zugegeben, diese Rechnung ist einfach, aber nicht erhellend. Wir prüfen die Voraussetzung von Zorns Lemma, das geht leicht, doch die Schlussfolgerung lässt uns etwas enttäuscht zurück.

😊 Sehen wir es positiv: Dies beweist die Existenz einer Basis, auch wenn die Beweismethode alles andere als konstruktiv ist. Eine schwache Aussage ist besser als gar keine Aussage.

Bemerkung: Meist gibt die Anwendung ein Erzeugendensystem vor, so wie in (1) erklärt. Wenn dabei K endlich ist, so sind wir fein raus. Für Aussage (3) jedoch müssen wir ein Erzeugendensystem wählen. Wenn uns dazu partout nichts Besseres einfällt, so nehmen wir notfalls die gesamte Menge V als Erzeugendensystem, also die Familie $(v)_{v \in V}$.

Anwendung: die Dimension von Vektorräumen

Korollar J2C: die Dimension eines Vektorraumes

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(1) Der Existenzsatz J2B garantiert:

Jeder Vektorraum V über R erlaubt eine Basis $\mathcal{B} = (b_i)_{i \in I}$.

(2) Die Invarianz der Dimension J1K besagt:

Jede weitere Basis von V hat dieselbe Mächtigkeit.

Wir können daher die **Dimension** von V definieren durch

$$\dim_R(V) := \#I.$$

Die Dimension ist wohldefiniert: Der Wert existiert und ist eindeutig.

😊 Die Dimension $\dim_R(V)$ eines linearen Raums V über einem Divisionsring R ist ein wichtiges Hilfsmittel in der Linearen Algebra und all ihren Anwendungen. Es lohnt sich daher, diesen zentralen Begriff und die nötigen Werkzeuge gründlich zu verstehen.

Anwendung: die Dimension von Vektorräumen

Übung: Welche Dimension hat $\mathbb{Q}[\sqrt{2}]$ über \mathbb{Q} ? Nennen Sie eine Basis!

Lösung: Wir betrachten $\mathbb{Q}[\sqrt{2}]$ als den kleinsten Teilring in \mathbb{R} , der \mathbb{Q} und $\sqrt{2}$ enthält. Dies führt zur Menge $\mathbb{Q}[\sqrt{2}] = \{x + \sqrt{2}y \mid x, y \in \mathbb{Q}\}$.

Somit ist $(1, \sqrt{2})$ ein Erzeugendensystem. Diese Familie ist zudem linear unabhängig: Aus $x, y \in \mathbb{Q}$ und $x + \sqrt{2}y = 0$ folgt $x = y = 0$, dank Irrationalität von $\sqrt{2}$ (A1F). Demnach ist $(1, \sqrt{2})$ linear unabhängig, also eine Basis. Daraus lesen wir die Dimension ab: $\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = 2$.

😊 Genau so wird die Dimension $\dim_R(V)$ definiert und in vielen typischen Fällen auch direkt berechnet: Wir finden eine geeignete Familie $(b_i)_{i \in I}$ von V , weisen für $(b_i)_{i \in I}$ lineare Unabhängigkeit und Erzeugung von V nach, und schließen so $\dim_R(V) = \#I$.

😊 Es genügt, dieses Verfahren für *eine* Basis zu durchlaufen: Jede andere Basis ist genauso gut und liefert dasselbe Ergebnis!

Beispiel J2D: Basis von \mathbb{R} über \mathbb{Q}

Zum Raum \mathbb{R} über \mathbb{Q} existiert dank Satz J2B eine Basis $\mathcal{B} = (b_i)_{i \in I}$.

Wir erhalten so die \mathbb{Q} -lineare Bijektion

$$\Phi_{\mathcal{B}} : \mathbb{Q}^{(I)} \xrightarrow{\sim} \mathbb{R}.$$

Dabei ist I überabzählbar, denn $\mathbb{Q}^{(\mathbb{N})}$ ist abzählbar (F2P).

Insbesondere gilt

$$\dim_{\mathbb{Q}}(\mathbb{R}) = \infty.$$

☹️ Der Beweis des Existenzsatzes J2B nutzt das Zornsche Lemma und ist daher nicht konstruktiv. Er sichert allein die Existenz, mehr nicht.

Niemand hat je eine Basis von \mathbb{R} über \mathbb{Q} gesehen.

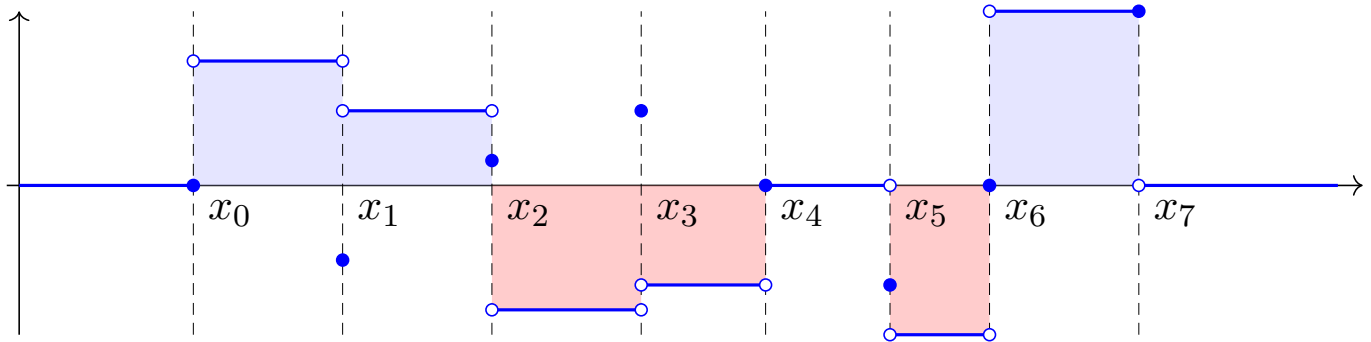
😊 Wir können immerhin eine unendliche, linear unabhängige Familie angeben (J127): Die Familie $(\ln p)_{p \in \mathbb{P}}$ in \mathbb{R} linear unabhängig über \mathbb{Q} .

Das ist sehr konkret und der Beweis ist lehrreich!

😊 Genau genommen ist \mathbb{R} über \mathbb{Q} nicht nur unendlich-dimensional, die Dimension ist wie hier zu sehen sogar überabzählbar unendlich.

Auf diese genauere Sichtweise gehe ich hier nicht näher ein.

Illustration: Treppenfunktionen



◆ Satz I1w: eindimensionale Treppenfunktionen

Die Treppenfunktionen $T(\mathbb{R}, \mathbb{R}) \leq \mathbb{R}^{\mathbb{R}}$ bilden einen \mathbb{R} -Untervektorraum. Dieser wird erzeugt von den Indikatorfunktionen $\mathbf{I}_{[a,b]}$ mit $a \leq b$ in \mathbb{R} .

Aufgabe: (1) Ist die Familie $(\mathbf{I}_{[a,b]})_{a \leq b}$ eine Basis von $T(\mathbb{R}, \mathbb{R})$?

