Grundlagen der Linearen Algebra in der Informatik

Wintersemester 2024/25

Dozent: Dipl.-Ing. Tim Lindemann

4. Dezember 2024

Test :)

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Lineare Algebra - Oranisatorisches

Lineare Algebra - Oranisatorisches

Dozent: Tim Lindemann

- Email: lindemann@lehre-dhbw.stuttgart.de
- MS-Teams: Beiträge im Kanal *Mathematik* oder schreiben Sie mir im Chat.

Vorlesung:

- 60 Semesterwochenstunden, siehe Rapla.
- Zwei Online-Termine: 11.12. und 18.12. in MS-Teams

Klausur:

- Termin: 03.03.2025, 08:30-10:00.
- Dauer: 90 Minuten
- Hilfsmittel: 6 DINA Seiten mit Notizen, **kein** Taschenrechner

Lineare Algebra - Oranisatorisches

Ziele der Vorlesung:

- Mathematische Fachsprache und Symbole verstehen und nutzen
- Beweisführungen nachvollziehen und anwenden
- Entwicklung einer Lösungstheorie für lineare Gleichungssystem
- Analyse und Lösung von linearen Gleichungssystemen
- Bedeutung von Matrizen und linearen Abbildungen
- Eigenwertprobleme
- Anwendungsbeispiele in der Numerik

1. Grundlegende Notationen

1. Grundlegende Notationen

- Wir nutzen die **Definitionszeichen** $:=$ bzw. $=:$, um Ausdrücke zu definieren oder abzukürzen. Dabei steht der Doppelpunkt auf der Seite des Terms, den wir durch den Term auf der anderen Seite neu definieren wollen. Zum Beispiel wird die *Fakultät* wie folgt definiert:

$$n! := 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n.$$

- Der **Allquantor** $\forall$ („für alle“) erlaubt es, eine allumfassende Aussage wie

  „**Jede** natürliche Zahl ist höchstens so groß wie ihr Quadrat.“

  symbolisch zu notieren:

$$\forall n \in \mathbb{N}: \quad n \leq n^2.$$

1. Grundlegende Notationen

- Der **Existenzquantor** $\exists$ („es gibt ein“) erlaubt es eine Existenzaussage zu formulieren. Aussagen wie

  „**Es gibt** eine natürliche Zahl, deren Wurzel wieder eine natürliche Zahl ist.“

  können wir damit kurz schreiben:

$$\exists n \in \mathbb{N} : \sqrt{n} \in \mathbb{N}.$$

  Die Existenz ist dabei im Sinne von „Es gibt *mindestens* ein ...“ zu verstehen.
- Der **Existenzquantor** $\exists!$ („es gibt *genau* ein“) gibt zusätzlich zur Existenz auch die Eindeutigkeit der Aussage, z.B.

$$\exists! n \in \mathbb{N} : \sqrt{n} = 2.$$

1. Grundlegende Notationen

- Mathematische Aussagen sind immer entweder **wahr** oder **falsch**.
- Wir können Aussagen A und B zu einer neuen Aussage verknüpfen:

  $$A \wedge B \text{ („}A \textbf{ und } B\text{“)} \quad \text{bzw.} \quad A \vee B \text{ („}A \textbf{ oder } B\text{“)}.$$

  Ebenso können wir das Gegenteil einer Aussage A durch die **Negation** $\neg A$ formulieren.
- Eine Aussage der Form *„Aus A folgt B“* nennen wir **Implikation**. Wir sagen auch *„A impliziert B“* oder *„Wenn A gilt, dann auch B“* und schreiben:

  $$A \quad \Rightarrow \quad B.$$

- Impliziert Aussage A die Aussage B und umgekehrt, sprechen wir von **Äquivalenz**. Wir sagen *„A ist äquivalent zu B“* oder *„A gilt genau dann, wenn B gilt“* und schreiben

  $$A \quad \Leftrightarrow \quad B.$$

1. Grundlegende Notationen

- Mathematische Ausdrücke sollten **eindeutig** sein.
- Wir werden oft viele Terme ähnlicher Art addieren, etwa

$$1 + 2 + \ldots + 2^n \quad \text{oder allgemeiner} \quad a_1 + a_2 + a_3 + \ldots + a_n.$$

- Hier kann es zu Missverständnissen kommen. Ist mit $1 + 2 + \ldots + 2^3$ also

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 \quad \text{oder} \quad 1 + 2 + 4 + 8$$

  gemeint?
- Daher führen wir eine spezielle **Summennotation** ein, um das Bildungsgesetz der Summanden eindeutig notieren zu können.

1. Grundlegende Notationen

Definition: Das Summenzeichen

Um die Summe der Zahlen $a_1, a_2, \ldots, a_m, \ldots, a_n$ auszudrücken, verwenden wir die Notation

$$\sum_{k=1}^{n} a_k := a_1 + a_2 + \ldots + a_n.$$

Allgemeiner schreiben wir auch

$$\sum_{k=m}^{n} a_k := a_m + a_{m+1} + a_{m+2} + \ldots + a_n.$$

Wir nennen m den **Startindex** der Summe, k ist den **Laufindex** und n ist den **Endindex**.

1. Grundlegende Notationen

Definition: Das Summenzeichen (Fortsetzung)

Für den Fall, dass $m > n$ gilt, definieren wir die **leere Summe**

$$\sum_{k=m}^{n} a_k := 0.$$

Der Laufindex muss nicht mit k bezeichnet werden, so ist z.B.

$$\sum_{k=m}^{n} a_k = \sum_{i=m}^{n} a_i = \sum_{j=m}^{n} a_j.$$

1. Grundlegende Notationen

Proposition: Rechenregeln

Seien die Zahlen c, a_1, a_2, $\ldots$, a_n, b_1, b_2, $\ldots$, b_n gegeben.

- **Summe und Differenz zweier Summen:**

$$\sum_{k=1}^{n} a_k \pm \sum_{k=1}^{n} b_k = \sum_{k=1}^{n} (a_k \pm b_k)$$

$$(a_1 + \ldots + a_n) + (b_1 + \ldots + b_n) = (a_1 + b_1) + (a_2 + b_2) + \ldots + (a_n + b_n)$$

- **Ausmultiplizieren und Ausklammern:**

$$c \sum_{k=1}^{n} a_k = \sum_{k=1}^{n} (c \cdot a_k)$$

$$c \cdot (a_1 + \ldots + a_n) = c \cdot a_1 + \ldots + c \cdot a_n$$

1. Grundlegende Notationen

Proposition: Rechenregeln (Fortsetzung)

Seien die Zahlen $c, a_1, a_2, \ldots, a_n$ und $b_1, b_2, \ldots, b_n$ gegeben.

- **Summentrennung:**
$$\sum_{k=1}^{n} a_k = \sum_{k=1}^{l} a_k + \sum_{k=l+1}^{n} a_k$$
- **Indexverschiebung:**
$$\sum_{k=m}^{n} a_k = \sum_{k=m-l}^{n-l} a_{k+l}$$
- **Vorsicht!** Im Allgemeinen gilt
$$\sum_{k=m}^{n} (a_k \cdot b_k) \neq \left(\sum_{k=m}^{n} a_k\right) \cdot \left(\sum_{k=m}^{n} b_k\right).$$

1. Grundlegende Notationen

Beispiele: Sei n eine natürliche Zahl.

- $\sum_{k=3}^{27} k = 3 + 4 + 5 + \ldots + 27$
- In der Summe müssen keineswegs nur natürliche Zahlen stehen:

$$\left(\frac{4}{7}\right)^2 + \left(\frac{5}{7}\right)^2 + \left(\frac{6}{7}\right)^2 + \ldots + \left(\frac{n}{7}\right)^2 = \sum_{j=4}^{n} \left(\frac{j}{7}\right)^2 = \left(\frac{1}{7}\right)^2 \sum_{j=4}^{n} j^2.$$

- Sei x eine reelle Zahl. Die sogenannte *geometrische Summe* ist

$$1 + x + x^2 + x^3 + x^4 + \ldots + x^n = \sum_{k=0}^{n} x^k.$$

1. Grundlegende Notationen

- Summenvorschrift finden, Indexverschiebung:

$$
\begin{aligned}
&(4+5+6+\ldots+n)+\left(5^4+6^5+7^6+\ldots+(n+1)^n\right) \\
&= \sum_{k=4}^{n} k + \sum_{k=5}^{n+1} k^{k-1} \\
&= \sum_{k=4}^{n} k + \sum_{k=5-1}^{(n+1)-1} (k+1)^k \\
&= \sum_{k=4}^{n} \left(k+(k+1)^k\right)
\end{aligned}
$$

1. Grundlegende Notationen

- Dieselbe Problematik ergibt sich bei der **Multiplikation**

$$1 \cdot 2 \cdot \ldots \cdot 2^n \quad \text{oder allgemeiner} \quad a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n.$$

- Erneut kann der erste Ausdruck sowohl

$$1 \cdot 2 \cdot \ldots \cdot 2^n = 1 \cdot 2 \cdot 4 \cdot 8 \cdot \ldots \cdot 2^n$$

als auch

$$1 \cdot 2 \cdots 2^n = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot 2^{n-1} \cdot 2^n$$

bedeuten.

- Auch für die Multiplikation gibt es daher eine spezielle Produktschreibweise.

1. Grundlegende Notationen

Definition: Das Produktzeichen

Um das Produkt der Zahlen $a_1, a_2, \ldots, a_m, \ldots, a_n$ auszudrücken, verwenden wir die Notation

$$\prod_{k=m}^{n} a_k := a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \ldots \cdot a_{n-1} \cdot a_n.$$

Hier ist m der **Startindex** des Produkts, k ist der **Laufindex** und n ist der **Endindex**. Ist $m > n$ so definiert man das **leere Produkt** durch

$$\prod_{k=m}^{n} a_k := 1.$$

1. Grundlegende Notationen

Proposition: Rechenregeln für Produkte

Seien die Zahlen c, a_1, a_2, ..., a_n, b_1, b_2, ..., b_n gegeben. Dann gilt

- Produkt von Produkten:

$$\prod_{k=m}^{n} a_k \cdot \prod_{k=m}^{n} b_k = \prod_{k=m}^{n} (a_k \cdot b_k)$$

- Ausklammern:

$$\prod_{k=1}^{n} c \cdot a_k = c^n \cdot \prod_{k=1}^{n} a_k$$

1. Grundlegende Notationen

Proposition: Rechenregeln für Produkte (Fortsetzung)

- Quotient von Produkten:

$$\frac{\prod_{k=m}^{n} a_k}{\prod_{k=m}^{n} b_k} = \prod_{k=m}^{n} \frac{a_k}{b_k}$$

- Indexverschiebung:

$$\prod_{k=m}^{n} a_k = \prod_{k=m-l}^{n-l} a_{k+l}$$

1. Grundlegende Notationen

Beispiele: Sei n eine natürliche Zahl.

- $3 \cdot 4 \cdot 5 \cdot \ldots \cdot 27 = \prod_{k=3}^{27} k.$
- Das Produkt der natürlichen Zahlen 1 bis n ist als **Fakultät** definiert und wird mit $n!$ abgekürzt.

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = \prod_{k=1}^{n} k =: n!$$

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot 10 = \prod_{k=1}^{10} k = 10!$$

- $1 \cdot 3 \cdot 5 \cdot \ldots \cdot 13 = \prod_{k=0}^{6} (2k+1)$

2. Mengenlehre

2. Mengenlehre

Allgemeines:

- Begründer der Mengenlehre: *Georg Cantor*, dt. Mathematiker (1874-1897)
- Die meisten Objekte in den Teilgebieten *Algebra*, *Analysis*, *Geometrie*, *Stochastik* oder *Topologie* können als Mengen definiert werden.
- Die moderne Mathematik basiert daher maßgeblich auf der Mengenlehre.
- Ziel ist die Untersuchung der Struktur von Mengen und der Beziehungen zwischen Mengen.

2.1 Darstellung von Mengen

2.1 Darstellung von Mengen

Definition nach Cantor: Menge

Unter einer **Menge** M verstehen wir jede Zusammenfassung von **bestimmten**, **wohlunterschiedenen** Objekten unserer Anschauung oder unseres Denkens, welche **Elemente** von M genannt werden, zu einem Ganzen.

Anmerkung: Mengen schreiben wir meist in Großbuchstaben, deren Elemente schreiben wir in geschweifte Klammern, z.B.

$$M = \{1, \nabla, 5, \alpha, +, \pi\}.$$

2.1 Darstellung von Mengen

Anmerkungen:

- *Bestimmt* bedeutet dabei, dass ein Element x entweder zu einer Menge gehört oder nicht. Ist ein Objekt x Element der Menge M, so schreiben wir

  $$x \in M \quad (\text{gesprochen: } x \text{ ist Element von } M)$$

  ansonsten

  $$x \notin M \quad (\text{gesprochen: } x \text{ ist \textit{kein} Element von } M).$$

- *Wohlunterschieden* bedeutet dabei, dass Elemente in der Menge unterscheidbar sein müssen, d.h. jedes Element tritt nur einmal in einer Menge auf.
- Die Reihenfolge spielt bei der Notation einer Menge keine Rolle, d.h.

  $$\{1, 2, 3\} = \{2, 3, 1\}.$$

2.1 Darstellung von Mengen

- Wir definieren die **leere Menge** als die Menge, die *keine* Elemente enthält, durch das Symbol
$$\emptyset \text{ oder } \{\}.$$
- Menge in **aufzählender Darstellung:**
$$M_1 := \{a_1,\ a_2, \ldots,\ a_n\}.$$
- Menge in **beschreibende Darstellung:**
$$M_2 := \{x \in X \mid x \text{ besitzt die vorgegebenen Eigenschaften } E_1,\ E_2,\ \ldots,\ E_m\},$$
wobei hier X eine große Menge ist, aus der nur diejenigen Elemente entnommen werden, die die Eigenschaften $E_1, \ldots, E_m$ erfüllen.

2.1 Darstellung von Mengen

Beispiele:

- Die Menge der **natürlichen Zahlen** ist

$$\mathbb{N} := \{1, 2, 3, 4, 5, \ldots\}.$$

- Die Menge der **ganzen Zahlen** ist

$$\mathbb{Z} := \{\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}.$$

- Die Menge der **rationalen Zahlen** ist

$$\mathbb{Q} := \{x \mid x \text{ ist ein endlicher oder periodischer Dezimalbruch}\}.$$

- Die Menge der **reellen Zahlen** ist

$$\mathbb{R} := \{x \mid x \text{ ist ein endlicher oder unendlicher Dezimalbruch}\}.$$

Übung: Formulieren Sie $\mathbb{Q}$ in Symbolschreibweise.

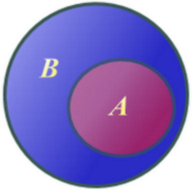
2.1 Darstellung von Mengen

Definition: Teilmenge

Eine Menge A heißt **Teilmenge** der Menge B, falls jedes Element von A auch ein Element von B ist, d.h.

$$A \subseteq B \text{ genau dann, wenn } x \in A \Rightarrow x \in B.$$

Venn-Diagramm zur Veranschaulichung:



2.1 Darstellung von Mengen

Definition: Gleichheit von Mengen

Zwei Mengen X und Y heißen **gleich**, wenn jedes Element von X auch in Y und jedes Element von Y auch in X ist, d.h.

$$X = Y \text{ genau dann, wenn } Y \subseteq X \text{ und } X \subseteq Y.$$

Eine Teilmenge Y von X heißt **echte Teilmenge**, geschrieben $Y \subset X$, wenn die Mengen ungleich sind, d.h. $Y \neq X$.

2.1 Darstellung von Mengen

Beispiele:

In der Lösungsmenge $\mathbb{L}$ einer Gleichung werden alle Elemente zusammengefasst, die die Gleichung erfüllen.

- Für $x \in \mathbb{N}$ hat $x + 1 = 0$ keine Lösung: $\mathbb{L} = \emptyset$. Wir müssen den Zahlenbereich also auf $\mathbb{Z}$ erweitern, wenn wir die Gleichung lösen möchten:

$$\mathbb{L} = \{x \in \mathbb{Z} \mid x + 1 = 0\} = \{-1\}.$$

- Für $x \in \mathbb{Z}$ hat $3x = 4$ keine Lösung: $\mathbb{L} = \emptyset$. Wir müssen den Zahlenbereich also auf $\mathbb{Q}$ erweitern, wenn wir die Gleichung lösen möchten:

$$\mathbb{L} = \{x \in \mathbb{Q} \mid 3x + 4 = 0\} = \{-\tfrac{4}{3}\}.$$

2.1 Darstellung von Mengen

- Für $x \in \mathbb{Q}$ hat $x^2 - 2 = 0$ keine Lösung: $\mathbb{L} = \emptyset$. Wir müssen den Zahlenbereich also auf $\mathbb{R}$ erweitern, wenn wir die Gleichung lösen möchten:

$$\mathbb{L} = \{x \in \mathbb{Q} \mid x^2 - 2 = 0\} = \{-\sqrt{2}, +\sqrt{2}\}.$$

- Für $x \in \mathbb{R}$ hat $x^2 + 2 = 0$ keine Lösung: $\mathbb{L} = \emptyset$. Wir müssen en Zahlenbereich wieder erweitern. Im Laufe der Vorlesung führen wir dazu die **komplexen Zahlen** $\mathbb{C}$ ein. Dabei gilt die (echte) **Inklusionskette**

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

- Die Lösungsmenge $\mathbb{L}$ der Gleichung $\sin(x) = 0$ lautet

$$\mathbb{L} := \{x \in \mathbb{R} \mid \sin(x) = 0\} = \{0, \pm\pi, \pm 2\pi, \pm 3\pi, \ldots\} = \{k\pi \mid k \in \mathbb{Z}\}.$$

2.1 Darstellung von Mengen

Definition: Endliche Intervalle

Seien $a, b \in \mathbb{R}$ mit $a < b$. Dann definieren wir ein **endliches Intervall** als Teilmenge der reellen Zahlen wie folgt:

$$\begin{aligned}
[a, b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\} \text{ (abgeschlossenes Intervall)},\\
(a, b) &= \{x \in \mathbb{R} \mid a < x < b\} \text{ (offenes Intervall)},\\
[a\ , b) &= \{x \in \mathbb{R} \mid a \leq x < b\} \text{ (nach rechts halboffenes Intervall)},\\
(a, b] &= \{x \in \mathbb{R} \mid a < x \leq b\} \text{ (nach links halboffenes Intervall)}.
\end{aligned}$$

2.1 Darstellung von Mengen

Definition: Unendliche Intervalle

Seien $a, b \in \mathbb{R}$. Dann definieren wir ein **unendliches Intervall** als Teilmenge der reellen Zahlen wie folgt:

$$\begin{aligned}
[a\,,\infty) &= \{x \in \mathbb{R} \mid a \leq x < \infty\},\\
(a,\infty) &= \{x \in \mathbb{R} \mid a < x < \infty\},\\
(-\infty, b] &= \{x \in \mathbb{R} \mid -\infty < x \leq b\},\\
(-\infty, b) &= \{x \in \mathbb{R} \mid -\infty < x < b\}.
\end{aligned}$$

Definition: Potenzmenge

Sei X eine Menge. Dann ist die **Potenzmenge** $\mathcal{P}(X)$ die Menge aller Teilmengen von X, also gilt

$$A \in \mathcal{P}(X) \quad :\Longleftrightarrow \quad A \subseteq X.$$

Beispiel: Sei $X = \{1, 5, 7\}$. Dann ist

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{5\}, \{7\}, \{1, 5\}, \{1, 7\}, \{5, 7\}, \{1, 5, 7\}\}.$$

Anmerkung: Die leere Menge und die Menge X selbst sind stets Teilmengen von X und heißen daher **triviale Teilmengen**.

2.1 Darstellung von Mengen

Definition: Mächtigkeit

Die Anzahl der Elemente in der Menge M heißt **Mächtigkeit** $|M|$.

Beispiele:

- Die *leere Menge* $\emptyset$ enthält kein Element, d.h. $|\emptyset| = 0$.
- Die Menge $A = \{1, 2, 3\}$ enthält drei Elemente, d.h. $|A| = 3$.
- Es gibt unendlich viele natürliche Zahlen, d.h. $|\mathbb{N}| = \infty$.
  Dagegen gilt aber $|\{\mathbb{N}\}| = 1$.
- Aufgrund der Inklusionskette gilt $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{R}| = |\mathbb{C}| = \infty$.
  Beachte: Streng genommen handelt es sich hier aber um verschiedene Arten von ∞: *abzählbar unendlich* und *überabzählbar unendlich* (S. Kap. 4.1).

2.2 Mengenoperationen

2.2 Mengenoperationen

Definition: Durchschnitt von Mengen

Seien A, B und X Mengen mit $A \subseteq X$ und $B \subseteq X$.

- Der **Durchschnitt von A und B**, geschrieben $A \cap B$, ist durch die Elemente, die sowohl in A als auch in B enthalten sind, gegeben:

$$A \cap B := \{x \in X \mid x \in A \quad \wedge \quad x \in B\}.$$

  Falls $A \cap B = \emptyset$, d.h., wenn sie keine gemeinsame Elemente enthalten, so heißen A und B **disjunkt**.

2.2 Mengenoperationen

Definition: Vereinigung von Mengen

Seien A, B und X Mengen mit $A \subseteq X$ und $B \subseteq X$.

- Die **Vereinigung von** A **und** B, geschrieben $A \cup B$, ist durch die Elemente, die entweder in A oder (auch) in B enthalten sind, gegeben:

$$A \cup B := \{x \in X \mid x \in A \quad \vee \quad x \in B\}\,.$$

Falls $A \cap B = \emptyset$, d.h. A und B disjunkt sind, so schreibt man für die Vereinigung auch $A \,\dot{\cup}\, B$.

2.2 Mengenoperationen

Definition: Differenzen und Komplemente von Mengen

Seien A, B und X Mengen mit $A \subseteq X$ und $B \subseteq X$.

- Die **Differenz von** A **und** B, geschrieben $A \setminus B$, ist durch die Elemente, die in A aber nicht in B enthalten sind, gegeben:

$$A \setminus B := \{x \in X \mid x \in A \ \wedge \ x \notin B\}\,.$$

- Das **Komplement von** A **in** X, geschrieben $\overline{A}$, ist durch die Elemente in X definiert, die nicht in A sind:

$$\overline{A} := X \setminus A.$$

2.2 Mengenoperationen

Definition: kartesisches Produkt

Seien A, B und X Mengen mit $A \subseteq X$ und $B \subseteq X$.

- Das **kartesische Produkt von** A **und** B, geschrieben $A \times B$, ist durch die **2-Tupel** (a, b) mit $a \in A$ und $b \in B$ gegeben:

$$A \times B = \{(a, b) \mid a \in A \quad \wedge \quad b \in B\}\,.$$

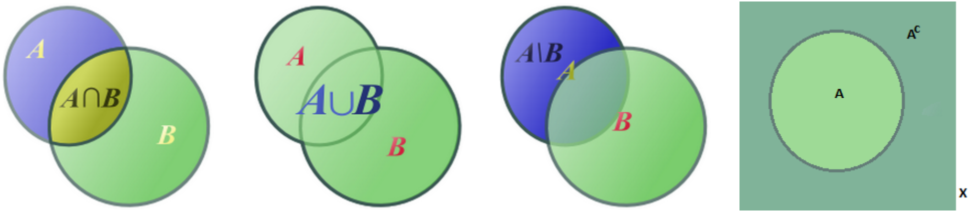
- Seien A_1, A_2, A_3, ..., A_n und X Mengen mit $A_i \subseteq X$. Das kartesische Produkt von A_1, ..., A_n ist dann definiert durch

$$A_1 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \;\; \forall\, i = 1, \ldots, n\}\,.$$

Die Elemente heißen **n-Tupel**.

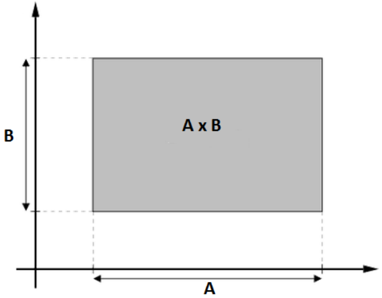
2.2 Mengenoperationen

Auch hier können die Zusammenhänge durch Venn-Diagramme veranschaulicht werden.



2.2 Mengenoperationen

Das kartesische Produkt zweier Intervalle $A := [a, b]$ und $B := [c, d]$ können wir uns in der Ebene als Rechteck veranschaulichen.



Entsprechend bildet $[a, b] \times [c, d] \times [e, f]$ die Punkte eines Quaders.

2.2 Mengenoperationen

Proposition: Rechengesetze für Mengen

Seien A, B, C und X Mengen mit $A \subseteq X$, $B \subseteq X$ und $C \subseteq X$. Dann gelten die

Kommutativgesetze

$$\begin{aligned} A \cup B &= B \cup A, \\ A \cap B &= B \cap A, \end{aligned}$$

Assoziativgesetze

$$\begin{aligned} (A \cup B) \cup C &= A \cup (B \cup C), \\ (A \cap B) \cap C &= A \cap (B \cap C). \end{aligned}$$

2.2 Mengenoperationen

Proposition: Rechengesetze für Mengen

Seien A, B, C und X Mengen mit $A \subseteq X$, $B \subseteq X$ und $C \subseteq X$. Dann gelten die

Distributivgesetze

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C). \end{aligned}$$

De Morgan-Regeln für Komplemente

$$\begin{aligned} \overline{(A \cup B)} &= \overline{A} \cap \overline{B}, \\ \overline{(A \cap B)} &= \overline{A} \cup \overline{B}. \end{aligned}$$

2.2 Mengenoperationen

Beispiel: Wir betrachten die Mengen

$$\begin{aligned} \mathbb{L}_1 &= \{x \in \mathbb{R} \mid 2x - 3 > 0\}, \\ \mathbb{L}_2 &= \{x \in \mathbb{R} \mid 2x - 4 \leq 0 \wedge x > 0\}. \end{aligned}$$

Durch einfache Termumformungen erhalten wir $\mathbb{L}_1$ in Form eines offenen Intervalls

$$2x - 3 > 0 \quad \Longleftrightarrow \quad 2x > 3 \quad \Longleftrightarrow \quad x > \frac{3}{2}, \ \text{also } \mathbb{L}_1 = \left(\frac{3}{2}, \infty\right).$$

Die Elemente x aus $\mathbb{L}_2$ liegen in einem halboffenen Intervall:

$$2x - 4 \leq 0 \quad \Longleftrightarrow \quad 2x \leq 4 \quad \Longleftrightarrow \quad x \leq 2, \ \text{also mit } x > 0 : \mathbb{L}_2 = (0, 2].$$

2.2 Mengenoperationen

Wir möchten nun die beiden Lösungsmengen miteinander verknüpfen.

- Welche $x \in \mathbb{R}$ liegen in beiden Lösungsmengen?

$$\mathbb{L}_1 \cap \mathbb{L}_2 = \left(\frac{3}{2}, \infty\right) \cap (0, 2] = \left(\frac{3}{2}, 2\right] .$$

- Welche $x \in \mathbb{R}$ liegen in einer der beiden Lösungsmengen?

$$\mathbb{L}_1 \cup \mathbb{L}_2 = \left(\frac{3}{2}, \infty\right) \cup (0, 2] = (0, \infty) .$$

- Welche $x \in \mathbb{R}$ liegen in $\mathbb{L}_1$ aber nicht in $\mathbb{L}_2$?

$$\mathbb{L}_1 \setminus \mathbb{L}_2 = \left(\frac{3}{2}, \infty\right) \setminus (0, 2] = (2, \infty) .$$

2.2 Mengenoperationen

- Die Komplemente von $\mathbb{L}_1$ und $\mathbb{L}_2$ in $\mathbb{R}$ finden wir mit Hilfe der De Morgan'schen Regeln:

$$\overline{\mathbb{L}_1} = \overline{\left\{x \in \mathbb{R} \,\middle|\, x > \tfrac{3}{2}\right\}} = \left\{x \in \mathbb{R} \mid x \leq \tfrac{3}{2}\right\} = \left(-\infty, \tfrac{3}{2}\right]$$

$$\overline{\mathbb{L}_2} = \overline{\{x \in \mathbb{R} \mid x \leq 2 \wedge x > 0\}} = \overline{((-\infty, 2] \cap (0, \infty))} = (-\infty, 0] \cup (2, \infty)$$

- Das kartesische Produkt von $\mathbb{L}_1$ und $\mathbb{L}_2$ ist gegeben durch

$$\mathbb{L}_1 \times \mathbb{L}_2 = \left\{(x, y) \mid x > \tfrac{3}{2} \;\wedge\; 0 < y \leq 2\right\}.$$

Es handelt sich also um einen nach rechts offenen Halbstreifen in der Ebene.

2.2 Mengenoperationen

Proposition: Mächtigkeiten von verknüpften Mengen

Seien A, B und X endliche Mengen mit $A \subseteq X$ und $B \subseteq X$. Dann gilt

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B|, \\ |\overline{A}| &= |X| - |A|, \\ |A \times B| &= |A| \cdot |B|. \end{aligned}$$

2.3 Binäre Relationen

2.3 Binäre Relationen

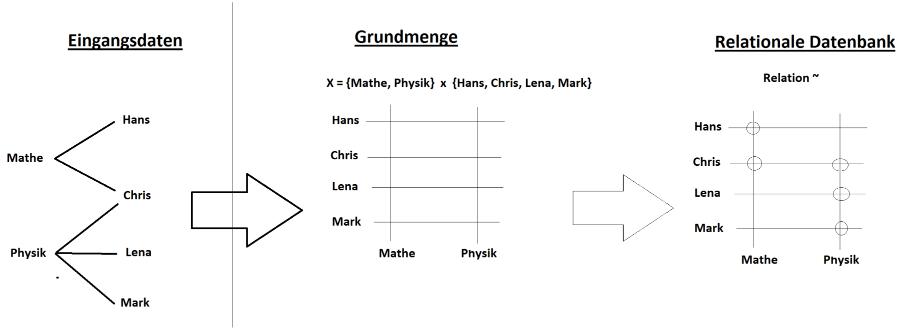
Definition: Binäre Relation

Seien X, Y gegebene Mengen.

- Eine (binäre) **Relation** ist eine Teilmenge $\sim$ von $X \times Y$. Gilt $(x, y) \in \sim$, so sagen wir "x steht in Relation zu y" und schreiben $x \sim y$.
- Sei $\sim$ eine Relation in $X \times X$. Diese Relation heißt
  - **reflexiv**, falls $(x, x) \in \sim$, also $x \sim x$ für alle $x \in X$,
  - **symmetrisch**, falls aus $(x, y) \in \sim$ auch $(y, x) \in \sim$ folgt $(x \sim y \Rightarrow y \sim x)$,
  - **transitiv**, falls mit $(x, y), (y, z) \in \sim$ auch $(x, z) \in \sim$ ist $(x \sim y \wedge y \sim z \Rightarrow x \sim z)$.
- Eine reflexive, symmetrische und transitive Relation heißt **Äquivalenzrelation**.

2.3 Binäre Relationen

Beispiel: Relationale Datenbanken. Hier stehen beispielsweise eine Tabelle mit Vorlesungen und eine Tabelle von Studierenden in Beziehung zueinander.



2.3 Binäre Relationen

Beispiele:

- Sei $X = \{a, b, c\}$ eine Menge von Menschen. Auf dieser Menge definieren wir, dass zwei Menschen x und y miteinander in Relation stehen, wenn sie befreundet sind, d.h.

  $$x \sim y \iff \text{Mensch x ist befreundet mit y.}$$

  Diese Relation muss weder symmetrisch, noch transitiv sein, ist also keine Äquivalenzrelation.

- Sei X die Menge aller Bewohner von Deutschland. Wir definieren die Äquivalenzrelation

  $$x \sim y \iff \text{Mensch } x \text{ und } y \text{ haben den Erstwohnsitz in derselben Kommune.}$$

2.3 Binäre Relationen

Aufgaben:

Untersuchen Sie die folgenden Relationen auf Reflexivität, Symmetrie und Transitivität:

- Sei $X = \mathbb{R}$ die Menge der reellen Zahlen und $\sim$ die Relation
$$x \sim y \iff x = y.$$
- Sei $X = \mathbb{R}$ die Menge der reellen Zahlen und $\sim$ die Relation
$$x \sim y \iff x \leq y.$$
- Sei $X = \mathbb{R}$ die Menge der reellen Zahlen und $\sim$ die Relation
$$x \sim y \iff x \geq y.$$

Definition: Äquivalenzklasse

Sei $\sim$ eine Äquivalenzrelation auf einer Menge X. Für $x \in X$ definieren wir die Menge

$$A(x) := \{y \in X \mid y \sim x\}.$$

Die Menge $A(x)$ heißt **Äquivalenzklasse** von x. Das Element x selbst heißt hierbei der **Repräsentant** der Äquivalenzklasse.

Beispiel: Sei $\sim$ die Relation auf $\mathbb{Z}$ gegeben durch

$$x \sim y \Leftrightarrow \text{„}x \text{ und } y \text{ haben denselben Rest bei Division durch 2“}.$$

- $\mathbb{Z}$ wird disjunkt in die beiden Äquivalenzklassen der geraden Zahlen $2\mathbb{Z}$ bzw. ungeraden Zahlen $2\mathbb{Z} + 1$.
- Dabei ist z.B. 14 ein Repräsentant von $2\mathbb{Z}$ und -113 ein Repräsentant von $2\mathbb{Z} + 1$.

Proposition: Disjunkte Äquivalenzklasse

Sei $\sim$ eine Äquivalenzrelation auf einer Menge X und $x, y \in X$. Dann gilt

- Äquivalente Elemente haben dieselbe Äquivalenzklasse:
$$x \sim y \quad \Rightarrow \quad A(x) = A(y),$$
- Äquivalenzklassen sind gleich oder disjunkt:
$$A(x) = A(y) \quad \text{oder} \quad A(x) \cap A(y) = \emptyset.$$

Anmerkung: Insbesondere liegt jedes Element in genau einer Äquivalenzklasse und durch die Äquivalenzrelation wird die Menge *partitioniert*.

2.3 Binäre Relationen

Beispiel: Auf $\mathbb{Z}$ definieren wir die Äquivalenzrelation $\mathbb{Z}_3 \subset \mathbb{Z} \times \mathbb{Z}$ durch

$$\mathbb{Z}_3 := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \exists\, k \in \mathbb{Z} : \quad x - y = 3k\},$$

d.h. zwei ganze Zahlen stehen in Relation zueinander, wenn sie sich um ein Vielfaches von 3 unterscheiden. Dadurch wird $\mathbb{Z}$ in drei Äquivalenzklassen aufgeteilt.

$$\begin{array}{ccccccccc} \ldots & -6 & -3 & 0 & 3 & 6 & 9 & 12 & \ldots \\ \ldots & -5 & -2 & 1 & 4 & 7 & 10 & 13 & \ldots \\ \ldots & -4 & -1 & 2 & 5 & 8 & 11 & 14 & \ldots \end{array}$$

Diese besonderen Äquivalenzklassen heißen auch **Restklassen**, da ihre Repräsentanten gleichen Rest bei Division (in diesem Fall) durch 3 haben. Hier verwenden wir auch die sogenannte “Modulo-Schreibweise”:

$$x \equiv y \pmod 3 \quad \Longleftrightarrow \quad x \sim y\,.$$

2.4 Abbildungen

2.4 Abbildungen: Definition

Definition: Abbildung

Seien A und B nicht-leere Mengen.

- Eine **Abbildung/Funktion** f von A nach B ist eine Vorschrift

$$f : A \to B, \quad a \mapsto b = f(a),$$

  die jedem $a \in A$ **genau** ein Element aus B zuordnet.
- Hierbei heißt $b = f(a)$ der **Funktionswert** oder das **Bild** von a unter f.
- Den Eingabewert a nennen wir das **Urbild** von b unter f.
- Die Menge A nennen wir **Definitionsbereich**, B den **Zielbereich** von f.
- Das **Bild** von f ist $\mathrm{Bild}(f) := \{b \in B \mid \exists\, a \in A : \; f(a) = b\} \subseteq B$.

2.4 Abbildungen: Eigenschaften

Definition: Injektivität, Surjektivität, Bijektivität

Eine Abbildung f von einer Menge A nach B heißt

- **injektiv**, falls für $x_1, x_2 \in A$ gilt: $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$,
- **surjektiv**, falls es für jedes $b \in B$ ein $a \in A$ gibt mit $f(a) = b$, d.h. $\mathrm{Bild}(f) = B$
- **bijektiv**, falls f injektiv und surjektiv ist.

2.4 Abbildungen

Beispiele: Die folgenden Abbildungen sind alle unterschiedlich:

$$\begin{aligned} f_1 &: \mathbb{Z} \to \mathbb{N}_0, & x &\mapsto f_1(x) := x^2 \\ f_2 &: \mathbb{Z} \to \mathbb{Z}, & x &\mapsto f_2(x) := x^2 \\ f_3 &: \mathbb{R} \to \mathbb{R}_{\geq 0}, & x &\mapsto f_3(x) := x^2 \end{aligned}$$

- Keine dieser Abbildungen ist injektiv, denn $f_i(2) = f_i(-2) = 4$ für $i = 1, 2, 3$.
- f_1 und f_2 sind nicht surjektiv, denn z.B. $3 \notin \text{Bild}(f_{1,2})$.
- Hingegen ist f_3 surjektiv.

2.4 Abbildungen

Beispiele: Wir betrachten

$$f_1 : \{1,2,3\} \to \{1,4,9\}, \quad \begin{cases} 1 \mapsto f_1(1) := 1 \\ 2 \mapsto f_1(2) := 4 \\ 3 \mapsto f_1(3) := 9 \end{cases}$$

$$f_2 : \{1,2,3\} \to \{1,4,5,9\}, \quad \begin{cases} 1 \mapsto f_2(1) := 1 \\ 1 \mapsto f_2(1) := 4 \\ 2 \mapsto f_2(2) := 5 \\ 3 \mapsto f_2(3) := 9 \end{cases}$$

- f_1 ist bijektiv.
- f_2 ist keine Abbildung, denn das Urbild 1 hat mehrere Bilder.

2.4 Abbildungen: Komposition

Definition: Komposition von Abbildungen

Seien $f\colon A \to B$ und $g\colon B \to C$ Abbildungen. Die **Komposition** (oder Verkettung) von f mit g, geschrieben $g \circ f$ („g nach f“), ist die Abbildung definiert durch

$$g \circ f : A \to C, \quad a \mapsto (g \circ f)(a) := g(f(a)).$$

Anmerkungen:

- Hierbei ist es entscheidend, dass f in den Definitionsbereich von g abbildet, d.h. $f \circ g$ macht im Allgemeinen keinen Sinn ($g(B) \subseteq C$ und f ist nicht auf C sondern auf A definiert).
- Mit dieser Definition können wir nun bijektive Abbildungen *umkehren*.

2.4 Abbildungen: Umkehrabbildung

Definition: Umkehrabbildung

Sei $f\colon X \to Y$ eine bijektive Abbildung. Dann gibt es genau eine Abbildung von Y nach X, genannt **Umkehrabbildung** (oder **Inverse**) von f und bezeichnet mit f^{-1}, sodass

$$\begin{aligned} \left(f^{-1} \circ f\right)(x) &= x \quad \text{für alle } x \in X, \\ \left(f \circ f^{-1}\right)(y) &= y \quad \text{für alle } y \in Y, \end{aligned}$$

Anmerkung: Das heißt jede bijektive Funktion ist umkehrbar!