(2) Können Sie aus $(\mathbf{I}_{[a,b]})_{a \leq b}$ eine Basis auswählen? (3) explizit?

Lösung:

(1) Es gelten die Relationen $\mathbf{I}_{[a,c]} = \mathbf{I}_{[a,b]} + \mathbf{I}_{[b,c]} - \mathbf{I}_{[b,b]}$ für $a < b < c$. Somit ist $(\mathbf{I}_{[a,b]})_{a \leq b}$ ein Erzeugendensystem, aber linear abhängig.

(2) Ja, dank Auswahlssatz J2B. (3) Hier muss man kreativ sein!

Illustration: Treppenfunktionen

😊 Dies ist eine unendlich-dimensionale, doch konkrete Illustration zu **Erzeugendensystemen** und **linearer Unabhängigkeit** und **Basen**:

Die Familie der Indikatorfunktionen $\mathbf{I}_{[a,b]}$ mit $a \leq b$ in \mathbb{R} erzeugt $T(\mathbb{R}, \mathbb{R})$, aber sie ist, wie hier zu sehen, linear abhängig und somit keine Basis.

😊 Dieses Beispiel ist vollkommen realistisch und naturgemäß vertrackt, aber zugleich noch einfach genug, um elementar gelöst zu werden.

Wenn Sie möchten, versuchen Sie es! Sie können daran viel lernen. Alternativ können Sie später einmal darauf zurückkommen...

😊 In der Analysis sind Treppenfunktionen ein erster wichtiger Schritt zur Integration von Funktionen $f: \mathbb{R} \rightarrow \mathbb{R}$ und allgemein $f: \mathbb{R}^n \rightarrow \mathbb{R}$.

Treppenfunktionen werden dort nur als Werkzeug eingesetzt, aber darüber hinaus nicht weiter betrachtet. Sie sind jedoch auch eine schöne Illustration und hier sogar selbst Untersuchungsgegenstand.

Beispiel J2E: eine Basis des Raums der Treppenfunktionen

Aus dem Erzeugendensystem $(\mathbf{I}_{[a,b]})_{a \leq b}$ wählen wir (etwas willkürlich, aber geschickt) die Teilfamilie $(\mathbf{I}_Q)_{Q \in I}$ wobei $I = I_0 \sqcup I_+ \sqcup I_-$ mit $I_0 = \{ [a, a] \mid a \in \mathbb{R} \}$, $I_+ = \{ [0, a] \mid a \in \mathbb{R}_{>0} \}$, $I_- = \{ [a, 0] \mid a \in \mathbb{R}_{<0} \}$.

Diese Familie $(\mathbf{I}_Q)_{Q \in I}$ ist eine Basis des Vektorraums $T(\mathbb{R}, \mathbb{R}) \leq \mathbb{R}^{\mathbb{R}}$.

Aufgabe: (Wenn Sie gerne knobeln. . .) Beweisen Sie dies!

Lösung: (1) Die Familie $(\mathbf{I}_Q)_{Q \in I}$ erzeugt $T(\mathbb{R}, \mathbb{R})$.

Hierzu genügt es, die Funktionen $\mathbf{I}_{[a,b]}$ für $a \leq b$ in \mathbb{R} zu erzeugen.

Die fehlenden Fälle $0 < a < b$ und $a < 0 < b$ und $a < b < 0$ sind klar:

$$0 < a < b : \quad \mathbf{I}_{[a,b]} = \mathbf{I}_{[0,b]} - \mathbf{I}_{[0,a]} + \mathbf{I}_{[a,a]}$$

$$a < 0 < b : \quad \mathbf{I}_{[a,b]} = \mathbf{I}_{[a,0]} + \mathbf{I}_{[0,b]} - \mathbf{I}_{[0,0]}$$

$$a < b < 0 : \quad \mathbf{I}_{[a,b]} = \mathbf{I}_{[a,0]} - \mathbf{I}_{[b,0]} + \mathbf{I}_{[b,b]}$$

(2) Die Familie $(\mathbf{I}_Q)_{Q \in I}$ ist linear unabhängig in $T(\mathbb{R}, \mathbb{R})$.

Zu jedem $P \in I$ betrachten wir die \mathbb{R} -lineare Abbildung φ_P :

$$\varphi_{[0,a]} : T(\mathbb{R}, \mathbb{R}) \rightarrow \mathbb{R} : f \mapsto \lim_{x \nearrow a} f(x) - \lim_{x \searrow a} f(x)$$

$$\varphi_{[a,0]} : T(\mathbb{R}, \mathbb{R}) \rightarrow \mathbb{R} : f \mapsto \lim_{x \searrow a} f(x) - \lim_{x \nearrow a} f(x)$$

$$\varphi_{[a,a]} : T(\mathbb{R}, \mathbb{R}) \rightarrow \mathbb{R} : f \mapsto \begin{cases} f(a) - \varphi_{[a,0]}(f) & \text{falls } a < 0 \text{ und} \\ f(a) - \varphi_{[0,a]}(f) & \text{falls } a > 0, \text{ sonst} \\ f(0) - \sum_{s < 0} \varphi_{[s,0]}(f) - \sum_{s > 0} \varphi_{[0,s]}(f) & \end{cases}$$

Für alle $P, Q \in I$ prüft man nun geduldig nach, dass folgendes gilt:

$$\varphi_P(\mathbf{I}_Q) = \begin{cases} 1 & \text{falls } P = Q, \\ 0 & \text{falls } P \neq Q. \end{cases}$$

Daraus folgt die lineare Unabhängigkeit der Familie $(\mathbf{I}_Q)_{Q \in I}$:

Hierzu sei $\lambda \in \mathbb{R}^{(I)}$ und $0 = \sum_{Q \in I} \lambda_Q \mathbf{I}_Q$. Für jedes $P \in I$

folgt $0 = \varphi_P(\sum_{Q \in I} \lambda_Q \mathbf{I}_Q) = \lambda_P$. Das zeigt $\lambda = 0$.

Satz J2F: Ordnung endlicher Vektorräume

Sei V ein Vektorraum über dem Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
 Dann gilt entweder $\#V = \infty$ oder $\#V = p^d$ mit $d \in \mathbb{N}$.

Beispiel: Es gibt Vektorräume der Ordnung 1, 2, 3, 4, 5, aber nicht 6.

Beweis: Nach Wahl einer Basis $\mathcal{B} = (b_i)_{i \in I}$ gilt $\Phi_{\mathcal{B}} : \mathbb{F}_p^{(I)} \xrightarrow{\sim} V$.
 Im endlichen Falle gilt $\#I = d \in \mathbb{N}$ und somit $\#V = \#\mathbb{F}_p^d = p^d$. QED

Satz J2G: Ordnung endlicher Körper

Sei K ein endlicher Körper (oder Divisionsring).
 Dann gilt $\#K = p^d$ mit $p \in \mathbb{N}_{\geq 2}$ prim und $d \in \mathbb{N}_{\geq 1}$.

Beispiel: Es gibt Körper der Ordnung 2, 3, 4, 5, aber nicht 6.