2.4 Abbildungen: Umkehrabbildung

Proposition: Eigenschaften der Umkehrabbildung

Seien $f\colon X \to Y$ und $g\colon Y \to Z$ bijektive Abbildungen. Dann gilt

- $\left(f^{-1}\right)^{-1}(x) = f(x)$ für alle $x \in X$,
- $(g \circ f) : X \to Z$ ist auch bijektiv und es gilt für alle $z \in Z$

$$(g \circ f)^{-1} : Z \to X, \;\; z \mapsto (g \circ f)^{-1}(z) = f^{-1}(g^{-1}(z)).$$

2.4 Abbildungen

Beispiele:

- Wir betrachten die bijektiven Funktionen

$$\begin{aligned} f &: \mathbb{R} \to \mathbb{R}, & x &\mapsto f(x) := 4x - 3, \\ g &: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, & x &\mapsto g(x) := \sqrt{x}, \\ h &: \mathbb{R} \to \mathbb{R}, & x &\mapsto h(x) := \tfrac{1}{4}x + \tfrac{3}{4}. \end{aligned}$$

  Dann ist

$$f \circ g : \mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto 4\sqrt{x} - 3,$$

  aber $g \circ f$ macht keinen Sinn, denn g kann nicht auf $f(0) = -3$ angewendet werden. Weiter gilt für alle $x \in \mathbb{R}$

$$(f \circ h)(x) = 4\left(\frac{1}{4}x + \frac{3}{4}\right) - 3 = x \quad \text{und} \quad (h \circ f)(x) = \frac{1}{4}(4x - 3) + \frac{3}{4} = x,$$

  das heißt f und h sind invers zueinander: $h = f^{-1}$.

2.4 Abbildungen

- Betrachte die Funktion
$$f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \;\; x \mapsto x^2.$$
Dann ist f bijektiv und deshalb umkehrbar. Die Umkehrfunktion ist die Wurzelfunktion
$$f^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \;\; x \mapsto \sqrt{x}.$$
- Betrachte die Funktion
$$g : \mathbb{R}_{\leq 0} \to \mathbb{R}_{\geq 0}, \;\; x \mapsto x^2.$$
Dann ist g bijektiv und deshalb umkehrbar. Die Umkehrfunktion ist die negative Wurzelfunktion
$$g^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\leq 0}, \;\; x \mapsto -\sqrt{x}.$$
Hier sieht man, dass Definitions- und Zielbereich von g und g^{-1} jeweils vertauscht sind.

- Der Viertelkreis im 1. Quadranten ist gegeben durch

$$f : [0,1] \to [0,1], \ \ x \mapsto \sqrt{1-x^2}.$$

Dann ist f bijektiv und die Inverse ist die Funktion f selbst.

- Betrachte die Mengen $X := \{1, 2, 3, \ldots, 26\}$ und $Y := \{a, b, c, \ldots, z\}$ und die Abbildung

$$f : X \to Y, \ \ n \mapsto f(n) := \text{n-ter Buchstabe des Alphabets.}$$

Dann ist f bijektiv und die Umkehrabbildung ist

$$f^{-1} : Y \to X,$$
$$\text{n-ter Buchstabe des Alphabets} \mapsto f^{-1}(\text{n-ter Buchstabe des Alphabets}) = n.$$

3. Beweistechniken

3. Beweistechniken

Mathematische Sätze bestehen aus drei Teilen:

- den Voraussetzungen,
- der Behauptung und
- dem Beweis.

Wir stellen drei Beweismethoden vor:

- Dirkter Beweis,
- Indirekter Beweis,
- Beweis durch vollständige Induktion.

Das **Ende des Beweises** wird in der Regel gekennzeichnet durch das Symbol $\Box$ oder die Abkürzung *QED* („quod erat demonstrandum“, lat. für „was zu beweisen war“).

3.1 Direkter Beweis

3.1 Beweistechniken: Direkter Beweis

Beim **direkten Beweis** kann aus der Voraussetzung V die Behauptung B direkt bewiesen werden.

Beispiel:

Voraussetzung V:	n ist eine ungerade Zahl
Behauptung B:	n^2 ist ungerade

Beweis:

- Da n ungerade ist, gibt es eine natürliche Zahl k, so $n = 2k - 1$.
- Daher gilt: $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1$.
- Da $2(2k^2 - 2k)$ eine gerade Zahl ist, folgt, dass n^2 ungerade ist. $\square$

3.2 Indirekter Beweis

3.2 Beweistechniken: Indirekter Beweis

- Beim **indirekten Beweis** oder **Beweis durch Widerspruch** nehmen wir an, dass die Behauptung B falsch ist.
- Man kann jetzt entweder einen Widerspruch zur Voraussetzung V herleiten oder mittels V einen Widerspruch zu einer bekannten wahren Aussage herleiten.
- Ist dies geschafft, so kann B nicht falsch gewesen sein und die Richtigkeit der Behauptung B folgt.

Beispiel 1:

Voraussetzung V: n ist eine ungerade Zahl

Behauptung B: n^2 ist ungerade

Beweis durch Widerspruch:

- Angenommen n^2 ist gerade, d.h. $\exists k \in \mathbb{Z} : n^2 = 2k$.
- Daher kommt 2 in der Primfaktorzerlegung von n^2 und damit auch in der von n vor.
- Damit wäre n gerade, was im Widerspruch zur Voraussetzung V steht, d.h. n^2 muss ungerade sein. $\square$

3.2 Beweistechniken: Indirekter Beweis

Beispiel 2:

Wir zeigen durch einen Widerspruch, dass $\sqrt{2}$ irrational ist, d.h. $\sqrt{2} \notin \mathbb{Q}$.

- Wir nehmen dazu an, dass $\sqrt{2} \in \mathbb{Q}$ ist.
- Das heißt es müsste $p, q \in \mathbb{Z}$ geben, sodass $\sqrt{2} = \frac{p}{q}$.
- Zusätzlich gehen wir davon aus, dass der Bruch $\frac{p}{q}$ vollständig gekürzt ist (p und q heißen dann **teilerfremd**).
- Unter diesen Annahmen gilt, dass

$$\sqrt{2} = \frac{p}{q} \text{ bzw. } p^2 = 2q^2.$$

- Das heißt die Zahl p^2 ist gerade. Dann muss aber auch p gerade sein. (Wir haben ja in 3.1 gezeigt, dass Quadrate ungerader Zahlen wieder ungerade sind.)

3.2 Beweistechniken: Indirekter Beweis

- Dann lässt sich p in der Form $p = 2r$ mit $r \in \mathbb{Z}$ schreiben und es folgt $p^2 = 4r^2$.
- Wegen
$$p^2 = 2q^2 \quad \Rightarrow \quad 4r^2 = 2q^2 \quad \Rightarrow \quad q^2 = 2r^2$$
muss q^2 also ebenfalls eine gerade Zahl sein, d.h. $\exists s \in \mathbb{Z} : q = 2s$.
- Dies ist ein Widerspruch zur Teilerfremdheit von p und q. Damit muss $\sqrt{2}$ irrational sein. $\square$

3.3 Beweis durch vollständige Induktion

3.3 Beweistechniken: Vollständige Induktion

Vorüberlegung:

- Das Axiomensystem von *Peano* für die natürlichen Zahlen enthält das wichtige Induktionsaxiom:

  Enthält eine Teilmenge $A \subseteq \mathbb{N}$ die Zahl 1 und mit jedem k auch $k+1$, dann ist $A = \mathbb{N}$.

  Das Induktionsaxiom besagt, dass man so *alle* natürlichen Zahlen erhält.
- Will man nun zeigen, dass eine Aussage $A(n)$ für alle natürlichen Zahlen richtig ist, muss man beweisen, dass diese Aussage für den Startwert 1 richtig ist und dass sie, falls sie für k richtig ist, auch für $k+1$ richtig ist.

Beweis durch vollständige Induktion

Möchten wir eine Aussage $A(n)$ mittels vollständiger Induktion beweisen, so gehen wir wie folgt vor:

1. **Induktionsstart:**
   Prüfe, ob die Aussage für einen Startwert n_0 gilt.
2. **Induktionsschritt:**
   Nehme an, dass die Aussage für ein bestimmtes k gilt. Zeige damit, dass sie auch für $k + 1$ gilt.
3. **Induktionsschluss:**
   Sind 1. und 2. erfüllt, dann gilt die Aussage $A(n)$ für jede natürliche Zahl $n \in \mathbb{N}$ mit $n \geq n_0$.

3.3 Beweistechniken: Vollständige Induktion

Beispiel 1:
Wir beweisen, dass für alle natürlichen Zahlen $n \in \mathbb{N}$ die Summe der natürlichen Zahlen von 1 bis n gleich $\frac{n(n+1)}{2}$ ist.

1. **Induktionsstart**: Wir prüfen, ob die Aussage für den Startwert $n_0 = 1$ gilt.

$$1 = \frac{1(1+1)}{2}$$

   ist offensichtlich richtig. Die Aussage ist wahr für $n = 1$.

2. **Induktionsschritt**: Wir nehmen an, dass die Aussage für ein bestimmtes k gilt, d.h. die die **Induktionsannahem** (IA) lautet

$$1 + 2 + \ldots + k = \frac{k(k+1)}{2}.$$

3.3 Beweistechniken: Vollständige Induktion

Mit Hilfe dieser Annahme zeigen wir, dass die Aussage auch für $k+1$ gilt:

$$\begin{aligned}\underbrace{1+2+\ldots+k}_{IA}+(k+1) &= \underbrace{\frac{k(k+1)}{2}}_{IA}+(k+1)\\ &= \frac{k(k+1)+2(k+1)}{2}\\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

3. **Induktionsschluss:**
   Da die Aussage für 1 gilt und - falls sie für k gilt - auch für $k+1$ gilt, ist obige Aussage für alle natürlichen Zahlen gültig. $\square$

3.3 Beweistechniken: Vollständige Induktion

Aufgaben:

1. Zeigen Sie, dass für alle natürliche Zahlen n gilt, dasss
$$\sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1).$$
2. Zeigen Sie, dass für alle natürliche Zahlen $n > 2$ gilt, dass $n^2 > 2n + 1$.

3.3 Beweistechniken: Vollständige Induktion

Beispiel 2: Wir beweisen die Aussage $\forall n \geq 5$ gilt $2^n > n^2$.

1. **Induktionsstart:** Wir prüfen, ob die Aussage für den Startwert $n_0 = 5$ gilt:

$$32 = 2^5 > 5^2 = 25,$$

   d.h. die Aussage ist wahr für $n = 5$.

2. **Induktionsschritt:** Wir nehmen an, dass die Aussage für ein bestimmtes k gilt (IA). Damit gilt für $k+1$:

$$2^{k+1} = 2 \cdot \underbrace{2^k}_{IA} > 2 \cdot \underbrace{k^2}_{IA} = k^2 + k^2 > k^2 + 2k + 1 = (k+1)^2, \quad \text{also} \quad 2^{k+1} > (k+1)^2.$$

3. **Induktionsschluss:**
   Da die Aussage für 5 und ein $k \geq 5$ gilt, gilt sie auch für $k+1$. $\square$

4. Grundlagen der diskreten Mathematik

4 Diskrete Mathematik

Die **diskrete Mathematik** ist ein Teilgebiet der Mathematik, das sich mit mathematischen Operationen auf *endlichen* und *abzählbar unendlichen* Mengen beschäftigt. Zu ihr zählen u.a. die folgenden Zweige:

- **Kombinatorik** (im vierten Semester),
- **Zahlentheorie** (s. 4.2),
- **Kryptographie** (s. 4.3) und Kodierungstheorie,
- Graphen- und Spieltheorie.

4.1 Verschiedene Unendlichkeiten

4.1 Diskrete Mathematik: Unendlichkeiten

Definition: Endliche, abzählbare und überabzählbare Mengen

- Zwei Mengen A und B heißen **gleichmächtig**, wenn jedem Element der einen Menge genau ein Element der anderen Menge zugeordnet werden kann und umgekehrt ebenso. Das heißt es existiert eine bijektive Abbildung zwischen A und B.
- Sei M eine Menge. Dann nennen wir M
  - eine **endliche Menge**, falls $|M| < \infty$,
  - eine **abzählbare Menge**, falls es eine Bijektion zwischen M und $\mathbb{N}$ gibt,
  - eine **überabzählbare Menge**, falls es keine Bijektion zwischen M und $\mathbb{N}$ gibt.

4.1 Diskrete Mathematik: Unendlichkeiten

Anmerkungen:

- Wir unterscheiden also verschiedene Arten von Unendlichkeit: *abzählbar unendlich* und *überabzählbar unendlich*.
- $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ sind abzählbare Mengen.
- *Abzählbar* bedeutet im Prinzip, dass die Elemente der Menge M sinnvoll durchnummeriert und dann wie die natürlichen Zahlen abgezählt werden können. Das heißt wir finden eine Bijektion zwischen M und $\mathbb{N}$.
- Dagegen sind $\mathbb{R}$ und $\mathbb{C}$ überabzählbare Mengen. Es gibt also keine sinnvolle Art *alle* reelle Zahlen zu zählen.

4.1 Diskrete Mathematik: Unendlichkeiten

Diskussion: Cantors erstes Diagonalargument

Cantors erstes Diagonalargument ist ein mathematisches Beweisverfahren, mit dem man gegebenenfalls zeigen kann, dass zwei unendliche Mengen gleichmächtig sind bzw. eine Menge M die gleiche Mächtigkeit wie die natürlichen Zahlen besitzt.

- Idee: Finde eine Bijektion zwischen $\mathbb{N}$ und M.
- Vorgehen: Ordne die Elemente von M in einem günstigen, zweidimensionalen Schema an und durchlaufen das Schema diagonal.

4.1 Diskrete Mathematik: Unendlichkeiten

Beispiel: Wir zeigen, dass die positiven rationalen Zahlen $\mathbb{Q}^+$ und die natürlichen Zahlen $\mathbb{N}$ gleichmächtig (also abzählbar unendlich) sind.

- Wir ordnen die positiven Dezimalbrüche zeilenweise nach aufsteigenden Zählern und spaltenweise nach aufsteigenden Nennern:

$$
\begin{array}{cccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots \\[1em]
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \cdots \\[1em]
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \cdots \\[1em]
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \cdots \\[1em]
\frac{5}{1} & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & \cdots \\[1em]
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

4.1 Diskrete Mathematik: Unendlichkeiten

- Nun nummerieren wir die Brüche entlang der Diagonalen durch, wobei wir nicht vollständig gekürzte Brüche überspringen:

$$
\begin{array}{ccccccccccc}
q_1 = \frac{1}{1} & \rightarrow & q_2 = \frac{1}{2} & & q_5 = \frac{1}{3} & \rightarrow & q_6 = \frac{1}{4} & & q_{11} = \frac{1}{5} & \rightarrow & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & & \\
q_3 = \frac{2}{1} & & q_x = \frac{2}{2} & & q_7 = \frac{2}{3} & & q_x = \frac{2}{4} & & \frac{2}{5} & & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & & & & \\
q_4 = \frac{3}{1} & & q_8 = \frac{3}{2} & & q_x = \frac{3}{3} & & \frac{3}{4} & & \frac{3}{5} & & \cdots \\
 & \swarrow & & \nearrow & & & & & & & \\
q_9 = \frac{4}{1} & & q_x = \frac{4}{2} & & \frac{4}{3} & & \frac{4}{4} & & \frac{4}{5} & & \cdots \\
\downarrow & \nearrow & & & & & & & & & \\
q_{10} = \frac{5}{1} & & \frac{5}{2} & & \frac{5}{3} & & \frac{5}{4} & & \frac{5}{5} & & \cdots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \ddots
\end{array}
$$

- Wir erhalten somit die Bijektion $\mathbb{N} = \{1, 2, 3, 4, \ldots\} \to \mathbb{Q}^+ = \{q_1, q_2, q_3, q_4, \ldots\}$:

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 1 & \frac{1}{2} & 2 & 3 & \frac{1}{3} & \frac{1}{4} & \frac{2}{3} & \frac{3}{2} & 4 & 5 & \ldots \end{array}$$

- Wir haben also eine Bijektion gefunden und damit gezeigt, dass $\mathbb{Q}^+$ und $\mathbb{N}$ abzählbar unendlich sind. $\square$

4.1 Diskrete Mathematik: Unendlichkeiten

Aufgaben:

1. Zeigen Sie, dass $\mathbb{Q}$ eine abzählbare Menge ist.

2. Zeigen Sie, dass $\mathbb{Z}$ und $\mathbb{N}$ gleichmächtig sind.

Diskussion: Cantors zweites Diagonalargument

Cantors zweites Diagonalargument ist ein mathematisches Beweisverfahren, das zeigt, dass die Menge der reellen Zahlen $\mathbb{R}$ überabzählbar ist.

- **Idee:** Zeige, dass es keine Bijektion zwischen $\mathbb{N}$ und $\mathbb{R}$ gibt.
- **Vorgehen:** Definiere eine beliebige Folge reeller Zahlen $z_1, z_2, z_3, \ldots$ im offenen Intervall $(0, 1)$ und zeige, dass es in diesem Intervall mindestens eine reelle Zahl gibt, die nicht in der Folge der z_i vorkommt.
- **Schlussfolgerung:** Es kann keine Folge geben, die alle reellen Zahlen in $(0, 1)$ enthält, d.h. die reellen Zahlen sind nicht abzählbar.

4.1 Diskrete Mathematik: Unendlichkeiten

- Wir schreiben die reellen Zahlen z_i der Folge in der Dezimalbruchentwicklung

$$
\begin{aligned}
z_1 &= 0.\, a_{11}\, a_{12} a_{13} a_{14} a_{15} \dots \\
z_2 &= 0. a_{21}\, a_{22}\, a_{23} a_{24} a_{25} \dots \\
z_3 &= 0. a_{31} a_{32}\, a_{33}\, a_{34} a_{35} \dots \\
z_4 &= 0. a_{41} a_{42} a_{43}\, a_{44}\, a_{45} \dots \\
&\vdots
\end{aligned}
$$

  wobei a_{ij} die j-te Stelle Dezimalstelle der i-ten Zahl in der Folge ist.
- Nun konstruieren wir eine Zahl z^*, die nicht in der Folge vorkommt, indem wir die Dezimalstellen z_i^* von z^* wie folgt wählen:

$$a_{ii} = 5 \quad \Rightarrow \quad z_i^* := 4, \quad \text{bzw.} \quad a_{ii} \neq 5 \quad \Rightarrow \quad z_i^* := 5.$$

4.1 Diskrete Mathematik: Unendlichkeiten

- Somit erhalten wir eine reelle Zahl $z^* \in (0,1)$, die sich von z_1 an der ersten Dezimalstelle, von z_2 an der zweiten Dezimalstelle, usw., unterscheidet.
- Damit liegt z^* nicht in der Folge $(z_1, z_2, z_3, \ldots)$, d.h. die reellen Zahlen in $(0,1)$ sind nicht abzählbar sondern überabzählbar.
- Da $(0,1) \subset \mathbb{R}$, muss auch $\mathbb{R}$ überabzählbar sein. $\square$

4.2 Grundlagen der Zahlentheorie: Teilbarkeitslehre

4.2 Diskrete Mathematik: Zahlentheorie, Teilbarkeitslehre

In dieser Sektion studieren wir die Struktur von $\mathbb{Z}$ und insbesondere die wichtigste Beziehung, die ganze Zahlen miteinander haben können: die Teilbarkeitsbeziehung.

Definition: Teilbarkeit

Seien a, $b \in \mathbb{Z}$ gegeben.

- Die Zahl a **teilt** b genau dann, wenn es ein $q \in \mathbb{Z}$ gibt, sodass $b = q \cdot a$. Wir schreiben dann $a|b$. Andere Sprechweisen sind „a ist ein **Teiler** von b" oder „b ist ein **Vielfaches** von a".
- Die Menge aller Teiler einer Zahl b nennen wir die **Teilermenge** T_b.

Beispiele

- Es gilt etwa $3|6$, denn $\underbrace{6}_{=b} = \underbrace{2}_{=q} \cdot \underbrace{3}_{=a}$ oder $-2|6$, denn $6 = (-3) \cdot (-2)$.
- Die Teilermenge von 6 ist $T_6 = \{\pm 1, \pm 2, \pm 3 \pm 6\}$.
- Wegen $0 = 0 \cdot a \ \forall \ a \in \mathbb{Z}$ ist 0 durch alle Zahlen teilbar. Andererseits teilt 0 keine andere Zahl in $\mathbb{Z}$, denn $b = q \cdot 0$ ist für $b \neq 0$ nicht lösbar.
- Für $b \in \mathbb{Z}$ heißen die Zahlen ± 1 und $\pm b$ **triviale Teiler**. Die Menge der **Primzahlen** ist dann definiert als

$$\mathbb{P} := \{p \in \mathbb{Z} \mid p \geq 2 \ \wedge \ \text{p hat nur die trivialen Teiler}\}\,.$$

Die Teilermenge einer Primzahl p ist also $T_p = \{\pm 1, \pm p\}$.

Proposition: Teilbarkeitsregeln

Seien $a, b, c \in \mathbb{Z}$.

- Wenn a Teiler von b ist, dann auch von bc:
$$a|b \quad \Rightarrow \quad a|bc.$$
- Wenn a Teiler von b ist und b Teiler von c, dann ist auch a ein Teiler von c:
$$a|b \;\wedge\; b|c \quad \Rightarrow \quad a|c.$$
- Wenn a sowohl Teiler von b als auch von c ist, ist a auch Teiler von $b \pm c$:
$$a|b \;\wedge\; a|c \quad \Rightarrow \quad a|(b+c) \;\wedge\; a|(b-c).$$

Satz: Division mit Rest

Seien a, $b \in \mathbb{Z}$ mit $b \neq 0$. Dann existieren q, $r \in \mathbb{Z}$, sodass a die eindeutige Darstellung

$$a = q \cdot b + r \quad \text{mit} \quad 0 \leq r < |b|,$$

hat. In diesem Fall schreibt man für den Rest auch $r = a \bmod b$.

Beweis: Wir müssen sowohl die *Existenz* als auch die *Eindeutigkeit* beweisen.

1. **Eindeutigkeit:** Angenommen, es gäbe zwei Darstellungen von a:

$$a = qb + r \quad \text{und} \quad a = q'b + r' \quad \text{mit} \quad 0 \leq r, r' < |b|.$$

Dann ist $r - r' = b(q - q')$ und damit ist b ein Teiler. Wegen $|r - r'| < |b|$ muss aber $r - r' = 0$ gelten und damit (wegen $b \neq 0$) auch $q = q'$.

2. **Existenz:** Dieser Beweisteil beruht auf einer wichtigen Tatsache:

   Jede nicht-leere Teilmenge von $\mathbb{N}$ enthält ein (eindeutiges) kleinstes Element.

   - Wir definieren $S := \{a - z \cdot b \in \mathbb{N} \mid z \in \mathbb{Z}\}$ und unterscheiden zwei Fälle:
     (1) $b > 0$: Wir können ein z klein genug finden, sodass $a - zb > 0$.
     (2) $b < 0$: Wir können ein z groß genug wählen, sodass $a - zb > 0$.
   - Also gilt $S \neq \emptyset$ und nach Definition $S \subseteq \mathbb{N}$ und S besitzt ein (eindeutiges) kleinstes Element $r := a - qb$.
   - Damit gilt $a = qb + r$ und $r \geq 0$, da $r \in S$ nach Konstruktion.
   - Angenommen, $r \geq |b|$. Dann gilt aber mit $0 \leq r - |b| < r$ auch, dass

   $$r' = r - |b| = a - qb - |b| = a - (q \pm 1)b \in S.$$

   - Diese Zahl r' ist aber kleiner als das minimale Element r, ein Widerspruch, d.h. es gilt $r \leq |b| - 1$. $\square$

Definition: größter gemeinensamer Teiler

- Für a, $b \in \mathbb{Z}$ heißt die größte Zahl $d \in \mathbb{N}$ mit $d|a$ und $d|b$ der **größte gemeinsame Teiler** (in Zeichen: $\mathrm{ggT}(a, b)$) von a und b.
- Gilt $\mathrm{ggT}(a, b) = 1$, so heißen a und b **teilerfremd**.

Anmerkung: Teilerfremd bedeutet nicht etwa, dass die beiden Zahlen keine gemeinsamen Teiler haben, nur dass ± 1 die einzigen gemeinsamen Teiler sind.

Beispiele:

- $\mathrm{ggT}(6,9) = \mathrm{ggT}(-6,9) = \mathrm{ggT}(6,-9) = \mathrm{ggT}(-6,-9) = 3$
- $a|b \implies \mathrm{ggT}(a,b) = |a|$.
- Falls $p \in \mathbb{P}$, so gilt $\mathrm{ggT}(a,p) = 1$ für alle $1 \leq a \leq p-1$. Also ist jede Primzahl teilerfremd zu allen positiven Vorgängern.
- Es gilt $\mathrm{ggT}(a,0) = |a|$, denn keine Zahl größer als $|a|$ teilt a und jede Zahl teilt 0.

4.2 Diskrete Mathematik: Zahlentheorie, Teilbarkeitslehre

Satz

Seien a, $b \in \mathbb{Z}$ mit $b \neq 0$ und die Darstellung durch Division mit Rest sei $a = q \cdot b + r$ mit $0 \leq r < |b|$. Dann gilt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r).$$

Beispiel: $a = 23$, $b = 5$, d.h. $23 = 4 \cdot 5 + 3$. Damit ist $r = 3$ und

$$\mathrm{ggT}(23, 5) = 1 = \mathrm{ggT}(5, 3).$$

4.2 Diskrete Mathematik: Zahlentheorie, Teilbarkeitslehre

Der Euklidische Algorithmus

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann berechnet sich der $\operatorname{ggT}(a, b)$ wie folgt:

1. Führe Division mit Rest durch: $a = qb + r$ mit $0 \leq r < b$.
2. Wenn $r = 0$, dann gilt $\operatorname{ggT}(a, b) = b$. Ansonsten, setze $a := b$ und $b := r$ und gehe zu 1..

Beispiel: Wir berechnen $\mathrm{ggT}(5740, 17)$:

a	b	a	$=$	q	$\cdot$	b	$+$	r	$\mathrm{ggT}(a,b)$	$=$	$\mathrm{ggT}(b,r)$
5740	17	5740	$=$	337	$\cdot$	17	$+$	11	$\mathrm{ggT}(5740, 17)$	$=$	$\mathrm{ggT}(17, 11)$
17	11	17	$=$	1	$\cdot$	11	$+$	6	$\mathrm{ggT}(17, 11)$	$=$	$\mathrm{ggT}(11, 6)$
11	6	11	$=$	1	$\cdot$	6	$+$	5	$\mathrm{ggT}(11, 6)$	$=$	$\mathrm{ggT}(6, 5)$
6	5	6	$=$	1	$\cdot$	5	$+$	1	$\mathrm{ggT}(6, 5)$	$=$	$\mathrm{ggT}(5, 1)$
5	1	5	$=$	5	$\cdot$	1	$+$	0	$\mathrm{ggT}(5, 1)$	$=$	$\mathrm{ggT}(1, 0) = 1$

Lemma von Bézout

Seien $a,\ b \in \mathbb{Z}$ und $d = \mathrm{ggT}(a, b)$. Dann gibt es $s,\ t \in \mathbb{Z}$, so dass

$$\mathrm{ggT}(a, b) = s \cdot a + t \cdot b.$$

Diese Darstellung des ggT heißt **Vielfachsummendarstellung**.

Beispiel: Wir berechnen eine Vielfachsummendarstellung von $\mathrm{ggT}(5740, 17) = 1$ mit Hilfe des **erweiterten Euklidischen Algorithmus**.

a	b	$a = q \cdot b + r$	$\mathrm{ggT} = s \cdot a + t \cdot b$
5740	17	$5740 = 337 \cdot 17 + 11$	$1 = 2 \cdot 17 - 3 \cdot (5740 - 337 \cdot 17)$ $= (-3) \cdot 5740 + 1013 \cdot 17$
17	11	$17 = 1 \cdot 11 + 6$	$1 = (-1) \cdot 11 + 2 \cdot (17 - 1 \cdot 11)$ $= 2 \cdot 17 - 3 \cdot 11$
11	6	$11 = 1 \cdot 6 + 5$	$1 = 6 - 1 \cdot (11 - 1 \cdot 6)$ $= (-1) \cdot 11 + 2 \cdot 6$
6	5	$6 = 1 \cdot 5 + 1$	$1 = 6 - 1 \cdot 5$
5	1	$5 = 5 \cdot 1 + 0$	

Die gesuchten Koeffizienten in der Vielfachsummendarstellung sind also

$$s = -3 \quad \text{und} \quad t = 1013.$$

4.3 Grundlagen der Zahlentheorie: Modulare Arithmetik

4.3 Diskrete Mathematik: Zahlentheorie, modulare Arithmetik

Einführung:

- Es ist bekannt, wie wir in unendlichen Mengen wie $\mathbb{N}$, $\mathbb{Q}$ oder $\mathbb{R}$ rechnen können
- Ein Computer kann aber nur mit einer endlichen Menge von Zahlen umgehen. Bedingt durch die Speicherkapazität kennt er etwa nur die Zahlen

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

- **Idee:** zyklische Rechnung bzw. Rechnung mit Rest.
- **Beispiel:** Uhrzeit. Es ist 17 Uhr. In 8 Stunden ist es 1:00 Uhr, vor 18 Stunden war es 23:00 Uhr Wir sind also in $\mathbb{Z}_{24}$ unterwegs und denken uns 24:00 Uhr wieder als 0:00 Uhr. Zyklische Addition und Subtraktion sind uns also aus dem Alltag durchaus bekannt.

4.3 Diskrete Mathematik: Zahlentheorie, modulare Arithmetik

Definition: Restklasse

Für $n \in \mathbb{N}_{\geq 2}$ definieren wir auf $\mathbb{Z}$ die Äquivalenzrelation

$$a \sim_n b :\Longleftrightarrow n|(a-b).$$

Die Äquivalenzklassen heißen hier **Restklassen** und wir bezeichnen diese mit $[a]$ für $a \in \mathbb{Z}$, d.h.

$$[a] := \{b \in \mathbb{Z} \mid n|(a-b)\}.$$

Darüber hinaus verwenden wir die **Modulo-Schreibweise**:

$$a \equiv b \pmod{n} \quad :\Longleftrightarrow \quad [a] = [b].$$

Satz

Es gilt $[a] = [b] \iff a \bmod n = b \bmod n$.

Beweis: Wir teilen den Äquivalenzbeweis in zwei Implikationen.

$\Rightarrow$ Es gelte $[a] = [b]$. Wir müssen zeigen, dass a und b bei Division durch n denselben Rest haben. Seien die Darstellungen der Division gegeben durch $a = q_1 \cdot n + r_1$ und $b = q_2 \cdot n + r_2$. Nach Voraussetzung existiert k, so dass $a - b = k \cdot n$. Wir erhalten

$$0 \leq |r_1 - r_2| = |a - q_1 n - b + q_2 n| = |a - b + (q_2 - q_1)n| = |(k + q_2 - q_1)| \cdot n,$$

also $n|(|r_1 - r_2|)$. Da aber $|r_1 - r_2| < n$ folgt $|r_1 - r_2| = 0$ und damit $r_1 = r_2$.

Satz

Es gilt $[a] = [b] \iff a \bmod n = b \bmod n$.

Beweis: Wir teilen den Äquivalenzbeweis in zwei Implikationen.

$\Leftarrow$ Nach Vorraussetzung haben wir Darstellungen $a = q_1 n + r$ und $b = q_2 n + r$. Dann folgt $a - b = q_1 n - q_2 n = (q_1 - q_2)n$, also $n|(a - b)$. Damit ist aber a und b in derselben Äquivalenzklasse und da diese entweder gleich oder disjunkt sind, gilt schon $[a] = [b]$. $\square$

4.3 Diskrete Mathematik: Zahlentheorie, modulare Arithmetik

Korollar

Es gilt $|\mathbb{Z}_n| = n$ und ein **Repräsentantensystem** der Äquivalenzrelation ist gegeben durch

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}.$$

Anmerkung:

$\mathbb{Z}$ wird in n verschiedene Mengen zerschnitten, von der jede einzelne unendlich viele Elemente enthält, die etwas gemeinsam haben (nämlich den Rest bei Division durch n).

Definition: Verknüpfung von Restklassen

Für a, $b \in \mathbb{Z}$ definieren wir

1. die Addition durch $[a] + [b] := [a + b]$,
2. die Multiplikation durch $[a] \cdot [b] := [a \cdot b]$.

Satz

Falls $[a] = [a']$ und $[b] = [b']$ so folgt $[a + b] = [a' + b']$ und $[a \cdot b] = [a' \cdot b']$.

Beweis:
Wir zeigen die Aussage exemplarisch für die Addition: Wegen $[a] = [a']$ existiert $q_1 \in \mathbb{Z}$, so dass $a - a' = q_1 n$. Analog existiert $q_2 \in \mathbb{Z}$ mit $b - b' = q_2 n$. Wir erhalten also

$$(a + b) - (a' + b') = (a - a') + (b - b') = q_1 n + q_2 n = (q_1 + q_2)n,$$

und daher unterscheiden sich $(a + b)$ und $(a' + b')$ nur um ein Vielfaches von n und bilden somit dieselbe Restklasse. $\square$

Beispiele:

- Wir rechnen in $\mathbb{Z}_7$:

$$\begin{aligned} [1] + [3] &= [1+3] = [4] \\ [5] + [2] &= [5+2] = [7] = [0] \\ [8] + [-11] &= [8-11] = [-3] = [4] \end{aligned}$$

- Als weiteres Beispiel betrachten wir die Additionstafel von $\mathbb{Z}_4$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Proposition: Addition von Restklassen

Für die modulare Addition gilt:

- **Kommutativität:** $[a] + [b] = [b] + [a]$
- **Assoziativität:** $([a] + [b]) + [c] = [a] + ([b] + [c])$
- $[a] + [0] = [a]$ für alle $a \in \mathbb{Z}$. Die Restklasse $[0]$ ist damit **Neutralelement** bezüglich der Addition (und auch das Einzige).
- Zu jeder Restklasse $[a]$ gibt es ein **inverses Element**, d.h. es existiert $[b]$ mit $[a] + [b] = [0]$. Dieses Element ist $[-a]$.

4.3 Diskrete Mathematik: Zahlentheorie, modulare Arithmetik

Beispiel: Wir betrachten die Multiplikationstafel von $\mathbb{Z}_4$:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Hierbei erkennt man, dass eine Zeile nicht, so wie bei der Addition, alle Elemente enthalten muss. Genauso herrscht keine Nullteilerfreiheit, denn

$$[2] \cdot [2] = [2 \cdot 2] = [4] = [0].$$

Proposition: Multiplikation von Restklassen

Für die modulare Multiplikation gilt:

- **Kommutativität:** $[a] \cdot [b] = [b] \cdot [a]$
- **Assoziativität:** $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$
- $[a] \cdot [1] = [a]$ für alle $a \in \mathbb{Z}$. Die Restklasse $[1]$ ist damit **Neutralelement** bezüglich der Multiplikation.

Aufgaben:

Modulo-Rechnungen

1. $12^{143} \bmod 21 =$
2. $43^{724} \bmod 57 =$
3. $11^{535} \bmod 43 =$
4. $12^{143} \bmod 21 =$

Proposition: Multiplikation von Restklassen

$[a]$ hat multiplikatives Inverses in $\mathbb{Z}_n$ genau dann, wenn $\mathrm{ggT}(a, n) = 1$.

Beweis:

$\Rightarrow$ Nach Voraussetzung existiert $[b]$ mit

$$[a] \cdot [b] = [1] \quad \Leftrightarrow \quad [ab] = [1] \quad \Leftrightarrow \quad ab - 1 = k \cdot n \quad (k \in \mathbb{Z}).$$

Falls t ein gemeinsamer Teiler von a und n ist, so folgt $t|ab$ und $t|(ab - kn)$. Damit teilt t aber schon 1 und $\mathrm{ggT}(a, n) = 1$.

Proposition: Multiplikation von Restklassen

$[a]$ hat multiplikatives Inverses in $\mathbb{Z}_n$ genau dann, wenn $\operatorname{ggT}(a, n) = 1$.

Beweis:

$\Leftarrow$ Es gelte $\operatorname{ggT}(a, n) = 1$. Mittels der Vielfachsummendarstellung im Lemma von Bézout existieren s, $t \in \mathbb{Z}$, so dass

$$1 = \operatorname{ggT}(a, n) = s \cdot a + t \cdot n.$$

Nach Definition der modularen Addition und Multiplikation folgt

$$[1] = [sa + tn] = [s] \cdot [a] + [t] \cdot [n] = [s] \cdot [a] + [t] \cdot [0] = [s] \cdot [a],$$

und damit hat $[a]$ die multiplikative Inverse $[s]$.

4.3 Diskrete Mathematik: Zahlentheorie, modulare Arithmetik

Beispiel:

- Wir möchten die Gleichung $[17] \cdot [x] = [1]$ in $\mathbb{Z}_{5740}$ lösen.
- Anders gesagt: wir suchen x, sodass $17x \equiv 1 \bmod 5740$.
- Diese Gleichung hat genau dann eine Lösung, wenn $[17]$ in $\mathbb{Z}_{5740}$ invertierbar ist.
- Dann können wir mit dem Inversen multiplizieren.

$$
\begin{aligned}
& [17] \cdot [x] = [1] \\
\Rightarrow\quad & [17]^{-1} \cdot [17][x] = [17]^{-1}[1] \\
\Rightarrow\quad & [x] = [17]^{-1}.
\end{aligned}
$$

- Ansonsten hat die Gleichung keine Lösung. [17] ist aber in $\mathbb{Z}_{5740}$ invertierbar, denn nach obigem Beispiel gilt $\mathrm{ggT}(17, 5740) = 1$. Die Vielfachsummendarstellung lautet

$$1 = \underbrace{1013}_{=s} \cdot 17 + \underbrace{(-3)}_{=t} \cdot 5740.$$

- Damit erhalten wir

$$[1] = [1013 \cdot 17 + (-3) \cdot 5740] = [1013] \cdot [17] + [-3] \cdot \underbrace{[5740]}_{=[0]}.$$

- Die Lösung der Gleichung lautet also $[x] = [17]^{-1} = [1013]$.

Aufgaben:

Bestimmen Sie, wenn möglich, die Lösungen der folgenden Gleichungen

1. $[29] \cdot [x] = [1]$ in $\mathbb{Z}_{231}$
2. $[11] \cdot [x] = [4]$ in $\mathbb{Z}_{198}$
3. $[37] \cdot [x] = [7]$ in $\mathbb{Z}_{112}$
4. $[59] \cdot [x] = [5]$ in $\mathbb{Z}_{317}$

4.4 Kryptographie

4.4 Diskrete Mathematik: Kryptographie

Kryptographie ist die Wissenschaft der Verschlüsselung von Informationen.

Beispiel: Caesar-Chiffre

- Dabei handelt es sich um eine Bijektion des Alphabets auf sich selbst durch eine Verschiebung der Buchstaben um k Stellen.
- Wir weisen jedem Buchstaben entsprechend seiner Stelle im Alphabet eine Zahl zu:

$$f : \{a, b, c, \ldots, z\} \to \mathbb{Z}_{26}, \quad n\text{-ter Buchstabe} \mapsto f(n) = n.$$

- Mit der Modulo-Rechnung können wir nun eine Nachricht m (für „message“) Buchstabe für Buchstabe verschlüsseln bzw. einen Code c wieder entschlüsseln.

4.4 Diskrete Mathematik: Kryptographie

- Die **Verschlüsselung** (encrypt) von m liefert den Code

$$c = e_k(f(m)) = f(m) + k \mod 26.$$

- Die **Entschlüsselung** (decrypt) von c ist

$$d_k(c) = c - k = f(m) \mod 26,$$

  also die **Inverse** von e_k.
- Mit Hilfe von f^{-1} erhalten wir den entschlüsselten Text.
- Da z.B. Bank-Transaktionen „etwas“ sicherer verschlüsselt sein sollten als mit der Caesar-Chiffre, betrachten wir die RSA-Verschlüsselung.

4.4 Diskrete Mathematik: Kryptographie

Public-Key-Kryptographie:

- Angenommen, es gibt eine Gruppe von n Teilnehmern, die untereinander Nachrichten versenden wollen.
- Es sollen immer nur Nachrichten zwischen zwei Teilnehmern ausgetauscht werden, die anderen dürfen die Nachrichten nicht lesen können.
- Jeder Teilnehmer T hat zwei Schlüssel: einen öffentlichen e_T und einen privaten (geheimen) d_T.
- e_T wird verwendet, um aus einer gegebenen Nachricht eine verschlüsselte Nachricht zu machen.
- Mit d_T wird die Nachricht entschlüsselt.

4.4 Diskrete Mathematik: Kryptographie

Public-Key-Kryptographie:

- Es darf praktisch nicht möglich sein, aus dem öffentlichen Schlüssel e_T den zugehörigen privaten Schlüssel d_T zu berechnen.
- Für jede Nachricht m, die mit e_T verschlüsselt wurde, kann mit d_T wieder entschlüsselt werden ("$d_T \circ e_T(m) = m$").
- **Frage:** Kann ein Sender einem Empfänger, mit welchem er keinen gemeinsamen Schlüssel besitzt, eine Nachricht zukommen lassen ohne dass die Nachricht abgefangen und entschlüsselt wird?
- Zunächst war nicht klar, ob ein solches Public-Key-Verschlüsselungssystem überhaupt existiert, d.h., eine Funktion d_T, die aus ihrer Inversen praktisch nicht errechnet werden kann.
- Ronald Rivest, Adi Shamir und Leonard Adleman entwickelten den **RSA-Algorithmus**, der eine Realisierung des Konzeptes liefert.

4.4 Diskrete Mathematik: Kryptographie

Public-Key-Kryptographie:
Das Senden einer Nachricht funktioniert dann so:

- Der Sender A holt sich den öffentlichen Schlüssel e_B des Empfängers B und verschlüsselt, indem er
$$c = e_B(m)$$
bildet.
- Den Geheimtext c sendet er an B, welcher diesen mit seinem privaten Schlüssel d_B, den nur er besitzt, entschlüsselt:
$$d_B(c) = d_B\left(e_B(m)\right) = m.$$

Definition: Einheitengruppe, Euler-φ-Funktion

- Die **Einheitengruppe** von $\mathbb{Z}_n$ ist definiert als

$$\mathbb{Z}_n^* := \{[m] \in \mathbb{Z}_n \mid [m] \text{ ist invertierbar}\}.$$

- Die **eulersche φ-Funktion** ist definiert durch

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad n \mapsto \varphi(n) := |\mathbb{Z}_n^*|.$$

Anmerkung: Die eulersche φ-Funktion ordnet jeder natürlichen Zahl n die Anzahl teilerfremder Zahlen kleiner n zu.

4.4 Diskrete Mathematik: Kryptographie

Proposition: Eigenschaften von $\mathbb{Z}_n^*$ und φ

- $[m] \in \mathbb{Z}_n^* \iff \mathrm{ggT}(m, n) = 1$
- $\varphi(p) = p - 1$ für alle $p \in \mathbb{P}$.
- $\varphi(p^k) = p^k - p^{k-1}$ für alle $p \in \mathbb{P}$.
- Falls $\mathrm{ggT}(a, b) = 1$ so gilt $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
- Insbesondere, falls $n = p \cdot q$ mit $p \neq q \in \mathbb{P}$, so gilt

$$\varphi(n) = (p - 1) \cdot (q - 1).$$

Beispiele:

$$\varphi(2) = 1,$$

$$\varphi(3) = 2,$$

$$\varphi(4) = \varphi(2^2) = 2^2 - 2^1 = 2,$$

$$\varphi(10) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4,$$

$$\varphi(99) = \varphi(3^2 \cdot 11) = \varphi(3^2) \cdot \varphi(11) = (3^2 - 3^1) \cdot 10 = 60.$$

Satz von Euler

Sei $n \in \mathbb{N}$, $1 \leq a \leq n-1$ und $\operatorname{ggT}(a,n) = 1$. Dann gilt

$$a^{\varphi(n)} \equiv 1 \mod n,$$

oder anders ausgedrückt, $n \mid \left(a^{\varphi(n)} - 1\right)$.

Anmerkung: Beweis siehe Skript.

RSA-Algorithmus: öffentlicher Schlüssel

Jeder Teilnehmer bestimmt für sich seinen öffentlichen Schlüssel.

- Wähle zwei sehr große Primzahlen $p \neq q$ und bilde $n := p \cdot q$.
- Berechne $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.
- Wähle e mit $1 < e < \varphi(n)$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$
  (z.B. kann immer eine bekannte Primzahl größer $\frac{\varphi}{2}$ gewählt werden)

(e, n) bildet den öffentlichen Schlüssel, der jedem der Teilnehmer verraten wird.

Beispiel: $p = 71$, $q = 83$ und damit $n = 71 \cdot 83 = 5893$.

$$\varphi(5893) = \varphi(71 \cdot 83) = (71-1)(83-1) = 5740.$$

Wähle $e = 17$. Dann ist zu $\mathrm{ggT}(e, \varphi(5893)) = 1$ und der *public key* $(e, n) = (17, 5893)$.

RSA-Algorithmus: privater Schlüssel

Jeder Teilnehmer bestimmt für sich seinen privaten Schlüssel.

- Berechne die Inverse von e in $\mathbb{Z}_{\varphi(n)}$, also die Zahl d mit
$$e \cdot d \equiv 1 \bmod \varphi(n).$$
Diese existiert, denn $\mathrm{ggT}(e, \varphi(n)) = 1$ nach Konstruktion.
- Bestimme die Vielfachsummendarstellung $1 = s \cdot e + t \cdot \varphi(n)$ und damit die Inverse $[s]$ von $[e]$ mit dem erweiterte euklidische Algorithmus.
- Bestimme den privaten Schlüssel d in der üblichen Repräsentanten Darstellung $d := s \bmod \varphi(n)$. Dieser wird niemandem verraten!

Beispiel: In $\mathbb{Z}_{5740}$ ist $[17]^{-1} = [1013]$. Der *private key* ist $d = 1013 \bmod 5893 = 1013$.

RSA-Algorithmus: Verschlüsselung einer Nachricht

Will ein Teilnehmer eine Nachricht m verschicken, so verschlüsselt er diese durch

$$c = m^e \mod n.$$

Diese Methode der Verschlüsselung mit (e, n) ist ebenfalls öffentlich und damit jedem Teilnehmer bekannt!

Beispiel: Wir wollen $m = 3$ verschlüsseln.

$$\begin{aligned} c = 3^{17} &\equiv 3^8 \cdot 3^9 \mod 5893 \equiv 6561 \cdot 3^9 \mod 5893 \\ &\equiv 668 \cdot 3^2 \cdot 3^7 \mod 5893 \equiv \ldots \equiv 961 \mod 5893. \end{aligned}$$

RSA-Algorithmus: Entschlüsselung der Nachricht

Der Empfänger erhält die Nachricht c und entschlüsselt diese mit seinem privaten Schlüssel d. Dazu bemerken wir zunächst, dass für ein $k > 0$ (denn $d, e, \varphi(n) > 0$)

$$[d] \cdot [e] - [1] = [0] \quad \Leftrightarrow \quad \varphi(n) | (de - 1) \quad \Leftrightarrow \quad 0 \leq de - 1 = k \cdot \varphi(n).$$

Jetzt kommt der entscheidende Schritt: die Entschlüsselung. Dass diese funktioniert sichert der Satz von Euler. Es gilt nämlich

$$\begin{aligned} c^d &\equiv (m^e)^d \mod n \equiv m^{de} \mod n \equiv m^{\varphi k + 1} \mod n \\ &\equiv (m^{\varphi})^k m \mod n \equiv 1^k \cdot m \mod n \equiv m \mod n. \end{aligned}$$

Beispiel: Wir berechnen $m = 961^{1013} \equiv \ldots \equiv 3 \mod 5893$.

RSA-Algorithmus: Diskussion

- Wie soll dieser Algorithmus der Geheimhaltung dienen?
- Er ist vollständig bekannt und jeder Schritt ist nachvollziehbar.
- Ein Angreifer aus der Gruppe, der die Nachricht abfängt, kennt ja auch den öffentlichen Schlüssel des Empfängers.
- Also kann er doch, genau wie der Empfänger, den privaten Schlüssel berechnen. Dazu muss er nur $\varphi(n)$ berechnen und dann mit dem erweiterten euklidischen Algorithmus eine Inverse zu der (bekannten) Zahl e in $\mathbb{Z}_{\varphi(n)}$ ermitteln.
- Hier liegt das Problem für den Angreifer:

Der Empfänger kennt $\varphi(n)$, der Angreifer nicht!

RSA-Algorithmus: Diskussion

- Die Euler'sche φ-Funktion auszurechnen war für den Empfänger einfach, denn er wusste, dass $n = p \cdot q$ und damit

$$\varphi(n) = \varphi(pq) = (p-1)(q-1).$$

- Der Angreifer muss die Primfaktorzerlegung von n erst finden. Diese wird nämlich nicht öffentlich gemacht!
- Die Primzahlen sind typischerweise im mindestens 300-Stelligen Bereich gewählt.
- Der Weltrekord im Faktorisieren einer Zahl n liegt bei 232 Dezimalstellen. Ein handelsüblicher Rechner hätte dafür 2000 Jahre gebraucht.
- Trotzdem sollte klar geworden sein, dass die Sicherheit des Verfahrens allein von der Tatsache abhängt, dass die Faktorisierung großer Zahlen schwierig ist.

RSA-Algorithmus: Diskussion

- Es werden aber jeden Tag leistungsfähigere Algorithmen für eine Faktorisierung enwickelt.
- Man kann also nicht garantieren, dass die heute als sehr sicher geltenden Verschlüsselungsalgorithmen morgen nicht schon geknackt werden können.
- **Fazit:** für die monetär Interessierten unter Ihnen ...

Entwickeln Sie leistungsfähige Algorithmen zur Verschlüsselung!
oder
Entwickeln Sie leistungsfähige Algorithmen zur Primfaktorzerlegung!
... und knüpfen Sie zwielichtige Kontakte im Darknet ;-)

5. Algebraische Strukturen

5. Algebraische Strukturen

Die **Algebra** ist ein mathematisches Teilgebiet, das sich mit der Eigenschaft von Rechenoperationen beschäftigt.

- Assoziativ-, Kommutativ- oder Distributivgesetze gelten in verschiedenen Teilgebieten der Mathematik, z.B. bei den Grundrechenarten reeller Zahlen, der Mengenlehre oder der Aussagenlogik.
- Es scheint also themenübergreifende algebraische Strukturen zu geben.
- Drei dieser Strukturen werden im Folgenden vorgestellt: die **Gruppe**, der **Ring** und der **Körper**.

5.1 Gruppen

5.1 Algebraische Strukturen: Gruppen

Definition: Gruppe

Eine **Gruppe** $(G, *)$ ist eine (nichtleere) Menge G, die bezüglich einer Verknüpfung $*$ abgeschlossen ist, d.h.

$$* : G \times G \to G, \quad (g_1, g_2) \mapsto g_1 * g_2,$$

und folgende Eigenschaften besitzt:

- Es gilt das **Assoziativgesetz**, d.h. für alle $g_1, g_2, g_3 \in G$ gilt
$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3.$$
- Für alle Elemente $g \in G$ gibt es ein **neutrales Element** $e \in G$, sodass gilt
$$e * g = g * e = g.$$

Definition: Gruppe (Fortsetzung)

- Für alle Elemente $g \in G$ gibt es ein **inverses Element** $h \in G$, sodass gilt
$$h * g = g * h = e.$$
Wir schreiben für h auch g^{-1}, um die Beziehung zu g zu verdeutlichen.

Gilt zusätzlich das **Kommutativgesetz**, d.h. für alle $g_1, g_2 \in G$ gilt

$$g_1 * g_2 = g_2 * g_1,$$

so nennen wir $(G, *)$ nach dem Mathematiker *Niels Abel (1802-1829)* eine **abelsche Gruppe** oder auch **kommutative Gruppe**.

5.1 Algebraische Strukturen: Gruppen

Anmerkungen:

- Nicht umsonst haben wir für die leere Summe den Wert des neutralen Elements der Addition, die Null, gewählt. Ebenso wird das leere Produkt entsprechend dem neutralen Element der Multiplikation, der Eins, gewählt.
- **Abgeschlossenheit** bezüglich der Verknüpfung bedeutet:

  Wenn wir zwei Elemente aus G miteinander verknüpfen, erhalten wir wieder ein Element aus G.
- Die genannten Eigenschaften werden auch als **Gruppenaxiome** bezeichnet.
- Das neutrale Element e ist eindeutig bestimmt.
- Das zu g inverse Element g^{-1} ist eindeutig bestimmt.

Anmerkungen:

- Wir schreiben manchmal auch $a \cdot b$ oder ab statt $a * b$ und G statt $(G, *)$.
- Aufgrund der Assoziativität können wir Klammern weglassen, d.h.

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3 = g_1 * g_2 * g_3.$$

- Beispiele für das Sternchensymbol $*$ sind die üblichen Verknüpfungen wie Addition $(+)$ oder Multiplikation $(\cdot)$.
- Die bekannte **Subtraktion** zweier Zahlen a und b kann als Addition von a mit dem additiv Inversen $b^{-1} = -b$ bezüglich b interpretiert werden:

$$a - b = a + (-b),$$

- Ebenso ist die Division von a durch b nichts anderes als die Multiplikation von a mit dem multiplikativen Inversen $b^{-1} = \frac{1}{b}$ von b:

$$a : b = a \cdot \frac{1}{b} = a \cdot b^{-1}.$$

5.1 Algebraische Strukturen: Gruppen

Hinweis: Möchten wir überprüfen, ob eine Menge M mit einer gegebenen Verknüpfung eine Gruppe bildet, müssen wir zeigen, dass alle Gruppenaxiome, also

- die **A**ssoziativität,
- die Existenz eines **N**eutralen Elements in der Menge,
- die Existenz von **I**nversen Elementen,
- eventuell die **K**ommutativität und
- und die Voraussetzungen der **A**bgeschlossenheit und nichtleeren Menge

gelten. Als Merkhilfe können die Anfangsbuchstaben dienen: **ANI(K)A**.
Die Eigenschaft, dass die Menge nichtleer ist, wird dabei durch die gegebene Menge direkt klar oder durch das Argument, dass es ein inverses bzw. neutrales Element in der Gruppe gibt.

5.1 Algebraische Strukturen: Gruppen

Beispiele: Addition / Subtraktion

1. Die ganzen Zahlen $\mathbb{Z}$ bilden mit der bekannten Additionsverknüpfung $+$ die abelsche Gruppe $(\mathbb{Z}, +)$. Das neutrale Element der Addition ist 0, das Inverse zur Zahl $a \in \mathbb{Z}$ ist die Zahl $-a \in \mathbb{Z}$.
2. Auch $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind abelsche Gruppen.
3. Dagegen ist $(\mathbb{N}, +)$ keine Gruppe, da es kein neutrales Element gibt. Nimmt man die Null hinzu, bildet $(\mathbb{N}_0, +)$ immer noch keine Gruppe, da es zu einer (positiven) Zahl $n \in \mathbb{N}$ kein inverses Elemente $-n$ in den natürlichen Zahlen gibt.
4. Wir betrachten die ganzen Zahlen $\mathbb{Z}$ mit der Subtraktionsverknüpfung $-$. Wie wir an einem einfachen Zahlenbeispiel erkennen, ist das Assoziativitätsgesetz verletzt:

$$(1-2)-3 = -1-3 = -4 \quad \neq \quad 2 = 1-(-1) = 1-(2-3)$$

$(\mathbb{Z}, -)$ ist folglich keine Gruppe.

5.1 Algebraische Strukturen: Gruppen

Beispiel: Multiplikation

5. Betrachten wir die **Multiplikation** als Verknüpfung und suchen eine Zahlenmenge, die gemeinsam mit $\cdot$ eine Gruppe bildet.
   - Starten wir mit $\mathbb{N}$:
     Abgeschlossenheit gilt und es gibt ein neutrales Element, die 1.
     Aber Zahlen größer 1 besitzen kein Inverses.
     D.h. $(\mathbb{N}, \cdot)$ ist keine Gruppe, ebenso wenig wie $(\mathbb{Z}, \cdot)$.
   - Prüfen wir $\mathbb{Q}$:
     Abgeschlossenheit, Assoziativität und Kommutativität gelten.
     Das neutrale Element ist die 1 und das Inverse eines Bruchs $\frac{p}{q}$ ist der Kehrwert $\frac{q}{p}$.
     Dennoch ist $(\mathbb{Q}, \cdot)$ keine Gruppe, denn das Inverse Element muss für alle Elemente existieren. Für $0 = \frac{0}{1}$ gibt es dies aber nicht, da $\frac{1}{0}$, also die Division durch 0, nicht definiert ist.
   - Entfernen wir die 0 aus $\mathbb{Q}$, ist $(\mathbb{Q} \setminus \{0\}, \cdot)$ eine abelsche Gruppe.

5.1 Algebraische Strukturen: Gruppen

Abstraktere Beispiele: Einelementige Menge

6. Betrachten wir zunächst eine Menge $G = \{g\}$ mit nur einem Element g und eine Verknüpfung $*$. Kann $(G, *)$ eine Gruppe sein kann? Wir prüfen:
   - Da G ein Element besitzt, ist G nicht leer.
   - Wenn $G = \{g\}$ bezüglich $*$ abgeschlossen sein soll, muss gelten
     $$g * g \in G \quad \Rightarrow \quad g * g = g.$$
   - Wenn aber g mit sich selbst verknüpft wieder g ergibt, muss es sich bei g um das neutrale Element handeln. Wir schreiben also $g = e$, um wieder die Notation als neutrales Element zu verwenden, d.h. $G = \{e\}$ und $e * e = e$. Die Existenz eines neutralen Elements in der Menge ist also gesichert.
   - Wenn nun das Element mit sich selbst verknüpft das neutrale Element ergibt, muss es sich zu sich selbst invers sein. Es existiert ein inverses Element $e^{-1} = e$ zum einzigen vorhandenen Element e. Damit ist die Existenz eines inversen Elements für "alle" Elemente gegeben.

   Es handelt sich bei $(\{e\}, *)$ also um eine Gruppe.

5.1 Algebraische Strukturen: Gruppen

Abstraktere Beispiele: Zwei- und dreielementige Menge

7. Stellen wir gleiche Überlegungen für eine zweielementige Menge $G = \{a, b\}$ an, muss offensichtlich eines der Elemente das neutrale Element e sein, also z.B. $b = e$. Da e selbstinvers ist und für jedes Element ein eindeutiges Inverses existieren muss, muss $a * a = e$ gelten. Das Element a ist demnach auch selbstinvers und wir erhalten die sogenannte Verknüpfstafel, der man alle Kombinationen von a und e entnehmen kann:

$$\begin{array}{c|cc} * & e & a \\ \hline e & e & a \\ a & a & e \end{array}.$$

8. **Übung:** Zeigen Sie, dass $(G, *)$ mit $G = \{a, b, c\}$ eine Gruppe ist und erstellen Sie die zugehörige Verknüpfungstafel!

Beispiel: Restklassen

9. Wir betrachten $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ mit der Additionsverknüpfung $\oplus$, die den Rest der Summe aus zwei Elementen bei Division durch 4 ergibt, d.h. wir rechnen die Summe $\mod 4$:

$$1 \oplus 3 = 2 \oplus 2 \equiv_4 0, \quad 2 \oplus 3 \equiv_4 1, \quad 3 \oplus 3 \equiv_4 2.$$

$(\mathbb{Z}_4, \oplus)$ ist eine sogenannte **zyklische Gruppe**, da ihre Elemente zyklisch, d.h. durch mehrfache Verknüpfung eines Elements mit sich, auseinander hervorgehen. Wir erhalten die Verknüpfungstafel:

$$\begin{array}{c|cccc} \oplus & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 0 & 3 & 1 & 2 \end{array}.$$

5.1 Algebraische Strukturen: Gruppen

Bemerkung:

- Möchten wir zwei verschiedene Verknüpfungen kombinieren, müssen wir überlegen, welche Regeln dort gelten sollen.
- Das Distributivgesetz regelt z.B. die Kombination von Durchschnitten und Vereinigungen in der Mengenlehre, von Addition und Multiplikation in der Arithmetik oder die Kombination von Konjunktionen und Disjunktionen in der Logik.
- Auch hier gibt es wieder eine übergeordnete Struktur, den sogenannten **Ring**.

5.2 Ringe

5.2 Algebraische Strukturen: Ringe

Definition: Ring

Ein **Ring** $(R, +, \cdot)$ ist eine (nichtleere) Menge R, die bezüglich der Verknüpfungen

$$\begin{aligned} + : \quad & R \times R \to R, \quad (a, b) \mapsto a + b, \\ \cdot : \quad & R \times R \to R, \quad (a, b) \mapsto a \cdot b \end{aligned}$$

abgeschlossen ist und folgende Eigenschaften besitzt:

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0 und additivem Inversen $-a \in R$ zu $a \in R$.
- $(R, \cdot)$ ist assoziativ und besitzt ein neutrales Element $1 \neq 0$.

5.2 Algebraische Strukturen: Ringe

Definition: Ring (Fortsetzung)

- Für alle Elemente $a, b, c \in R$ gelten die Distributivgesetze

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Falls auch $a \cdot b = b \cdot a$ gilt, heißt $(R, +, \cdot)$ **kommutativer Ring**.

5.2 Algebraische Strukturen: Ringe

Anmerkungen:

- Wir nennen das neutrale Element der Addition auch **Nullelement**, das neutrale Element der Multiplikation **Einselement**.
- Beispiele für kommutative Ringe mit Nullelement 0 und Einselement 1 sind $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$.
- Wir können uns mit $\mathbb{Z}$ auch einen Ring konstruieren, bei denen 1 das Nullelement und 0 das Einselement ist, indem wir folgende Verknüpfungen definieren:

$$a \boxplus b := a + b - 1, \quad \text{und} \quad a \boxtimes b := a + b - ab.$$

  Das additive Inverse zu a ist in diesem Fall $2 - a$.
- Zum Nachweis eines Rings müssen wieder alle Eigenschaften gezeigt werden.

5.2 Algebraische Strukturen: Ringe

Bemerkung:

- Wir haben gesehen, dass $(\mathbb{Z}, \cdot)$ durch Entfernen der Null eine kommutative Gruppe wird.
- Erweitern wir nun die Eigenschaften eines Ring $(R, +, \cdot)$ und entfernen das Nullelement aus der Menge R, wird auch $(R \setminus \{0\}, \cdot)$ zu einer abelschen Gruppe.
- Eine solche algebraische Struktur nennen wir Körper.

5.3 Körper

5.3 Algebraische Strukturen: Körper

Definition: Körper

Ein **Körper** $\mathbb{K}$ ist kommutativer ein Ring $(R, +, \cdot)$, für den zusätzlich $(R \setminus \{0\}, \cdot)$ eine kommutative Gruppe ist.

Anmerkungen:

- Die zusätzliche Eigenschaft, die aus einem kommutativen Ring einen Körper macht ist die Existenz eines multiplikativen Inversen für alle Element von R außer dem Nullelement 0.
- Nach Definition sind unter anderem $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ Körper. Da $\mathbb{Q} \subset \mathbb{R}$ und $\mathbb{R} \subset \mathbb{C}$ ist, sprechen wir bei $\mathbb{Q}$ auch von einem **Teilkörper** von $\mathbb{R}$ bzw. ist $\mathbb{R}$ ein Teilkörper von $\mathbb{C}$.

6. Die Komplexen Zahlen

6.1 Einführung

6.1 Komplexe Zahlen: Herleitung

Vorüberlegungen:

- Wir können *komplexe Zahlen* als Erweiterung der reellen Zahlen zur Lösung polynomialer Gleichungen mit reellen Koeffizienten einführen.
- Wählen wir für -1 eine *imaginäre* (Quadrat-)Zahl i^2, könnten wir z.B. folgende Gleichungen lösen,

$$x^2 = -4 = -1 \cdot 4 = \mathrm{i}^2 \cdot 2^2 = (2\,\mathrm{i})^2 \quad \Rightarrow \quad x_{1,2} = \pm 2\,\mathrm{i},$$

  wenn wir die üblichen Rechenregeln für reelle Zahlen anwenden.
- Wünschenswert wäre es natürlich, wenn *alle* Axiome der reellen Zahlen $\mathbb{R}$ auch auf komplexe Zahlen $\mathbb{C}$ übertragbar wären. Dann wäre $\mathbb{C}$ mit entsprechend definierten Verknüpfungen $+$ und $\cdot$ ein Körper $(\mathbb{C}, +, \cdot)$.

6.1 Komplexe Zahlen: Herleitung

Vorüberlegungen:

- **Problem:** Die reellen Zahlen sind eine *dichte* Menge, d.h. zwischen zwei reellen Zahlen passt immer noch eine weitere reelle Zahl. Anders gesagt: der Zahlenstrahl ist *vollständig* besetzt.
- **Frage:** Wohin also mit den „imaginären“ Zahlen?
- **Antwort:** Wir erweitern den Zahlenstrahl zur Zahlenebene und drücken die komplexe Zahlen als Punkte mit zwei Koordinaten aus.

6.1 Komplexe Zahlen: Herleitung

Vorüberlegungen:

- Die Abbildung
$$\mathbb{R} \to \mathbb{C}, \quad x \mapsto (x, 0)$$
nennen wir die (Körper-)Einbettung von $\mathbb{R}$ in $\mathbb{C}$.
- Dabei liegen die reellen Zahlen auf der x-Achse, die wir daher die **reelle Achse** nennen. Die davon unabhängige y-Achse, die den Zahlenstrahl zur Ebene erweitert, nennen wir **imaginäre Achse**.
- **Konsequenz:** jetzt benötigen wir „nur" noch eine sinnvolle Definition einer Addition und Multiplikation, die jeweils konsistent ist zu den Verknüpfungen $+$ und $\cdot$ für reelle Zahlen, d.h.

$$(x_1, 0) + (x_2, 0) = (x_1 + x_2, 0) \quad \text{bzw.} \quad (x_1, 0) \cdot (x_2, 0) = (x_1 \cdot x_2, 0).$$

6.1 Komplexe Zahlen: Herleitung

Vorüberlegungen:

- Vektoraddition und skalare Multiplikation, wie wir sie aus der Schule kennen, legen nahe, dass für $k \in \mathbb{R}$ und $(x_1, y_1), (x_2, y_2) \in \mathbb{C}$ folgendes gelten muss

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \quad \text{bzw.} \quad k \cdot (x_1, y_1) = (kx_1, ky_1).$$

- Komplexe Zahlen $\mathbb{C}$ können wir also auch als Vektoren in $\mathbb{R}^2$ geometrisch interpretieren (Vektoraddition im Sinne von „Pfeilende an Pfeilanfang“, skalare Multiplikation im Sinne einer Vektorstreckung um den Faktor k).
- Wie aber sollten wir die Multiplikation zweier komplexer Zahlen $(x_1, y_1) \cdot (x_2, y_2)$ definieren, sodass wieder eine komplexe Zahl (x_3, y_3) entsteht?
- Starten wir zunächst mit unserer Definition $\mathrm{i}^2 := -1$.

6.1 Komplexe Zahlen: Herleitung

Vorüberlegungen:

- Die Erweiterung der natürlichen Zahlen um die negativen Zahlen, spiegelbildlich links von der Null notiert, ergibt die ganzen Zahlen.
- Wir können uns z.B. -4 als einen Punkt auf dem Zahlenstrahl mit vier Einheiten Abstand von der Null vorstellen, wobei das Minuszeichen die Richtung nach links anzeigt.
- Die Multiplikation einer Zahl mit -1 bzw. i^2 entspricht also einer Spiegelung dieser Zahl am Ursprung.
- Was aber bedeutet die Multiplikation der Zahl mit der „imaginären" Zahl i?

6.1 Komplexe Zahlen: Herleitung

Idee:

- Statt einer Spiegelung könnten wir uns die Multiplikation mit -1 auch als eine Drehung um π bzw. 180° vorstellen.
- Damit können wir die zweimalige Multiplikation einer reellen Zahl mit i auch als zweimalige Drehung um 90° vorstellen.
- Dies rechtfertigt die Definition von i als das 2-Tupel $\mathrm{i} := (0, 1)$ und $\mathrm{i}^2 = -1$ ist äquivalent zu $(0, 1)^2 = (-1, 0)$. Es gilt

$$(1, 0) \cdot (1, 0) = (1, 0), \quad (1, 0) \cdot (0, 1) = (0, 1) \quad (0, 1) \cdot (0, 1) = (-1, 0).$$

Dies ist der letzte Schritt zur Definition einer sinnvollen Multiplikation zweier komplexer Zahlen miteinander.

6.1 Komplexe Zahlen: Herleitung

- Es folgt $(a, b) \cdot (c, d) = ((a, 0) + (0, b)) \cdot ((c, 0) + (0, d))$

$$
\begin{aligned}
&= (a, 0)(c, 0) + (a, 0)(0, d) + (c, 0)(0, b) + (0, b)(0, d) \\
&= ac(1, 0)(1, 0) + ad(1, 0)(0, 1) + bc(1, 0)(0, 1) + bd(0, 1)(0, 1) \\
&= ac(1, 0) + (ad + bc)(0, 1) + bd(-1, 0) \\
&= (ac - bd, ad + bc).
\end{aligned}
$$

- Nutzen wir $1 := (1, 0)$ und $\mathrm{i} := (0, 1)$, können wir kurz schreiben:

$$(a, b) = a \cdot (1, 0) + b \cdot (0, 1) =: a \cdot 1 + b \cdot \mathrm{i} = a + b\,\mathrm{i}\,.$$

- Die Multiplikation komplexer Zahlen genügt also dem Distributivgesetz:

$$(a+b\,\mathrm{i})(c+d\,\mathrm{i}) = ac+ad\,\mathrm{i}+bc\,\mathrm{i}+bd\,\mathrm{i}^2 = ac+ad\,\mathrm{i}+bc\,\mathrm{i}-bd = (ac-bd)+(ad+bc)\,\mathrm{i}\,.$$

6.1 Komplexe Zahlen: Anwendungen

Beispiele:

- **Fundamentalsatz der Algebra:** Ein Poylnom vom Grad n

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

  besitzt genau n (nicht notwendigerweise verschiedene) Nullstellen in $\mathbb{C}$.
- Manche Integrale können erst durch den Übergang zu den komplexen Zahlen gelöst werden.
- Bei der Stabilitätsanalyse von schwingenden Strukturen wie z.B. Brücken geben komplexe Zahlen Auskunft über das reale Bewegungsverhalten. Genaue Analysen und Simulation können damit katastrophale Folgen wie bei der Takoma-Brücke vermeiden.

http://www.youtube.com/watch?v=3mclp9QmCGs

6.1 Komplexe Zahlen: Anwendungen

Beispiele:

- Eines der meist diskutierten mathematischen Probleme der letzten 150 Jahre ist die *Riemannsche Vermutung*, ein Problem aus der komplexen Analysis, welches auf der komplexen Ebene definiert ist.

  http://de.wikipedia.org/wiki/Riemannsche_Vermutung

  Sie ist bis heute zwar nicht bewiesen, bei den Beweisversuchen wurden aber bereits zahlreiche Erkenntnisse über die Struktur der reellen und natürlichen Zahlen sowie über die Verteilung von Primzahlen gewonnen, was für die Kodierungstheorie von Bedeutung ist.
- Sonstige Anwendungsgebiete: Modellierung in der Wechselstromrechnung, Relativitätstheorie, Regelungstechnik, uvm. Außerdem benutzt man sie zur Konstruktion sogenannter Fraktale, wie etwa der Mandelbrot-Menge.

  http://de.wikipedia.org/wiki/Mandelbrot-Menge

6.2 Die Gauß'sche Zahlenebene

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Definition: Menge der komplexen Zahlen

Eine **komplexe Zahl** z ist ein geordnetes Tupel (x, y) mit $x, y \in \mathbb{R}$. Die Konvention

$$1 := (1, 0) \text{ und } \mathrm{i} := (0, 1)$$

ermöglicht mit den Rechengesetzen der Addition und skalaren Multiplikation in der Ebene die Schreibweise

$$z = (x, y) = x \cdot (1, 0) + y \cdot (0, 1) = x + y\,\mathrm{i}\,.$$

Die **Menge der komplexen Zahlen** ist $\mathbb{C} := \{x + y\,\mathrm{i} \mid x, y \in \mathbb{R}\}$. Sie kann assoziiert werden mit dem $\mathbb{R}^2$.

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Anmerkungen:

- Komplexe Zahlen können in der sogenannten **Gauß'schen Zahlenebene** veranschaulicht werden.
- Die Darstellungsform $z = x + y\,\mathrm{i}$ heißt die **Normalform** einer komplexen Zahl.
- Die komplexen Zahlen in Normalform bilden mit den eingeführten Verknüpfungen $+$ und $\cdot$ einen Körper $(\mathbb{C}, +, \cdot)$
- Wir nennen $x \in \mathbb{R}$ den **Realteil** $\mathrm{Re}(z)$ von z und $y \in \mathbb{R}$ den **Imaginärteil** $\mathrm{Im}(z)$ von z.
- Es gilt $z \in \mathbb{R} \quad \Leftrightarrow \quad y = \mathrm{Im}(z) = 0$. Die komplexen Zahlen mit $\mathrm{Re}(z) = 0$ heißen **(rein) imaginäre Zahlen**.

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Definition: Gleichheit komplexer Zahlen

Zwei komplexe Zahlen z_1 und z_2 heißen **gleich**, wenn

$$\operatorname{Re}(z_1) = \operatorname{Re}(z_2) \quad \text{und} \quad \operatorname{Im}(z_1) = \operatorname{Im}(z_2).$$

Anmerkung: Eine Ordnungsrelation „$<$“ oder „$>$“ gibt es in $\mathbb{C}$ nicht!

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Definition: Betrag und Abstand

Unter dem **Betrag** $|z|$ einer komplexen Zahl $z = x + y\,\mathrm{i}$ versteht man den Abstand des Punktes (x, y) vom Ursprung, also

$$|z| := \sqrt{x^2 + y^2}.$$

Der Abstand zweier komplexer Zahlen $z_1 = x_1 + y_1\,\mathrm{i}$ und $z_2 = x_2 + y_2\,\mathrm{i}$ ist damit

$$|z_1 - z_2| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

Anmerkungen:

- Die Definition nutzt den Satz des Pythagoras.
- $z_1, z_2 \in \mathbb{C}$ mit $|z_1| = |z_2|$ liegen auf demselben Kreis um den Ursprung.

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Proposition: Eigenschaften des Betrags

Sei $z = x + y\,\mathrm{i}$ eine komplexe Zahl und $a \in \mathbb{R}$. Dann gilt

- Definitheit:
$$|z| = 0 \quad \Leftrightarrow \quad z = 0,$$
- Positivität:
$$|z| > 0, \quad \text{für} \quad z \neq 0,$$
- Homogenität:
$$|a \cdot z| = |a| \cdot |z|,$$
- Dreiecksungleichung:
$$\max\{|x|, |y|\} \leq |z| \leq |x| + |y|.$$

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Definition: Komplex konjugierte Zahl

Zu $z = x + y\,\mathrm{i}$ definiert man die **komplex konjugierte Zahl** $\overline{z} \in \mathbb{C}$ durch

$$\overline{z} := x + (-y)\,\mathrm{i} = x - y\,\mathrm{i}\,.$$

Anmerkung: Die Konjugation ändert das Vorzeichen des Imaginärteils und entspricht daher einer Spiegelung an der reellen Achse.

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Proposition: Eigenschaften der Konjugierten

Seien $z = x + y\,\mathrm{i}$ und $w = u + v\,\mathrm{i}$ komplexe Zahlen. Dann gilt

1. $\mathrm{Re}(\overline{z}) = \mathrm{Re}(z)$ und $\mathrm{Im}(\overline{z}) = -\mathrm{Im}(z)$,
2. $|z| = \sqrt{x^2 + y^2} = \sqrt{x^2 + (-y)^2} = |\overline{z}|$,
3. $\overline{\overline{z}} = z$,
4. $z = \overline{z} \quad \Leftrightarrow \quad z \in \mathbb{R}$,
5. $\overline{z + w} = \overline{z} + \overline{w}$,
6. $\overline{zw} = \overline{z} \cdot \overline{w}$,
7. $z + \overline{z} = 2\,\mathrm{Re}(z)$,
8. $z - \overline{z} = 2\,\mathrm{i}\,\mathrm{Im}(z)$,

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Beispiele:

$$
\begin{array}{lll}
z_1 = 3 + 4\,\mathrm{i} & z_2 = 3 - 4\,\mathrm{i} & z_3 = -3 + 4\,\mathrm{i} \\
z_4 = -2 + 0\,\mathrm{i} & z_5 = 0 + \mathrm{i} & z_6 = -3 - 4\,\mathrm{i}
\end{array}
$$

Die Zahlen haben folgende Eigenschaften:

$$
\begin{array}{ll}
\mathrm{Re}(z_1) = 3, & \mathrm{Im}(z_1) = 4, \\
\mathrm{Re}(z_2) = 3, & \mathrm{Im}(z_2) = -4, \\
\overline{z_1} = z_2, & \overline{z_6} = z_3, \\
 & \\
|z_4| = 2, & |z_5| = 1, \\
\overline{z_5} = i(-1), & \overline{z_4} = z_4 \\
|z_1| = \sqrt{3^2 + 4^2} = 5 & |z_2| = \sqrt{3^2 + (-4)^2} = 5.
\end{array}
$$

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Definition: Polarkoordinaten, Polarform, Exponentialform

Sei $z = x + y\,\mathrm{i} \in \mathbb{C} \setminus \{0\}$. Seien $r = |z|$ und φ der Winkel zwischen positiver reeller Achse und dem Vektor z im Bogenmaß. Dann gilt folgender Zusammenhang zwischen den kartesischen Koordinaten (x, y) und den **Polarkoordinaten** (r, φ)

$$x = r \cdot \cos(\varphi), \quad y = r \cdot \sin(\varphi)$$

und wir schreiben z in der **Polarform**

$$z = r \cdot (\cos(\varphi) + \mathrm{i}\sin(\varphi)).$$

Eine weitere Darstellung ist die **Exponentialform**

$$z = re^{\mathrm{i}\,\varphi}.$$

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Anmerkungen:

- Wir werden im nächsten Semester die Euler-Formel

$$e^{\mathrm{i}\,\varphi} = \cos(\varphi) + \mathrm{i}\sin(\varphi)$$

  beweisen.
- Diese liefert übrigens die berühmte Identität

$$e^{\mathrm{i}\,\pi} + 1 = 0$$

- **Interpretation:** Eine komplexe Zahl können wir als **Drehung** des Vektors $(1, 0)$ um den Winkel φ gegen den Uhrzeigersinn bei gleichzeitiger **Streckung** um den Faktor r interpretieren.