Beweis: Der Körper K enthält seinen charakteristischen Unterkörper $\text{Char}(K) \cong \mathbb{F}_p$ mit $p \in \mathbb{N}_{\geq 2}$ prim (G2H). Hierüber ist K ein Vektorraum.
 Dank J2F folgt $\mathbb{F}_p^d \xrightarrow{\sim} K$ und $\#K = \#\mathbb{F}_p^d = p^d$ mit $d \in \mathbb{N}_{\geq 1}$. QED

Ordnung der Gruppe $GL_3 \mathbb{F}_2$

😊 Es ist oft lehrreich, neu definierte Objekte zu zählen. Dies zwingt, die Definition genau zu verstehen und klärt so Missverständnisse auf.
 Eine weitere schöne Zählaufgabe ist die folgende:

Aufgabe: Wie viele Elemente hat der Ring $\mathbb{F}_2^{3 \times 3}$? die Gruppe $GL_3 \mathbb{F}_2$?
 Wenn Sie zufällig eine 3×3 -Matrix A mit Nullen und Einsen befüllen, mit welcher Wahrscheinlichkeit ist dann A in $\mathbb{F}_2^{3 \times 3}$ invertierbar?

Lösung: (1) Der Matrixring $\mathbb{F}_2^{3 \times 3}$ hat genau $2^9 = 512$ Elemente.
 (2) In $(\mathbb{F}_2^{3 \times 3}, \cdot)$ ist eine Matrix $A \in \mathbb{F}_2^{3 \times 3}$ genau dann invertierbar, wenn ihre Spalten a_1, a_2, a_3 eine Basis von \mathbb{F}_2^3 über \mathbb{F}_2 bilden (B2D).

- 1 Für $a_1 \in \mathbb{F}_2^3 \setminus \{0\}$ haben wir zunächst $2^3 - 1 = 7$ Möglichkeiten.
- 2 Für $a_2 \in \mathbb{F}_2^3 \setminus \langle a_1 \rangle$ bleiben dann $2^3 - 2 = 6$ Möglichkeiten.
- 3 Für $a_3 \in \mathbb{F}_2^3 \setminus \langle a_1, a_2 \rangle$ bleiben $2^3 - 2^2 = 4$ Möglichkeiten.

Demnach hat die Gruppe $GL_3 \mathbb{F}_2$ genau $7 \cdot 6 \cdot 4 = 168$ Elemente.

(3) Die gesuchte Wahrscheinlichkeit ist $168/512 = 0.328125$.

Ordnung der Gruppe $GL_n \mathbb{F}_q$

Satz J2H: Ordnung der Gruppe $GL_n \mathbb{F}_q$

(1) Sei \mathbb{F}_q ein endlicher Körper mit q Elementen. Für alle $n \in \mathbb{N}$ gilt

$$\# GL_n \mathbb{F}_q = \prod_{k=0}^{n-1} (q^n - q^k) = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

(2) Die Anzahl der linear unabhängigen Familien (a_1, \dots, a_ℓ) in \mathbb{F}_q^n ist

$$b_q(n, \ell) = \prod_{k=0}^{\ell-1} (q^n - q^k) = (q^n - 1)(q^n - q) \cdots (q^n - q^{\ell-1}).$$

(3) Die Anzahl der ℓ -dimensionalen Unterräume $U \leq \mathbb{F}_q^n$ ist

$$\frac{b_q(n, \ell)}{b_q(\ell, \ell)} = \prod_{k=0}^{\ell-1} \frac{q^n - q^k}{q^\ell - q^k} = \prod_{k=0}^{\ell-1} \frac{q^{n-k} - 1}{q^{\ell-k} - 1} =: \binom{n}{\ell}_q$$

😊 Formel (3) ist eine schöne Anwendung der Klassengleichung E3C.

Ordnung der Gruppe $GL_n \mathbb{F}_q$

Beweis: (1) Eine Matrix $A \in \mathbb{F}_q^{n \times n}$ ist genau dann invertierbar, wenn ihre Spalten $a_1, \dots, a_n \in \mathbb{F}_q^n$ eine Basis von \mathbb{F}_q^n über \mathbb{F}_q bilden (B2D). Somit ist die Formel (1) ein Spezialfall der allgemeinen Formel (2).

(2) Für $B_q(n, \ell) = \{ (a_1, \dots, a_\ell) \in (\mathbb{F}_q^n)^\ell \text{ linear unabhängig} \}$ zeigen wir:

$$\# B_q(n, \ell) = b_q(n, \ell)$$

Wir führen Induktion über ℓ : Die Formel gilt für $\ell = 0$.

Sei nun $\ell \geq 1$ und $(a_1, \dots, a_{\ell-1})$ in \mathbb{F}_q^n linear unabhängig.

Die möglichen linear unabhängigen Ergänzungen sind

$$a_\ell \in \mathbb{F}_q^n \setminus \langle a_1, \dots, a_{\ell-1} \rangle_{\mathbb{F}_q}.$$

Mit der Induktionsvoraussetzung folgt daraus die behauptete Formel:

$$\# B_q(n, \ell) = \# B_q(n, \ell - 1)(q^n - q^{\ell-1}) = b_q(n, \ell - 1)(q^n - q^{\ell-1}) = b_q(n, \ell)$$

(3) Die Anzahl der linear unabhängigen Familien (a_1, \dots, a_ℓ) ist $b_q(n, \ell)$. Jede erzeugt einen Unterraum $U = \langle a_1, \dots, a_\ell \rangle_{\mathbb{F}_q}$ der Dimension ℓ .

Jeweils $b_q(\ell, \ell)$ davon erzeugen denselben Unterraum U . ◻

Wie wahrscheinlich ist Invertierbarkeit?

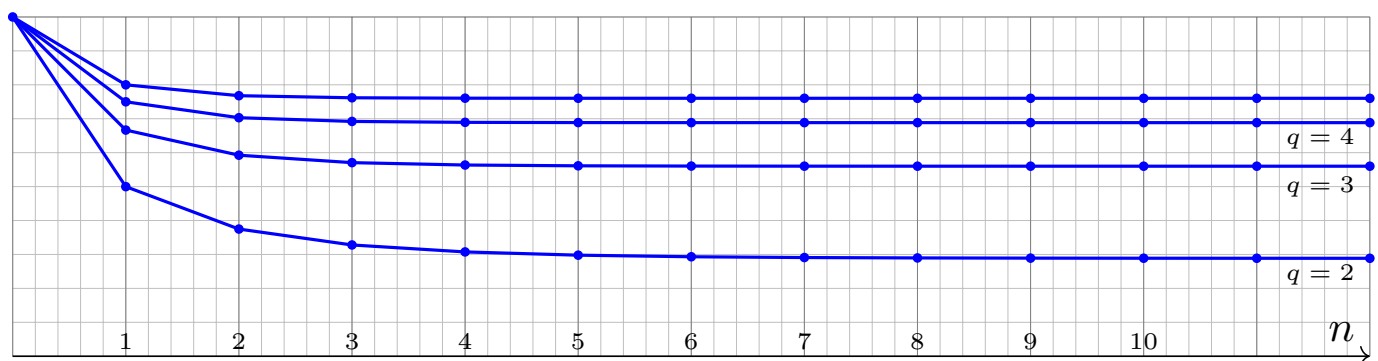
Aufgabe: Sei \mathbb{F}_q ein endlicher Korper mit q Elementen und $n \in \mathbb{N}$. Sie wahlen zufallig (gleichverteilt) eine Matrix $A \in \mathbb{F}_q^{n \times n}$. Mit welcher Wahrscheinlichkeit ist A invertierbar? Fur groe q ? Fur groe n ?