Proposition

Sei $z = x + y\,\mathrm{i}$. Dann gilt für den Radius r und das Argument $\varphi \in [0, 2\pi)$ von z

$$r = |z| = \sqrt{x^2 + y^2}, \quad \tan(\varphi) = \frac{y}{x}.$$

Bei der Umkehrfunktion arctan des Tangens gilt es, den Quadranten zu beachten:

$$\varphi = \begin{cases} \arctan\left|\frac{y}{x}\right|, & z \text{ im 1. Quadrant,} \\ -\arctan\left|\frac{y}{x}\right| + \pi, & z \text{ im 2. Quadrant,} \\ \arctan\left|\frac{y}{x}\right| + \pi, & z \text{ im 3. Quadrant,} \\ \arctan\left|\frac{y}{x}\right| + 2\pi, & z \text{ im 4. Quadrant.} \end{cases}$$

6.2 Komplexe Zahlen: Gauß'sche Zahlenebene

Aufgabe:
Bestimmen Sie für die folgenden komplexen Zahlen jeweils die Normal-, Polar- und Exponentialform

$$\begin{array}{lll} z_1 = \sqrt{3} + \mathrm{i} & z_2 = \sqrt{2}e^{\mathrm{i}\cdot\frac{\pi}{4}} & z_3 = \mathrm{i} \\ z_4 = -3 & z_5 = 2e^{\mathrm{i}\cdot\frac{3\pi}{2}} & z_6 = -\mathrm{i}. \end{array}$$

6.3 Komplexe Rechnung

6.3 Komplexe Zahlen: Komplexe Rechnung

Beobachtungen in $\mathbb{R}$:

- In $\mathbb{R}$ nutzen wir die Subtraktion als Umkehrung der Addition bzw. die Division als Umkehrung der Multiplikation.
- Für alle $x \in \mathbb{R}$ existiert das additive Inverse $-x$ und für alle $x \in \mathbb{R} \setminus 0$ existiert das multiplikative Inverse $x^{-1} = \frac{1}{x}$.

Überlegungen in $\mathbb{C}$:

- Für alle $z = x + y\,\mathrm{i} \in \mathbb{C}$ ist das additive Inverse $-z$ offensichtlich $-z := (-1) \cdot z = -x - y\,\mathrm{i}$.
- Wie aber dividieren wir sinnvoll durch eine komplexe Zahl bzw. was ist z^{-1}?

6.3 Komplexe Zahlen: Komplexe Rechnung

Idee: Wir nutzen die Eigenschaften, dass $z \cdot \overline{z} = |z|^2$ eine reelle Zahl ist.

$$z \cdot \overline{z} = (x + y\,\mathrm{i})(x - y\,\mathrm{i}) = x^2 - y^2\,\mathrm{i}^2 = x^2 + y^2 = |z|^2$$

Somit finden wir das multiplikativ inverse Element

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

Damit lässt sich auch eine Division zweier komplexer Zahlen z_1, z_2 formulieren:

$$\frac{z_1}{z_2} := z_1 \cdot z_2^{-1}.$$

Proposition: Das Multiplikative Inverse

Für $z = x + y\,\mathrm{i} \in \mathbb{C} \setminus \{0\}$ gibt es genau ein multiplikatives Inverses, bezeichnet mit $z^{-1} = \frac{1}{z}$, d.h. z^{-1} ist das einzige Element für das gilt

$$z \cdot z^{-1} = z^{-1} \cdot z = 1.$$

Darüber hinaus gilt

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

6.3 Komplexe Zahlen: Komplexe Rechnung

Körperaxiome von $(\mathbb{C}, +, \cdot)$

1. Assoziativität der Addition: für alle $z_1, z_2, z_3 \in \mathbb{C}$ gilt
$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3,$$
2. Kommutativität der Addition: für alle $z_1, z_2 \in \mathbb{C}$ gilt
$$z_1 + z_2 = z_2 + z_1,$$
3. Neutrales Element der Addition: für alle $z \in \mathbb{C}$ gilt
$$\exists 0 := 0 + 0 \cdot \mathrm{i} \in \mathbb{C} : \quad z + 0 = z,$$

6.3 Komplexe Zahlen: Komplexe Rechnung

Körperaxiome von $(\mathbb{C}, +, \cdot)$

4. Inverses Element der Addition: für alle $z \in \mathbb{C}$ gilt

$$\exists \ (-z) := (-1) \cdot z \in \mathbb{C} : \quad z + (-z) = 0.$$

5. Assoziativität der Multiplikation: für alle $z_1, z_2, z_3 \in \mathbb{C}$ gilt

$$z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) + z_3,$$

6. Kommutativität der Multiplikation: für alle $z_1, z_2 \in \mathbb{C}$ gilt

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

6.3 Komplexe Zahlen: Komplexe Rechnung

Körperaxiome von $(\mathbb{C}, +, \cdot)$

7. Neutrales Element der Multiplikation: für alle $z \in \mathbb{C}$ gilt

$$\exists\ 1 := 1 + 0 \cdot \mathrm{i} \in \mathbb{C} : \quad 1 \cdot z = z,$$

8. Inverses Element der Multiplikation: für alle $z = x + y\,\mathrm{i} \in \mathbb{C} \setminus \{0\}$ gilt

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

9. Distributivität: für alle $z_1, z_2, z_3 \in \mathbb{C}$ gilt

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3.$$

Proposition: Multiplikation und Division in Exponentialform

Seien $z_1 = r_1 e^{\mathrm{i}\varphi_1}$ und $z_2 = r_2 e^{\mathrm{i}\varphi_2}$ gegebene komplexe Zahlen. Dann ist das **Produkt** dieser Zahlen gegeben durch

$$z_1 \cdot z_2 = (r_1 \cdot r_2) e^{\mathrm{i}(\varphi_1 + \varphi_2)}.$$

Für $z_2 \neq 0$ ist der **Quotient** von z_1 und z_2 gegeben durch

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} e^{\mathrm{i}(\varphi_1 - \varphi_2)}.$$

Anmerkungen:

- Hier erkennt man wieder die Eigenschaft einer Drehstreckungen.
- Faustregel: Multiplikation/Division in Polarform, Addition/Subtraktion in Normalform.
- In Polarform gilt analog:

$$z_1 \cdot z_2 = r_1 r_2 \cdot (\cos(\varphi_1 + \varphi_2) + \mathrm{i} \sin(\varphi_1 + \varphi_2)).$$

6.3 Komplexe Zahlen: Komplexe Rechnung

Aufgabe:
Leiten Sie mit Hilfe der Identität

$$e^{(\alpha+\beta)\,\mathrm{i}} = e^{\alpha\,\mathrm{i}} \cdot e^{\beta\,\mathrm{i}}$$

die folgenden Additionstheoreme her:

$$\begin{aligned} \sin(\alpha+\beta) &= \cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\beta) \\ \cos(\alpha+\beta) &= \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta). \end{aligned}$$

6.3 Komplexe Zahlen: Komplexe Rechnung

Korollar: Potenzen und Wurzeln

Sei $z = re^{\mathrm{i}\varphi}$ eine gegebene komplexe Zahl. Dann ist die **Potenz** dieser Zahlen gegeben durch

$$z^n = r^n e^{\mathrm{i}\cdot n\varphi} = r^n(\cos(n\varphi) + \mathrm{i}\sin(n\varphi)).$$

Die n-ten **Einheitswurzeln** von z sind komplexe Zahlen w_k mit $w_k^n = z$:

$$w_k = \sqrt[n]{r} e^{\mathrm{i}\cdot \frac{\varphi + 2\pi k}{n}}, \quad k = 0, \ldots, n-1.$$

(Formel von Moivre)

Anmerkung: Die Einheitswurzeln verteilen sich äquidistant auf dem Kreis mit Radius $\sqrt[n]{r}$ um den Ursprung.

6.3 Komplexe Zahlen: Komplexe Rechnung

Beispiele:

- Für die Potenzen von i gilt zyklisch

$$\mathrm{i}^2 = -1, \quad \mathrm{i}^3 = \mathrm{i}\cdot\mathrm{i}^2 = -\mathrm{i}, \quad \mathrm{i}^4 = (-1)(-1) = 1, \quad \mathrm{i}^5 = \mathrm{i}, \quad \dots$$

- Für die Inverse von i gilt:

$$\mathrm{i}^{-1} = \frac{1}{\mathrm{i}} = \frac{\bar{\mathrm{i}}}{|\,\mathrm{i}\,|^2} = \frac{-\mathrm{i}}{1} = -\mathrm{i}\,.$$

- Betrachte die komplexen Zahlen $z_1 = 4 - 8\,\mathrm{i}$, $z_2 = 3 + 4\,\mathrm{i}$. Dann gilt

$$\begin{aligned}\frac{z_1}{z_2} &= z_1 \cdot (z_2)^{-1} = z_1 \cdot \frac{\overline{z}_2}{|z_2|^2} = (4 - 8\,\mathrm{i}) \cdot \left(\frac{3}{25} + \mathrm{i}\,\frac{-4}{25}\right) \\ &= \left(\frac{12}{25} - \frac{32}{25}\right) + \mathrm{i}\left(-\frac{24}{25} - \frac{16}{25}\right) \\ &= -\frac{4}{5} - \mathrm{i}\,\frac{8}{5}.\end{aligned}$$

6.3 Komplexe Zahlen: Komplexe Rechnung

Beispiele:

- Betrachte die komplexen Zahlen

$$z_1 = 3e^{\mathrm{i}\cdot\frac{\pi}{5}}, \quad z_2 = 2e^{\mathrm{i}\cdot\frac{\pi}{6}}.$$

Dann gilt für das Produkt

$$z_1 \cdot z_2 \quad = \quad (2\cdot 3)e^{\mathrm{i}\left(\frac{\pi}{5}+\frac{\pi}{6}\right)} = 6e^{\mathrm{i}\,\frac{11\pi}{30}}.$$

Der Quotient ergibt

$$\frac{z_1}{z_2} \quad = \quad \frac{3}{2}e^{\mathrm{i}\left(\frac{\pi}{5}-\frac{\pi}{6}\right)} = \frac{3}{2}e^{\mathrm{i}\,\frac{\pi}{30}}.$$

6.3 Komplexe Zahlen: Komplexe Rechnung

Aufgaben:

1. Seien $z = -\,\mathrm{i}^{23} + 3\,\mathrm{i}^{14}$ und $w = 2\,\mathrm{i}^5 - \mathrm{i}^{24}$. Bestimmen Sie
$$z + w, \quad z \cdot w, \quad \frac{z}{w}, \quad \frac{w}{\overline{z}}.$$
2. Für welche z gilt folgende Gleichung?
$$2 - 9\,\mathrm{i} = (1 - 2\,\mathrm{i})(z - 3 + 4\,\mathrm{i})$$
3. Skizzieren Sie die Menge aller $z \in \mathbb{C}$, für die gilt
$$|z - \mathrm{i}\,| = |z + (2 - 3\,\mathrm{i})|.$$

6.4 Der Fundamentalsatz der Algebra

Allgemeine Lösungsformel für quadratische Gleichungen

Seien $a \in \mathbb{R} \setminus \{0\}$, $b, c \in \mathbb{R}$ und die Diskriminante $D := b^2 - 4ac$. Dann besitzt die quadratische Gleichung $az^2 + bz + c = 0$ im Fall

- $D > 0$ zwei verschiedene reelle Lösungen: $\quad z_{1,2} = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$,
- $D = 0$ eine (doppelte) reelle Lösung: $\quad z_{1,2} = -\dfrac{b}{2a}$,
- $D < 0$ zwei konjugiert komplexe Lösungen: $\quad z_{1/2} = \dfrac{-b}{2a} \pm \dfrac{\sqrt{|b^2 - 4ac|}}{2a}\mathrm{i}$

und das Polynom zerfällt (über $\mathbb{C}$) stets in Linearfaktoren:

$$az^2 + bz + c = a(z - z_1)(z - z_2).$$

6.4 Komplexe Zahlen: Der Fundamentalsatz

Fundamentalsatz der Algebra

Sei $a_k \in \mathbb{R}$ für $0 \leq k \leq n-1$ die Koeffizienten eines Polynoms p vom Grad n über den komplexen Zahlen $\mathbb{C}$:

$$p(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0, \quad z \in \mathbb{C}.$$

- Dann gibt es n (nicht notwendigerweise) verschiedene komplexe Nullstellen $z_1, \ldots, z_n$, d.h. $p(z_k) = 0, \quad 1 \leq k \leq n$.
- Hierbei treten nicht-reelle Lösungen in komplex konjugierten Paaren auf. Darüber hinaus zerfällt p über $\mathbb{C}$ vollständig in Linearfaktoren, d.h. es gilt

$$p(z) = (z - z_1) \cdot (z - z_2) \cdot \ldots \cdot (z - z_n) = \prod_{k=1}^{n} (z - z_k).$$

6.4 Komplexe Zahlen: Der Fundamentalsatz

Beispiel: Das Poylnom dritten Grades

$$p(z) = z^3 - z^2 + 4z - 4$$

hat drei Nullstellen $z_1, z_2, z_3 \in \mathbb{C}$. Durch 'Raten' erkennt man, dass $z_1 = 1$ eine Lösung der Gleichung $p(z) = 0$ ist:

$$p(1) = 1^3 - 1^2 + 4 \cdot -4 = 0.$$

Eine **Polynomdivision** liefert

$$(z^3 - z^2 + 4z - 4) : (z - 1) = z^2 + 4.$$

Die restlichen Nullstellen erhalten wir z.B. durch Faktorisieren:

$$z^2 + 4 = z^2 - (-4) = z^2 - (2\,\mathrm{i})^2 = (z - 2\,\mathrm{i})(z + 2\,\mathrm{i}) \quad \Rightarrow \quad z_{2/3} = \pm 2\,\mathrm{i}\,.$$

Bemerkungen:

- Beim Raten einer Nullstelle hilft es zu wissen, dass ganzzahlige Nullstellen Teiler des konstanten Koeffizienten a_0 sein müssen, d.h. bei

$$p(z) = a_n z^n + \ldots + a_2 z^2 + a_1 z + 6$$

  sollten man die Zahlen $\pm 1, \pm 2, \pm 3$ oder ± 6 testen.
- Es gibt auch allgemeine Formeln für Polynome dritten Grades (*cardanische Formeln*) und vierten Grades:

  https://de.wikipedia.org/wiki/Cardanische_Formeln
- Es gibt dagegen keine allgemeinen Formeln für Polynome vom Grad $n = 5$ oder höher, die nur die Grundrecharten und Wurzelziehen benötigen.

7. Vektorräume

7. Vektorräume

Ausblick:

- Die **Lineare Algebra** befasst sich u.a. mit **linearen Abbildungen** sowie **linearen Gleichungssystemen** und deren Lösungsverhalten.
- Die Zustandsräume, in denen die lineare Abbildungen defininert sind, nennen wir **Vektorräume**.
- Ebenso werden lineare Gleichungssysteme und deren Lösungen in diesen Räumen formuliert.
- **Ziel** ist es, eine Lösungstheorie zu entwickeln, die uns erlaubt eine Aussage über die **Existenz** und die **Eindeutigkeit** der Lösung zu treffen.

7. Vektorräume

Ausblick:

- Darüber hinaus stellen wir das Gauß-Jordan-Verfahren zur Lösung eines LGS vor.
- Im weiteren Verlauf werden wir uns mit linearen Abbildungen wie Drehung, Spiegelungen, Streckung und Projektionen beschäftigen.
- Determinante, Inverse, Eigenwerte und Eigenvektoren von Matrizen.
- Abschließend betrachten wir noch numerische Methoden zur Lösung linearer Gleichungssysteme.

7.1 Allgemeine Vektorräume

7.1 Allgemeine Vektorräume: Definition

Definition: Vektorraum

Eine algebraische Struktur in Form einer Menge V zusammen mit einer Additionsverknüpfung

$$+ : V \times V \to V, \quad (v_1, v_2) \mapsto +(v_1, v_2) := v_1 + v_2$$

und einer Verknüpfung skalare Multiplikation

$$\cdot : \mathbb{R} \times V \to V, \quad (\lambda, v) \mapsto \cdot(\lambda, v) := \lambda \cdot v$$

heißt **reeller Vektorraum** ($\mathbb{R}$-Vektorraum), wenn für die Verknüpfungen '$+$' und '$\cdot$' die folgenden Axiome gelten. Wir schreiben dann auch kurz V statt $(V, +, \cdot)$ und nennen die Elemente des $\mathbb{R}$-Vektorraums V **Vektoren**.

Proposition: Vektorraumaxiome

Für die Addition gelten folgende Regeln:

1. **Assoziativität:** für alle $x, y, z \in V$ gilt
$$(x+y)+z = x+(y+z).$$
2. **Kommutativität:** für alle $x, y \in V$ gilt
$$x+y = y+x.$$
3. **Neutralelement:** es gibt genau ein Element $\mathbb{O} \in V$, sodass für alle $x \in V$
$$x+\mathbb{O} = x.$$
4. **Additives Inverses:** für alle $x \in V$ gibt es ein Element $y \in V$, sodass
$$x+y = \mathbb{O}.$$

7.1 Allgemeine Vektorräume: Definition

Proposition: Vektorraumaxiome

Für die skalare Multiplikation gilt:

5. **Assoziativität:** $\forall\ \lambda, \mu \in \mathbb{R}$ und $x \in V$ gilt $\lambda \cdot (\mu x) = (\lambda\mu) \cdot x$.
6. **Neutrales Element:** $\forall\ x \in V$ gilt $1 \cdot x = x$.

Schließlich fordern wir noch die **Distributivgesetze**

7. $\forall\ \lambda \in \mathbb{R}$ und $x, y \in V$ gilt $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$.
8. $\forall\ \lambda, \mu \in \mathbb{R}$ und $x \in V$ gilt $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$.

7.1 Allgemeine Vektorräume: Definition

Anmerkungen:

- Statt einem $\mathbb{R}$-Vektorraum können wir Vektorräume auch über anderen Körpern wie z.B. $\mathbb{Q}$ oder $\mathbb{C}$ definieren.
- Klassische Beispiele für Vektorräume sind die Ebene des $\mathbb{R}^2$ oder der dreidimensionale Raum $\mathbb{R}^3$.
- Wir können aber auch abstraktere Vektorräume betrachten:
  1. der n dimensionale Vektorraum $\mathbb{R}^n$, $n \in \mathbb{N}$,
  2. der Vektorraum der reellen Folgen $(a_1, a_2, \ldots, a_n)$,
  3. der reelle Vektorraum der komplexen Zahlen $\mathbb{C}^n$ mit $\cdot : \mathbb{R} \times \mathbb{C}^n \to \mathbb{C}^n$,
  4. der komplexe Vektorraum der komplexen Zahlen $\mathbb{C}^n$ mit $\cdot : \mathbb{C} \times \mathbb{C}^n \to \mathbb{C}^n$,
  5. der Vektorraum der Matrizen,
  6. der Vektorraum der stetigen Funktionen, etc.

7.1 Allgemeine Vektorräume: Definition

Anmerkungen:

- Dagegen ist $(\mathbb{R}^2, +, \cdot)$ mit $\cdot : \mathbb{C} \times \mathbb{R}^2$ kein Vektorraum, da z.B. $\mathrm{i} \cdot (1, 1) = (i, i) \notin \mathbb{R}^2$.
- Ebenso ist $[0, 1]$ kein Vektorraum, da z.B. $0.8 + 0.6 = 1.4 \notin [0, 1]$
- Im Allgemeinen gibt es in Vektorräumen keine (innere) Multiplikation, wie man sie in etwa $\mathbb{R}^n$ durch

$$* : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n, (x, y) \mapsto (x_1 \cdot y_1, \ldots, x_n \cdot y_n)$$

definieren könnte. Erst recht kann man also i.A. nicht durch Vektoren dividieren!

7.1 Allgemeine Vektorräume: Beispiel

Beispiel: Wir betrachten die Menge

$$V := \{f \mid f : [0,1] \to \mathbb{R} \ \text{ist eine Funktion}\}$$

Wir wollen zeigen, dass V zu einem $\mathbb{R}$-Vektorraum gemacht werden kann. Dafür definieren wir punktweise die Verknüpfungen

$$\begin{array}{llllll} +: & V \times V \to V, & (f,g) & \mapsto & [+(f,g)](x) & := & f(x)+g(x), & x \in [0,1], \\ \cdot: & \mathbb{R} \times V \to V, & (\lambda, f) & \mapsto & [\cdot(\lambda,f)](x) & := & \lambda f(x), & x \in [0,1]. \end{array}$$

Wir schreiben wieder kurz $f + g := +(f,g)$ und $\lambda \cdot f := \cdot(\lambda, f)$ für die resultierenden Funktionen und nennen zwei Funktionen gleich, d.h. $f = g$, wenn sie in allen Funktionswerten übereinstimmen, d.h. $f(x) = g(x)$ für alle $x \in [0,1]$.

7.1 Allgemeine Vektorräume: Beispiel

Vorgehen:

- Offensichtlich sind $f + g$ und $\lambda \cdot f$ durch diese Definition wieder Funktionen auf $[0, 1]$ mit Werten in $\mathbb{R}$.
- Die Funktionen sind damit wohldefiniert und die Verknüpfungen sind abgeschlossen.
- Um zu beweisen, dass V zusammen mit diesen Verknüpfungen ein Vektorraum wird, müssen wir die acht Axiome nachweisen.
- Dazu müssen wir jeweils die Gleichheit von Funktionen nachweisen, indem wir zeigen, dass diese in *allen* Funktionswerten übereinstimmen.

7.1 Allgemeine Vektorräume: Beispiel

1. **Assoziativität der Addition:** für alle $f, g, h \in V$ gilt

$$\begin{aligned}
[(f+g)+h](x) &= [f+g](x) + h(x) \\
&= (f(x)+g(x)) + h(x) \\
&= f(x) + (g(x)+h(x)) \\
&= f(x) + [g+h](x) \\
&= [f+(g+h)](x), \quad x \in [0,1].
\end{aligned}$$

2. **Kommutativität der Addition:** für alle $f, g \in V$ gilt

$$\begin{aligned}
[f+g](x) &= f(x) + g(x) \\
&= g(x) + f(x) \\
&= [g+f](x), \quad s \in [0,1].
\end{aligned}$$

7.1 Allgemeine Vektorräume: Beispiel

3. Neutralelement der Addition: Wir definieren die Nullfunktion $\mathbb{O}$ durch

$$\mathbb{O} : [0,1] \to \mathbb{R}, \quad x \mapsto \mathbb{O}(x) := 0,$$

sodass $f + \mathbb{O} = f$ für alle $f \in V$ gilt

$$\begin{aligned} [f + \mathbb{O}]\,(x) &= f(x) + \mathbb{O}(x) \\ &= f(x) + 0 \\ &= f(x), \quad x \in [0,1]. \end{aligned}$$

Streng genommen, müssten wir noch zeigen, dass $\mathbb{O}$ die einzige Funktion in V ist, die diese Eigenschaft hat (**Übung!**).

7.1 Allgemeine Vektorräume: Beispiel

4. Inverse Element der Addition: Wir definieren die in V liegende Funktion

$$-f : [0,1] \to \mathbb{R}, \quad x \mapsto (-f)(x) := -f(x),$$

sodass $f + (-f) = \mathbb{O}$ für alle $f \in V$ gilt

$$\begin{aligned} [f + (-f)]\,(x) &= f(x) + (-f)(x) \\ &= f(x) - f(x) \\ &= 0 \\ &= \mathbb{O}(x), \;\; x \in [0,1]. \end{aligned}$$

Damit sind die Regeln für die **Addition nachgewiesen**.

7.1 Allgemeine Vektorräume: Beispiel

5. Assoziativität der skalaren Multiplikation: für alle $\lambda, \mu \in \mathbb{R}$ und alle $f \in V$ gilt

$$\begin{aligned} [\lambda(\mu f)](x) &= \lambda \cdot ([\mu f](x)) \\ &= \lambda(\mu f(x)) \\ &= (\lambda\mu) \cdot f(x) \\ &= [(\lambda\mu) f](x), \quad x \in [0,1]. \end{aligned}$$

6. Neutralelement der skalaren Multiplikation: $\exists r \in \mathbb{R}$, sodass für alle $f \in V$ gilt

$$\begin{aligned} [1 \cdot f](x) &= 1 \cdot f(x) \\ &= f(x), \quad x \in [0,1]. \end{aligned}$$

7.1 Allgemeine Vektorräume: Beispiel

7. **Distributivgesetz I:** für alle $\lambda \in \mathbb{R}$ und alle $f, g \in V$ gilt

$$\begin{aligned} [\lambda \cdot (f+g)]\,(x) &= \lambda\,[f+g]\,(x) \\ &= \lambda(f(x)+g(x)) \\ &= \lambda f(x) + \lambda g(x) \\ &= [\lambda f]\,(x) + [\lambda g]\,(x), \quad s \in [0,1], \end{aligned}$$

8. **Distributivgesetz II:** für alle $\lambda, \mu \in \mathbb{R}$ und alle $f \in V$ gilt

$$\begin{aligned} [(\lambda+\mu) f]\,(x) &= (\lambda+\mu) \cdot f(x) \\ &= \lambda f(x) + \mu f(x) \\ &= [\lambda f](x) + [\mu f](x), \quad x \in [0,1]. \end{aligned}$$

Damit ist $(V, +, \cdot)$ ein $\mathbb{R}$-Vektorraum ist, der Vektorraum der reellwertigen Funktionen auf dem Intervall $[0,1]$. Dieser und seine Unterräume spielen eine herausragende Rolle in der Analysis.

7.1 Allgemeine Vektorräume: Aufgaben

Aufgaben:

1. Zeigen Sie, dass die Ebene E

$$E = s \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad s, t \in \mathbb{R},$$

   mit der üblichen Addition und skalaren Multiplikation ein Vektorraum ist.

2. Zeigen Sie, dass die Kugel $K = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$ kein Vektorraum ist.

7.2 Unterräume

7.2 Unterräume: Definition

Definition: Unterraum

Sei V ein Vektorraum und U eine nicht-leere Teilmenge von V. Dann heißt U ein **Unterraum von** V, wenn U bezüglich der Vektoraddition und skalaren Multiplikation abgeschlossen ist. Das heißt

- für alle $x, y \in U$ ist auch $x + y \in U$,
- für alle $\lambda \in \mathbb{R}$ und $x \in U$ ist auch $\lambda x \in U$-

Wir schreiben dann $U \leq V$.

7.2 Unterräume: Eigenschaften

Proposition: Eigenschaften von Unterräumen

Ist V ein $\mathbb{R}$-Vektorraum und $U \leq V$ dann gilt:

- Der Nullvektor $\mathbb{O}$ aus V ist auch in U enthalten.
- Mit $x \in U$ ist auch sein Inverses $-x$ in U.
- U ist selbst wieder ein $\mathbb{R}$-Vektorraum (mit den auf diesen beschränkten Verknüpfungen).

Darüber hinaus gilt:

- V enthält immer die trivialen Unterräume $\{\mathbb{O}\}$ und V.
- Gilt $U_1, U_2 \leq V$ so ist $U_1 \cap U_2 \leq V$. Dies ist der größte Vektorraum, der sowohl in U_1 als auch in U_2 enthalten ist.

7.2 Unterräume: Beispiele

Anmerkungen/Beispiele:

- Ob eine Teilmenge U eines Vektorraums V ebenfalls ein Vektorraum ist, lässt sich statt durch Nachweis der 8 Vektorraumaxiome auch durch Nachweis der Unterraum-Eigenschaften zeigen:
  1. U enthält das Nullelement von V, ist also nicht leer,
  2. U ist bezüglich der Addition abgeschlossen,
  3. U ist bezüglich der skalaren Multiplkation abgeschlossen.
- Der $\mathbb{R}$-Vektorraum $\mathbb{R}$ enthält nur die trivialen Unterräume $\{0\}$ und sich selbst, denn mit einer Zahl müssen auch schon alle Vielfachen enthalten sein.
- Neben den trivialen Unterräumen $\{(0,0)\}$ und $\mathbb{R}^2$ enthält der $\mathbb{R}^2$ nur noch die Ursprungsgeraden als Unterräume. Jede andere Gerade kann kein Unterraum sein, da $(0,0)$ in jedem Unterraum enthalten sein muss.

7.2 Unterräume: Beispiele

Anmerkungen/Beispiele:

- Nicht-triviale Unterräume des $\mathbb{R}^3$ sind wiederum die Ursprungsgeraden und alle Ebenen, die den Ursprung enthalten. Schneidet man eine Ursprungsgerade mit solch einer Ebene (oder mit einer anderen Ursprungsgeraden) so erhält man den trivialen Unterraum $\{\mathbb{O}\}$. Schneidet man zwei verschiedene Ebenen, die durch den Ursprung gehen, so erhält man als Unterraum eine Ursprungsgerade.
- Die *Ursprungsgerade* $U := \{x \in \mathbb{R}^n \mid x_1 = \ldots = x_n\}$ ist ein Unterraum des $\mathbb{R}^n$. Ist nämlich $x = (x_1, \ldots, x_1)$ und $y = (y_1, \ldots, y_1)$ und $\lambda \in \mathbb{R}$ so gilt

$$\begin{aligned} \mathbb{O} = (0, \ldots, 0) \in U \quad &\Rightarrow \quad U \neq \emptyset, \\ x + y \quad &= \quad (x_1 + y_1, \ldots, x_n + y_n) \in U, \\ \lambda \cdot x \quad &= \quad (\lambda x_1, \ldots, \lambda x_n) \in U. \end{aligned}$$

7.2 Unterräume: Beispiele

Anmerkungen/Beispiele:

- Die Menge der Polynome

$$P := \left\{ f : [0,1] \to \mathbb{R} \;\middle|\; \exists\, k \geq 0,\ a_1, \ldots, a_k \in \mathbb{R} :\ \ f(x) = \sum_{m=0}^{k} a_m x^m \ \forall\, x \in [0,1] \right\}$$

  ist ein Unterraum der Menge aller reellwertigen Funktionen auf $[0,1]$. Denn die Summe von zwei Polynomen ist wieder ein Polynom (Koeffizientenaddition!) und das mit einem Skalar λ multiplizierte ebenfalls (alle Koeffizienten werden mit λ multipliziert!).
- Wir werden später noch sehen, dass die Lösungsmenge eines homogenen linearen Gleichungssystems in n Unbekannten ein Unterraum des $\mathbb{R}^n$ ist.

7.2 Unterräume: Aufgaben

Aufgaben:

1. Zeigen Sie, dass
$$U = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + 2z = 0\}$$
ein Unterraum des $\mathbb{R}^3$ ist.
2. Untersuchen Sie, ob $U = \{(x, y, z) \in \mathbb{R}^3 \mid x \cdot y \cdot z = 0\}$ ein Unterraum des $\mathbb{R}^3$ ist.
3. Zeigen Sie, dass
$$V = \{f \mid f : [0, 1] \to \mathbb{R},\ \ x \mapsto f(x) := ax^2,\ \ a \in \mathbb{R}\}$$
ein Vektorraum ist.

7.3 Länge und Winkel im $\mathbb{R}^n$

7.3 Länge und Winkel im $\mathbb{R}^n$: Euklidische Norm

Definition: Euklidische Norm

Sei $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Dann definieren wir die **euklidische Norm** des Vektors x durch

$$\|x\|_2 := \sqrt{x_1^2 + \ldots + x_n^2}.$$

Wir assoziieren diese mit der Länge des Vektors x und dem Abstand des Punkts x vom Ursprung.

Beispiel:

- Im Fall des $\mathbb{R}^1$ entspricht die Norm gerade dem Betrag einer Zahl, d.h.

$$\|x\|_2 = \sqrt{x_1^2} = |x_1|$$

- Im Fall des $\mathbb{R}^2$ (oder des $\mathbb{R}^3$) ergibt sich mit dem Satz des Pythagoras, dass die Norm eines Vektors x, also

$$\|(x_1, x_2)\|_2 = \sqrt{x_1^2 + x_2^2}$$

gerade der Abstand vom Ursprung ist. So ist etwa der Vektor $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$ auf dem Einheitskreis zu finden, denn

$$\left\|\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)\right\|_2 = \sqrt{\frac{1}{\sqrt{2}^2} + \frac{1}{\sqrt{2}^2}} = 1.$$

7.3 Länge und Winkel im $\mathbb{R}^n$: Euklidische Norm

Beispiel:

- Die Standardeinheitsvektoren $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$ des $\mathbb{R}^n$ haben alle Norm 1.
- Da diese Norm jedem Vektor genau eine Zahl zuordnet, kann sie als Abbildung interpretiert werden, indem man einfach definiert

$$\|\cdot\|_2 : \mathbb{R}^n \to \mathbb{R}, \ \ x \mapsto \|x\|_2 := \sqrt{x_1^2 + \ldots + x_n^2}$$

- Achtung: Im Allgemeinen gilt $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$ für $x, y \in \mathbb{R}$ (z.B. $x = 4$, $y = 9$). Insbesondere gilt im Allgemeinen

$$\|(x_1, \ldots, x_n)\|_2 = \sqrt{x_1^2 + \ldots + x_n^2} \neq |x_1| + |x_2| + \ldots + |x_n|.$$

Proposition: Eigenschaften der Norm

- **Positivität:** für alle $x \in \mathbb{R}^n \setminus \{\mathbb{O}\}$ gilt $\|x\|_2 > 0$.
- **Definitheit:** es gilt $\|x\|_2 = 0$ genau dann, wenn $x = (0, \dots, 0)$.
- **Homogenität:** für alle $\lambda \in \mathbb{R}$, $x \in \mathbb{R}^n$ gilt

$$\|\lambda x\|_2 = |\lambda| \cdot \|x\|_2.$$

- **Dreiecksungleichung:** für alle $x, y \in \mathbb{R}^n$ gilt

$$\|x + y\|_2 \leq \|x\|_2 + \|y\|_2.$$

7.3 Länge und Winkel im $\mathbb{R}^n$: Skalarprodukt

Definition: Skalarprodukt, Winkel

Seien $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$. Dann heißt

$$\langle x, y\rangle := x_1 \cdot y_1 + x_2 \cdot y_2 + \ldots + x_n \cdot y_n$$

das **euklidische Skalarprodukt** der Vektoren x und y. Der **Winkel** $\alpha(x, y)$ zwischen diesen beiden Vektoren ist definiert durch

$$\cos(\alpha(x, y)) := \frac{\langle x, y\rangle}{\|x\|_2 \cdot \|y\|_2}, \quad 0 \leq \alpha(x, y) \leq 180^\circ.$$

7.3 Länge und Winkel im $\mathbb{R}^n$: Skalarprodukt

Bemerkungen/Beispiele:

- Im $\mathbb{R}^2$ handelt es sich bei $\alpha(x, y)$ um den anschaulichen Winkel zwischen zwei Vektoren x und y.
- Für zwei verschiedene Standardeinheitsvektoren e_i und e_j gilt

  $$\langle e_i, e_j \rangle = 0$$

  und damit $\alpha(e_i, e_j) = 90^\circ$, die Einheitsvektoren stehen also **orthogonal** aufeinander.
- Allgemein: Zwei Vektoren x und $y \in \mathbb{R}^n$ stehen genau dann orthogonal aufeinander, wenn $\langle x, y \rangle = 0$.

7.3 Länge und Winkel im $\mathbb{R}^n$: Skalarprodukt

Bemerkungen/Beispiele:

- Oft wird das Skalarprodukt von x, $y \in \mathbb{R}^n$ auch durch $x \cdot y$ geschrieben. Es handelt sich aber um kein Produkt im eigentlichen Sinne, denn $x \cdot y$ ist eine reelle Zahl, kein Vektor. Insbesondere macht ein Ausdruck $x \cdot y \cdot z$ keinerlei Sinn, denn i.A. gilt *kein Assoziativgesetz*, d.h.

$$(x \cdot y) \cdot z \neq x \cdot (y \cdot z).$$

  Beide Seiten stellen hier einen Vektor dar. Links wird z um den Wert des Skalarprodukt $x \cdot y$ gestreckt, rechts wird x um den Wert des Skalarprodukts $y \cdot z$ gestreckt.

7.3 Länge und Winkel im $\mathbb{R}^n$: Skalarprodukt

Proposition: Eigenschaft des Skalarprodukts

Seien $x, y, z \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$. Dann gilt

- **Bilinearität**, d.h. Linearität in bezüglich beider Vektoren:

$$\langle x, y+z\rangle = \langle x, y\rangle + \langle x, z\rangle, \qquad \langle \lambda x, y\rangle = \lambda\langle x, y\rangle,$$
$$\langle x+y, z\rangle = \langle x, z\rangle + \langle y, z\rangle, \qquad \langle x, \lambda y\rangle = \lambda\langle x, y\rangle,$$

- **Symmetrie:** $\langle x, y\rangle = \langle y, x\rangle$,
- **Skalarproduktnorm:** $\|x\|_2 = \sqrt{\langle x, x\rangle}$,
- **Skalarprodukt des Nullvektors:** $\langle 0, x\rangle = 0$.

7.4 Darstellung in Vektorräumen

7.4 Darstellung in Vektorräumen: Linearkombination

Definition: Linearkombination, Aufspann

Sei V ein $\mathbb{R}$-Vektorraum. Eine **($\mathbb{R}$-)Linearkombination** von Vektoren $v_1, \ldots, v_k \in V$ ist ein Vektor der Form

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k, \quad \lambda_i \in \mathbb{R}.$$

Die Menge aller ($\mathbb{R}$-)Linearkombinationen

$$\mathrm{span}\{v_1, \ldots, v_k\} := \{\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k \mid \lambda_i \in \mathbb{R}\}$$

nennen wir den **($\mathbb{R}$-)Aufspann von** $v_1, \ldots, v_k$. Dieser ist ein Unterraum von V.

7.4 Darstellung in Vektorräumen: Linearkombination

Beispiele:

- Der Vektor $(3, 5, 7)$ ist eine Linearkombination aus $(1, 1, 1)$, $(1, 2, 1)$ und $(-1, -1, 1)$, denn es gilt:

$$(3, 5, 7) = 3 \cdot (1, 1, 1) + 2 \cdot (1, 2, 1) + 2 \cdot (-1, -1, 1).$$

- Die Vektoren $e_1 := (1, 0)$, $e_2 := (0, 1)$ heißen Standardeinheitsvektoren in $\mathbb{R}^2$. Jeder Vektor (x, y) ist als Linearkombination aus e_1 und e_2 darstellbar:

$$(x, y) = (x, 0) + (0, y) = x \cdot (1, 0) + y \cdot (0, 1) = x \cdot e_1 + y \cdot e_2.$$

  Insbesondere ist $\mathbb{R}^2$ der Aufspann von e_1 und e_2.

7.4 Darstellung in Vektorräumen: Linearkombination

Beispiele:

- Allgemeiner heißt im $\mathbb{R}^n$ der Vektor $e_i := (0, 0, \ldots, 0, \underbrace{1}_{i-te}, 0, \ldots, 0)$ i-ter Standardeinheitsvektor ($1 \leq i \leq n$). Jeder Vektor $(x_1, \ldots, x_n)$ lässt sich als Linearkombination von e_1, ..., e_n darstellen:

  $$(x_1, \ldots, x_n) = x_1(1, 0, \ldots, 0) + x_2(0, 1, 0, \ldots, 0) + \cdots + x_n(0, \ldots, 0, 1) = \sum_{i=1}^{n} x_i e_i.$$

  Insbesondere ist $\mathbb{R}^n$ der Aufspann von e_1, e_2, ..., e_n.
- Sei U eine Ursprungsgerade im $\mathbb{R}^2$ und $\mathbb{O} \neq x \in U$. Dann besteht U aus allen Linearkombination des Vektors x, d.h. $U = \{\lambda x \mid \lambda \in \mathbb{R}\}$ und U ist der Aufspann von x.

7.4 Darstellung in Vektorräumen: Linearkombination

Beispiele:

- Betrachte den Vektorraum der Polynome P und die Vektoren

  $$f_i : [0,1] \to \mathbb{R}, \quad s \mapsto s^i, \ \ i \in \mathbb{N}.$$

  Dann ist jedes Polynom eine (endliche) Linearkombination der f_i, denn sei p ein Polynom gegeben durch $p(x) = \sum_{k=1}^{m} a_k x^k$, dann gilt

  $$p(x) = \sum_{k=1}^{m} a_k x^k = \sum_{k=1}^{m} a_k f_k(x) = \left(\sum_{k=1}^{m} a_k f_k\right)(x).$$

  Es gilt also

  $$P = \left\{ \sum_{k=1}^{n} \lambda_k f_k \mid \lambda_k \in \mathbb{R}, \ \ n \in \mathbb{N} \right\},$$

  und man sagt, dass P der Aufspann der Vektoren f_k ($k \in \mathbb{N}$) ist.

7.4 Darstellung in Vektorräumen: Lineare (Un-)Abhängigkeit

Definition: Lineare (Un-)Abhängigkeit

Seien V ein $\mathbb{R}$-Vektorraum und $M := \{v_1, \ldots, v_k\} \subset V$. Wenn die Linearkombination

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k = \mathbb{O}$$

- nur durch die triviale Lösung $\lambda_1 = \ldots = \lambda_k = 0$ erfüllt ist, so heißt M **($\mathbb{R}$-) linear unabhängig**.
- Gibt es auch nicht-triviale Lösungen dieser Linearkombination, d.h. $\exists \lambda_i \neq 0$, dann nennen wir M **($\mathbb{R}$-)linear abhängig**.
- Eine **unendliche Menge** heißt **($\mathbb{R}$-)linear unabhängig**, wenn jede endliche Teilmenge linear unabhängig ist.

Bemerkungen:

- Ist der Nullvektor in der Menge, so ist diese immer linear abhängig. Ist etwa $M = \{\mathbb{O}, v_1, \ldots, v_k\}$ so kann man nämlich immer die Linearkombination

$$\mathbb{O} = 1 \cdot \mathbb{O} + 0 \cdot v_1 + 0 \cdot v_2 + \ldots + 0 \cdot v_k$$

  bilden und findet z.B. $\lambda_1 = 1 \neq 0$.

- Die Menge der Standardeinheitsvektoren $\{e_j \mid j = 1, \ldots, n\}$ im $\mathbb{R}^n$ ist linear unabhängig, denn

$$(0, \ldots, 0) = \lambda_1 e_1 + \lambda_2 e_2 + \ldots, \lambda_n e_n = (\lambda_1, \lambda_2, \ldots, \lambda_n)$$

  erzwingt, dass $\lambda_i = 0$ für alle i.

- Die Menge $\{(1, 1), (1, 2)\}$ ist offenbar linear unabhängig, denn keiner der beiden Vektoren lässt sich als Linearkombination des anderen schreiben. Darüber hinaus ist der Aufspann dieser Vektoren $\mathbb{R}^2$.

Bemerkungen:

- Ist eine Menge linear abhängig, so kann man *mindestens* einen der Vektoren als Linearkombination der anderen schreiben.
- **Achtung:** Es muss dann nicht gelten, dass jeder der Vektoren sich als Linearkombination der anderen schreiben lässt. Betrachte z.B. die Menge $\{(1,2),(1,1),(7,7)\}$. Diese Menge ist linear abhängig, denn

  $$0 \cdot (1,2) + (1,1) - \frac{1}{7} \cdot (7,7) = \mathbb{0}$$

  aber $(1,2)$ kann nicht als Linearkombination aus $(1,1)$ und $(7,7)$ geschrieben werden.
- Betrachte den Vektorraum $V = \mathbb{R}^n$ und eine Menge M mit $|M| \geq n+1$. Dann ist M linear abhängig.

Proposition: Eindeutige Darstellung

Die Menge $\{v_1, \dots, v_k\}$ sei ($\mathbb{R}$-)linear unabhängig in V. Dann hat jedes Element $x \in \operatorname{span}\{v_1, \dots, v_k\}$ eine **eindeutige Darstellung** als ($\mathbb{R}$-)Linearkombination der v_i.

Beispiele:

- Die Menge $\{(1,1),(1,2)\}$ ist linear unabhängig. Der Vektor $(7,7)$ ist in ihrem Aufspann und lässt sich nur beschreiben durch die Linearkombination

$$(7,7) = 7 \cdot (1,1) + 0 \cdot (1,2).$$

7.4 Darstellung in Vektorräumen: Lineare (Un-)Abhängigkeit

- Die Menge $\{(1,0,0),(1,1,0),(1,1,1)\}$ ist linear unabhängig. Der Vektor $(-1,10,100)$ ist in ihrem Aufspann und lässt sich auf genau eine Art als Linearkombination schreiben:

$$(-11)\cdot(1,0,0)+(-90)\cdot(1,1,0)+100\cdot(1,1,1)=(-1,10,100).$$

- Die Menge $\{(1,1),(1,2),(1,3)\}$ ist linear abhängig in $\mathbb{R}^2$. In der Tat haben die Elemente von $\operatorname{span}\{(1,1),(1,2),(1,3)\}$ dann auch keine eindeutige Darstellung. Zum Beispiel gilt:

$$\begin{aligned}(1,0) &= 1\cdot(1,1)+1\cdot(1,2)-1\cdot(1,3)\\ (1,0) &= 2\cdot(1,1)-1\cdot(1,2)+0\cdot(1,3).\end{aligned}$$

7.4 Darstellung in Vektorräumen: Basis

Definition: Basis, Dimension

Sei V ein Vektorraum und die Vektoren $b_1, \ldots, b_n$ seien so beschaffen, dass

1. die Menge $\mathcal{B} := \{b_1, \ldots, b_n\}$ ($\mathbb{R}$-)linear unabhängig ist und
2. $V = \text{span}\{b_1, \ldots, b_n\}$.

- Dann nennen wir $\mathcal{B}$ eine **($\mathbb{R}$-)Basis** des Vektorraums V.
- Die **Dimension** des Vektorraums V ist definiert durch die Anzahl der Basisvektoren in $\mathcal{B}$, d.h. $\dim(V) := |\mathcal{B}|$.

Anmerkungen:

- Eine Basis eines Vektorraums ist die kleinste Menge von Vektoren, die den Vektorraum aufspannt.
- Jede Menge aus n linear unabhängigen Vektoren in $\mathbb{R}^n$ ist eine Basis des $\mathbb{R}^n$.

7.4 Darstellung in Vektorräumen: Basis

Beispiele:

- Die Menge der Einheitsvektoren in $\mathbb{R}^n$ spannt diesen auf und ist linear unabhängig. Sie Bildet die sogenannte **kanonische Einheitsbasis**.
- So ist also auch die Menge $\{(1,0,0),(1,1,0),(1,1,1)\}$ eine Basis des $\mathbb{R}^3$. Um dies zu beweisen muss man das folgende (homogene) lineare Gleichungssystem lösen:

$$\begin{aligned} \lambda_1 \cdot 1 + \lambda_2 \cdot 1 + \lambda_3 \cdot 1 &= 0 \\ \lambda_2 \cdot 1 + \lambda_3 \cdot 1 &= 0 \\ \lambda_3 \cdot 1 &= 0. \end{aligned}$$

- Basen werden im Zusammenhang mit linearen Gleichungssystemen eine wichtige Rolle spielen. Insbesondere werden sie es uns gestatten alle Lösungen eines solchen möglichst übersichtlich darzustellen (Stichwort: Bild einer linearen Abbildung).

7.4 Darstellung in Vektorräumen: Basis

Beispiele:

- Betrachten wir den $\mathbb{R}$-Vektorraum $\mathbb{C}$ so bildet die Menge $\{1, \mathrm{i}\}$ eine Basis, denn
$$\lambda_1 \cdot 1 + \lambda_2 \, \mathrm{i} = 0$$
impliziert $\lambda_{1/2} = 0$, denn wir müssen diese Skalare ja aus $\mathbb{R}$ wählen.
- Betrachten wir dagegen den $\mathbb{C}$-Vektorraum $\mathbb{C}$ so bildet die Menge $\{1, \mathrm{i}\}$ keine Basis, denn
$$\lambda_1 \cdot 1 + \lambda_2 \, \mathrm{i} = 0$$
besitzt neben der trivialen Lösung $\lambda_{1/2} = 0$, z.B. die Lösung $\lambda_1 = 1$ und $\lambda_2 = \mathrm{i}$, denn nun können wir die Skalare aus $\mathbb{C}$ wählen.

7.4 Darstellung in Vektorräumen: Basis

Beispiele:

- Sei U eine Ursprungsgerade in $\mathbb{R}^2$. Dann definiert jeder Vektor in U, der nicht der Null-Vektor ist eine Basis von U.
- Ist $\{b_1, \ldots, b_n\}$ eine Basis eines Vektorraums V, so hat jede andere Basis auch genau n Elemente. Jede Basis des $\mathbb{R}^3$ hat genau drei Elemente (Standardeinheitsvektoren bilden eine Basis), d.h. dieser Raum ist durch Linearkombination dreier beliebiger linear unabhängiger Vektoren beschrieben.

7.4 Darstellung in Vektorräumen: Basis

Austauschsatz von Steinitz

Sei $B_0 := \{b_1, \ldots, b_n\}$ eine Basis des Vektorraums V und $U := \{u_1, \ldots, u_k\}$ eine Menge linear unabhängiger Vektoren ($k \leq n$). Dann kann U durch Vektoren aus B zu einer Basis von V ergänzt werden:

1. Schreibe u_1 als Linearkombination der Basis B_0: $\quad u_1 = \sum_{j=1}^{n} \lambda_j b_j.$
2. Ersetze ein b_j mit $\lambda_j \neq 0$ aus B durch u_1: $\quad B_1 := B_0 \setminus \{b_j\} \cup \{u_1\}.$
3. Schreibe nach und nach $u_2, \ldots, u_k$ als Linearkombinationen der neuen Basen $B_1, \ldots, B_{k-1}$ und ersetze die Vektoren b_j aus B_i mit $\lambda_j \neq 0$ durch Vektoren aus U.

Dann ist die Menge B_k eine Basis von V, die U enthält.

7.4 Darstellung in Vektorräumen: Basis

Beispiel: Wir ergänzen $U = \{(1,1,0,0),(1,1,1,0)\}$ zu einer Basis des $\mathbb{R}^4$. Start:

$$B_0 = \{e_1, e_2, e_3, e_4\} = \{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}.$$

1. $u_1 := (1,1,0,0)$ als Linearkombination der Vektoren aus B_0:

   $$u_1 = 1 \cdot e_1 + 1 \cdot e_2 + 0 \cdot e_3 + 0 \cdot e_4.$$

   Wir ersetzen e_1, da $\lambda_1 = 1 \neq 0$:

   $$B_1 = B_0 \backslash \{e_1\} \cup \{u_1\} = \{(0,1,0,0),(0,0,1,0),(0,0,0,1),(1,1,0,0)\}.$$

2. $u_2 := (1,1,1,0)$ als Linearkombination der Vektoren aus B_1:

   $$u_2 = 0 \cdot e_2 + 1 \cdot e_3 + 0 \cdot e_4 + 1 \cdot u_1.$$

   Wir ersetzen e_3, da $\lambda_3 = 1 \neq 0$:

   $$B_2 = B_1 \backslash \{e_3\} \cup \{u_2\} = \{(0,1,0,0),(0,0,0,1),(1,1,0,0),(1,1,1,0)\}.$$

8. Lineare Abbildungen

8. Lineare Abbildungen

Ausblick:

- Lineare Abbildungen zwischen Vektorräumen können als Drehungen, Streckungen, Spiegelungen oder Projektionen interpretiert werden.
- Additivität und Homogenität sind deren zentrale Eigenschaften.
- Darstellung mit Hilfe von Matrizen.
- Anwendungen in der Computergraphik, Kodierungstheorie, lineare Optimierung, uvm.

8.1 Grundlagen linearer Abbildungen im $\mathbb{R}^n$

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Definition

Definition: Vektorraum

- Eine Abbildung $f : \mathbb{R}^n \to \mathbb{R}^m$ heißt **linear**, wenn gilt

$$\begin{aligned} f(x+y) &= f(x)+f(y), \quad && x,y \in \mathbb{R}^n && \text{(Additivität)},\\ f(\lambda \cdot x) &= \lambda \cdot f(x), && \lambda \in \mathbb{R},\ \ x \in \mathbb{R}^n && \text{(Homogenität)}. \end{aligned}$$

- Eine lineare Abbildung f heißt auch **Homomorphismus** und falls f bijektiv ist, **Isomorphismus**. Zwangsweise gilt hier $n = m$.

Anmerkung: Anders gesagt ist eine Abbildung linear, wenn das Bild einer Linearkombination von Urbildern x, y der Linearkombination der Bilder von x, y mit denselben Koeffizienten gleicht, d.h. für alle $x, y \in \mathbb{R}^n$

$$f(\alpha \cdot x + \beta \cdot y) = \alpha \cdot f(x) + \beta \cdot f(y), \quad \alpha, \beta \in \mathbb{R}.$$

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Aufgabe

Aufgabe:

Zeigen Sie, dass die folgende Abbildung linear ist:

$$f : \mathbb{R}^2 \to \mathbb{R}, \quad (x_1, x_2) \mapsto x_1 + x_2.$$

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Definition

Definition: Kern und Bild einer linearen Abbildung

- Der **Kern** der linearen Abbildung f ist die Menge der Vektoren aus $\mathbb{R}^n$, die durch f auf den Nullvektor abgebildet werden:

$$\ker f := \{x \in \mathbb{R}^n \mid f(x) = \mathbb{O}\} \subseteq \mathbb{R}^n.$$

- Das **Bild** der linearen Abbildung f ist die Menge aller Bildvektoren unter f:

$$\mathrm{Bild}\, f := \{f(x) \in \mathbb{R}^m \mid x \in \mathbb{R}^n\} \subseteq \mathbb{R}^m.$$

- Der **Kern-Bild-Satz** lautet

$$\dim(\mathbb{R}^n) = \dim(Kern(f)) + \dim(Bild(f)).$$

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Beispiele

Beispiele:

- Die Abbildung $f\colon \mathbb{R} \to \mathbb{R},\ \ x \mapsto ax$ ist linear. Es gilt

$$\ker f = \begin{cases} \{0\}, & \text{für } a \neq 0, \\ \mathbb{R}, & \text{für } a = 0 \end{cases} \quad \text{und} \quad \operatorname{Bild} f = \begin{cases} \mathbb{R}, & \text{für } a \neq 0, \\ \{0\}, & \text{für } a = 0. \end{cases}$$

  Die Abbildung ist für $a \neq 0$ bijektiv, also ein Isomorphismus und es gilt

$$\dim(\ker(f)) + \dim(\operatorname{Bild}(f)) = 0 + 1 = 1 = \dim(\mathbb{R}).$$

- Die Abbildung $f : \mathbb{R}^3 \to \mathbb{R},\ \ (x_1, x_2, x_3) \mapsto x_1 + x_2$ ist linear. Es gilt

$$\ker f = \left\{(x_1, -x_1, x_3) \in \mathbb{R}^3 \mid x_1, x_3 \in \mathbb{R}\right\} \ \text{ und } \ \operatorname{Bild} f = \mathbb{R}$$

  und $\dim(\ker(f)) + \dim(\operatorname{Bild}(f)) = 2 + 1 = 3 = \dim(\mathbb{R}^3)$. Diese Abbildung ist surjektiv, aber nicht injektiv, also kein Isomorphismus.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Beispiele

Beispiele:

- Die Abbildung $f\colon \mathbb{R} \to \mathbb{R},\ \ x \mapsto ax + b$ für $b \neq 0$ ist *nicht linear* (sondern *affin*), genauso wie $g\colon \mathbb{R} \to \mathbb{R},\ \ x \mapsto x^2$.
- Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2,\ \ (x_1, x_2) \mapsto (-x_2, x_1)$ ist linear, denn

$$\begin{array}{lllllll} f(x+y) & = & (-x_2 - y_2, x_1 + y_1) & = & (-x_2, x_1) + (-y_2, y_1) & = & f(x) + f(y), \\ f(\lambda x) & = & (-\lambda x_2, \lambda x_1) & = & \lambda(-x_2, x_1) & = & \lambda f(x). \end{array}$$

Es handelt sich um eine Drehung der Vektoren um 90° im Gegen-Uhrzeigersinn (um den Nullpunkt). Es gilt

$$\ker f = \{\mathbb{O}\} \ \text{ und } \ \operatorname{Bild} f = \mathbb{R}^2$$

Insbesondere ist die Abbildung ein Isomorphismus.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Beispiele

Beispiele:

- Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2, \ (x_1, x_2) \mapsto (x_1 - x_2, x_2 - x_1)$ ist linear. Es gilt

$$\ker f = \{(x, x) \mid x \in \mathbb{R}\} \ \text{ und } \ \operatorname{Bild} f = \{(x, -x) \mid x \in \mathbb{R}\}$$

  Insbesondere ist die Abbildung weder injektiv noch bijektiv.
- Seien $a_{ij} \in \mathbb{R}$ für $1 \leq i \leq m$, $1 \leq j \leq n$. Die Abbildung

$$f : \mathbb{R}^n \to \mathbb{R}^m, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \sum_{j=1}^n a_{1j} x_j \\ \sum_{j=1}^n a_{2j} x_j \\ \vdots \\ \sum_{j=1}^n a_{mj} x_j \end{pmatrix}$$

  ist linear. In der Tat werden wir feststellen, dass man zu jeder linearen Abbildung von $\mathbb{R}^n$ nach $\mathbb{R}^m$ Koeffizienten a_{ij} finden kann, so dass sie in dieser Form dargestellt werden kann.

8.1 Lineare Abbildungen im $\mathbb{R}^n$

Bemerkung:

- Anhand der letzten Beispiele deutet sich an, dass die Mengen $\ker f$ und $\operatorname{Bild} f$ mehr Struktur haben.
- Darüber hinaus können wir den Begriff der Basis verwenden um lineare Abbildungen zu beschreiben.
- Es genügt eine lineare Abbildung auf dieser Basis zu definieren um sie bereits überall zu kennen.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Eigenschaften

Proposition: Eigenschaften linearer Abbildungen

Sei $f\colon \mathbb{R}^n \to \mathbb{R}^m$ linear. Dann gilt

- $\ker f$ und $\operatorname{Bild} f$ sind Unterräume von $\mathbb{R}^n$ bzw. $\mathbb{R}^m$,
- f ist genau dann **injektiv**, wenn der Kern nur den Nullvektor enthält:

$$f \text{ ist injektiv} \quad \Longleftrightarrow \quad \ker f = \{\mathbb{O}\}.$$

- Ist $\{b_1, \ldots, b_n\}$ eine Basis des $\mathbb{R}^n$ und sind $v_1, \ldots, v_n$ Vektoren im $\mathbb{R}^m$. Dann ist die Abbildung f durch die Bilder der Basisvektoren

$$f(b_i) = v_i, \quad i = 1, \ldots, n,$$

vollständig bestimmt.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Aufgabe

Aufgabe:
Untersuchen Sie die folgende Abbildung auf Injektivität und Surjektivität:

$$f : \mathbb{R}^2 \to \mathbb{R}^3, \quad (x_1, x_2) \mapsto (x_2, x_1, x_1 - x_2).$$

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Eigenschaften

Beweis: Sei $v \in \mathbb{R}^n$ gegeben. Da $\{b_1, \ldots, b_n\}$ eine Basis von $\mathbb{R}^n$ ist können wir v darstellen als

$$v = \sum_{j=1}^{n} \lambda_j b_j$$

mit eindeutigen Koeffizienten λ_j. Da f linear ist gilt dann

$$f(v) = f\left(\sum_{j=1}^{n} \lambda_j b_j\right) = \sum_{j=1}^{n} f\left(\lambda_j b_j\right) = \sum_{j=1}^{n} \lambda_j f(b_j)$$

und damit ist $f(v)$ bereits eindeutig bestimmt. $\square$

Übung: beweisen Sie 1. und 2.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Beispiel

Beispiel: Wir betrachten die kanonische Standardbasis $\{(1,0),(0,1)\}$ des $\mathbb{R}^2$ und die lineare Abbildung

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \begin{cases} (1,0) \mapsto (1,-1), \\ (0,1) \mapsto (-1,1). \end{cases}$$

Dann ist f schon eindeutig bestimmt. Der Funktionswert für einen Vektor $(x_1, x_2) \in \mathbb{R}^2$ bestimmt sich durch

$$\begin{aligned} f((x_1,x_2)) &= f\left(x_1 \cdot (1,0) + x_2 \cdot (0,1)\right) \\ &= f\left(x_1 \cdot (1,0)\right) + f\left(x_2 \cdot (0,1)\right) \\ &= x_1 \cdot f\left((1,0)\right) + x_2 \cdot f\left((0,1)\right) \\ &= x_1(1,-1) + x_2 \cdot (-1,1) \\ &= (x_1 - x_2, x_2 - x_1). \end{aligned}$$

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Komposition

Bemerkungen:

- Wir können lineare Abbildungen auch miteinander verknüpfen.
- Die Menge der linearen Abbildungen wird oft $\mathrm{Hom}(\mathbb{R}^n, \mathbb{R}^m)$ bezeichnet.
- Wir definieren die für diese Menge entscheidenden Verknüpfungen der Addition und skalaren Multiplikation *punktweise*.
- Damit ist diese Menge wiederum selbst ein Vektorräume.
- Die Komposition wird hierbei als Hintereinanderausführung von Abbildungen definiert.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Komposition

Definition: Addition und skalare Multiplikation linearer Abbildungen

Seien $f\colon \mathbb{R}^n \to \mathbb{R}^m$ und $g\colon \mathbb{R}^n \to \mathbb{R}^m$ lineare Abbildungen und $\lambda \in \mathbb{R}$. Definieren wir **Addition** und **skalare Multiplikation** durch

$$\begin{aligned} f+g : \mathbb{R}^n \to \mathbb{R}^m, &\qquad x \mapsto [f+g](x) := f(x) + g(x), \\ \lambda f : \mathbb{R}^n \to \mathbb{R}^m, &\qquad x \mapsto [\lambda f](x) := \lambda \cdot f(x), \end{aligned}$$

so wird die Menge der linearen Abbildungen zu einem Vektorraum.

- Das neutrale Element der Addition ist dabei die Nullfunktion.
- Das additive Inverse zu f ist $(-1) \cdot f$.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Komposition

Definition: Komposition linearer Abbildungen

Seien $f\colon \mathbb{R}^k \to \mathbb{R}^m$ und $g\colon \mathbb{R}^n \to \mathbb{R}^k$ lineare Abbildungen. Die **Komposition** $f \circ g$ ist dann definiert durch

$$f \circ g : \mathbb{R}^n \to \mathbb{R}^m, \qquad x \mapsto [f \circ g](x) := f(g(x)).$$

Anmerkung: Ist f ein Isomorphismus, so existiert eine Umkehrabbildung f^{-1}, die ebenfalls bijektiv und linear ist, d.h. f^{-1} ist auch ein Isomorphismus.
Übung: Zeigen Sie, dass die Umkehrfunktion eines Isomorphismus linear.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Komposition

Beispiele:

- Betrachte die Abbildungen

$$
\begin{aligned}
f &: \mathbb{R}^2 \to \mathbb{R}^2, && (x_1, x_2) \mapsto f(x) := (-x_1, -x_2),\\
g &: \mathbb{R}^2 \to \mathbb{R}^2, && (x_1, x_2) \mapsto g(x) := (x_1 - x_2, x_2 - x_1).
\end{aligned}
$$

  Dann ist $f + g : \mathbb{R}^2 \to \mathbb{R}^2, (x_1, x_2) \mapsto (-x_2, -x_1)$.

- Betrachte die linearen Abbildungen f, die eine Drehung um 90° beschreibt, und g, die eine Projektion in die x-y-Ebene beschreibt, also

$$
\begin{aligned}
f &: \mathbb{R}^2 \to \mathbb{R}^2, && (x_1, x_2) \mapsto f(x) := (-x_2, x_1),\\
g &: \mathbb{R}^3 \to \mathbb{R}^2, && (x_1, x_2, x_3) \mapsto g(x) := (x_1, x_2).
\end{aligned}
$$

  Dann ist $f \circ g : \mathbb{R}^3 \to \mathbb{R}^2, (x_1, x_2, x_3) \mapsto (-x_2, x_1)$. Ein Vektor wird dabei zunächst in die x-y-Ebene projiziert und danach um 90° gedreht.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Isomorphismen

Bemerkungen:

- Isomorphismen bilden eine ausgezeichnete Klasse unter den linearen Abbildungen.
- Sie erhalten zentrale *lineare Eigenschaften* einer Menge.
- So ist das Bild einer linear unabhängigen Menge in $\mathbb{R}^n$ unter dem Isomorphismus $f\colon \mathbb{R}^n \to \mathbb{R}^n$ wieder linear unabhängig.
- Insbesondere wird eine Basis durch einen Isomorphismus wieder auf eine Basis abgebildet.

Bemerkungen:

- **Achtung:** Im Allgemeinen ist das Bild linear unabhängiger Mengen unter linearen Abbildungen nicht linear unabhängig, z.B. bildet

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \ \ (x_1, x_2) \mapsto (x_1 - x_2, x_2 - x_1)$$

  die linear unabhängige Menge $\{(1,1),(1,2)\}$ auf die linear abhängige Menge $\{(0,0),(-1,1)\}$ ab.

- Isomorphismen erhalten allerdings nicht alle Eigenschaften. Betrachten wir den Isomorphismus

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \ \ (x_1, x_2) \mapsto (2x_1, x_2)$$

  so wird ein Kreis $U = \{(x_1, x_2) \mid x_1^2 + x_2^2 = 1\}$ etwa nicht auf einen Kreis abgebildet. Ein Kreis besitzt also keine lineare Eigenschaft.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Isomorphismen

Proposition

Sei $f\colon \mathbb{R}^n \to \mathbb{R}^n$ eine lineare Abbildung. Dann ist

$$\text{f injektiv} \iff \text{f surjektiv} \iff \text{f bijektiv.}$$

Anmerkung: Um zu zeigen, dass $f\colon \mathbb{R}^n \to \mathbb{R}^n$ ein Isomorphismus ist, muss eigentlich geprüft werden, ob

$$\ker f = \{\mathbb{O}\} \;\; \textit{und} \;\; \operatorname{Bild} f = \mathbb{R}^n.$$

Die Proposition besagt, dass bereits eine der beiden Eigenschaften ausreicht.

8.1 Lineare Abbildungen im $\mathbb{R}^n$: Beispiele

Beispiele:

- Für $f : \mathbb{R}^2 \to \mathbb{R}^2, \ (x_1, x_2) \mapsto (x_1 + x_2, x_1)$ gilt

$$f((x_1, x_2)) = (x_1 + x_2, x_1) = (0, 0) \quad \Rightarrow \quad \ker f = \{\mathbb{O}\}.$$

  Damit ist f injektiv und wegen $n = m$ bijektiv, also ein Isomorphismus.

- Für $f : \mathbb{R}^2 \to \mathbb{R}^2, \ (x_1, x_2) \mapsto (x_1 - x_2, x_2 - x_1)$ gilt

$$f((x_1, x_2)) = (x_1 - x_2, x_2 - x_1) = (0, 0) \quad \Rightarrow \quad \ker f = \operatorname{span}\{(1, 1)\} \neq \{\mathbb{O}\}.$$

  Damit ist f nicht injektiv, also nicht bijektiv und wegen $n = m$ auch nicht surjektiv.

8.2 Matrizen

8.2 Lineare Abbildungen: Matrizen

Vorbemerkung:

- Wir werden noch auf spezielle lineare Abbildungen wie Streckungen, Drehungen, Spiegelungen und Projektionen eingehen.
- Zunächst versuchen wir aber eine praktischere Notation mit Hilfe von Matrizen zu finden.
- Wir werden sehen, dass wir jede lineare Abbildung in Matrix-Schreibweise formulieren können.
- Umgekehrt kann auch jeder Matrix eine lineare Abbildung zugeordnet werden.

8.2 Lineare Abbildungen: Matrizen

Definition: Matrix

- Eine (reelle) $m \times n$-**Matrix** A ist ein rechteckig angeordnetes Zahlenschema bestehend aus m Zeilen und n Spalten, deren Einträge Elemente a_{ij} aus $\mathbb{R}$ sind.
- Die $a_{ij} \in \mathbb{R}$ nennen wir **Koeffizienten der Matrix**, $i = 1, \ldots, m$ ist der **Zeilenindex** und $j = 1, \ldots, n$ der **Spaltenindex**. Dann ist die zugehörige Matrix

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

8.2 Lineare Abbildungen: Matrizen

Definition: Matrix (Fortsetzung)

- Eine Matrix, die nur Nullen enthält, heißt **Nullmatrix**. Symbol: $\mathbb{O}$.
- Das Zahlenpaar $m \times n$ nennen wir die **Dimensionen der Matrix**. Für die Menge der reellen $m \times n$-Matrizen schreiben wir kurz $M^{m \times n}(\mathbb{R})$.
- Zwei Matrizen A und B heißen gleich (in Zeichen $A = B$), wenn sie von gleicher Dimension sind und in allen Einträgen übereinstimmen.

8.2 Lineare Abbildungen: Matrizen

Bemerkung/Beispiel:

- Analog definieren wir Matrizen über anderen Körpern, z.B. komplexe Matrizen mit Elementen aus $\mathbb{C}$.
- Ein Vektor $x \in \mathbb{R}^n$ kann damit auch als eine $n \times 1$-Matrix interpretiert werden.
- Beispiele für Matrizen verschiedener Dimensionen über verschiedene Körper:

$$\begin{pmatrix} \sqrt{2} \\ 2 \end{pmatrix} \in M^{2\times 1}(\mathbb{R}), \quad \begin{pmatrix} 2 & 1 \end{pmatrix} \in M^{1\times 2}(\mathbb{Q}), \quad \begin{pmatrix} 1 & 2 & \pi \\ \sqrt{2} & -2 & 43 \end{pmatrix} \in M^{2\times 3}(\mathbb{R}),$$

$$\begin{pmatrix} 0.1 \\ 0.2 \\ 0.4 \end{pmatrix} \in M^{3\times 1}(\mathbb{Q}), \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \in M^{3\times 2}(\mathbb{R}), \quad \begin{pmatrix} \pi & 2 & 1+2i \\ \sqrt{2} & -2 & 43 \\ 1 & 3i & \ln 2 \end{pmatrix} \in M^{3\times 1}(\mathbb{C}).$$

8.2 Lineare Abbildungen: Matrizen

Beispiel: Graphentheorie.
Ein **Graph** besteht aus n **Knoten** und m **Kanten**, die diese miteinander verbinden. Dann kann man die sogenannte **Adjazenzmatrix**

$$a_{ij} = \begin{cases} 1, & \exists \text{ Kante zwische Knoten } i \text{ und } j, \\ 0, & \text{sonst.} \end{cases}$$

eines Graphen aufstellen. Der Graph in Form eines Dreiecks, bei dem die drei Knoten 1, 2 und 3 an den Ecken jeweils durch eine Kante mit den zwei anderen Ecken verbunden sind, besitzt die Adjazenzmatrix

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Definition: Transponierte Matrix

- Die Elemente einer Matrix mit gleichem Zeilen-/Spaltenindex nennen wir **Zeilen-/Spaltenvektoren**. Eine $m \times n$-Matrix besteht also aus n Spaltenvektoren und m Zeilenvektoren. **Notation:** $A_{i,*}$ für die i-te Zeile einer Matrix A und $A_{*,j}$ für die j-te Spalte.
- Die **transponierte Matrix** $A^\top \in M^{n\times m}$ entsteht aus einer Matrix $A \in M^{m\times n}$, durch das Tauschen von Zeilen und Spalten:
  1. Tausch von Zeilen- und Spaltenindizes: $a_{ik}^\top = a_{ki}$,
  2. Tausch von Zeilen- und Spaltenvektoren: $A_{i,*} = A_{*,i}^\top$,
  3. Transponierte der Transponierten: $\left(A^\top\right)^\top = A$.

8.2 Lineare Abbildungen: Transponierte Matrix

Beispiel:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 2 \\ 3 & 3 & 5 & 2 \end{pmatrix} \quad \Rightarrow \quad A^\top = \begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 3 \\ 3 & 1 & 5 \\ 4 & 2 & 2 \end{pmatrix}.$$

Dann sind die Zeilenvektoren von A gegeben durch

$$A_{1,*} = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}, \ A_{2,*} = \begin{pmatrix} 0 & 1 & 1 & 2 \end{pmatrix}, \ A_{3,*} = \begin{pmatrix} 3 & 3 & 5 & 2 \end{pmatrix}$$

und die Spaltenvektoren von A durch

$$A_{*,1} = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}, \ A_{*,2} = \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}, \ A_{*,3} = \begin{pmatrix} 3 \\ 1 \\ 5 \end{pmatrix}, \ A_{*,4} = \begin{pmatrix} 4 \\ 2 \\ 2 \end{pmatrix}.$$

Definition: Quadratische Matrix

- Eine Matrix mit gleich vielen Zeilen und Spalten, d.h. $m = n$, nennen wir **quadratisch**.
- Bei einer quadratischen Matrix bilden die Elemente a_{ii} mit gleichem Zeilen- und Spaltenindex die **Hauptdiagonale**.
- Die **Spur** einer quadratischen Matrix ist die Summe der Hauptdiagonalelemente:

$$\mathrm{Sp}(A) := a_{11} + a_{22} + \ldots + a_{nn} = \sum_{i=1}^{n} a_{ii}.$$

8.2 Lineare Abbildungen: Quadratische Matrizen

Defintion: spezielle quadratischer Matrizen

Sei A eine $n \times n$ Matrix. Dann heißt A

- **symmetrisch**, wenn $A^\top = A$,
- **schiefsymmetrisch**, wenn $A^\top = -A$,
- **Diagonalmatrix**, wenn alle Einträge außerhalb der Hauptdiagonalen verschwinden, d.h.

$$a_{ij} = 0 \text{ falls } i \neq j.$$

Wir schreiben dann $A = \operatorname{diag}(a_{ii})_{i=1}^n$.

Defintion: spezielle quadratischer Matrizen

Sei A eine $n \times n$ Matrix. Dann heißt A

- **obere Dreiecksmatrix**, wenn alle Einträge unterhalb der Hauptdiagonalen verschwinden, d.h.

$$a_{ij} = 0 \text{ falls } i > j,$$

- **untere Dreiecksmatrix**, wenn alle Einträge oberhalb der Hauptdiagonalen verschwinden, d.h.

$$a_{ij} = 0 \text{ falls } i < j,$$

- **Einheitsmatrix**, bezeichnet mit E oder Id_n, wenn A eine Diagonalmatrix ist mit

$$a_{ii} = 1, \quad i = 1, \ldots, n.$$

8.2 Lineare Abbildungen: Quadratische Matrizen

Beispiele: Betrachte die quadratischen Matrizen

$$\begin{pmatrix} 1 & 4 & 2 \\ 4 & 6 & 5 \\ 2 & 5 & 3 \end{pmatrix}, \quad \begin{pmatrix} 0 & 4 & -2 \\ -4 & 0 & 5 \\ 2 & -5 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 4 & 2 \\ 0 & 6 & 5 \\ 0 & 0 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Dann sind diese 3×3-Matrizen der Reihe nach symmetrisch, schiefsymmetrisch, diagonal, in Dreiecksform und eine Einheitsmatrix.

8.2 Lineare Abbildungen: Matrixoperationen

Definition: Matrixaddition

Seien $A, B \in M^{m\times n}$. Dann definieren wir die **Addtition** von A und B komponentenweise durch

$$A + B := \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2n}+b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \dots & a_{mn}+b_{mn} \end{pmatrix}.$$

Achtung: Bei der Addition zweier Matrizen müssen immer die Dimensionen übereinstimmen, sonst ist diese Operation nicht definiert!

8.2 Lineare Abbildungen: Matrixoperationen

Definition: Matrixaddition und skalare Multiplikation

Seien $A \in M^{m \times n}$ und $\lambda \in \mathbb{R}$. Dann definieren wir die **skalare Multiplikation** komponentenweise durch

$$\lambda \cdot A := \begin{pmatrix} \lambda \cdot a_{11} & \lambda \cdot a_{12} & \dots & \lambda \cdot a_{1n} \\ \lambda \cdot a_{21} & \lambda \cdot a_{22} & \dots & \lambda \cdot a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda \cdot a_{m1} & \lambda \cdot a_{m2} & \dots & \lambda \cdot a_{mn} \end{pmatrix}.$$

Anmerkung: Durch die Definitionen wird $(M_{m \times n}(\mathbb{R}), +, \cdot)$ zu einem $\mathbb{R}$-Vektorraum, wobei die Nullmatrix $\mathbb{O} \in M^{m \times n}(\mathbb{R})$ das Neutralelement bildet und $(-1) \cdot A$ die additive Inverse einer Matrix A durch gegeben ist.

8.2 Lineare Abbildungen: Matrixoperationen

Proposition: Vektorraumaxiome für Matrizen

Seien A, B und C $m \times n$-Matrizen. Dann gilt

1. **Assoziativität der Addition:** $(A + B) + C = A + (B + C)$,
2. **Kommutativität der Addition:** $A + B = B + A$,
3. **Assoziativität der skalaren Mulitplikation:** $\forall\, \lambda, \mu \in \mathbb{R}$
$$\lambda \cdot (\mu A) = (\lambda\mu) \cdot A,$$
4. **Distributivgesetze:**
$$\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B \quad \forall\, \lambda \in \mathbb{R},$$
$$(\lambda + \mu) \cdot A = \lambda \cdot A + \mu \cdot A \quad \forall\, \lambda, \mu \in \mathbb{R}.$$

8.2 Lineare Abbildungen: Matrixoperationen

Ausblick:

- Wie bei linearen Abbildungen können wir auch Matrizen miteinander verketten.
- In der Menge der Matrizen gibt es eine entsprechende Verknüpfung: das *Produkt* zweier Matrizen.
- Intuitiv könnten wir das Produkt auch komponentenweise definieren. Allerdings hat dies keine relevanten Anwendungen.
- Wir erinnern stattdessen an das Skalarprodukt von Vektoren und wenden dies auf Zeilen- und Spaltenvektoren der Matrizen an.

8.2 Lineare Abbildungen: Matrixoperationen

Definition: Produkt von Matrizen

Sei $A \in M_{m \times n}$ und $B \in M_{n \times p}$. Dann definieren wir das **Produkt** C von A und B (in Zeichen $C = A \cdot B$) durch die $m \times p$-Matrix, gegeben durch

$$c_{ij} := \langle A_{i,*}, B_{*,j} \rangle = \sum_{k=1}^{n} a_{ik} b_{kj} = a_{i1} b_{1j} + a_{i2} b_{2j} + a_{i3} b_{3j} + \ldots + a_{in} b_{nj},$$

wobei $1 \leq i \leq m$ und $1 \leq j \leq p$.

Achtung: Für die Berechnung des Produktes AB ist es notwendig, dass die Spaltenanzahl von A mit der Zeilenanzahl von B übereinstimmt. Sonst ist das Produkt nicht definiert.

8.2 Lineare Abbildungen: Matrixoperationen

Proposition: Eigenschaften der Multiplikation

- Falls die Multiplikation und Addition in den folgenden Termen definiert ist, gelten die folgenden Gesetze:

$$\begin{aligned} A(BC) &= (AB)C \\ A(B+C) &= AB + AC \\ (A+B)C &= AC + BC \\ \mathrm{Id}_n A &= A\,\mathrm{Id}_n = A \\ (AB)^\top &= B^\top A^\top \end{aligned}$$

- Im Allgemeinsen ist das Matrixprodukt nicht kommutativ, d.h.

$$A \cdot B \neq B \cdot A.$$

8.2 Lineare Abbildungen: Matrixoperationen

Beispiele:

- Für $A \in M^{3\times 3}$ und $B \in M^{3\times 2}$ ist $A \cdot B \in M^{3\times 2}$ und

$$A \cdot B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \\ 3 & 4 \end{pmatrix}.$$

  $B \cdot A$ ist dagegen nicht definiert.

- Die Matrizenmultiplikation ist nicht kommutativ:

$$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = B \cdot A$$

8.2 Lineare Abbildungen: Aufgaben

Aufgaben:

Gegeben seien die Matrizen

$$A = \begin{pmatrix} 3 & 4 & 0 \\ -1 & 5 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} -3 & 3 \\ 1 & -1 \\ 0 & 2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 4 & 0 \\ 2 & 1 & 3 \end{pmatrix}.$$

Berechnen Sie mit diesen Matrizen (soweit möglich):

(a) $A^\top$, $B^\top$ und $C^\top$

(b) $A \cdot B - C \cdot C^\top$. Ist das Ergebnis eine symmetrische Matrix?