Losung: (1) Es gibt q^{n^2} Matrizen, die invertierbaren bilden den Anteil

$$\varphi(q, n) = \frac{\#\text{GL}_n \mathbb{F}_q}{\#\mathbb{F}_q^{n \times n}} = \prod_{k=0}^{n-1} \frac{q^n - q^k}{q^n} = (1 - q^{-1})(1 - q^{-2}) \dots (1 - q^{-n}).$$

(2) Fur $q \rightarrow \infty$ erhalten wir $\varphi(q, n) \rightarrow 1$. Uber einem groen endlichen Korper \mathbb{F}_q ist eine zufallige Matrix also „nahezu sicher“ invertierbar.

(3) Bei festem q konvergiert $\varphi(q, n)$ fur $n \rightarrow \infty$ sehr schnell:



Wie wahrscheinlich ist Invertierbarkeit?

😊 Solche Zahlen(bei)spiele geben uns eine hilfreiche Anschauung, wie hufig invertierbare Matrizen sind. Ebenso konnen wir fragen, mit welcher Wkt k Vektoren linear unabhangig sind, oder ahnliches.

Wir stellen erstaunt fest, dass die invertierbaren Matrizen gar nicht selten sind, wie man vielleicht vermuten konnte, sondern die Mehrheit.

Anschauliche Uberschlagsrechnung: Fur groe q vernachlassigen wir die Faktoren $(1 - q^{-2}), \dots, (1 - q^{-n})$, denn sie liegen recht nahe bei 1.

Der Anteil der invertierbaren Matrizen ist dann

$$\frac{\#\text{GL}_n \mathbb{F}_q}{\#\mathbb{F}_q^{n \times n}} = (1 - q^{-1})(1 - q^{-2}) \dots (1 - q^{-n}) \lesssim (1 - q^{-1}).$$

Im Beispiel $q = 11$ finden wir $0.900832 < \varphi(q, n) \leq 10/11 < 0.909091$. Die Schatzung ist bereits auf 1% genau, was uns hier genugen soll.

😊 Der Anteil der invertierbaren Matrizen in $\mathbb{F}_q^{n \times n}$ ist kaum geringer als der Anteil der invertierbaren Skalare in \mathbb{F}_q , also $1 - 1/q$.

Aufgabe: (0) Zu $q \in \mathbb{R}_{>1}$ und $n, k \in \mathbb{N}$ setzen wir

$$[n]_q := \frac{q^n - 1}{q - 1} = 1 + q + \cdots + q^{n-1},$$

$$[n]_q! := [n]_q \cdot [n-1]_q \cdots [3]_q \cdot [2]_q \cdot [1]_q.$$

(1) Damit erhalten wir die Darstellung:

$$\binom{n}{k}_q := \frac{[n]_q!}{[n-k]_q! [k]_q!} = \prod_{i=0}^{k-1} \frac{q^{n-i} - 1}{q^{k-i} - 1} = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}.$$

(2) Ist \mathbb{F}_q ein endlicher Körper mit q Elementen, so ist $\binom{n}{k}_q$ die Anzahl der k -dimensionalen Unterräume $U \leq \mathbb{F}_q^n$. Was erhalten Sie für $q \searrow 1$?

Lösung: (1) Wir setzen (0) ein und formen dies sorgsam um.

(2) Im Grenzwert $q \rightarrow 1$ finden wir $[n]_q \rightarrow n$ und $[n]_q! \rightarrow n!$, also

$$\binom{n}{k}_q = \frac{[n]_q!}{[n-k]_q! [k]_q!} \rightarrow \frac{n!}{(n-k)! k!} = \binom{n}{k}.$$

😊 Die linke Seite ist die Anzahl k -dimensionaler Unterräume $U \leq \mathbb{F}_q^n$. Die rechte Seite ist der übliche Binomialkoeffizient! Er gibt die Anzahl der k -elementigen Teilmengen in einer Menge von n Elementen (E2i).

Natürlich ist der Grenzwert für $q \searrow 1$ zunächst nur numerisch.

Die geometrische Interpretation als Anzahl der k -dimensionalen Teilräume in \mathbb{F}_q^n gilt ja nur für $q = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, \dots$

Dennoch ist es bemerkenswert, dass wir für den Grenzwert $\binom{n}{k}$ eine ganz ähnliche Interpretation bereits aus einem anderen Kontext kennen!

Es gibt zahlreiche weitere solcher kombinatorisch-numerischer Zufälle. Diese Phänomene fasst man provokativ unter dem Schlagwort „der Körper mit einem Element“ zusammen: Natürlich hat jeder Körper \mathbb{F}_q mindestens zwei Elemente, da $0 \neq 1$, aber der Grenzwert $q \searrow 1$ ist dennoch faszinierend und lädt zu interessanten Spekulationen ein.

😊 Für uns ist es vor allem eine schöne numerische Illustration. Das konkrete Abzählen hilft dem Verständnis und der Intuition.

Invarianz der Dimension

😊 Analog zur Invarianz der Elementzahl E1H gilt für die Dimension:

Korollar J2I: Invarianz der Dimension

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Vorgelegt sei eine lineare Abbildung $f: U \rightarrow V$ zwischen Vektorräumen über R .

1 Ist $f: U \xrightarrow{\sim} V$ bijektiv, so folgt $\dim U = \dim V$.

2 Ist $f: U \twoheadrightarrow V$ surjektiv, so folgt $\dim U \geq \dim V$.
Gilt zudem $\dim U \leq \dim V < \infty$, so ist f bijektiv.

3 Ist $f: U \hookrightarrow V$ injektiv, so folgt $\dim U \leq \dim V$.
Gilt zudem $\infty > \dim U \geq \dim V$, so ist f bijektiv.

$$\begin{array}{ccc} U & \xrightarrow{f} & V \\ \cong \uparrow \Phi_U & & \cong \uparrow \Phi_V \\ R^n & \xrightarrow{g} & R^m \end{array}$$

Per Kontraposition folgt aus (3) analog zum Schubfachprinzip E1I:

4 Gilt $\dim U > \dim V$, so ist $f: U \rightarrow V$ nicht injektiv:
Es existiert $u \neq 0$ in U mit $f(u) = 0$ in V .

Beispiel: Für $A \in R^{m \times n}$ mit $m < n$ hat $Ax = 0$ nicht-triviale Lösungen.

Invarianz der Dimension

😊 Als lineares Gleichungssystem $Ax = 0$ gelesen: Gibt es mehr Variablen als Gleichungen, so existieren nicht-triviale Lösungen.

😊 Gibt es umgekehrt mehr Gleichungen als Variablen, so ist die Gleichung $Ax = b$ für manche rechte Seiten b nicht lösbar.

😊 Dies wissen Sie bereits vor und unabhängig von jeder Rechnung! Das ist oft nützlich, zur Prognose oder Prüfung konkreter Rechnungen.

Beweis: Zu U und V existieren Basen \mathcal{U} und \mathcal{V} dank Satz J2B.

So erhalten wir Isomorphismen $\Phi_U: R^{(I)} \xrightarrow{\sim} U$ und $\Phi_V: R^{(J)} \xrightarrow{\sim} V$ sowie die Dimensionen $\dim_R(U) = \#I$ und $\dim_R(V) = \#J$.

Jede lineare Abbildung $f: U \rightarrow V$ definiert $g = \Phi_V \circ f \circ \Phi_U^{-1}$.

Genau dann ist $g: R^{(I)} \rightarrow R^{(J)}$ sur/in/bijektiv, wenn $f: U \rightarrow V$ dies ist.

Für $g: R^{(I)} \rightarrow R^{(J)}$ nutzen wir nun die Invarianz der Dimension (J1N).

Im endlichen Fall können wir g zudem als Matrix $A \in R^{m \times n}$ darstellen, den Gauß-Algorithmus anwenden und den Rang nutzen (B2D). QED

Satz J2J: Klassifikation endlich-dimensionaler Vektorräume

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Zwei endlich-dimensionale Vektorräume U und V über R sind genau dann isomorph, wenn sie dieselbe Dimension haben.

Beweis: Nach Wahl von Basen (J2B) haben wir:

$$\begin{array}{ccc}
 U & \xrightarrow{\quad f \quad} & V \\
 \cong \uparrow \Phi_U & & \cong \uparrow \Phi_V \\
 R^n & \xrightarrow{\quad g \quad} & R^m
 \end{array}$$

😊 Die Lineare Algebra mag Ihnen zwar anfangs abstrakt erscheinen, doch die betrachteten Objekte sind schließlich einfach und übersichtlich! Das Isomorphieproblem für Vektorräume über R wird durch eine einzige Zahl gelöst: die Dimension (als Kardinalität einer / jeder Basis).

Aus Satz E1H kennen wir die wichtigste Invariante der Mathematik: Die Elementezahl ändert sich nicht unter Anwendung von Bijektionen! Hier bestaunen wir nun die wichtigste Invariante der Linearen Algebra: Die R -Dimension ändert sich nicht unter R -linearen Bijektionen! Wir nutzen dazu insb. alle Techniken zur Elementezahl aus Kapitel E, denn die Dimension ist nichts anderes als die Elementezahl einer Basis.

Allgemein versteht die Mathematik unter einer **Invariante** folgendes: Jedem der betrachteten Objekte (hier: R -Vektorräume) wird eine Größe zugeordnet (hier: ihre R -Dimension); diese Größe ändert sich nicht unter den betrachteten Umformungen (hier: R -Isomorphismen).

Invarianten sind ein wichtiges Hilfsmittel bei Klassifikationsproblemen: Objekte mit unterschiedlichen Invarianten sind wesentlich verschieden. Manchmal gilt sogar die Umkehrung, und Objekte mit gleichen Werten unter der Invariante lassen sich ineinander umformen. Wir sprechen dann von einer **vollständigen Invarianten**. Genau das liegt hier vor!

Dimension von Unterräumen

😊 Auch folgende Eigenschaft ist erfreulich, beruhigend und nützlich. Aussage und Beweis entsprechen dem Abzählen von Mengen (E2B).

Satz J2K: Dimension von Unterräumen

Sei V ein Vektorraum über dem Divisionsring R .

(1) Für jeden Unterraum $U \leq V$ gilt $\dim_R(U) \leq \dim_R(V)$.

(2) Gilt zudem $\dim_R(U) = \dim_R(V) < \infty$, so folgt $U = V$.

Beweis: Vermöge Satz J2B wählen wir eine Basis $(v_i)_{i \in I}$ von U und ergänzen diese zu einer Basis $(v_j)_{j \in J}$ von V , wobei $I \subseteq J$.

(1) Daraus folgt $\dim_R(U) = \#I \leq \#J = \dim_R(V)$. (E2B)

(2) Im Falle $\dim_R(U) = \dim_R(V) < \infty$ gilt $I = J$. (E2B)

□

⚠ Für (2) ist $\dim_R(V) < \infty$ wesentlich: In $V = \mathbb{R}[X]$ ist $U = X\mathbb{R}[X]$ ein echter Teilraum, dennoch gilt $\dim_{\mathbb{R}}(U) = \dim_{\mathbb{R}}(V) = \infty$.

Dimension von Unterräumen

⚠ Es gibt Situationen in der Mathematik (und auch sonst im Leben), wo das Unterobjekt U komplizierter sein kann als das Gesamtobjekt V . Für Vektorräume kann dieses Problem zum Glück nicht auftreten. Das ist nicht selbstverständlich, sondern muss bewiesen werden.

Beispiel: Sei K ein Körper und $R = K^{\mathbb{N}}$ der Ring aller Folgen mit punktweiser Addition und Multiplikation (G2N). Dann ist $V = R = K^{\mathbb{N}}$ ein R -linearer Raum. Er ist frei, mit dem Einselement 1 als Basis. Hierin liegt der Unterraum $U = K^{(\mathbb{N})}$ der Folgen mit endlichem Träger. Anders als V über R ist der Unterraum $U \leq V$ nicht endlich erzeugt!

Beispiel: Sei $M = \{X, Y\}^* = \{1, X, Y, XX, XY, YX, YY, XXX, \dots\}$ die Menge aller endlichen Wörter über den Buchstaben X, Y . Diese Wörter betrachten wir nun als „Monome“ und $\mathbb{R}[M]$ als „Polynomring“ in den nicht-kommutierenden Variablen X, Y . Der Ring $\mathbb{R}[M]$ enthält den Teilkörper \mathbb{R} im Zentrum und hat die Menge M als Basis über \mathbb{R} . Dann ist $V = \mathbb{R}[M]$ frei über $\mathbb{R}[M]$, mit dem Einselement 1 als Basis. Hierin ist $U = X\mathbb{R}[M] \oplus Y\mathbb{R}[M]$ ein Unterraum mit Basis (X, Y) .

Korollar J2L: Dimensionskriterium für Basen

Sei V ein Vektorraum über dem Divisionsring R .

Ist die Dimension $\dim_R(V) = n$ endlich, so gilt:

- 1 Jedes Erzeugendensystem $v_1, \dots, v_n \in V$ der Länge n ist minimal, also eine Basis.
- 2 Jede linear unabhängige Familie $v_1, \dots, v_n \in V$ der Länge n ist maximal, also eine Basis.