(c) $A^\top - B - 3C^\top$

(d) $A - 2C + B$

8.2 Lineare Abbildungen: Matrixoperationen

Achtung: Ein Symbol - viele Operationen:

- Reelle Multiplkation:

$$\odot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad (x, y) \mapsto \odot(x, y) := x \odot y$$

- Skalare Multiplikation:

$$\odot : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n, \quad (x, y) \mapsto \odot(\lambda, x) := (\lambda \odot x_1, \dots, \lambda \odot x_n)$$

- Euklidisches Skalarprodukt:

$$\odot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}, \quad (x, y) \mapsto \langle x, y \rangle := x \odot y := x_1 \odot y_1 + \dots x_n \odot y_n$$

- Matrix-(Vektor)-Multiplikation:

$$\odot : M^{m \times n} \times M^{n \times p} \to M^{m \times p}, \quad (A, B) \mapsto \odot(A, B) =: C, \ \text{ mit } \ c_{ij} = \sum_{k=0}^{n} a_{ik} \odot b_{kj}$$

8.2 Lineare Abbildungen: Matrixoperationen

Ausblick:

- Die Matrix-Vektor-Multiplikation spielt im Folgenden eine entscheidende Rolle.
- Wir knüpfen nun den Zusammenhang zu den linearen Abbildungen.
- Einen Vektor $x \in \mathbb{R}^n$ können wir als $n \times 1$-Matrix auffassen und mit einer $m \times n$-Matrix A multiplizieren:

$$A \cdot x = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \end{pmatrix}.$$

- Das Ergebnis ist eine $1 \times m$-Matrix, ein Vektor $y \in \mathbb{R}^m$.
- Die Matrix bildet x auf y ab. Wir können zeigen, dass diese Abbildung linear ist.

8.3 Darstellung linearer Abbildungen durch Matrizen

8.3 Lineare Abbildungen: Darstellungsmatrizen

- Die Resultate über lineare Abbildungen sind äußerst nützlich bei der Untersuchung linearer Gleichungssysteme.
- Auf der anderen Seite werden wir auch zeigen, dass jede linearen Abbildung eine Matrix-Darstellung besitzt.
- Mit Matrizen lässt sich sehr einfach rechnen kann, im Gegensatz zu linearen Abbildungen.
- Wir definieren zunächst zu einer Matrix A eine korrespondierende lineare Abbildung.

8.3 Lineare Abbildungen: Darstellungsmatrizen

Defnition: Darstellungsmatrix

Sei $A \in M^{m\times}$. Die zu A gehörige lineare Abbildung f_A ist definiert durch

$$f_A : \mathbb{R}^n \to \mathbb{R}^m, \quad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mapsto Ax = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Die Matrix A heißt **Darstellungsmatrix**. Die Abbildung ist linear:

$$\begin{array}{lllllll} f_A(x+y) & = & A(x+y) & = & Ax + Ay & = & f_A(x) + f_A(y) \\ f_A(\lambda x) & = & A(\lambda \cdot x) & = & \lambda(Ax) & = & \lambda f_A(x). \end{array}$$

8.3 Lineare Abbildungen: Darstellungsmatrizen

Beispiel:
Die zur Matrix

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 1 \\ 3 & 2 \end{pmatrix}$$

gehörige lineare Abbildung f_A ist

$$f_A : \mathbb{R}^2 \to \mathbb{R}^3, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + 2x_2 \\ 3x_1 + x_2 \\ 3x_1 + 2x_2 \end{pmatrix}.$$

8.3 Lineare Abbildungen: Darstellungsmatrizen

Proposition: Bestimmung der Darstellungsmatrix

- Ist $f\colon \mathbb{R}^n \to \mathbb{R}^m$ eine lineare Abbildung, so gibt es *genau eine* Darstellungsmatrix $m \times n$-Matrix A, sodass

$$f(x) = f_A(x), \;\; \forall\, x \in \mathbb{R}^n.$$

  Mit der Standardeinheitsbasis $B = \{e_1, \ldots, e_n\}$ des $\mathbb{R}^n$ ist diese Matrix gegeben durch

$$A = \begin{pmatrix} f(e_1) & f(e_2) & \ldots & f(e_n) \end{pmatrix},$$

  d.h. die Bilder der Basisvektoren stehen in den Spalten der Matrix A.
- Ist $g\colon \mathbb{R}^k \to \mathbb{R}^n$ eine weitere lineare Abbildung mit Darstellungsmatrix B, so ist die Darstellungsmatrix von $g \circ f$ gerade das Matrixprodukt $B \cdot A$.

8.3 Lineare Abbildungen: Darstellungsmatrizen

Beispiele:

- Wir berechnen die Darstellungsmatrix zu

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}.$$

  Dazu berechnen wir

$$f(e_1) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad f(e_2) = \begin{pmatrix} -1 \\ 0 \end{pmatrix} \quad \Rightarrow \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

  Mittels Matrix-Vektor-Multiplikation prüft man sofort nach, dass

$$f_A : \mathbb{R}^2 \to \mathbb{R}^2, (x_1, x_2) \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}$$

  und damit auch $f_A = f$ gilt.

8.3 Lineare Abbildungen: Darstellungsmatrizen

Beispiele:

- Wir berechnen die zu

$$f : \mathbb{R}^3 \to \mathbb{R}, \quad (x_1, x_2, x_3) \mapsto x_1 + x_2$$

gehörige Darstellungsmatrix. Dazu berechnen wir

$$f(e_1) = 1, \quad f(e_2) = 1 \text{ und } f(e_3) = 0$$

und erhalten somit

$$A = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$$

Mittels Matrix-Vektor-Multiplikation prüft man sofort nach, dass

$$f_A : \mathbb{R}^3 \to \mathbb{R}, (x_1, x_2, x_3) \mapsto \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_1 + x_2$$

und damit auch $f_A = f$ gilt.

8.2 Lineare Abbildungen: Aufgabe

Aufgabe:

Betrachten Sie die lineare Abbildung

$$f : \mathbb{R}^3 \to \mathbb{R}^2, \ \ (x_1, x_2, x_3) \mapsto (x_2, x_1 - x_3).$$

1. Geben Sie die Darstellungsmatrix A (bzgl. der Standardeinheitsbasis) an.
2. Berechnen Sie außerdem den Kern der Abbildung.
3. Ist sie surjektiv?

8.3 Lineare Abbildungen: Darstellungsmatrizen

Beispiel: Es geht auch abstrakter! Die Ableitung als lineare Abbildung.

- Die Ableitung ist eine lineare Abbildung, denn für Funktionen g, h aus der Menge der stetig differenzierbaren reellen Funktionen $\mathcal{C}^1(\mathbb{R})$ gilt für alle $x \in \mathbb{R}$
$$(a \cdot g(x) + b \cdot h(x))' = a \cdot g'(x) + b \cdot h'(x)$$
mit Konstanten $a, b \in \mathbb{R}$.
- Betrachten wir speziell die Menge der reellen Polynome dritter Ordnung auf $\mathbb{R}$:
$$P_3[\mathbb{R}] := \left\{p \in \mathcal{C}^1(\mathbb{R}) \mid p(x) = a \cdot x^3 + b \cdot x^2 + c \cdot x + d \cdot 1; \;\; a, b, c, x \in \mathbb{R}\right\}$$
Diese bildet mit den eingeführten Verknüpfungen einen Vektorraum.
- Für $p \in P_3[\mathbb{R}]$ gilt für alle $x \in \mathbb{R}$
$$\begin{array}{rrcrcrcrcr} & p(x) & = & a \cdot x^3 & + & b \cdot x^2 & + & c \cdot x & + & d \cdot 1 \\ \Rightarrow & p'(x) & = & 0 \cdot x^3 & + & 3a \cdot x^2 & + & 2b \cdot x & + & c \cdot 1. \end{array}$$

8.3 Lineare Abbildungen: Darstellungsmatrizen

Beispiel: Es geht auch abstrakter! Die Ableitung als lineare Abbildung.

- Wir können alle Polynome mit Hilfe der (geordneten) Basis $\mathcal{B} = \{x^3, x^2, x, 1\}$ auch als Vektoren darstellen:

$$\begin{array}{rcrlcrlcrlcrl}
p(x) & = & a\cdot & x^3 & + & b\cdot & x^2 & + & c\cdot & x & + & d\cdot 1 & \sim (a,b,c,d)^\top \\
p'(x) & = & 0\cdot & x^3 & + & 3a\cdot & x^2 & + & 2b\cdot & x & + & c\cdot 1 & \sim (0,3a,2b,c)^\top
\end{array}$$

- Der Raum der Polynome 3. Grades hat also Dimension 4. Wir berechnen die Bilder der Basisvektoren:

$$\begin{array}{rcccccccccccl}
(x^3)' & = & 3x^2 & = & 0\cdot x^3 & + & 3\cdot x^2 & + & 0\cdot x & + & 0\cdot 1 & \sim & (0,3,0,0)^\top \\
(x^2)' & = & 2x & = & 0\cdot x^3 & + & 0\cdot x^2 & + & 2\cdot x & + & 0\cdot 1 & \sim & (0,0,2,0)^\top \\
(x)' & = & 1 & = & 0\cdot x^3 & + & 0\cdot x^2 & + & 0\cdot x & + & 1\cdot 1 & \sim & (0,0,0,1)^\top \\
(1)' & = & 0 & = & 0\cdot x^3 & + & 0\cdot x^2 & + & 0\cdot x & + & 0\cdot 1 & \sim & (0,0,0,0)^\top.
\end{array}$$

8.3 Lineare Abbildungen: Darstellungsmatrizen

Beispiel: Es geht auch abstrakter! Die Ableitung als lineare Abbildung.

- Damit ist die Darstellungsmatrix der Ableitung eines Polynomsdritter Ordnung

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{für} \quad \mathcal{B} = \{x^3, x^2, x, 1\}.$$

- Nun können wir Ableitung als lineare Abbildung in Matrix-Vektor-Notation formulieren:

$$f_A : P_3[\mathbb{R}] \to P_3[\mathbb{R}], \quad p \mapsto f_A(p) := p' = A \cdot p,$$

  wobei $p = (a, b, c, d)$ der Koeffizientenvektor von $p(x) = ax^3 + bx^2 + cx + d$ in der Darstellung der Basis $\mathcal{B}$ ist.

8.3 Lineare Abbildungen: Darstellungsmatrizen

Beispiel: Es geht auch abstrakter! Die Ableitung als lineare Abbildung.

- Für $p(x) = 2x^3 + x^2 + 1 \sim (2, 1, 0, 1)$ gilt

$$f_A((2,1,0,1)) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 6 \\ 2 \\ 0 \end{pmatrix}$$

und $(0, 6, 2, 0) \sim p'(x) = 0 \cdot x^3 + 6 \cdot x^2 + 2 \cdot x + 0 \cdot 1 = 6x^2 + 2x.$

8.4 Spezielle lineare Abbildungen

8.4 Lineare Abbildungen: Streckungen

Streckung eines Vektors

Die Diagonalmatrix

$$\operatorname{diag}(a, b, c) = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$$

streckt einen Vektor $(v_1, v_2, v_3)^\top$ um a in x_1-Richtung, um b in x_2-Richtung und um c in x_3-Richtung.

Anmerkungen:

- Falls alle Streckfaktoren gleich sind, handelt es sich um eine skalare Multiplikation.
- Sind nicht alle Streckfaktoren a, b, c gleich, wird der Vektor auch rotiert!

8.4 Lineare Abbildungen: Drehungen

Drehung eines Vektors in der Ebene

Die (orthogonale) **Drehmatrix**

$$D_\varphi = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

dreht einen Vektor $(v_1, v_2)^\top$ in der x_1x_2-Ebene um den Winkel φ gegen den Uhrzeigersinn. Der gedrehte Vektor ist $v' = D_\varphi \cdot v$.

Anmerkung: Die Vektoren einer orthogonalen Matrix sind paarweise orthogonal zueinander (daher der Name!). Für diese Matrizen gilt $Q^\top Q = \mathrm{Id}$.

Drehung eines Vektors im Raum

Seien $c := \cos(\cdot)$ und $s := \sin(\cdot)$. Die (orthogonalen) **Drehmatrizen**

$$D_{x,\alpha} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & -s \\ 0 & s & c \end{pmatrix}, \quad D_{y,\beta} = \begin{pmatrix} c & 0 & -s \\ 0 & 1 & 0 \\ s & 0 & c \end{pmatrix}, \quad D_{z,\gamma} = \begin{pmatrix} c & -s & 0 \\ s & c & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

drehen einen Vektor $(v_1, v_2, v_3)^\top$ um den Winkel α um die x-Achse, um β um die y-Achse und um γ um die z-Achse.

Anmerkung: Jede Drehung um eine beliebige Achse mit Richtung v kann durch Komposition von Drehungen um die x-,y- und z-Achse ausgedrückt werden.

8.4 Lineare Abbildungen: Projektionen

Vorüberlegungen:

- Eine **Projektion** $P : V \to U$ ist eine lineare Abbildung, die einen Vektor $v \in V$ auf einen Unterraum U von V abbildet.
- Wir beschränken uns auf **orthogonale** Abbildungen auf Geraden und Ebenen im $\mathbb{R}^2$ oder $\mathbb{R}^3$.
- In diesem Fall bilden das Urbild v (der Punkt, der projiziert werden soll), das Bild $P(v) \in U$ (der projizierte Punkt) und der Ursprung ein rechtwinkliges Dreieck mit Hypotenuse v und Katheten $P(v)$ bzw. $v - P(v)$.
- Die Katheten stehen senkrecht auf einander und es gilt der Satz des Pythagoras

$$\langle P(v), v - P(v) \rangle = 0, \quad \|v\|_2^2 = \|P(v)\|_2^2 + \|v - P(v)\|_2^2.$$

8.4 Lineare Abbildungen: Projektionen

Vorüberlegungen:

- Da $P(v) \in U$, kann $P(v)$ durch eine Linearkombination der Spannvektoren von U dargestellt werden. Im Fall einer Projektion eines Vektors $v \in \mathbb{R}^2$ auf eine Ursprungsgerade mit Einheitsrichtungsvektor u gilt

$$P(v) = |P(v)| \cdot u.$$

- Für den Winkel α zwischen v und $P(v)$ bzw. u besteht der Zusammenhang

$$\frac{\langle v, P(v) \rangle}{\|v\|_2 \cdot \|P(v)\|_2} = \cos(\alpha) = \frac{\langle v, u \rangle}{\|v\|_2 \cdot \|u\|_2}.$$

- Ein Punkt $u \in U$ wird auf sich selbst projiziert, d.h.

$$P(u) = u \quad \text{und} \quad P(P(v)) = P(v).$$

Herleitung: Wir suchen eine Darstellungsmatrix P der Projektion: Sei u mit $\|u\|_2 = 1$ der Richtungsvektor der Ursprungsgeraden $U \leq \mathbb{R}^2$ und α der Winkel zwischen $v \in \mathbb{R}^2$ und $P(v)$ bzw. u. Dann gilt

$$
\begin{aligned}
P(v) &= \|P(v)\|_2 \cdot u = \|v\|_2 \cos(\alpha) \cdot u = \|u\|_2 \|v\|_2 \cos(\alpha) \cdot u = \langle u, v \rangle \cdot u \\
&= \begin{pmatrix} u_1^2 v_1 & + & u_1 u_2 v_2 \\ u_1 u_2 v_1 & + & u_2^2 v_2 \end{pmatrix} = \begin{pmatrix} u_1^2 & u_1 u_2 \\ u_1 u_2 & u_2^2 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} =: P \cdot v.
\end{aligned}
$$

Die **Projektionsmatrix** ist damit

$$
P = \begin{pmatrix} u_1^2 & u_1 u_2 \\ u_1 u_2 & u_2^2 \end{pmatrix} = u \cdot u^\top.
$$

Das Vorgehen können wir auf den $\mathbb{R}^3$ übertragen.

Orthogonale Projektion eines Vektors auf einen Unterraum

Eine **Projektion** $P : V \to U$ ist eine lineare Abbildung, die einen Vektor $v \in V$ auf einen Unterraum U von V abbildet.

- Die **Projektionsmatrix**

  $$P_G = u \cdot u^\top$$

  projiziert den Vektor $v \in V$ **orthogonal auf die Ursprungsgerade** U mit Einheitsrichtungvektor $u \in U$. Der projizierte Vektor ist $v' = P_G \cdot v$.

- Die **Projektionsmatrix**

  $$P_E = \mathrm{Id} - n \cdot n^\top$$

  projiziert einen Vektor (v_1, v_2, v_3) **orthogonal auf die Ursprungsebene** U mit Einheitsnormalenvektor $n \perp U$. Der projizierte Vektor ist $v' = P_E \cdot v$.

8.4 Lineare Abbildungen: Spiegelungen

Vorüberlegungen:

- Wir betrachten Spiegelungen eines Vektors v des $\mathbb{R}^2$ oder $\mathbb{R}^3$ an deren Unterräumen.
- Urbild v und Spiegelpunkt $S(v)$ liegen im gleichen Abstand zum Unterraum U. Ihre Verbindungslinie steht senkrecht zu U, d.h. das Spiegelzentrum ist die orthogonale $P(v)$

$$S(v) = v + 2(P(v) - v) = 2P(v) - v = 2P \cdot v - \mathrm{Id} \cdot v = (2P - I) \cdot v =: S \cdot v.$$

8.4 Lineare Abbildungen: Spiegelungen

Spiegelung eines Vektors an einem Unterraum

Die **Spiegelmatrix** für die Spiegelung an einer **Ursprungsgerade** mit Einheitsrichtungsvektor u gegeben durch

$$S_G = 2P_G - \mathrm{Id} = 2uu^\top - \mathrm{Id}\,.$$

Die **Spiegelmatrix** für die Spiegelung an einer **Ursprungsebene** mit Einheitsnormalenvektor n lautet

$$S_E = 2P_E - \mathrm{Id} = 2(\mathrm{Id} - nn^\top) - \mathrm{Id} = \mathrm{Id} - 2nn^\top.$$

8.4 Lineare Abbildungen: Spiegelungen

Spiegelung eines Vektors an einer Ursprungsebene im $\mathbb{R}^2$

Wir können die Spiegelung eines Vektors an einer Ursprungsgeraden im $\mathbb{R}^2$ auch über den Neigungswinkel der Geraden ausdrücken. Die orthogonale Matrix

$$S_G = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix}.$$

spiegelt einen Vektor $v \in \mathbb{R}^2$ an einer Geraden mit Neigungswinkel $\frac{\alpha}{2}$ gegenüber der x-Achse (gemessen im Gegenuhrzeigersinn). Der Spiegelvektor ist $v' = S_G \cdot v$.

9. Determinante und Inverse einer Matrix

9. Determinante und Inverse

Ziel: Entwicklung einer Lösungstheorie für lineare Gleichungssysteme

Zentrale Fragen:

1. Existiert eine Lösung des linearen Gleichungssystems?
2. Wenn eine Lösung existiert, ist diese eindeutig?
3. Wie kann man diese Lösung berechnen?

Entscheidende Hilfsmittel zur Beantwortung der Fragen werden der **Rang** und die **Determinante** der Matrix sein.

9.1 Determinanten von 2×2-Matrix

9.1 Determinanten von 2×2-Matrix: Herleitung

Diskussion:
Wir betrachten zunächst ein Gleichungssystem mit $m = 2$ Gleichungen und $n = 2$ Unbekannten:

$$\begin{array}{lrcl} (1) & a_{11}x_1 + a_{12}x_2 & = & b_1, \\ (2) & a_{21}x_1 + a_{22}x_2 & = & b_2, \end{array}$$

Wir eliminieren x_2, indem wir Gleichung (1) mit a_{22}, Gleichung (2) mit $(-a_{12})$ multiplizieren und beide Zeilen addieren. Wir erhalten eine Gleichung für x_1:

$$\begin{array}{rlcll} (1) & a_{11}x_1 + a_{12}x_2 & = & b_1 & \mid \cdot a_{22} \\ +(2) & a_{21}x_1 + a_{22}x_2 & = & b_2 & \mid \cdot (-a_{12}) \\ \hline & (a_{11}a_{22} - a_{12}a_{21})\, x_1 & = & b_1 a_{22} - b_2 a_{12} & \end{array}$$

9.1 Determinanten von 2×2-Matrix: Herleitung

Analog bestimmen wir x_2:

$$
\begin{array}{rrcll}
(1) & a_{11}x_1 + a_{12}x_2 & = & b_1 & \mid \cdot (-a_{21}) \\
+(2) & a_{21}x_1 + a_{22}x_2 & = & b_2 & \mid \cdot a_{11} \\
\hline
 & (a_{11}a_{22} - a_{12}a_{21})\, x_2 & = & b_2 a_{11} - b_1 a_{21} &
\end{array}
$$

1. Falls $(a_{11}a_{22} - a_{12}a_{21}) \neq 0$, hat das LGS die **eindeutige Lösung**

$$
x_1 = \frac{b_1 a_{22} - b_2 a_{12}}{a_{11}a_{22} - a_{12}a_{21}},
$$
$$
x_2 = \frac{b_2 a_{11} - b_1 a_{21}}{a_{11}a_{22} - a_{12}a_{21}}.
$$

9.1 Determinanten von 2×2-Matrix: Herleitung

2. Falls $(a_{11}a_{22} - a_{12}a_{21}) = 0$, kann nur noch eine Lösung existieren, wenn beide rechten Seiten identisch Null sind, d.h.

$$\begin{aligned} b_1 a_{22} - b_2 a_{12} &= 0, \\ b_2 a_{11} - b_1 a_{21} &= 0. \end{aligned}$$

   Dann allerdings ist die **Lösung nicht eindeutig**, denn jeder Vektor $(x_1, x_2) \in \mathbb{R}^2$ erfüllt das lineare Gleichungssystem.

3. Falls $(a_{11}a_{22} - a_{12}a_{21}) = 0$ und nicht beide rechte Seiten null, existiert **keine Lösung**.

9.1 Determinanten von 2×2-Matrix: Herleitung

Fazit:
Die Zahl $(a_{11}a_{22} - a_{12}a_{21})$ **determiniert** also das Lösungsverhalten des Gleichungssystems und wird folgerichtig als Determinante bezeichnet. Notieren wir das LGS in Matrixschreibweise:

$$\underbrace{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

Wir können also bereits anhand der Matrix A ablesen, ob ein LGS eine eindeutige Lösung hat.

9.1 Determinanten von 2×2-Matrix: Definition

Definition: Determinante einer 2×2-Matrix

Die **Determinante** einer 2×2-Matrix A ist die Zahl

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

9.1 Determinanten von 2×2-Matrix: Beispiele

Beispiele: Wir untersuchen die Matrizen

$$A = \begin{pmatrix} 3 & 5 \\ -2 & 4 \end{pmatrix}, \quad A^\top = \begin{pmatrix} 3 & -2 \\ 5 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 3 \\ -10 & -6 \end{pmatrix} \quad C = \begin{pmatrix} 5 & 3 \\ 0 & -6 \end{pmatrix}$$

und berechnen

$$\begin{aligned}
\det A &= \begin{vmatrix} 3 & 5 \\ -2 & 4 \end{vmatrix} = 3 \cdot 4 - 5 \cdot (-2) = 22 \\
\det A^\top &= \begin{vmatrix} 3 & -2 \\ 5 & 4 \end{vmatrix} = 3 \cdot 4 - (-2) \cdot 5 = 22 \\
\det B &= \begin{vmatrix} 5 & 3 \\ -10 & -6 \end{vmatrix} = 5 \cdot (-6) - 3 \cdot (-10) = 0 \\
\det C &= \begin{vmatrix} 5 & 3 \\ 0 & -6 \end{vmatrix} = 5 \cdot (-6) - 3 \cdot 0 = 5 \cdot (-6) = -30.
\end{aligned}$$

9.1 Determinanten von 2×2-Matrix: Eigenschaften

Proposition: Determinanten spezieller Matrizen

Die Determinante einer 2×2-Dreiecksmatrix A ist

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{vmatrix} = a_{11} \cdot a_{22}$$

Die Determinante der Transponierten Matrix $A^\top$ ist

$$\det A^\top = \begin{vmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \det A.$$

Anmerkung: Bei Vertauschung der Zeilen mit den Spalten ändert sich die Determinante nicht.

9.1 Determinanten von 2×2-Matrix: Eigenschaften

Satz: Determinante bei linearer Abhängigkeit

Sind die Zeilenvektoren (bzw. Spaltenvektoren) der Matrix A linear abhängig, so gilt

$$\det A = 0.$$

Beweis: Lineare Abhängigkeit der Zeilenvektoren bedeutet im 2×2-Fall), dass die Vektoren Vielfache voneinander sind, d.h.

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ ka_{11} & ka_{12} \end{vmatrix} = a_{11} \cdot (ka_{12}) - a_{12} \cdot (ka_{11}) = 0$$

$\square$

9.1 Determinanten von 2×2-Matrix: Eigenschaften

Satz: Elementare Zeilen-/Spaltenoperationen

Sei A eine 2×2-Matrix und $\lambda \in \mathbb{R}\backslash\{0\}$. Dann gilt.

1. Die Determinante der Matrix A', die aus A durch das Tauschen zweier Zeilen bzw. Spalten entsteht, ist $-\det A$.
2. Die Determinante der Matrix A', die aus A durch Multiplikation einer Zeile bzw. Spalte mit einem Skalar λ entsteht, ist $\lambda \det A$.
3. Die Determinante der Matrix A', die aus A durch Addition einer mit einem Vielfachen λ multiplizierten Zeile/Spalte zu einer anderen Zeile/Spalte entsteht, ist $\det A$.

Anmerkung: Diese Umformung ist vor allem für die Bestimmung von Determinanten großer Matrizen äußerst nützlich.

9.1 Determinanten von 2×2-Matrix: Eigenschaften

Beweis:

1. Es gilt
$$\det A' = \begin{vmatrix} a_{21} & a_{22} \\ a_{11} & a_{12} \end{vmatrix} = a_{21}a_{12} - a_{22}a_{11} = -\det A.$$
2. Es gilt z.B. für die erste Zeile
$$\det A' = \begin{vmatrix} \lambda a_{11} & \lambda a_{12} \\ a_{21} & a_{22} \end{vmatrix} = (\lambda a_{11})a_{22} - (*\lambda a_{12})a_{21} = \lambda \det A.$$
3. Bei Addition des λ-fachen der zweiten Zeile zur ersten erhalten wir
$$\begin{aligned} \det A' &= \begin{vmatrix} a_{11} + \lambda a_{21} & a_{12} + \lambda a_{22} \\ a_{21} & a_{22} \end{vmatrix} \\ &= (a_{11} + \lambda a_{21})\, a_{22} - (a_{12} + \lambda a_{22})\, a_{21} \\ &= a_{11}a_{22} - a_{12}a_{21} = \det A. \square \end{aligned}$$

9.1 Determinanten von 2×2-Matrix: Eigenschaften

Beispiel: Wir können die Matrix

$$A = \begin{pmatrix} 3 & 6 \\ -2 & 4 \end{pmatrix}$$

in Dreicksform bringen, indem wir zur zweiten Zeile das $2/3$-fache der ersten addieren:

$$\det A = \begin{vmatrix} 3 & 6 \\ 0 & 8 \end{vmatrix} = 3 \cdot 8 = 24$$

Anmerkung: Das Verfahren ist für 2×2-Matrizen noch wenig einleuchtend, aber für große Matrizen sehr effizient.

9.1 Determinanten von 2×2-Matrix: Eigenschaften

Satz: Determinanten-Multiplikationssatz

Seien A, B 2×2-Matrizen. Dann gilt

$$\det(A \cdot B) = (\det A) \cdot (\det B).$$

Anmerkung: Die Determinante eines Produktes lässt sich über die Einzeldeterminanten ohne die aufwendige Matrizenmultiplikation berechnen.

9.1 Determinanten von 2×2-Matrix: Eigenschaften

Beispiel: Wir betrachten die 2×2-Matrizen

$$A = \begin{pmatrix} 3 & 6 \\ -2 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ -2 & -2 \end{pmatrix}.$$

Um $\det(A \cdot B)$ zu bestimmen, genügt es zu sehen, dass die Zeilen von B linear abhängig sind. Damit gilt dann schon

$$\det(A \cdot B) = \det A \cdot \det B = 0.$$

9.1 Determinanten von 2×2-Matrix: Interpretation

Diskussion: Geometrische Interpretation der Determinante

- Wir wissen bereits, dass die Multiplikation einer Matrix mit einem Vektor diesen strecken, drehen, projizieren oder spiegeln kann.
- Betrachten wir die Multiplikation einer Matrix mit den Einheitsvektoren e_1, e_2:

$$A \cdot e_1 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix}, \quad A \cdot e_2 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{21} \\ a_{22} \end{pmatrix}.$$

- Die Urbildvektoren spannen das Einheitsquadrat mit Flächeninhalt 1 auf.
- Die Bildvektoren Ae_1 und Ae_2 spannen ein Parallelogramm auf. Sei $\alpha \in (0^\circ, 180^\circ)$ der Winkel zwischen Ae_1 und Ae_2.

Diskussion: Geometrische Interpretation der Determinante

- Die Formel für den Flächeninhalt F des Parallelogramms gilt

$$
\begin{aligned}
F &= \|Ae_1\|_2 \cdot \|Ae_2\|_2 \cdot \sin(\alpha) \\
&= \|Ae_1\|_2 \cdot \|Ae_2\|_2 \cdot \sqrt{1 - \cos^2(\alpha)} \\
&= \sqrt{\|Ae_1\|_2^2 \cdot \|Ae_2\|_2^2 - \|Ae_1\|_2^2 \cdot \|Ae_2\|_2^2 \cos^2(\alpha)} \\
&= \sqrt{\|Ae_1\|_2^2 \cdot \|Ae_2\|_2^2 - \langle Ae_1, Ae_2 \rangle^2} \\
&= \sqrt{(a_{11}^2 + a_{21}^2) \cdot (a_{12}^2 + a_{22}^2) - (a_{11}a_{12} + a_{21}a_{22})^2} \\
&= \sqrt{(a_{11}a_{12})^2 - 2a_{11}a_{12}a_{21}a_{22} + (a_{21}a_{12})^2} \\
&= \sqrt{(a_{11}a_{22} - a_{21}a_{12})^2} = |a_{11}a_{22} - a_{21}a_{12}| = |\det(A)|.
\end{aligned}
$$

9.1 Determinanten von 2×2-Matrix: Interpretation

Diskussion: Geometrische Interpretation der Determinante

- Der Betrag der Determinante einer Matrix ist also der Flächeninhalt des von den Spaltenvektoren aufgespannten Parallelogramms.
- Die Determinante ist also so etwas wie ein Streckfaktor für die Fläche des Einheitsquadrats.
- Ein negatives Vorzeichen der Determinante deutet dabei an, dass sich die Orientierung der Bildvektoren gegenüber den Urbildvektoren geändert hat, d.h. der Winkel von Ae_1 gegen den Uhrzeigen nach Ae_2 ist $\alpha \in (180^\circ, 360^\circ)$.

9.2 Determinanten von $n \times n$-Matrix

9.2 Determinanten von $n \times n$-Matrix: Übersicht

Ausblick: Wir möchten die Determinante für eine $n \times n$-Matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

bestimmen. Im Allgemeinen gibt es zwei Möglichkeiten:

- Umformung von A in Dreiecksform mittels Zeilen- und Spaltenopeartionen.
- Entwicklungssatz von Laplace.

Sonderfälle:

- Für $n = 2$ gilt die Formel $\det(A) = a_{11}a_{22} - a_{12}a_{21}$.
- Für $n = 3$ gilt die Formel von Sarrus.

9.2 Determinanten von $n \times n$-Matrix: mittels Dreicksform

Determinante: Mit Hilfe elementarer Zeilen-/Spaltenoperationen

- Wir bringen Matrix A mit Hilfe elementarer Zeilenumformungen in Dreiecksform.
- Dabei merken die Anzahl k an Zeilen- bzw. Spaltentauschungen und mit welchen Faktoren $\lambda_1, \ldots \lambda_l$ wir Zeilen/Spalten multipliziert haben.
- Die Determinante der Dreiecksmatrix D ist das Produkt der Hauptdiagonalenelemente

$$\det(D) = d_{11} \cdot \ldots \cdot d_{nn}$$

- Die Determinante von A ist dann

$$\det(A) = (-1)^k \cdot \prod_{i=1}^{l} \frac{1}{\lambda_i} \cdot \det(D).$$

Anmerkung: Für große Matrizen mit vielen Nullen eignet sich auch der *Entwicklungssatz nach Laplace*.

9.2 Determinanten von $n \times n$-Matrix: Entwicklungssatz

Der Entwicklungssatz von Laplace

Für eine $n \times n$-Matrix A definiere die **Determinante** als die Zahl

$$\det A := \begin{cases} a_{11}, & n = 1, \\ \sum_{j=1}^{n} (-1)^{1+j} a_{1j} \cdot \det(A_{1j}), & n \geq 2, \end{cases}$$

wobei A_{1j} die $(n-1) \times (n-1)$-Matrix ist, die aus A durch Streichen der ersten Zeile und j-ten Spalte entsteht.

Anmerkung: Die Definition nennt man die *Entwicklung der Determinanten nach der ersten Zeile*.

9.2 Determinanten von $n \times n$-Matrix: Entwicklungssatz

Anmerkungen:

- Die Determinante kann nach jeder Zeile entwickelt werden:

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}), \quad i \in \{1, \ldots, n\}.$$

- Ebenso kann man nach jeder Spalte entwickeln:

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}), \quad j \in \{1, \ldots, n\}.$$

- Der Faktor A_{ij} bezeichnet hierbei die durch Streichung der i-ten Zeile und j-ten Spalte erhaltene Matrix.
- In der Anwendung entwickelt man nach einer Zeile/Spalte, die möglichst viele Nullen enthält.

9.2 Determinanten von $n \times n$-Matrix: Entwicklungssatz

Beispiele:

- Für $n = 2$ gilt auch mit dem Entwicklungssatz die bereits bekannte Formel:

$$\begin{aligned} \det(A) &= \sum_{j=1}^{2} (-1)^{1+j} a_{1j} \det(A_{1j}) \\ &= (-1)^{1+1} a_{11} \det(A_{11}) + (-1)^{1+2} a_{12} \det(A_{12}) \\ &= a_{11} a_{22} - a_{12} a_{21}. \end{aligned}$$

- Für $n = 3$ gilt $\quad \det(A) = \sum_{j=1}^{3} (-1)^{1+j} a_{1j} \det(A_{1j})$

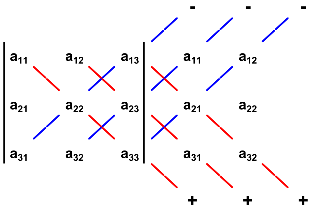
$$= (-1)^{1+1} a_{11} \cdot \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} + (-1)^{1+2} a_{12} \cdot \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + (-1)^{1+3} a_{13} \cdot \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

$$= a_{11} a_{22} a_{33} - a_{11} a_{23} a_{32} - a_{12} a_{21} a_{33} + a_{12} a_{23} a_{31} + a_{13} a_{21} a_{32} - a_{13} a_{22} a_{31}.$$

9.2 Determinanten von $n \times n$-Matrix: Entwicklungssatz

Beispiele:

- Der Entwicklungssatz ist für $n = 3$ nur bei vielen Nullen praktisch. Andernfalls bietet sich die sogenannte **Regel von Sarrus** an:



Hier addiert man die entlang der roten Linien multiplizierten Elemente, subtrahiert die Produkte entlang der blauen Linien und erhält den obigen Ausdruck in einer etwas anderen Reihenfolge:

$$\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}.$$

9.2 Determinanten von $n \times n$-Matrix: Entwicklungssatz

Beispiele:

- Die Vorzeichen für den Entwicklungssatz finden wir anhand des „Schachbrettmusters"

$$\begin{pmatrix} + & - & + & - & + & \dots \\ - & + & - & + & - & \dots \\ + & - & + & - & + & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

- Die Determinante der 4×4-Matrix berechnen wir durch Entwicklung nach der 3. Zeile entsprechend der Vorzeichen des Schachbretts:

$$A = \begin{pmatrix} 1 & 2 & -3 & 4 \\ 0 & 4 & 5 & 1 \\ \color{red}{1} & \color{green}{0} & \color{blue}{0} & \color{orange}{2} \\ -1 & 3 & 4 & 0 \end{pmatrix} \quad \text{mit} \quad \begin{pmatrix} + & - & + & - \\ - & + & - & + \\ \color{red}{\oplus} & \color{green}{\ominus} & \color{blue}{\oplus} & \color{orange}{\ominus} \\ - & + & - & + \end{pmatrix}.$$

Es folgt

$$\det(A) = (+1)\det\begin{pmatrix} \cancel{1} & 2 & -3 & 4 \\ \cancel{0} & 4 & 5 & 1 \\ \cancel{1} & \cancel{0} & \cancel{0} & \cancel{2} \\ \cancel{-1} & 3 & 4 & 0 \end{pmatrix} + (-0)\det\begin{pmatrix} 1 & \cancel{2} & -3 & 4 \\ 0 & \cancel{4} & 5 & 1 \\ \cancel{1} & \cancel{0} & \cancel{0} & \cancel{2} \\ -1 & \cancel{3} & 4 & 0 \end{pmatrix}$$

$$+ (+0)\det\begin{pmatrix} 1 & 2 & \cancel{-3} & 4 \\ 0 & 4 & \cancel{5} & 1 \\ \cancel{1} & \cancel{0} & \cancel{0} & \cancel{2} \\ -1 & 3 & \cancel{4} & 0 \end{pmatrix} + (-2)\det\begin{pmatrix} 1 & 2 & -3 & \cancel{4} \\ 0 & 4 & 5 & \cancel{1} \\ \cancel{1} & \cancel{0} & \cancel{0} & \cancel{2} \\ -1 & 3 & 4 & \cancel{0} \end{pmatrix}$$

$$= \det\begin{pmatrix} 2 & -3 & 4 \\ 4 & 5 & 1 \\ 3 & 4 & 0 \end{pmatrix} - 2\cdot\det\begin{pmatrix} 1 & 2 & -3 \\ 0 & 5 & 1 \\ -1 & 4 & 0 \end{pmatrix} = -13 - 2\cdot(-21) = 29.$$

Die Berechnung der Unterdeterminanten erfolgt hierbei nach der Regel von Sarrus.

9.2 Determinanten von $n \times n$-Matrix: Entwicklungssatz

Anmerkungen:

- Zur allgemeinen Berechnung einer Determinante für $n \geq 4$ ist das Entwicklungsverfahren sehr aufwendig.
- Es ist meist effektiver die Matrix in eine Dreiecksmatrix umzuformen, dann wie bereits bekannt die Hauptdiagonalenelemente zu multiplizieren und dabei für jeden Zeilen- bzw. Spaltentausch einen Vorzeichenwechsel vorzunehmen.
- Auch die anderen Eigenschaften der Determinante können wir auf $n \times n$-Matrizen übertragen.

9.2 Determinanten von $n \times n$-Matrix: Elementaroperationen

Satz: Elementare Zeilen- und Spaltenoperationen

Sei A eine $n \times n$-Matrix. Dann gilt.

1. Die Determinante der Matrix, die aus A durch eine Zeilenvertrauschung (**oder** eine Spaltenvertauschung) entsteht ist $-\det A$.
2. Die Determinante der Matrix, die aus A durch Multiplikation einer Zeile (**oder** Spalte) mit einem Skalar λ entsteht ist $\lambda \det A$. Insbesondere gilt
$$\det(\lambda A) = \lambda^n \det A.$$
3. Die Determinante der Matrix, die aus A durch Addition einer mit einem Vielfachen λ multiplizierten Zeile/Spalte zu einer anderen Zeile/Spalte entsteht ist $\det A$.

9.2 Determinanten von $n \times n$-Matrix: Eigenschaften

Satz: Eigenschaften der Determinante

Sei A eine $n \times n$-Matrix. Dann gilt.

- Ist A in Dreiecksform, so ist die Determinante das Produkt der Diagonaleinträge, also

$$\det A = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}.$$

- Es gilt $\det A^\top = \det A$.
- Falls die Zeilenvektoren linear abhängig sind, so gilt $\det A = 0$.
- Ist B eine weitere $n \times n$-Matrix so gilt der Multiplikationssatz

$$\det(A \cdot B) = (\det A) \cdot (\det B).$$

9.2 Determinanten von $n \times n$-Matrix

Beispiele:

- Wir transponieren die Matrix (keine Änderung der Determinante) und tauschen dann die erste und zweite Spalte (Mult. der Determinanten mit (-1)) und erhalten eine Dreiecksmatrix:

$$\det A = \begin{vmatrix} 1 & 3 & 0 \\ 1 & 0 & 0 \\ 2 & 4 & 5 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 2 \\ 3 & 0 & 4 \\ 0 & 0 & 5 \end{vmatrix} = - \begin{vmatrix} 1 & 1 & 2 \\ 0 & 3 & 4 \\ 0 & 0 & 5 \end{vmatrix} = -1 \cdot 3 \cdot 5 = -15$$

- Oft ist Ausklammern praktisch, um große Zahlen zu vermeiden:

$$\begin{vmatrix} 3 & 6 & 0 \\ 3 & 12 & 15 \\ 0 & 9 & 0 \end{vmatrix} = \left| 3 \cdot \begin{pmatrix} 1 & 2 & 0 \\ 1 & 4 & 5 \\ 0 & 3 & 0 \end{pmatrix} \right| = 3^3 \cdot \left| \begin{pmatrix} 1 & 2 & 0 \\ 1 & 4 & 5 \\ 0 & 3 & 0 \end{pmatrix} \right| = 27 \cdot (-15)$$

9.2 Determinanten von $n \times n$-Matrix

Beispiele:

- Betrachte die Matrizen

$$A = \begin{pmatrix} 1 & 4 & -2 \\ 0 & 3 & 1 \\ 1 & -5 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

  Dann ist aufgrund der Nullzeile $\det(B) = 0$ und es folgt

$$\det(AB) = (\det A) \cdot (\det B).$$

9.2 Determinanten von $n \times n$-Matrix: Aufgabe

Aufgabe:

Berechnen Sie die Determinanten der folgenden Matrizen

$$\begin{pmatrix} 3 & 11 \\ x & 2x \end{pmatrix}, \quad \begin{pmatrix} a & b \\ a & b \end{pmatrix}, \quad \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}, \quad \begin{pmatrix} 3 & 4 & 10 \\ -7 & 4 & 1 \\ 0 & 2 & 8 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 3 & 4 \\ -2 & 1 & 0 & 3 \\ 1 & 4 & 1 & 5 \\ 0 & 2 & 2 & 0 \end{pmatrix}.$$

9.3 Die Inverse einer Matrix

9.3 Inverse einer Matrix

Überlegungen:

- Bijektive Abbildungen besitzen eine Umkehrabbildung.
- Die Umkehrfunktion eines Isomorphismus ist linear.
- Jede lineare Abbildung besitzt eine Darstellungsmatrix.
- Wir müssten also eine Darstellungsmatrix der Umkehrabbildung, die **inverse Matrix**, finden können.
- Dazu nutzen wir die Tatsachen, dass eine Abbildung eindeutig bestimmt wird durch die Bilder der Basisvektoren und dass Isomorphismen Basen wieder auf Basen abbilden.

9.3 Inverse einer Matrix

Ergebnis:
Mit der Inversen einer Matrix können wir dann ein lineares Gleichungssystems der Form

$$Ax = b, \quad A \in M^{n \times n}, \;\; b \in \mathbb{R}^n, \;\; x \in \mathbb{R}^n$$

lösen, falls die Abbildung f_A bijektiv ist. Dies ist z.B. für Streckungen, Spiegelungen und Drehungen sowie deren Kombinationen der Fall.

9.3 Inverse: Definition

Definition: Inverse einer Matrix

Sei A eine gegebene $n \times n$ Matrix. Gibt es eine $n \times n$-Matrix B, so dass

$$A \cdot B = B \cdot A = \mathrm{Id}_n$$

so heißt die Matrix A **invertierbar**. Eine solche Matrix B heißt dann die **Inverse** der Matrix A und wird mit A^{-1} bezeichnet.

Anmerkung: Ist eine Matrix invertierbar, so ist ihre Inverse eindeutig. Genügt eine Matrix B der Gleichung

$$AB = \mathrm{Id}_n$$

so ist sie bereits die Inverse von A, es gilt also automatisch $BA = \mathrm{Id}_n$.

9.3 Inverse

Bemerkungen/Beispiele:

- Im Fall $n = 1$ ist jede Matrix A eine Zahl und diese ist genau dann invertierbar mit Inverser $1/A$, wenn sie ungleich Null ist.
- Die Matrizen
$$\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}$$
sind invers zueinander, denn
$$\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
- Die Nullmatrix ist nicht invertierbar.

9.3 Inverse

Bemerkungen/Beispiele:

- Zu jeder Matrix A können wir die zugehörige lineare Abbildung

$$f_A : \mathbb{R}^n \to \mathbb{R}^n, \;\; x \mapsto Ax$$

betrachten. Dann ist A invertierbar genau dann, wenn f als Abbildung umkehrbar - also ein Isomorphismus - ist. Es gilt dann

$$(f_A)^{-1} = f_{A^{-1}},$$

d.h. $(f_A)^{-1}$ ist dann explizit gegeben durch

$$(f_A)^{-1} : \mathbb{R}^n \to \mathbb{R}^n, \;\; x \mapsto A^{-1}x.$$

9.3 Inverse: Eigenschaften

Proposition: Eigenschaften der Inversen

Sei A eine $n \times n$-Matrix.

1. A ist invertierbar genau dann, wenn $\det A \neq 0$.
2. Ist A invertierbar, so auch A^{-1} und es gilt
$$\left(A^{-1}\right)^{-1} = A \quad \text{und} \quad \det(A^{-1}) = \frac{1}{\det A}.$$
3. Sind A und B invertierbare $n \times n$-Matrizen so ist $A \cdot B$ auch invertierbar und es gilt
$$(AB)^{-1} = B^{-1}A^{-1}.$$

9.3 Inverse

Beispiele: Betrachte die Matrizen

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Anhand der Determinante liest man sofort ab, dass die ersten drei nicht invertierbar sind, die letzten beiden sehr wohl.

9.3 Inverse: Berechnungsverfahren

Diskussion: Berechnung der Inversen

Sei A eine gegebene $n \times n$-Matrix mit $\det A \neq 0$.

- Da ein Isomorphismus eine Basis wieder auf eine Basis abbildet, suchen wir die Vektoren b_1, b_2 und b_3, die durch A auf die Standardbasisvektoren abgebildet werden.
- D.h. wir müssen die folgenden linearen Gleichungssysteme lösen

$$Ab_1 = e_1, \quad Ab_2 = e_2, \quad Ab_3 = e_3.$$

- Dazu verwenden wir die bereits vorgestellten Zeilenoperationen bis auf der linken Seite die Einheitsmatrix steht.

9.3 Inverse: Berechnungsverfahren

Diskussion: Berechnung der Inversen

- Da die Zeilenoperationen für die 3 LGS jeweils identisch sind, können wir Arbeit sparen, indem wir die Umformungen auf die drei rechten Seiten gleichzeitig anwenden, d.h. wir lösen

$$A \cdot B = \mathrm{Id}$$

  nach $B = (b_1 \ \ b_2 \ \ b_3) \in M^{n \times n}$.
- Kurz: wir formen wir $(A | \mathrm{Id})$ zu $(\mathrm{Id} | B)$ um.
- B ist dann die gesuchte Inverse, d.h. $A^{-1} := B$.

Das Berechnungsverfahren wird auch **Gauß-Jordan-Algorithmus** genannt.

9.4 Das Gauß-Jordan-Verfahren

9.4 Inverse: Das Gauß-Jordan-Verfahren

Der Gauß-Jordan-Algorithmus

Seien eine invertierbaren Matrix $A \in M^{n \times n}$ und $b \in \mathbb{R}^n$ gegeben.

- Wir formen ein Gleichungssystem $Ax = b$ durch elementare *Zeilen*operationen in ein System $\mathrm{Id}\, x = \tilde{b}$ um.
- Dabei ist $\tilde{b}$ die *eindeutige* Lösung des LGS.
- Zur Berechnung der Lösung gehen wir wie folgt vor:

1. Schreibe das Gleichungssystem als **erweiterte Koeffizientenmatrix** $(A|b)$.

$$\left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \dots & a_{nn} & b_n \end{array}\right).$$

Der Gauß-Jordan-Algorithmus

2. Falls $a_{11} = 0$ ist, tausche Zeile 1 mit einer Zeile mit $a_{k,1} \neq 0$.
3. Falls dieses $a_{k,1} \neq 1$, dividiere die ganze Zeile durch $a_{k,1}$.
4. Addiere ein geeignetes Vielfaches der ersten Zeile zu den anderen Zeilen so hinzu, dass $a_{i,1} = 0$ für alle $i = 2, \ldots, n$. Das LGS hat dann die Form

$$\left(\begin{array}{cccc|c} 1 & * & \ldots & * & * \\ 0 & * & \ldots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & * & \ldots & * & * \end{array}\right).$$

Der Gauß-Jordan-Algorithmus

5. Verfahre analog mit der $(n-1) \times (n-1)$-Matrix (a_{ij}) für $2 \leq i, j \leq n$ bis eine obere Dreiecksmatrix entsteht:

$$\left(\begin{array}{cccc|c} 1 & * & \dots & * & * \\ 0 & \ddots & \ddots & \vdots & * \\ \vdots & \ddots & \ddots & * & * \\ 0 & \dots & 0 & 1 & * \end{array}\right).$$

Anmerkung: Da die Matrix invertierbar ist, sind alle Hauptdiagonalelement ungleich null.

9.4 Inverse: Das Gauß-Jordan-Verfahren

Der Gauß-Jordan-Algorithmus

6. Addiere ein geeignetes Vielfaches der letzten Zeile zu den darüberliegenden Zeilen so hinzu, dass oberhalb von $a_{n,n}$ eine Nullspalte entsteht, d.h. $a_{n,i} = 0$ für $i = 1, \ldots, n-1$.
7. Verfahre analog für die Spalten $n-1$, $n-2$, …, 2, 1, sodass links die **Einheitsmatrix** steht. Rechts steht dann die Lösung $\tilde{b}$ des LGS:

$$\left(\begin{array}{cccc|c} 1 & 0 & \ldots & 0 & \tilde{b}_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & \tilde{b}_n \end{array}\right).$$

9.4 Inverse: Das Gauß-Jordan-Verfahren

Beispiel: Wir berechnen die Inverse einer 2×2-Matrix A. Dazu lösen wir gleichzeitig die beiden Gleichungssysteme $Ax = e_1$ und $Ax = e_2$:

$$(A|\,\mathrm{Id}) = \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ c & d & 0 & 1 \end{array}\right)$$

$$\to \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & ad-bc & -c & a \end{array}\right) \quad \to \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & 1 & \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{array}\right)$$

$$\to \left(\begin{array}{cc|cc} a & 0 & 1+\frac{bc}{ad-bc} & \frac{-ba}{ad-bc} \\ 0 & 1 & \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & 0 & \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ 0 & 1 & \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{array}\right) = (\mathrm{Id}\,|A^{-1})$$

9.4 Inverse: Das Gauß-Jordan-Verfahren

Bemerkungen:

- Wir haben eine Formel für die Inverse einer 2×2-Matrix gefunden:

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

- Das letzte Beispiel zeigt den Zusammenhang zwischen der Determinante und der Inversen. Die Berechnung von A^{-1} funktioniert also nur, falls

$$\det(A) = ad - bc \neq 0.$$

- Tatsächlich gilt sogar Äquivalenz:

$$\det(A) \neq 0 \quad \Leftrightarrow \quad \exists A^{-1}.$$

9.4 Inverse: Das Gauß-Jordan-Verfahren

Bemerkungen/Beispiel:

- Ist in einem Schritt des Algorithmus kein von Null verschiedenes Spaltenelement auffindbar, so ist die Determinante Null und die Matrix nicht invertierbar.
- Das Vorgehen zur Berechnung der Inversen einer Matrix $A \in M^{n\times n}$ funktioniert analog durch Umformen von $(A|\,\mathrm{Id}) \in M^{n\times 2n}$ zu $(\mathrm{Id}\,|A) \in M^{n\times 2n}$.
- Wir berechnen die Inverser der Matrix

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{pmatrix}.$$

9.4 Inverse: Das Gauß-Jordan-Verfahren

$$
(A|\,\mathrm{Id}) = \left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \end{array}\right) \quad \begin{array}{l} II' = II - I \\ \\ IV' = IV - I \end{array}
$$

$$
\rightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & -1 & 0 & 0 & 1 \end{array}\right) \quad III' = III + II
$$

$$
\rightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 & -1 & 0 & 0 & 1 \end{array}\right) \quad IV' = IV + III
$$

9.4 Inverse: Das Gauß-Jordan-Verfahren

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & -2 & 1 & 1 & 1 \end{array}\right) \qquad \begin{array}{lcl} II' & = & II + 0.5 \cdot IV \\ III' & = & III - 0.5 \cdot IV \\ IV' & = & IV : 2 \end{array}$$

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & -1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right) \quad = \quad (\mathrm{Id}\,|A^{-1})$$

Die Matrix A ist also invertierbar und A^{-1} ist nun auf der rechten Seite der letzten Umformung erkennbar.

9.4 Inverse: Das Gauß-Jordan-Verfahren

Aufgabe:

Berechnen Sie die Inverse der folgenden Matrix:

$$\begin{pmatrix} 0 & 1 & -1 & 0 \\ 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

10. Lösungstheorie für Lineare Gleichungssysteme

10.1 Rang einer Matrix: Hintergrund

- **Hintergrund:** Lineare Gleichungssystem haben vielseitige Anwendungsbereiche.
  - Berechnung statischer und dynamischer Systeme: Brücken, Gebäude, elektrische Netzwerke;
  - Betriebswirtschaftliche Optimierungsaufgaben;
  - Wettervorhersage, Strömungssimulation, Crashsimulationen;
  - Computergrafik, Suchmaschinen.
- **Schwierigkeiten:** Sehr große lineare Systeme mit Millionen von Gleichungen und Unbekannte, müssen unter Umständen hunderte Male gelöst werden.
- **Ziel:** Entwicklung leistungsfähiger Lösungsverfahren zur Lösung linearer Gleichungssysteme mit Hilfe der numerischen Mathematik.
- **Ausblick:** Wir werden nun die drei fundamentalen Fragen nach Existenz, Eindeutigkeit und Berechnung von Lösungen beantworten. Für eine umfassende Lösungstheorie fehlt uns noch ein letzter Baustein, der *Rang* einer Matrix.

10.1 Der Rang einer Matrix

10.1 Rang einer Matrix: Definition

Definition und Eigenschaften: Rang einer Matrix

Sei A eine $m \times n$-Matrix. Die maximale Anzahl linear unabhängiger Zeilen bzw. Spalten von A wird als **Zeilen-** bzw. **Spalten-Rang** $\text{Rg}(A)$ von A bezeichnet.

1. Da der Zeilen-Rang gleich dem Spalten-Rang ist, sprechen wir auch einfach vom Rang von A.
2. Offensichtlich muss $\text{Rg}(A) \leq \min(m, n)$ gelten.
3. Der Rang $\text{Rg}(A)$ ist invariant unter elementaren Zeilenoperationen und kann daher auch anhand der zugehörigen **Zeilen-Stufen-Form** bestimmt werden.
4. In der **Zeilen-Stufen-Form** entspricht der Rang der Anzahl der Nicht-Nullzeilen.

Bemerkungen/Beispiele:

- Bei einer Matrix in **Zeilen-Stufen-Form**, beginnen die von Null verschiedenen Einträge jeder folgender Zeiler mindestens einen Eintrag später:

$$\left(\begin{array}{cccc|cccc}
a_{11} & a_{12} & \cdots & a_{1s} & a_{1(s+1)} & a_{1(s+2)} & \cdots & a_{1n} \\
0 & a_{22} & \cdots & a_{2s} & a_{2(s+1)} & a_{2(s+2)} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_{rs} & a_{r(s+1)} & a_{r(s+2)} & \cdots & a_{rn} \\
\hline
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0
\end{array}\right)$$

Offensichtlich sind gerade die ersten r Zeilen linear unabhängig.

10.1 Rang einer Matrix

Bemerkungen/Beispiele:

- Für eine quadratische, invertierbare $n \times n$-Matrix A gilt $\det(A) \neq 0$, d.h. die Zeilen-Stufen-Form von A ist eine Dreiecksmatrix und es gilt $a_{ii} \neq 0$ für alle i.
- Die maximale Anzahl linear unabhängiger Zeilen ist dann offenbar n, also hat eine solche Matrix **vollen Rang** n. Es gilt:

$$\exists A^{-1} \quad \Longleftrightarrow \quad \det(A) \neq 0 \quad \Longleftrightarrow \quad \mathrm{Rg}(A) = n.$$

- Für die folgenden Matrizen gilt $\mathrm{Rg}(A) = 2$, $\mathrm{Rg}(B) = 1$, $\mathrm{Rg}(C) = 3$, $\mathrm{Rg}(D) = 3$.

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix}.$$

10.1 Rang einer Matrix

Bemerkungen/Beispiele:

- Wir berechnen den Rang der Matrix

$$A = \begin{pmatrix} 1 & 3 & -5 & 0 \\ 2 & 7 & -8 & 7 \\ -1 & 0 & 11 & 21 \end{pmatrix}.$$

Durch elementare Zeilenoperationen erhalten wir

$$\begin{pmatrix} 1 & 3 & -5 & 0 \\ 2 & 7 & -8 & 7 \\ -1 & 0 & 11 & 21 \end{pmatrix} \to \begin{pmatrix} 1 & 3 & -5 & 0 \\ 0 & 1 & 2 & 7 \\ 0 & 3 & 6 & 21 \end{pmatrix} \to \begin{pmatrix} 1 & 3 & -5 & 0 \\ 0 & 1 & 2 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Damit lesen wir ab: $\mathrm{Rg}(A) = 2$.

10.2 Das Lösungsverhalten allgemeiner LGS

10.2 Lösungsverhalten allgemeiner LGS

Vorüberlegung:

- Um das lineare Gleichungssystem $Ax = b$ untersuchen, betrachten wir die A zugeordnete lineare Abbildung:

$$f_A : \mathbb{R}^n \to \mathbb{R}^m, \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mapsto Ax = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

- Es fällt folgender Sachverhalt auf:
  1. Ist $x \in \mathbb{R}^n$ Lösung von $Ax = b$, so gilt $f_A(x) = Ax = b$, d.h. b ist im Bild von f_A.
  2. Ist x Lösung von $Ax = b$ und $y \neq 0$ mit $y \in \ker(f_A)$, d.h. $f_A(y) = Ay = \mathbb{O}$, so gilt

     $$A(x + y) = Ax + Ay = Ax + f_A(y) = b + \mathbb{O} = b,$$

     d.h. ist f_A nicht injektiv, so ist mit x auch $x + y$ eine Lösung (keine Eindeutigkeit).

10.2 Lösungsverhalten allgemeiner LGS

Satz: Existenz und Eindeutigkeit der Lösung eines LGS

- Es existiert eine Lösung von $Ax = b$ genau dann, wenn $b \in \text{Bild}(f_A)$.
- $Ax = b$ hat für alle $b \in \mathbb{R}^m$ eine Lösung genau dann, wenn f_A surjektiv ist.
- Ist $x \in \mathbb{R}^n$ eine Lösung von $Ax = b$, so ist diese Lösung eindeutig genau dann, wenn f_A injektiv ist.

Anmerkung: Wir möchten diese Beobachtungen nun mit dem Rang von A in Verbindung setzen, um ein praktikableres Kriterium für die Existenz von Lösungen eines LGS erhalten.

10.2 Lösungsverhalten allgemeiner LGS

Überlegungen:

- Das Bild der linearen Abbildung f_A beschreibt gerade alle rechten Seiten b, zu denen eine Lösung des LGS existiert.
- Die Matrix liefert eine sehr genaue Darstellung des Bildes, denn

$$Ax = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + \dots + x_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}.$$

- Das Bild(f_A) ist also gerade der Aufspann der Spaltenvektoren von A.

10.2 Lösungsverhalten allgemeiner LGS

Überlegungen:

- $Ax = b$ ist also genau dann lösbar, wenn die rechte Seite b im Aufspann dieser Spaltenvektoren liegt:

$$\text{span}\{A_{*1}, A_{*2}, \ldots, A_{*n}\} = \text{span}\{A_{*1}, A_{*2}, \ldots, A_{*n}, b\}$$

- Wir müssen nur prüfen, ob der Rang der **erweiterten Koeffizientenmatrix** $(A|b)$ mit dem Rang von A übereinstimmt. In diesem Fall erhöht sich die Anzahl linear unabhängiger Spaltenvektoren nicht und somit ist b im Aufspann der Spaltenvektoren von A.
- Gilt hingegen $\text{Rg}(A) < \text{Rg}(A|b)$, so ist b eben nicht in diesem Aufspann enthalten.

10.2 Lösungsverhalten allgemeiner LGS

Satz: Existenz der Lösung eines LGS

Seien $A \in M^{m \times n}$ und $b \in \mathbb{R}^m$ gegeben. Dann *existiert* für das lineare Gleichungsystem $Ax = b$ eine Lösung $x \in \mathbb{R}^n$ genau dann, wenn $\operatorname{Rg}(A) = \operatorname{Rg}(A|b)$.

Frage: Können wir auch die Eindeutigkeit der Lösung mit Hilfe des Rangs charakterisieren?

- Wir gehen nun davon aus, dass es eine Lösung gibt, d.h. es gilt $\operatorname{Rg}(A) = \operatorname{Rg}(A|b)$.
- Eine Lösung des LGS ist genau dann eindeutig, wenn f_A injektiv ist.
- Wir behaupten, dass dies der Fall ist genau dann, wenn $\operatorname{Rg}(A) = n$.

Beweis: Nehmen wir an, dass $\mathrm{Rg}(A) < n$. D.h. die Spalten von A sind linear abhängig. Also gibt es reelle Zahlen $y_1, \ldots, y_n$, die nicht alle null sind, sodass

$$y_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + y_2 \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} + \ldots + y_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Dies können wir umformulieren zu

$$Ay = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Damit ist $y \in \ker(f_A)$ mit $y \neq \mathbb{O}$, was bedeutet, dass f_A nicht injektiv ist. $\square$

10.2 Lösungsverhalten allgemeiner LGS

Satz: Existenz der Lösung eines LGS

Seien $A \in M^{m \times n}$ und $b \in \mathbb{R}^m$ gegeben. Dann besitzt das lineare Gleichungsystem $Ax = b$ eine *eindeutige* Lösung $x \in \mathbb{R}^n$ genau dann, wenn

$$\mathrm{Rg}(A) = \mathrm{Rg}(A|b) = n.$$

Anmerkung: Insbesondere kann es kein Gleichungssystem mit 2, 3, 4, ..., k Lösungen geben! Ein LGS hat entweder *keine* Lösung, *genau eine* Lösung oder *unendlich viele* Lösungen!

10.2 Lösungsverhalten allgemeiner LGS

Existenz und Eindeutigkeit der Lösung eines $m \times n$-LGS

$Ax = b \quad \text{mit} \quad A \in M^{m \times n},\ x \in \mathbb{R}^n,\ b \in R^m$		
$\text{Rg}(A) = \text{Rg}(A\|b) = n$	$\text{Rg}(A) = \text{Rg}(A\|b) < n$	$\text{Rg}(A) < \text{Rg}(A\|b)$
Genau eine Lösung	∞ viele Lösungen	Keine Lösung

Beispiele:

- Wir untersuchen das folgende LGS auf Existenz und Eindeutigkeit von Lösungen:

$$\begin{pmatrix} 3 & -4 \\ -1 & 5 \\ 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 12 \end{pmatrix}.$$

Wir formen die erweiterte Koeffizientenmatrix $(A|b)$ in Zeilen-Stufen-Form um

$$\left(\begin{array}{rr|r} 3 & -4 & 2 \\ -1 & 5 & 4 \\ 5 & 2 & 12 \end{array}\right) \to \left(\begin{array}{rr|r} 3 & -4 & 2 \\ -1 & 5 & 4 \\ 5 & 2 & 12 \end{array}\right) \to \left(\begin{array}{rr|r} 3 & -4 & 2 \\ 0 & 11 & 14 \\ 0 & 27 & 32 \end{array}\right) \to \left(\begin{array}{rr|r} 3 & -4 & 2 \\ 0 & 11 & 14 \\ 0 & 0 & 26 \end{array}\right)$$

und lesen ab, dass $\mathrm{Rg}(A) = 2$ und $\mathrm{Rg}(A|b) = 3$. Wegen $\mathrm{Rg}(A) < \mathrm{Rg}(A|b)$ besitzt das System keine Lösung.

Beispiele:

- Untersuchen wir ein weiteres LGS, das bereits in Form (A, b) gegeben ist, auf Existenz und Eindeutigkeit von Lösungen:

$$\left(\begin{array}{rrr|r} 1 & 0 & 2 & 0 \\ 4 & -1 & -1 & 6 \\ -1 & 2 & 2 & 2 \\ 3 & -1 & 0 & 3 \end{array}\right) \to \left(\begin{array}{rrr|r} 1 & 0 & 2 & 0 \\ 0 & -1 & -9 & 6 \\ 0 & 2 & 4 & 2 \\ 0 & -1 & -6 & 3 \end{array}\right)$$

$$\to \left(\begin{array}{rrr|r} 1 & 0 & 2 & 0 \\ 0 & -1 & -9 & 6 \\ 0 & 0 & -14 & 14 \\ 0 & 0 & 3 & -3 \end{array}\right) \to \left(\begin{array}{rrr|r} 1 & 0 & 2 & 0 \\ 0 & -1 & -9 & 6 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Wegen $\mathrm{Rg}(A) = \mathrm{Rg}(A|b) = n = 3$ gibt es eine eindeutige Lösung.

10.3 Das Lösungsverhalten quadratischer LGS

10.3 Lösungsverhalten quadratischer LGS

Überlegungen:

- Für das LGS $Ax = b$ mit quadratischer Matrix A haben wir noch die Determinante $\det(A)$ und Inverse A^{-1} zur Charakterisierung der Lösung.
- Wir wissen berreits, dass $\det(A) \neq 0 \iff \operatorname{Rg}(A) = n$.
- Falls $A \in M^{n\times n}$, ist $(A|b) \in M^{n\times(n+1)}$ mit $\operatorname{Rg}(A|b) \leq n$.
- Falls $\det(A) \neq 0$, muss also $n = \operatorname{Rg}(A) = \operatorname{Rg}(A|b)$ gelten und das System ist eindeutig lösbar.
- Falls $\det(A) = 0$, ist A nicht invertierbar und es gilt $\operatorname{Rg}(A) < n$. Dann gibt es wieder zwei Fälle:
  1. $\operatorname{Rg}(A) = \operatorname{Rg}(A|b) < n$: es gibt unendlich viele Lösungen,
  2. $\operatorname{Rg}(A) \neq \operatorname{Rg}(A|b)$: es gibt keine Lösung.

10.3 Lösungsverhalten quadratischer LGS

Existenz und Eindeutigkeit der Lösung eines $n \times n$-LGS

<table>
<tr><td colspan="3">$Ax = b \quad \text{mit} \quad A \in M^{n \times n},\ x, b \in \mathbb{R}^n$</td></tr>
<tr><td>$\det(A) \neq 0$</td><td colspan="2">$\det(A) = 0$</td></tr>
<tr><td>$\text{Rg}(A) = \text{Rg}(A|b) = n$
Genau eine Lösung</td><td>$\text{Rg}(A) = \text{Rg}(A|b) < n$
∞ viele Lösungen</td><td>$\text{Rg}(A) < \text{Rg}(A|b)$
keine Lösung</td></tr>
</table>

10.3 Lösungsverhalten quadratischer LGS

Bemerkungen:

- Oft ist es nötig quadratische lineare Gleichungssysteme mit derselben Matrix A aber unterschiedlichen rechten Seiten b zu lösen (z.B. Sensitivitätsberechnungen in elektrischen Netzen, Störungen der Daten, etc.).
- Wir suchen Kriterien interessiert, die garantieren, dass das System immer eine Lösung besitzt.
- Wenn $\det(A) \neq 0$ existiert immer eine Lösung.
- Falls aber $\det(A) = 0$ gibt es **immer** ein Problem:

  Es gibt rechte Seiten b, für die $Ax = b$ keine Lösung besitzt.

Falls $\det(A) = 0$, ist A nicht invertierbar. Die zugehörige lineare Abbildung

$$f_A : \mathbb{R}^n \to \mathbb{R}^n, \quad x \mapsto Ax$$

ist kein Isomorphismus, also nichts bijektiv. Da f_A von $\mathbb{R}^n$ in den $\mathbb{R}^n$ abbildet, ist diese nicht injektiv und insbesondere, nicht surjektiv. Es gibt also einen Vektor $\tilde{b} \notin \text{Bild}(f_A)$. Wir haben aber gezeigt, dass nur für die Vektoren im Bild von f_A eine Lösung existiert.

10.3 Lösungsverhalten quadratischer LGS

Bemerkungen:

- Falls $\det(A) = 0$, ist A nicht invertierbar. Die zugehörige lineare Abbildung

$$f_A : \mathbb{R}^n \to \mathbb{R}^n, \quad x \mapsto Ax$$

  ist kein Isomorphismus, also nichts bijektiv.
- Da f_A von $\mathbb{R}^n$ in den $\mathbb{R}^n$ abbildet, ist diese nicht injektiv und insbesondere, nicht surjektiv.
- Es gibt also einen Vektor $\tilde{b} \notin \text{Bild}(f_A)$. Wir haben aber gezeigt, dass nur für die Vektoren im Bild von f_A eine Lösung existiert.

Existenz und Eindeutigkeit der Lösung eines LGS

Ein quadratisches LGS $Ax = b$ ist genau dann für alle $b \in \mathbb{R}^n$ lösbar, wenn $\det(A) \neq 0$. In diesem Fall existiert die Inverse A^{-1} und die Lösung (für festes b) ist eindeutig. Sie ist geben durch $x = A^{-1}b$.

Anmerkungen:

- Wir können das LGS $Ax = b$ durch Multiplikation mit A^{-1} von links lösen, wenn wir die Inverse kennen.

$$Ax = b \quad \Leftrightarrow \quad A^{-1}Ax = A^{-1}b \quad \Leftrightarrow \quad \mathrm{Id}\, x = A^{-1}b \quad \Leftrightarrow \quad x = A^{-1}b.$$

- Ist A^{-1} noch nicht berechnet, ist die Lösung mit Hilfe des Gauß-Jordan-Verfahrens schneller, da dieses die Invertierung und Multiplikation mit der rechten Seite b entspricht.

10.3 Lösungsverhalten quadratischer LGS

Beispiele:

- Betrachte das LGS
$$\begin{pmatrix} 1 & -1 \\ 2 & -2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix}.$$
Dann gilt $\det(A) = 1 \cdot (-2) - (-1) \cdot 2 = 0$, also ist das System nicht eindeutig lösbar. Des Weiteren lesen wir ab, dass $\text{Rg}(A) = 1$. Wir bringen noch die erweiterte Koeffizientenmatrix $(A|b)$ in Zeilen-Stufen-Form und erhalten
$$\left(\begin{array}{cc|c} 1 & -1 & 3 \\ 2 & -2 & 6 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 3 \\ 0 & 0 & 0 \end{array}\right).$$
Somit gilt $\text{Rg}(A|b) = 1 = \text{Rg}(A)$ und das Gleichungssystem hat unendlich viele Lösungen.

Beispiele:

- Wählt man in (ii) als rechte Seite den Vektor $(1, 3)$, so hat das LGS keine Lösung, denn die erweiterte Koeffizientenmatrix in Zeilen-Stufen-Form ist dann

$$\left(\begin{array}{cc|c} 1 & -1 & 1 \\ 2 & -2 & 3 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 1 \\ 0 & 0 & 1 \end{array}\right).$$

  Man erkennt hier zwei linear unabhängige Zeilen, also $\mathrm{Rg}(A|b) = 2 > \mathrm{Rg}(A) = 1$. Es existiert also keine Lösung.

10.4 Lösungsverfahren für allgemeine LGS

10.4 Lösungsverhalten quadratischer LGS

Ausblick:

- Wir haben das Gauß-Jorden-Verfahren bereits für quadratische LGS $Ax = b$ mit invertierbarer Matrix A vorgestellt.
- Wir können das Verfahren auch für nicht-invertierbaren oder nicht-quadratische Matrizen A anwenden.
- Ziel ist es nach wie vor $(A|b)$ in eine Form zu bringen, bei der auf der linken Seite Standardbasisvektoren in den Spalten stehen.

Ausblick:

- Falls $\mathrm{Rg}(A) = \mathrm{Rg}(A|b) < n$ treten in der Zeilen-Stufen-Form auch Nichtbasisvektoren auf und es gibt unendlich viele Lösungen.

$$\left(\begin{array}{cccccccccc|c} 1 & * & \cdots & * & 0 & * & \cdots & * & 0 & \cdots & * \\ 0 & 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & \cdots & * \\ 0 & \vdots & \cdots & \vdots & 0 & 0 & \cdots & 0 & 1 & \cdots & * \\ 0 & \vdots & \cdots & \vdots & 0 & 0 & \cdots & 0 & 0 & \cdots & * \\ \vdots & & & & \vdots & & & & \vdots & & \vdots \end{array}\right).$$

- Für jeden dieser Nichtbasisvektoren gibt es in der Lösung einen freien Parameter und damit eine Dimension des Lösungsraums.

10.4 Lösungsverhalten quadratischer LGS

Beispiel: 3×4-System

- Wir formen das folgende 3×4-LGS in Zeilen-Stufen-Form um:

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 2 & 2 & 2 & 0 \end{array}\right) \to \left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 2 & 2 & 2 & 0 \end{array}\right) \to \left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 \end{array}\right) \to$$

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 \end{array}\right) \to \left(\begin{array}{cccc|c} 1 & 2 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right) \to \left(\begin{array}{cccc|c} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right).$$

  Das System besitzt unendlich viele Lösungen $\mathrm{Rg}(A) = 3 = \mathrm{Rg}(A|b) < 4 = n$.

- Die zweite Spalte ist kein Standardbasisvektor. Also wählen wir $x_2 := s$ als freien Parameter.

10.4 Lösungsverhalten quadratischer LGS

- Der Lösungsvektor lautet:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + s \cdot \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad s \in \mathbb{R}.$$

- Der Lösungsraum ist der eindimensionale Unterraum des $\mathbb{R}^4$:

$$\mathbb{L} = \operatorname{span}\left\{ \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

10.4 Lösungsverhalten quadratischer LGS

Beispiel: 3×5-System

- Betrachten wir das 3×5-LGS mit erweiterter Koeffizientenmatrix:

$$\left(\begin{array}{ccccc|c} 1 & 2 & 3 & 1 & 1 & 0.0 \\ 0 & 0 & 1 & 1 & 1 & 1.0 \\ 0 & 0 & 1 & 1 & 3 & 2.0 \end{array}\right) \to \left(\begin{array}{ccccc|c} 1 & 2 & 3 & 1 & 1 & 0.0 \\ 0 & 0 & 1 & 1 & 1 & 1.0 \\ 0 & 0 & 1 & 1 & 3 & 2.0 \end{array}\right) \to \left(\begin{array}{ccccc|c} 1 & 2 & 3 & 1 & 1 & 0.0 \\ 0 & 0 & 1 & 1 & 1 & 1.0 \\ 0 & 0 & 0 & 0 & 2 & 1.0 \end{array}\right)$$

$$\left(\begin{array}{ccccc|c} 1 & 2 & 3 & 1 & 1 & 0.0 \\ 0 & 0 & 1 & 1 & 1 & 1.0 \\ 0 & 0 & 0 & 0 & 1 & 0.5 \end{array}\right) \to \left(\begin{array}{ccccc|c} 1 & 2 & 3 & 1 & 0 & -0.5 \\ 0 & 0 & 1 & 1 & 0 & 0.5 \\ 0 & 0 & 0 & 0 & 1 & 0.5 \end{array}\right) \to \left(\begin{array}{ccccc|c} \color{blue}{1} & 2 & \color{blue}{0} & -2 & \color{blue}{0} & -2.0 \\ \color{blue}{0} & 0 & \color{blue}{1} & 1 & \color{blue}{0} & 0.5 \\ \color{blue}{0} & 0 & \color{blue}{0} & 0 & \color{blue}{1} & 0.5 \end{array}\right)$$

- Die zweite und vierte Spalte sind keine Standardbasisvektoren. Wir wählen also

$$x_2 := r, \quad x_4 := s.$$

10.4 Lösungsverhalten quadratischer LGS

Beispiel: 3×5-System

- Insgesamt erhalten wir einen affinen Vektorraum als Lösung:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ 0.5 \\ 0 \\ 0.5 \end{pmatrix} + r \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + s \begin{pmatrix} 2 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \quad s, r \in \mathbb{R}.$$

- Die Lösung setzt sich aus der Lösung des **homogenen LGS** $Ax = \mathbb{O}$ und einer speziellen Lösung des **inhomogenen LGS** $Ax = b$ zusammen:

$$\mathbb{L} = (-2, 0, 0.5, 0, 0.5)^\top + \operatorname{span}\left\{(-2, 1, 0, 0, 0)^\top, (2, 0, -1, 1, 0)^\top\right\}.$$

10.4 Lösungsverhalten quadratischer LGS: Aufgaben

Aufgaben:

1. Zeigen Sie, dass das LGS

$$\begin{array}{rcrcrcr} x_1 & + & x_2 & - & x_3 & = & 2 \\ -2x_1 & & & + & x_3 & = & -2 \\ 5x_1 & - & x_2 & + & 2x_3 & = & 4 \\ 2x_1 & + & 6x_2 & - & 3x_3 & = & 5 \end{array}$$

   keine Lösung besitzt.

2. Untersuchen Sie die folgenden LGS auf Existenz und Eindeutigkeit von Lösungen. Geben Sie im Fall der Existenz alle Lösungen an:

$$\left(\begin{array}{rrrr|r} 1 & 5 & 7 & 9 & 0 \\ 2 & 0 & 0 & -2 & 1 \\ -1 & 0 & 1 & 1 & 3 \end{array}\right), \quad \left(\begin{array}{rrr|r} -2 & 1 & 1 & 0 \\ 1 & -2 & 1 & 0 \\ 1 & 1 & -2 & 0 \end{array}\right), \quad \left(\begin{array}{rrr|r} 1 & 2 & 0 & 3 \\ 1 & 7 & 4 & 18 \\ 3 & 13 & 4 & 30 \end{array}\right).$$

11.1 Eigenwerte und Eigenvektoren: Aufgabe

Aufgabe:
Bestimmen Sie die Eigenwerte und Eigenräume der Matrizen

$$-3, \begin{pmatrix} 1 & 2 \\ 2 & -2 \end{pmatrix}, \begin{pmatrix} 1 & \mathrm{i} \\ -\mathrm{i} & 1 \end{pmatrix}, \begin{pmatrix} 3 & 4 & -3 \\ 2 & 7 & -4 \\ 3 & 9 & -5 \end{pmatrix}$$

und von

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} -2 & 2 & -3 \\ 2 & 1 & -6 \\ -1 & -2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

11. Das Eigenwertproblem

11. Das Eigenwertproblem: Einführung

Ausblick:

- In diesem Abschnitt untersuchen wir stets quadratische Matrizen über dem Körper der komplexen Zahlen.
- Zu einer gegebenen quadratischen Matrix A suchen wir nun einen Vektor v, der durch Anwendung von A lediglich gestreckt wird, d.h.

$$Av = \lambda v, \quad \lambda \in \mathbb{C}.$$

- Dann heißt v ein Eigenvektor von A zum Eigenwert λ.
- Zur Lösung dieses sogenannten Eigenwertproblems nutzen wir unser Wissen über Gleichungssysteme.
- Anwendungsgebiete: Physik, Elektrotechnik, Statik/Dynamik, Biologie, Informatik, Wirtschaftswissenschaften, etc.