Beweis: Dies folgt dank Basisauswahl / Basisergänzung (J2B) und der Invarianz der Dimension (J1K): Wir können die Familie v_1, \dots, v_n verkürzen / ergänzen zu einer Basis – derselben Länge! QED

😊 Dieses Kriterium erspart Ihnen jeweils die eine Hälfte der Arbeit! Eigentlich müssten Sie in (1) noch lineare Unabhängigkeit nachweisen, ebenso müssten Sie in (2) noch Erzeugung nachweisen. Den zweiten Teil der Arbeit können Sie sich sparen, wenn die Dimension passt.

Das klingt intuitiv recht plausibel, doch auch hier ist es heilsam, sich nocheinmal mögliche Gegenbeispiele vor Augen zu führen.

Beispiel: Ist R ein Ring mit $R^4 \cong R^7$ wie in J1O, so gibt es im Raum R^7 über R Erzeugendensysteme v_1, \dots, v_7 , die sich noch verkürzen lassen. Ebenso gibt es im Raum R^4 linear unabhängige Familien u_1, \dots, u_4 , die sich noch ergänzen lassen. Wer hätte das gedacht?

Warum erzähle ich Ihnen das so ausführlich?

- 😊 Die illustrativen Gegen/Beispiele zeigen Ihnen, dass präzise Sätze hier tatsächlich nötig sind.
- 😊 Unsere gründlichen Beweise garantieren Ihnen, dass am Ende alles gut ausgeht, so wie erhofft.

Die Mühe ist also notwendig, und sie lohnt sich!

Zusammensetzen von Basen

Satz J2M: exakte Sequenz und Dimensionsformel

Sei R ein Ring. Gegeben sei eine kurze exakte Sequenz:

$$\begin{array}{ccccccc}
 0 & \xrightarrow{0} & U & \xrightarrow{f} & V & \xrightarrow{g} & W \xrightarrow{0} 0 \\
 & & u_i & \xrightarrow{\quad} & v_i & & \text{Basis} \\
 & & \text{Basis} & & v_j & \xrightarrow{\quad} & w_j
 \end{array}$$

Sei $(u_i)_{i \in I}$ eine Basis von U und $(w_j)_{j \in J}$ eine Basis von W .

Wir können $I \cap J = \emptyset$ annehmen und setzen $K = I \sqcup J$.

(1) Für $i \in I$ sei $v_i := f(u_i) \in V$. Für $j \in J$ wählen wir ein Urbild $v_j \in V$ mit $g(v_j) = w_j$ dank Surjektivität. Dann ist $(v_k)_{k \in K}$ eine Basis von V .

(2) Daher gilt $V = V_1 \oplus V_2$ mit $V_1 = \text{im}(f) = \ker(g) = \langle v_i \mid i \in I \rangle_R^!$ und $V_2 = \langle v_j \mid j \in J \rangle_R^!$. Dabei gilt $f|_{V_1} : V_1 \xrightarrow{\sim} V_1$ und $g|_{V_2} : V_2 \xrightarrow{\sim} W$.

(3) Für die Dimensionen folgt $\dim_R(V) = \dim_R(U) + \dim_R(W)$.

Für (3) setzen wir voraus, dass R die Invarianz der Dimension erfüllt.

Zusammensetzen von Basen

$$\begin{array}{ccccccc}
 0 & \xrightarrow{0} & U & \xrightarrow{f} & V & \xrightarrow{g} & W \xrightarrow{0} 0 \\
 & & u_i & \xrightarrow{\quad} & v_i & & \text{Basis} \\
 & & \text{Basis} & & v_j & \xrightarrow{\quad} & w_j
 \end{array}$$

Beweis: (1) Wir zeigen, dass $(v_k)_{k \in K}$ eine Basis von V ist.

Lineare Unabhängigkeit: Sei $0 = \sum_{k \in K} v_k \lambda_k$ mit $\lambda \in R^{(K)}$.

Dann gilt $0 = g(\sum_{k \in K} v_k \lambda_k) = \sum_{j \in J} w_j \lambda_j$, also $\lambda|_J = 0$.

Es gilt $0 = \sum_{i \in I} v_i \lambda_i = f(\sum_{i \in I} u_i \lambda_i)$, also $\sum_{i \in I} u_i \lambda_i = 0$.

Daraus folgt $\lambda|_I = 0$, insgesamt also $\lambda = 0$.

Erzeugendensystem: Vorgelegt sei $v \in V$.

Wir haben $g(v) = w = \sum_{j \in J} w_j \lambda_j$ für ein $\lambda|_J \in R^{(J)}$.

Für $v_2 = \sum_{j \in J} v_j \lambda_j$ in V gilt ebenfalls $g(v_2) = w$ in W .

Für $v_1 = v - v_2$ folgt $g(v_1) = 0$, also $v_1 \in \ker(g) = \text{im}(f)$.

Das bedeutet $v_1 = f(u)$ mit $u = \sum_{i \in I} u_i \lambda_i$ in U und $\lambda|_I \in R^{(I)}$.

Daraus folgt $v = v_1 + v_2 = \sum_{i \in I} v_i \lambda_i + \sum_{j \in J} v_j \lambda_j = \sum_{k \in K} v_k \lambda_k$. □ QED

Die Dimensionsformel für lineare Abbildungen

😊 Ich betone noch einmal Ziel und Zweck exakter Sequenzen: Diese Technik bündelt nützliche Informationen auf effiziente Weise. Die nachstehenden Folgerungen illustrieren dies eindrücklich.

Satz J2N: die Dimensionsformel für lineare Abbildungen

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Für jede R -lineare Abbildung $f: V \rightarrow W$ gilt die Dimensionsformel:

$$\dim_R(V) = \dim_R \ker(f) + \dim_R \operatorname{im}(f)$$

Beweis: Dies folgt dank Satz J2M aus der kurzen exakten Sequenz

$$0 \xrightarrow{0} \ker(f) \xrightarrow{\iota} V \xrightarrow{\hat{f}} \operatorname{im}(f) \xrightarrow{0} 0.$$

Hierbei ist $\iota: \ker(f) \hookrightarrow V: v \mapsto v$ die Inklusion des Kerns und $\hat{f}: V \twoheadrightarrow \operatorname{im}(f): v \mapsto f(v)$ die Surjektion auf das Bild. □ QED

😊 Wir können Basen wie in Satz J2M zusammensetzen.

Die Dimensionsformel für lineare Abbildungen

😊 Für die Dimensionsformel J2N setzen wir einen Divisionsring voraus; damit sichern wir sowohl die Eindeutigkeit der Dimension (J1K) als auch die Existenz von Basen (J2B), hier angewendet auf $\ker(f)$ und $\operatorname{im}(f)$.

😊 Im vorangegangenen Satz J2M hingegen ist R ein beliebiger Ring. Die benötigten Basen von U und V werden als Eingabedaten geliefert, der Satz fügt diese dann wie gezeigt zu einer Basis von V zusammen.

😊 Auch die Dimensionsformel J2N können wir genauso formulieren: Ist $f: V \rightarrow W$ eine R -lineare Abbildung und sind $\ker(f)$ und $\operatorname{im}(f)$ frei, so ist auch V frei, und es gilt die Dimensionsformel

$$\dim_R(V) = \dim_R \ker(f) + \dim_R \operatorname{im}(f).$$

Diese Formulierung ist allgemeiner, doch leider auch etwas technisch. Ich präsentiere daher die vereinfachte Version J2N über Divisionsringen.

Beispiel: Über \mathbb{Z} ist die Sequenz $0 \rightarrow \mathbb{Z} \hookrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$ exakt, aber die Dimensionsformel lässt sich nicht anwenden.

Satz J20: die Dimensionsformel für direkte Summen

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(1) Für jede direkte Summe von R -Vektorräumen $V_1, \dots, V_n \leq W$ gilt

$$\dim_R(V_1 \oplus \dots \oplus V_n) = \dim_R(V_1) + \dots + \dim_R(V_n)$$

Genauer: Ist eine Basis $(v_i)_{i \in I_k}$ von V_k gegeben für jedes k , so erhalten wir zu $V = \bigoplus_k V_k$ die Basis $(v_i)_{i \in I}$ mit $I = \bigsqcup_k I_k$.

(2) Dank $V_1 \times \dots \times V_n \cong V_1 \oplus \dots \oplus V_n$ folgt insbesondere

$$\dim_R(V_1 \times \dots \times V_n) = \dim_R(V_1) + \dots + \dim_R(V_n).$$

Beweis: Der Fall $n = 2$ folgt dank Satz J2M aus der exakten Sequenz

$$0 \xrightarrow{0} V_1 \xrightarrow[\substack{f \\ v_1 \mapsto v_1 + 0}}{V_1 \oplus V_2} V_1 \oplus V_2 \xrightarrow[\substack{g \\ v_1 + v_2 \mapsto v_2}]{V_2} V_2 \xrightarrow{0} 0.$$

Der allgemeine Fall $n \in \mathbb{N}$ folgt daraus per Induktion. □ QED

Die Dimensionsformel für direkte Summen

Aussagen und Beweise zu Dimensionen entsprechen dem Abzählen von Basen, hier also der Mächtigkeit einer disjunkten Vereinigung:

$$\#(I_1 \sqcup I_2 \sqcup \dots \sqcup I_n) = \#I_1 + \#I_2 + \dots + \#I_n$$

Dies folgt per Induktion aus dem Fall $n = 2$ (Satz E2A):

$$\#(I_1 \sqcup I_2) = \#I_1 + \#I_2$$

Im Falle eines nicht-leeren Schnitts haben wir (Satz E2B):

$$\#(I_1 \cup I_2) = \#I_1 + \#I_2 - \#(I_1 \cap I_2)$$

Dieselbe Eigenschaft finden wir für die Dimension von Vektorräumen! Dazu müssen wir nur geeignete Basen konstruieren, etwa mit Satz J2M.

😊 Das sind zwei der guten Gründe, warum ich Abzählungen von Mengen in Kapitel E so ausführlich diskutiert, ja zelebriert habe:

- Sie bieten gutes Anschauungs- und Lernmaterial für den Einstieg.
- Sätze und Techniken übertragen sich auf Basen von Vektorräumen.

Die Dimensionsformel für beliebige Summen

Satz J2P: die Dimensionsformel für beliebige Summen

Sei R ein Divisionsring, etwa ein Körper wie $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(1) Für je zwei Unterräume $V_1, V_2 \leq W$ gilt:

$$\dim_R(V_1 + V_2) + \dim_R(V_1 \cap V_2) = \dim_R(V_1) + \dim_R(V_2)$$

(2) Sind alle Dimensionen endlich, so folgt:

$$\dim_R(V_1 + V_2) = \dim_R(V_1) + \dim_R(V_2) - \dim_R(V_1 \cap V_2)$$

Dieser allgemeine, aber einfache Zusammenhang ist bemerkenswert. Die Gleichung folgt leicht aus... der zugehörigen exakten Sequenz!

Beweis: (1) Dies folgt aus Satz J2M und der exakten Sequenz I2I:

$$0 \xrightarrow{0} V_1 \cap V_2 \xrightarrow[\substack{f \\ w \mapsto (-u, u)}]{} V_1 \times V_2 \xrightarrow[\substack{g \\ (v_1, v_2) \mapsto v_1 + v_2}]{} V_1 + V_2 \xrightarrow{0} 0$$

(2) Dies folgt aus (1) durch Umstellung in \mathbb{N} .

QED

Die Dimensionsformel für beliebige Summen

😊 Damit kennen wir die Dimension, hierzu existieren Basen:

Satz J2P: angepasste Basis zu $U = V_1 \cap V_2$ und $V = V_1 + V_2$

(3) Wir wählen zunächst eine Basis $(v_i)_{i \in I_0}$ von U , dank J2B.

Wir ergänzen $(v_i)_{i \in I_0}$ zu einer Basis $(v_i)_{i \in I_1}$ von V_1 , dank J2B.

Wir ergänzen $(v_i)_{i \in I_0}$ zu einer Basis $(v_i)_{i \in I_2}$ von V_2 , dank J2B.

Dabei vergeben wir keinen Index doppelt, also $I_1 \cap I_2 = I_0$.

Dann ist $(v_i)_{i \in I}$ mit $I = I_1 \cup I_2$ eine Basis von $V = V_1 + V_2$.

Beweis im endlichen Fall: Die Familie $(v_i)_{i \in I}$ erzeugt V .

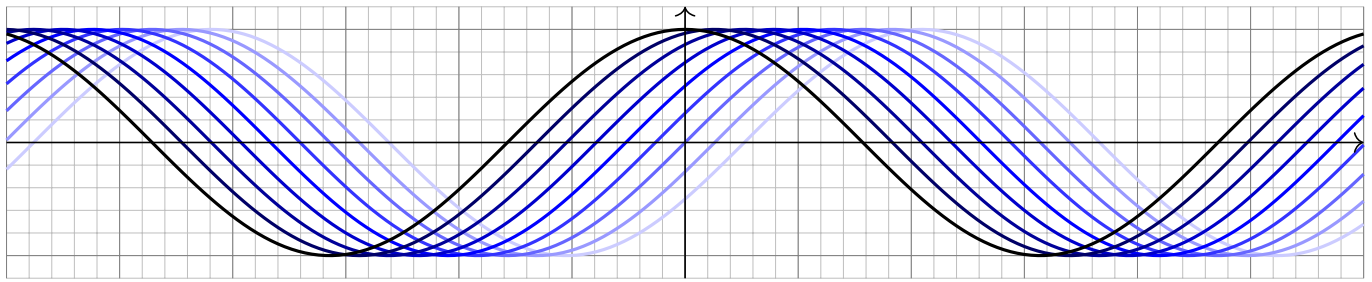
Zudem gilt $\dim_R(V) = \#I_1 + \#I_2 - \#I_0 = \#I$, dank J2P.

Also ist $(v_i)_{i \in I}$ eine Basis von V , dank J2L.

QED

Der **Zassenhaus-Algorithmus** führt die Konstruktion für $V_1, V_2 \leq R^n$ explizit aus: Eingabe sind Erzeugendensysteme von V_1 und V_2 in R^n . Ausgabe ist eine angepasste Basis von $U = V_1 \cap V_2$ und $V = V_1 + V_2$. So wird das Problem in Computer-Algebra-Systemen effizient gelöst.

📖 Literatur: Das Lernbuch von Fischer stellt dies ausführlich dar.



Über dem Körper \mathbb{R} betrachten wir den Funktionenraum $V = \text{Abb}(\mathbb{R}, \mathbb{R})$ aller reellen Abbildungen $f : \mathbb{R} \rightarrow \mathbb{R}$ und darin speziell den Unterraum

$$U := \langle f_\alpha \mid \alpha \in \mathbb{R} \rangle_{\mathbb{R}}$$

erzeugt von den Funktionen $f_\alpha : \mathbb{R} \rightarrow \mathbb{R} : t \mapsto \cos(t - \alpha)$.

Aufgabe: Welche Dimension hat dieser Vektorraum U über \mathbb{R} ?

⚠ Das angegebene Erzeugendensystem $(f_\alpha)_{\alpha \in \mathbb{R}}$ ist überabzählbar, und auch der Raum U sieht zunächst riesig aus. Doch das täuscht!

😊 Es gibt letztlich nur einen Weg, die Dimension zu bestimmen: Wir müssen eine Basis von U finden! Bitte schauen Sie genau hin.

Lösung: Die Euler-Formel $e^{it} = \cos t + i \sin t$ und die Homomorphie $e^{x+y} = e^x e^y$ führen zu den bekannten Additionstheoremen:

$$\begin{aligned} \cos(u \pm v) &= \cos u \cdot \cos v \mp \sin u \cdot \sin v \\ \sin(u \pm v) &= \sin u \cdot \cos v \pm \cos u \cdot \sin v \end{aligned}$$

Für unsere Funktionenschar $(f_\alpha)_{\alpha \in \mathbb{R}}$ bedeutet das

$$f_\alpha : \mathbb{R} \rightarrow \mathbb{R} : t \mapsto \cos(t - \alpha) = \cos t \cdot \cos \alpha + \sin t \cdot \sin \alpha.$$

Somit wird unser Raum U bereits erzeugt von $\cos = f_0$ und $\sin = f_{\pi/2}$. Diese beiden Funktionen sind linear unabhängig, denn die Auswertung

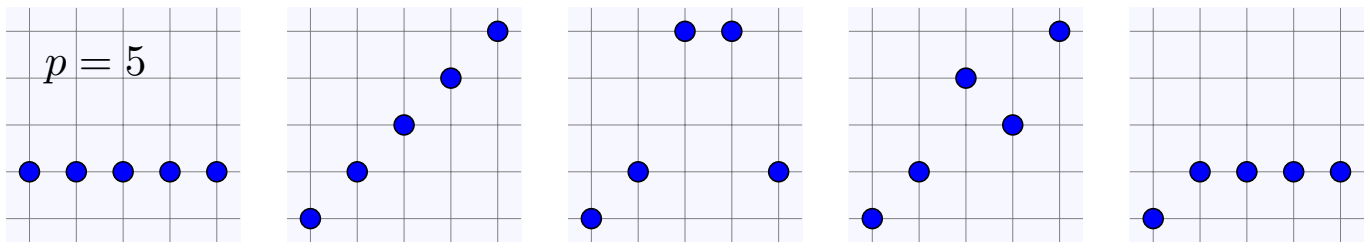
$$\Psi : U \rightarrow \mathbb{R}^2 : f \mapsto (f(0), f(\pi/2))$$

ist linear und erfüllt $\Psi(\cos) = (1, 0)$ und $\Psi(\sin) = (0, 1)$, siehe J11.

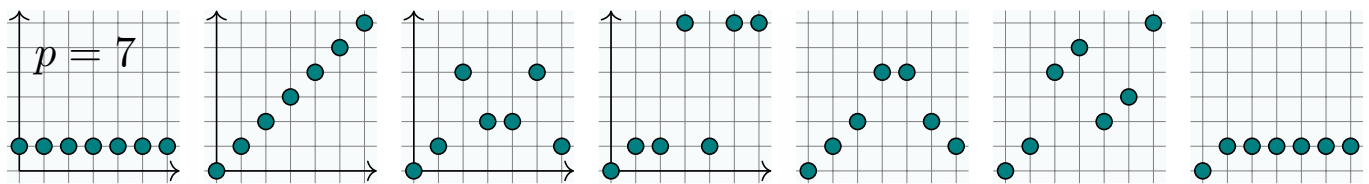
Wir erhalten damit schließlich eine sehr übersichtliche Basis:

$$U := \langle \cos, \sin \rangle_{\mathbb{R}} \quad \text{und} \quad \Psi : U \xrightarrow{\sim} \mathbb{R}^2$$

Insbesondere finden wir so die Dimension $\dim_{\mathbb{R}}(U) = 2$.



Über dem endlichen Körper \mathbb{F}_p betrachten wir den Funktionenraum $V = \text{Abb}(\mathbb{F}_p, \mathbb{F}_p)$ und darin speziell den Unterraum $U := \langle f_k \mid k \in \mathbb{N} \rangle_{\mathbb{F}_p}$ erzeugt von den Potenzfunktionen $f_k : \mathbb{F}_p \rightarrow \mathbb{F}_p : x \mapsto x^k$ für alle $k \in \mathbb{N}$.



Aufgabe: Welche Dimension haben die Vektorräume U und V über \mathbb{F}_p ?

😊 Die Funktionen f_k sehen zunächst verwirrend unstrukturiert aus. Welche algebraische Struktur steckt dahinter? Schauen Sie genau hin.

Lösung: Jedes Polynom $A = \sum_{i=0}^n a_i X^i \in \mathbb{F}_p[X]$ definiert seine zugehörige Polynomfunktion $f_A : \mathbb{F}_p \rightarrow \mathbb{F}_p : x \mapsto A(x) = \sum_{i=0}^n a_i x^i$.

Wir erhalten so den Ringhomomorphismus $\Phi : \mathbb{F}_p[X] \rightarrow \text{Abb}(\mathbb{F}_p, \mathbb{F}_p)$. Wegen $X^k \mapsto f_k$ gilt $\text{im}(\Phi) = U$. Dank G3M haben wir die Bijektion

$$\Psi : \mathbb{F}_p[X]_{<p} \xrightarrow{\sim} \text{Abb}(\mathbb{F}_p, \mathbb{F}_p) : A \mapsto f_A.$$

In Worten: Zu beliebig vorgegebenen Werten $y_0, y_1, \dots, y_{p-1} \in \mathbb{F}_p$ existiert genau ein interpolierendes Polynom $A \in \mathbb{F}_p[X]_{<p}$ mit

$$A(0) = y_0, A(1) = y_1, \dots, A(p-1) = y_{p-1}.$$

Somit schließen wir $\dim_{\mathbb{F}_p}(U) = p$ und $U = V$, genauer:

$$U = V = \langle f_0, f_1, \dots, f_{p-1} \rangle_{\mathbb{F}_p}!$$

😊 Das sieht man obigen Graphen der Funktionen f_k wohl kaum an. Die Arithmetik des Polynomrings hilft, damit erkennen wir die Struktur.