11. Das Eigenwertproblem: Einführung

Beispiel: Suchmaschinen (s. Skript ab S.119)

- Bei Eingabe eines Suchbegriffes wird ein Index durchforstet, um alle Websites, die den Begriff enthalten, zu finden.
- Dies sind in der Regel mehrere Tausend Treffer.
- Man braucht jetzt ein Kriterium, um den Info-Müll von den relevanten Websites zu trennen.
- Ziel ist es die Suchergebnisse in Form einer Liste für den Nutzer zur Verfügung zu stellen.
- Auf dieser Liste sollen die bedeutsamen Einträge auf den vorderen Plätzen vertreten sein (Page-Ranking).

11. Das Eigenwertproblem: Einführung

Beispiel: Dynamische Systeme

- Jeder Zustand eines dynamischen Systems kann durch mehreren charakteristische Komponenten, also einen Vektor des $\mathbb{R}^n$, beschrieben werden.
- Der Zustand wird in jeder Minute ermittelt und man weiß, dass er sich aus dem alten Zustand und einer für dieses System charakteristischen Matrix entwickelt, die die Struktur enthält.
- Ist etwa $x^{(n)}$ der Zustand zum Zeitpunkt $n \in \mathbb{N}$ und A die System-Matrix, so erhalten wir das dynamische System

$$x^{(n)} = Ax^{(n-1)}, \quad n \in \mathbb{N}_{>0}.$$

- Eine wichtige Frage ist nun die Langzeitentwicklung des Systems. So möchte man etwa, dass die Komponenten des Systems innerhalb gewisser Grenzen bleiben.
- Die Lage der Eigenwerte der Matrix A ist hierfür das entscheidende Kriterium.

11. Das Eigenwertproblem: Einführung

Beispiel: Eigenschwingungen von Bauwerken (s. Skript ab S.121)

- Hier können sogenannte Resonanzkatastrophen bis zur Zerstörung führen.
- Die Brücke von Angers soll 1850 durch den Gleichschritt darüber marschierender Soldaten zum Einsturz gebracht worden sein.
- Das Schwingungsverhalten von Brücken kann durch partielle Differentialgleichungen (Balkengleichungen) modelliert werden.
- Mittels numerischer Methoden (finite Differenzen) kann man das System diskretisieren und auf ein Matrixsystem reduzieren.
- Die Lage der Eigenwerte der betreffenden Matrix entscheidet über die Stabilität des Systems.

11.1 Eigenwerte und Eigenvektoren quadratischer Matrizen

11.1 Eigenwerte und Eigenvektoren: Definition

Definition: Eigenwerte und Eigenvektoren einer Matrix

Sei $A \in M^{n \times n}(\mathbb{C})$ eine quadratische Matrix über dem Körper der komplexen Zahlen. Ein Skalar $\lambda \in \mathbb{C}$ heißt **Eigenwert von** A, wenn es einen Vektor $v \in \mathbb{C}^n$ mit $v \neq \mathbb{O}$ gibt, sodass

$$Av = \lambda v.$$

Ein solches λ heißt **Eigenwert**, der Vektor v heißt dann **Eigenvektor von** A zum Eigenwert λ.

Anmerkung: Da $v = \mathbb{O}$ die Gleichung trivialerweise für alle A und λ erfüllt, schließen wir diese Lösung des Gleichungssystems $Ax = \lambda x$ aus.

11.1 Eigenwerte und Eigenvektoren: Herleitung

Herleitung: Wir gehen aus von der Gleichung des Eigenwertproblems.

$$\begin{aligned} Av &= \lambda v \\ \Leftrightarrow \quad Av - \lambda v &= \mathbb{O} \\ \Leftrightarrow \quad (A - \lambda \operatorname{Id}_n)v &= \mathbb{O} \end{aligned}$$

Diese Gleichung ermöglicht es uns, die Eigenwerte zu bestimmen. Da $v \neq \mathbb{O}$ sein soll, das LGS aber weitere Lösungen besitzen soll, muss

$$\det(A - \lambda \operatorname{Id}_n) = 0.$$

Das LGS besitzt also unendlich viele Lösungen. Dies erklärt, warum jedes Vielfache eines Eigenvektors wieder ein Eigenvektor ist:

$$A(rx) = rAx = r\lambda x = \lambda(rx).$$

11.1 Eigenwerte und Eigenvektoren: Eigenraum

Definition: Eigenraum, geometrische Vielfachheit

Sei A eine quadratische Matrix über dem Körper der komplexen Zahlen.

- Der **Eigenraum** $\mathrm{Eig}(\lambda)$ zum Eigenwert λ ist definiert durch den Kern der linearen Abbildung $f(x) = (A - \lambda \, \mathrm{Id}_n)x$, d.h.

$$\mathrm{Eig}(\lambda) := \ker(A - \lambda \, \mathrm{Id}_n).$$

- Dieser entspricht der Lösung des homogenen Gleichungssystems

$$(A - \lambda \, \mathrm{Id}_n)x = \mathbb{0}.$$

- Die Dimension des Eigenraums heißt **geometrische Vielfachheit** $\#_g(\lambda)$ des Eigenwerts λ.

11.1 Eigenwerte und Eigenvektoren: Charakteristisches Polynom

Definition: Charakteristisches Polynom, algebraische Vielfachheit

Sei A eine quadratische Matrix über dem Körper der komplexen Zahlen.

- Die Determinante der Matrix $(A - \lambda \, \mathrm{Id}_n)$ ist ein Polynome

$$p_{char}(\lambda) := \det(A - \lambda \, \mathrm{Id}_n) = (-\lambda)^n + a_{n-1}\lambda^{n-1} + \ldots a_2\lambda^2 + a_1\lambda + a_0$$

  vom Grad n, welches wir das **charakteristisches Polynom** von A nennen.
- Die Nullstellen des charakteristischen Polynoms sind die Eigenwerte von A. Die Vielfachheit einer Nullstelle heißt **algebraische Vielfachheit** $\#_a(\lambda)$ des Eigenwerts λ.

Anmerkung: Nach dem *Fundamentalsatz der Algebra* hat A auch n (nicht notwendigerweise verschiedene) Eigenwerte!

11.1 Eigenwerte und Eigenvektoren

Proposition

Für eine $n \times n$-Matrix A und deren Eigenwerte $\lambda \in \mathbb{C}$ sind folgende Aussagen äquivalent

1. λ ist ein Eigenwert von A,
2. $\det(A - \lambda \cdot \mathrm{Id}_n) = 0$,
3. $\mathrm{Eig}(\lambda) = \ker(A - \lambda \cdot \mathrm{Id}_n) \neq \{\}$.

Folglich gilt

$$\lambda = 0 \quad \Leftrightarrow \quad \det(A) = 0 \quad \Rightarrow \quad \nexists A^{-1}.$$

11.1 Eigenwerte und Eigenvektoren

Geometrische Interpretation:

- Die Eigenwerte sind die skalaren Streckfaktoren der Eigenwerte.
- Falls ein Eigenwert $\lambda = 0$ ist, wird der Raum entlang der zugehörigen Eigenvektorrichtung um projiziert und um eine Dimension reduziert.
- Eine Projektion ist eine nicht-bijektive lineare Abbildung, d.h. die Projektionsmatrix ist nicht invertierbar.
- Die Determinante $\det(A)$ entspricht dem Faktor, um den der ursprüngliche Raum gestreckt wird. Die Reduzierung des Raumes um eine Dimension erzeugt einen Unterraum dessen Volumen im höherdimensionalen Raum null ist, z.B. hat eine Ebene nur eine Flächenausdehnung, aber kein Volumen im $\mathbb{R}^3$.

11.1 Eigenwerte und Eigenvektoren

Beispiel: Allgemeine 2×2-Matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

- Das charakteristische Polynom lautet

$$\begin{aligned} \det(A - \lambda \operatorname{Id}_2) &= (a_{11} - \lambda)(a_{22} - \lambda) - a_{12}a_{21} \\ &= \lambda^2 - (a_{11} + a_{22})\lambda + (a_{11}a_{22} - a_{12}a_{21}) \\ &= \lambda^2 - \operatorname{Sp}(A)\lambda + \det(A). \end{aligned}$$

- Nach dem Fundamentalsatz hat jedes Polynom vom Grad n auch n Nullstellen und kann in Linearfaktoren zerlegt werden:

$$\begin{aligned} p(\lambda) &= (\lambda - \lambda_1)(\lambda - \lambda_2) \\ &= \lambda^2 - (\lambda_1 + \lambda_2)\lambda + \lambda_1\lambda_2. \end{aligned}$$

11.1 Eigenwerte und Eigenvektoren

- Durch einen Koeffizientenvergleich folgt

$$\lambda_1 + \lambda_2 = a_{11} + a_{22} = \mathrm{Sp}(A) \quad \text{und} \quad \lambda_1 \cdot \lambda_2 = a_{11}a_{22} - a_{12}a_{21} = \det(A).$$

Tatsächlich lassen sich diese beiden Beziehungen auf $n \times n$-Matrizen verallgemeinern.

Proposition: Algebraische Vielfachheit

Für eine $n \times n$-Matrix A und deren Eigenwerte $\lambda_i \in \mathbb{C}$, $i = 1, \dots, r \leq n$, mit algebraischen Vielfachheiten $m_i := \#_a(\lambda_i)$ gilt

$$\sum_{i=1}^{r} m_i \lambda_i = \sum_{i=1}^{n} a_{ii} = \mathrm{Sp}(A) \quad \text{und} \quad \prod_{i=1}^{n} \lambda_i^{m_i} = \det(A).$$

11.1 Eigenwerte und Eigenvektoren

Beispiel: 2×2-Diagonalmatrix

$$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

- Wir bestimmen die Eigenwerte:

$$\det(A - \lambda \, \mathrm{Id}_2) = \det \begin{pmatrix} a - \lambda & 0 \\ 0 & b - \lambda \end{pmatrix} = (a - \lambda)(b - \lambda) = 0.$$

  Für $a \neq b$ sind $\lambda_1 = a$ und $\lambda_2 = b$ die Eigenwerte von A mit den algebraischen Vielfachheiten $\#_a(\lambda_1) = \#_a(\lambda_2) = 1$.
- Wir bestimmen noch die zugehörigen Eigenvektoren durch $(A - \lambda \, \mathrm{Id}_2)x = \mathbb{O}$.

- Für $\lambda_1 = a$ gilt mit $a \neq b$

$$\left(\begin{array}{cc|c} 0 & 0 & 0 \\ 0 & b-a & 0 \end{array}\right) \quad \Rightarrow \quad x = \begin{pmatrix} t \\ 0 \end{pmatrix}$$

  und ein Eigenvektor zum Eigenwert $\lambda_1 = a$ ist $x_{\lambda_1} = (1,0)^\top$.

- Der Eigenraum von $\lambda_1 = a$ ist

$$\mathrm{Eig}(\lambda_1 = a) = \ker(A - \lambda_1 \,\mathrm{Id}) = \mathrm{span}\{(1,0)^\top\}, \quad \#_g(\lambda_1) = 1.$$

- Analog erhalten wir für $\lambda_2 = b$

$$\mathrm{Eig}(\lambda_2 = b) = \ker(A - \lambda_2 \,\mathrm{Id}) = \mathrm{span}\{(0,1)^\top\}, \quad \#_g(\lambda_2) = 1.$$

11.1 Eigenwerte und Eigenvektoren

Beispiel: 2×2-Diagonalmatrix

$$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

- Wir bestimmen die Eigenwerte:

$$\det(A - \lambda \operatorname{Id}_2) = \det \begin{pmatrix} a - \lambda & 0 \\ 0 & a - \lambda \end{pmatrix} = (a - \lambda)^2 = 0.$$

  Der einzige Eigenwert ist $\lambda = a$ mit der algebraischen Vielfachheiten $\#_a(\lambda) = 2$.
- Wir bestimmen noch den zugehörigen Eigenraum:

$$\left(\begin{array}{cc|c} 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right) \quad \Rightarrow \quad \operatorname{Eig}(a) = \operatorname{span}\{(1,0)^\top, (0,1)^\top\}, \quad \#_g(\lambda) = 2 = \#_a(\lambda).$$

11.1 Eigenwerte und Eigenvektoren

Beispiel: 2×2-Dreicksmatrix

$$A = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$$

- Wir bestimmen die Eigenwerte der Diagonalmatrix $\operatorname{diag}(a, b) \in \mathbb{R}^2$:

$$\det(A - \lambda \operatorname{Id}_2) = \det \begin{pmatrix} a - \lambda & 0 \\ 0 & b - \lambda \end{pmatrix} = (a - \lambda)^2 = 0.$$

  Es gibt wieder nur den Eigenwert $\lambda = a$ mit algebraischer Vielfachheit $\#_a(\lambda) = 2$.
- Wir bestimmen noch den zugehörigen Eigenraum:

$$\left(\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right) \quad \Rightarrow \quad \operatorname{Eig}(a) = \ker(A - \lambda \operatorname{Id}) = \operatorname{span}\{(1, 0)^\top\}, \quad \#_g(\lambda) = 1 < \#_a(\lambda).$$

Proposition: Eigenwerte einer Dreiecksmatrix

Seien $A \in M^{n \times n}(\mathbb{C})$ eine Dreiecksmatrix. Dann entsprechen die Eigenwerte λ_i den Hauptdiagonalelementen a_{ii}. Das heißt für alle $i = 1, \ldots, n$ gilt

$$\lambda_i = a_{ii}.$$

11.1 Eigenwerte und Eigenvektoren

Proposition: algebraische und geometrische Vielfachheit

Seien $A \in M^{n \times n}(\mathbb{C})$ und λ_i, $i = 1, 2, \ldots, r \leq n$, die Eigenwerte von A mit den algebraischen Vielfachheiten $\#_a(\lambda_i)$.

- Für die algebraischen Vielfachheiten gilt

$$\sum_{i=1}^{r} \#_a(\lambda_i) = \#_a(\lambda_1) + \ldots + \#_a(\lambda_r) = n.$$

- Für die geometrische Vielfachheit eines Eigenwerts λ_i gilt

$$1 \leq \#_g(\lambda_i) \leq \#_a(\lambda_i) \leq n.$$

11.1 Eigenwerte und Eigenvektoren

Beispiel: Wir berechnen die Eigenwerte der Matrix

$$A = \begin{pmatrix} -2 & -5 \\ 1 & 4 \end{pmatrix}.$$

- Das charakteristische Polynom lautet

$$\det(A - \lambda) = \lambda^2 - \mathrm{Sp}(A)\lambda + \det(A) = \lambda^2 - 2\lambda - 3.$$

- Dessen Nullstellen sind die Eigenwerte von A:

$$\lambda_1 = -1, \ \ \lambda_2 = 3, \quad \#_a(-1) = \#_a(3) = 1.$$

- Wir berechnen nun die zugehörigen Eigenvektoren durch $(A - \lambda \, \mathrm{Id}_2)x = \mathbb{O}$.

11.1 Eigenwerte und Eigenvektoren

- Für $\lambda_1 = -1$ gilt

$$(A - (-1)\,\mathrm{Id}_2)x = \mathbb{O} \quad \Rightarrow \quad \left(\begin{array}{rr|r} -1 & -5 & 0 \\ 1 & 5 & 0 \end{array}\right) \to \left(\begin{array}{rr|r} -1 & -5 & 0 \\ 0 & 0 & 0 \end{array}\right).$$

  Wir setzen $x_2 := r$ und damit ist $x_1 = -5r$.

- Der Eigenraum ist von λ_1 ist $\quad \mathrm{Eig}(-1) = \mathrm{span}\,(-5, 1)^\top, \quad \#_g(-1) = 1.$
- Wir bestimmen den Eigenvektor zu $\lambda_2 = 3$ analog:

$$(A - 3\,\mathrm{Id}_2)x = \mathbb{O} \quad \Rightarrow \quad \left(\begin{array}{rr|r} 1 & 1 & 0 \\ -5 & -5 & 0 \end{array}\right) \to \left(\begin{array}{rr|r} 1 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

  Wir setzen $x_2 := r$ und damit ist $x_1 = -r$.

- Der Eigenraum von λ_2 ist $\quad \mathrm{Eig}(3) = \mathrm{span}\{(-1, 1)^\top\}, \quad \#_g(3) = 1.$

11.1 Eigenwerte und Eigenvektoren

Beispiel: Wir berechnen die Eigenwerte der Matrix

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

- Eigenwerte:

$$\det(A - \lambda) = \det \begin{pmatrix} -\lambda & 1 \\ -1 & -\lambda \end{pmatrix} = \lambda^2 + 1 = 0 \quad \Rightarrow \quad \lambda_1 = \mathrm{i}, \ \ \lambda_2 = -\mathrm{i}\,.$$

- Eigenvektoren zu $\lambda_1 = i$:

$$(A - \mathrm{i} \cdot \mathrm{Id}_2)x = \left(\begin{array}{cc|c} -\mathrm{i} & 1 & 0 \\ -1 & -\mathrm{i} & 0 \end{array}\right) \quad \Rightarrow \quad \left(\begin{array}{cc|c} -\mathrm{i} & 1 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

Wir setzen $x_1 = r$ und damit ist $x_2 = \mathrm{i}\, r$, d.h. $\mathrm{Eig}(\lambda_1) = \mathrm{span}\{(1, \mathrm{i})^\top)\}$.

11.1 Eigenwerte und Eigenvektoren

- Eigenvektoren zu $\lambda_2 = -i$:

$$(A - \mathrm{i} \cdot \mathrm{Id}_2)x = \left(\begin{array}{cc|c} \mathrm{i} & 1 & 0 \\ -1 & \mathrm{i} & 0 \end{array}\right) \quad \Rightarrow \quad \left(\begin{array}{cc|c} \mathrm{i} & 1 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

Wir setzen $x_1 = r$ und damit ist $x_2 = -\mathrm{i}\, r$, d.h. $\mathrm{Eig}(\lambda_2) = \mathrm{span}\{(1, -\mathrm{i})^\top)\}$.

Anmerkungen:

- Obwohl A nur reelle Koeffizienten hat, sind die Eigenwerte komplex.
- Sowohl die Eigenwerte als auch die Eigenvektoren sind konjugiert komplexe Paare.

11.1 Eigenwerte und Eigenvektoren

Proposition: Komplexe Eigenwerte und Eigenvektoren

Sei $A \in M^{n \times n}(\mathbb{C})$ eine Matrix mit reellen Koeffizienten $a_{ij} \in \mathbb{R}$ und Eigenwerten λ_i.

- Dann gibt es nach dem Fundamentalsatz der Algebra n nicht notwendigerweise verschiedene Eigenwerte von A.
- Falls A komplexe Eigenwerte besitzt, treten diese als Paare konjugiert komplexer Zahlen auf.
- Die zughörigen Eigenwerte zu den konjugiert komplexen Eigenwerten sind ebenfalls komplex konjugiert.

11.1 Eigenwerte und Eigenvektoren

Beispiel: Wir bestimmen die Eigenwert und -vektoren der 3×3-Matrix

$$A = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 3 & 0 \\ 0 & -3 & 0 \end{pmatrix}.$$

- Die Eigenwerte von A sind $\lambda_1 = 1, \quad \lambda_2 = 3, \quad \lambda_3 = 0.$
- Wir berechnen noch die Eigenräume. Für $\lambda_1 = 1$ erhalten wir

$$\left(\begin{array}{ccc|c} 1-1 & 0 & 0 & 0 \\ -1 & 3-1 & 0 & 0 \\ 0 & -3 & -1 & 0 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \Rightarrow \mathrm{Eig}(\lambda_1) = \mathrm{span}\left\{\begin{pmatrix} 2 \\ 1 \\ -3 \end{pmatrix}\right\}.$$

11.1 Eigenwerte und Eigenvektoren

- Eigenraum zu $\lambda_2 = 3$:

$$\left(\begin{array}{ccc|c} 1-3 & 0 & 0 & 0 \\ -1 & 3-3 & 0 & 0 \\ 0 & -3 & -3 & 0 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \Rightarrow \text{Eig}(\lambda_2) = \text{span}\left\{\begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}^\top\right\}.$$

- Analog ergibt sich $\text{Eig}(\lambda_3) = \text{span}\left\{(0,0,1)^\top\right\}$.
- Die Menge der Eigenvektoren ist offensichtlich linear unabhängig:

$$\left\{\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -3 \end{pmatrix}\right\}$$

Tatsächlich gilt das für alle Matrizen!

11.1 Eigenwerte und Eigenvektoren

Proposition: Lineare Unabhängigkeit von Eigenvektoren

Seien $A \in M^{n \times n}(\mathbb{C})$ und λ_i die Eigenwerte von A zu den Eigenvektoren x_i.

- Dann ist die Menge der Eigenvektoren von A linear unabhängig.
- Ist A zusätzlich symmetrisch mit reellen Einträgen, so stehen die Eigenvektoren sogar orthogonal zueinander und die Eigenwerte sind stets reell.

11.1 Eigenwerte und Eigenvektoren

Beispiel: Die Matrix

$$A = \begin{pmatrix} 6 & -2 \\ -2 & 9 \end{pmatrix}$$

Besitzt die Eigenwerte und Eigenvektoren

$$\lambda_1 = 10, \quad v_1 = \begin{pmatrix} -1 \\ 2 \end{pmatrix}, \quad \lambda_2 = 5, \quad v_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

Die Eigenvektoren sind offensichtlich lineare unabhängig. Da A symmetrisch ist, stehen die Eigenvektoren zudem senkrecht aufeinander, denn

$$\langle v_1, v_2 \rangle = -1 \cdot 2 + 2 \cdot 1 = 0.$$

11.1 Eigenwerte und Eigenvektoren: Aufgabe

Aufgabe:
Bestimmen Sie die Eigenwerte und Eigenräume der Matrizen

$$-3, \quad \begin{pmatrix} 1 & 2 \\ 2 & -2 \end{pmatrix}, \quad \begin{pmatrix} 1 & \mathrm{i} \\ -\mathrm{i} & 1 \end{pmatrix}, \quad \begin{pmatrix} 3 & 4 & -3 \\ 2 & 7 & -4 \\ 3 & 9 & -5 \end{pmatrix}$$

und von

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} -2 & 2 & -3 \\ 2 & 1 & -6 \\ -1 & -2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

11.2 Diagonalisierbarkeit

Definition: Ähnlichkeitstransformation

Die Matrizen $A, B \in M^{n\times n}(\mathbb{C})$ heißen **ähnlich** genau dann, wenn sie dieselben Eigenwerte besitzen. Dann existiert eine invertierbare Matrix $T \in M^{n\times n}(\mathbb{C})$ und A geht durch die **Ähnlichkeitstransformation**

$$A = T \cdot B \cdot T^{-1}$$

aus B hervor. Ist A ähnlich zu einer Diagonalmatrix D, so heißt A **diagonalisierbar**.

11.2 Diagonalisierbarkeit

Beweis: Sei v ein Eigenvektor von $A \in M^{n\times n}$ zum Eigenwert λ und $T \in M^{n\times n}$ invertierbar. Dann haben A und $B := T^{-1}AT$ dieselben Eigenwerte, denn

$$\begin{aligned} Av &= \lambda v \\ \leftrightarrow A \cdot T \cdot T^{-1}v &= \lambda v \\ \leftrightarrow T^{-1} \cdot A \cdot T \cdot T^{-1}v &= T^{-1} \cdot \lambda v \\ \leftrightarrow B \cdot T^{-1}v &= \lambda \cdot T^{-1}v \end{aligned}$$

Folglich ist λ auch ein Eigenwert von B zum Eigenvektor $w := T^{-1}v$. $\square$

11.2 Diagonalisierbarkeit

Proposition: Diagonalisierbarkeit

- Eine Matrix $A \in M^{n \times n}(\mathbb{C})$ ist **diagonalisierbar** genau dann, wenn für *alle* Eigenwerte λ von A gilt, dass die algebraische Vielfachheit gleich der geometrischen Vielfachheit ist.
- Die Diagonalmatrix D der Zerlegung $A = T \cdot D \cdot T^{-1}$ enthält die Eigenwerte von A auf der Hauptdiagonalen. Mehrfache Eigenwerte müssen dabei in benachbarten Spalten eingetragen werden. Abgesehen davon ist die Reihenfolge der Eigenwerte beliebig.
- Die Matrix T der Zerlegung $A = T \cdot D \cdot T^{-1}$ enthält die Basisvektoren der Eigenräume von A, notiert in der zu D passenden Reihenfolge der Eigenwerte.
- Ist A symmetrisch mit reellen Koeffizienten, so ist A diagonalisierbar.

Anwendung: Potenzieren von Matrizen

- Ist A diagonalisierbar, gibt es eine invertierbare Matrix T und eine Diagonalmatrix $\operatorname{diag}(d_1, \ldots, d_n)$ und es gilt

$$\begin{aligned} A^k &= (T \cdot D \cdot T^{-1})^k = (T \cdot D \cdot T^{-1}) \cdot (T \cdot D \cdot T^{-1}) \cdot \ldots \cdot (T \cdot D \cdot T^{-1}) \\ &= T \cdot D \cdot \underbrace{(T^{-1} T)}_{=\mathrm{Id}} \cdot D \cdot \underbrace{(T^{-1} T)}_{=\mathrm{Id}} \ldots D \cdot T^{-1} \\ &= T \cdot D^k T^{-1} = T \cdot \operatorname{diag}(d_1, \ldots, d_n)^k \cdot T^{-1} \\ &= T \cdot \operatorname{diag}(d_1^k, \ldots, d_n^k) \cdot T^{-1} \end{aligned}$$

- Der Aufwand einer vielfachen Matrizenmultiplikationen reduziert sich nach der Zerlegung von A in TDT^{-1} auf zwei Multiplikationen.

11.2 Diagonalisierbarkeit

Anwendung: Potenzieren von Matrizen

- Für eine symmetrische reelle Matrizen existiert immer eine solche Zerlegung mit den Eigenwerten von A auf der Hauptdiagonalen von D und T mit Eigenvektoren von A als Spaltenvektoren.
- Die Eigenvektoren stehen in diesem Fall senkrecht aufeinander.
- Werden diese normiert, ist T eine Orthogonalmatrix, d.h. $Q^T Q = \mathrm{Id}$. Damit gilt aber auch, dass $T^\top = T^{-1}$ und sogar die Berechnung der Inversen entfällt.

11.2 Diagonalisierbarkeit

Anwendungen: Hauptachsentransformation

Die Gleichung

$$ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz = 1$$

beschreibt eine Fläche im $\mathbb{R}^3$.

- Wir können diese auch in Matrixschreibweise umformulieren:

$$(x, y, z) \cdot \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 1$$

  oder kurz $x^\top A x = 1$.

- Da A eine reelle symmetrische Matrix ist, ist A diagonalisierbar in $A = TDT^{-1}$ mit den Eigenvektoren von A als Spalten von T.

11.2 Diagonalisierbarkeit

Anwendungen: Hauptachsentransformation

- Normieren wir die Eigenvektoren, entsteht eine orthogonale Matrix Q, sodass $A = Q^\top DQ$ und

$$x^\top Ax = x^\top Q^\top DQx = (Qx)^\top D(Qx) =: u^\top Du,$$

  mit $u = (u, v, w)$. In einem Koordinatensystem mit den Achsen u, v und w könnten wir die Fläche auch schreiben als

$$d_1 u^2 + d_2 v^2 + d_3 w^2 = 1.$$

- Sind zusätzlich alle Eigenwerte positiv, könnten wir D auch schreiben als

$$D = \operatorname{diag}(d_1, d_2, d_3) = \operatorname{diag}(\sqrt{d_1}^2, \sqrt{d_2}^2, \sqrt{d_3}^2) = \operatorname{diag}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})^2$$
$$=: \sqrt{D} \cdot \sqrt{D} = \sqrt{D}^\top \cdot \sqrt{D}.$$

11.2 Diagonalisierbarkeit

Anwendungen: Hauptachsentransformation

- Wir haben also von der Einheitssphäre $r^\top r = 1$ ausgehend aus dem *rst*-Koordinatensystem in ein Ellipsoid $u^\top Du = 1$ im *uvw*-System verzerrt. Anschließend fand eine Drehung ins *xyz*-System statt und wir erhalten $x^\top Ax = 1$.
- Die Zerlegung von A zeigt uns also welche Transformationen zwischen den Koordinatensystemen nötig waren.
- Die Hauptachsen des Ellipsoid im *xyz*-Systems zeigen dabei in Richtung der Eigenvektoren von A.

Anwendungen: Hauptachsentransformation

- Mit $r = (r, s, t)$ wird die Fläche zu

  $$u^\top D u = u^\top \sqrt{D^\top} \cdot \sqrt{D} u = (\sqrt{D} u)^\top (\sqrt{D} u) =: r^\top r = \langle r, r \rangle = 1,$$

  und beschreibt damit eine Kugel im *rst*-Koordinatensystem mit Radius $\rho = 1$ um den Ursprung. Denn es gilt

  $$1 = \langle r, r \rangle = \|(r, s, t)\|_2^2.$$

  Dies sind alle Punkte im *rst*-Koordinatensystem mit euklidischem Abstand zum Ursprung, also die Einheitssphäre.
- Für andere Vorzeichen ergeben sich andere Flächenformen, die zusammengefasst **Quadriken** genannt werden.

  https://de.wikipedia.org/wiki/Quadrik

12. Numerische Methoden

Einführung:

- Im Allgemeinen sind die betrachteten LGS sehr groß.
- Numerischen Behandlung von LGS und Eigenwertproblemen erforderlich.
- Dabei treten neue numerische Probleme auf.
- Muss man LGS sehr oft für unterschiedliche rechte Seiten lösen, so könnte man die Inverse einer Matrix bestimmen und diese jeweils mit der rechten Seite multiplizieren, um die Lösung zu erhalten.
- **Nachteile** der Matrixinversion:
  - Die Invertierung ist kein numerisch stabiles Verfahren, d.h. der Algorithmus verstärkt Störungen der Eingabedaten.
  - Bandmatrizen oder spärlich besetzte Matrizen mit vielen Nullen benötigen wenig Speicherplatz. Diese Struktur geht mit der Invertierung meist verloren.
- LR- und QR-Zerlegung vermeiden solche Strukturbrüche und verhalten sich *numerisch gutartig*.

12 Numerische Methoden: Einführung

Beispiel: Gauß-Algorithmus ist im Allgemeinen numerisch sehr instabil.

- Wir betrachten das folgende LGS und dessen exakte Lösung

$$\left(\begin{array}{cc|c} 10^{-4} & 1 & 1 \\ 1 & 1 & 2 \end{array}\right) \quad \Rightarrow \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1.\overline{0001} \\ 0.\overline{9998} \end{pmatrix}.$$

- Bei dreistelliger Gleitpunktarithmetik, also Rundung von Ergebnis auf drei Nachkommastellen nach jedem Schritt, folgt nach einem Gauß-Schritt

$$\left(\begin{array}{cc|c} 10^{-4} & 1 & 1 \\ 0 & -9999 & -9998 \end{array}\right) \quad \Rightarrow \quad x_2 = \frac{-9998}{-9999} = 0.99989998\cdots \approx 1.$$

- Einsetzten in die erste Gleichung liefert dann das falsche Ergebnis

$$10^{-4}x_1 + x_2 = 1 \quad \Longleftrightarrow \quad 10^{-4}x_1 + 1 = 1 \quad \Longleftrightarrow \quad x_1 = 0.$$

Anmerkung: Um solche Probleme zu umgehen, nutzt man **Pivotisierungsstrategien**.

12 Numerische Methoden: Einführung

Beispiel: Bei Eigenwertproblemen suchen wir Nullstellen eines Polynoms.

- Bei einer Diagonalmatrix stehen die Eigenwerte auf der Hauptdiagonalen, z.B.

$$A = \operatorname{diag}(10, 11, 12, 13, 14, 15, 16).$$

- Müsste man die Nullstellen des ausmultiplizierten charakteristischen Polynoms

$$p_{char}(\lambda) = -\lambda^7 + 91\lambda^6 - 3535\lambda^5 + \ldots - 31813200\lambda + 57675600 = 0$$

numerisch mit einfacher Maschinengenauigkeit bestimmen, ergeben sich dagegen

$\lambda_1 = 9.952;\ \ \lambda_{2/3} = 11.31 \pm \mathrm{i}\,0.47;\ \ \lambda_4 = 13.65; \lambda_{5/6} = 14.26 \pm \mathrm{i}\,0.51;\ \ \lambda_7 = 16.23.$

- Der QR-Algorithmums umgeht diese Problematik.

12.1 Die LR-Zerlegung

12.1 Numerische Methoden: LR-Zerlegung

Bisher: Gauß-Verfahren zur Lösung eines LGS immer mit fester rechter Seite.
Ziel: Um Gleichungssysteme unabhängig von der rechten Seite zu lösen, möchten wir eine Zerlegung der Matrix A in eine untere und eine obere Dreiecksmatrix finden.

LR-Zerlegung einer Matrix

Sei $A \in M^{n\times n}$. Dann verstehen wir unter der **LR-Zerlegung** von A das Produkt einer oberen Dreiecksmatrix R und einer unteren Dreiecksmatrix L mit $l_{11} = \ldots = l_{nn} = 1$, sodass

$$A = L \cdot R = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ l_{n1} & l_{n2} & \cdots & 1 \end{pmatrix} \cdot \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ 0 & r_{22} & \cdots & r_{2n} \\ \vdots & \ddots & & \vdots \\ 0 & \cdots & 0 & r_{nn} \end{pmatrix}.$$

Lösung eines LGS durch LR-Zerlegung

Sei A eine Matrix mit LR-Zerlegung $A = L \cdot R$. Dann wird die Lösung des LGS $Ax = b$ wie folgt bestimmt.

1. Definiere $y := Rx$, sodass das LGS zu $Ax = LRx = Ly = b$ wird.
2. Löse $Ly = b$ durch Vorwärtssubstitution von oben nach unten:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ l_{n1} & l_{n2} & \cdots & 1 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

ergibt $y_1 = b_1, \;\; y_2 = b_2 - l_{21} y_1, \;\; \ldots, \;\; y_n = b_n - \sum_{i=1}^{n-1} l_{ni} \cdot y_i$.

12.1 Numerische Methoden: LR-Zerlegung

Lösung eines LGS durch LR-Zerlegung

3. Löse $Rx = y$ durch Rückwärtssubstitution von unten nach oben:

$$\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ 0 & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & r_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

ergibt, falls alle $r_{ii} \neq 0$ für alle $i = 1, \ldots, n$ gilt,

$$x_n = \frac{y_n}{r_{nn}}, \quad x_{n-1} = \frac{y_{n-1} - r_{n-1,n} \cdot x_n}{r_{n-1,n-1}}, \quad \ldots, \quad x_1 = \frac{y_1 - \sum_{i=2}^{n} r_{1i} \cdot x_i}{r_{11}}.$$

12.1 Numerische Methoden: LR-Zerlegung

Frage: Wie bekommen wir eine solche Zerlegung?

Antwort:

- Der Gauß-Algorithmus liefert durch elementare Zeilenoperationen eine obere Dreiecksmatrix R.
- Die Zeilenoperationen selbst liefern die untere Dreiecksmatrix L.
- Wir drücken nun die dafür nötigen elemenataren Zeilenoperationen durch Matrixmultiplikation aus.

12.1 Numerische Methoden: LR-Zerlegung

1. **Zeilentausch:** Für eine allgemeine 2×2-Matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

bewirkt die Matrix $T_{12} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ gerade eine Zeilenvertauschung von A:

$$T_{12} \cdot A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{21} & a_{22} \\ a_{11} & a_{12} \end{pmatrix}.$$

12.1 Numerische Methoden: LR-Zerlegung

2. **Zeilenmultiplikation:** Für eine allgemeine 2×2-Matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

multipliziert die Matrix $S_1(\alpha) := \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ die 1. Zeile von A mit α:

$$S_1(\alpha) \cdot A = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Analog multipliziert die Matrix $S_2(\alpha) := \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$ die 2. Zeile von A mit α.

12.1 Numerische Methoden: LR-Zerlegung

3. **Zeilenaddition:** Für eine allgemeine 2×2-Matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

addiert die Matrix $L_{21}(\alpha) := \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$ das α-fache der 1. Zeile von A zur 2.:

$$L_{21}(\alpha) \cdot A = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} + \alpha a_{11} & a_{22} + \alpha a_{12} \end{pmatrix}.$$

Wir verallgemeinern diese Beobachtungen auf den $\mathbb{R}^n$.

12.1 Numerische Methoden: LR-Zerlegung

Proposition: Elementarmatrizen

Sei $A \in M_{n \times n}(\mathbb{C})$. Dann gibt es eine Matrix,

1. bezeichnet T_{ij}, so dass $T_{ij} \cdot A$ gerade durch **Vertauschung** der i-ten und j-ten Zeile in A hervorgeht. Die Matrix ist die Einheitsmatrix, in der die i-te und j-te Zeile vertauscht ist.
2. bezeichnet $S_i(\alpha)$, so dass $S_i(\alpha) \cdot A$ gerade durch **Multiplikation** der i-ten Zeile mit α aus A hervorgeht. Die Matrix ist die Einheitsmatrix, bei der die Koordinate (i, i) durch α ersetzt wird.
3. bezeichnet $L_{ij}(\alpha)$, so dass $L_{ij}(\alpha) \cdot A$ gerade durch **Addition** der mit α multiplizierten j-ten Zeile zur i-ten Zeile aus A hervorgeht.

Die Matrizen T_{ij}, $S_i(\alpha)$, $L_{ij}(\alpha)$ heißen **Elementarmatrizen**.

12.1 Numerische Methoden: LR-Zerlegung

Bemerkungen:

- Die Matrix $L_{ij}(\alpha)$ ist die Einheitsmatrix mit zusätzlichem α an der Stelle (i,j).
- Für die Inverse einer $L_{ij}(\alpha)$-Matrix gilt

$$(L_{ij}(\alpha))^{-1} = L_{ij}(-\alpha).$$

- Ist $i > j$, so ist $L_{ij}(\alpha)$ eine untere Dreiecksmatrix. Insbesondere ist $(L_{ij}(\alpha))^{-1}$ auch eine untere Dreiecksmatrix.
- Die Matrix, die durch Multiplikation von links die erste und dritte Zeile einer Matrix $A \in M_{3\times 3}(\mathbb{R})$ vertauscht ist

$$T_{13} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

12.1 Numerische Methoden: LR-Zerlegung

Vorgehen:

- Um eine $n \times n$-Matrix mittels Gauss-Algorithmus in Dreiecksform zu bringen, müssen wir eventuell (zwischendurch) Zeilenvertauschungen durchführen, um von Null verschiedene Leitkoeffizienten zu erhalten.
- Führen wir diese Zeilenvertauschungen gleich zu Beginn durch, können wir diese in einer einzigen **Permutationsmatrix** P zusammenfassen:

$$\underbrace{T_{25} \cdot T_{13}}_{=:P} \cdot A = P \cdot A.$$

- Aus der Matrix $P \cdot A$ müssen wir zur Transformation in eine Dreiecksform nur noch die Matrizen $L_{ij}(\alpha)$ mit $i > j$ verwenden.

12.1 Numerische Methoden: LR-Zerlegung

Vorgehen:

- Insgesamt erhält man also die Dreiecksmatrix R als Produkt

$$R = L_{i_k,j_k}(\alpha_k) \cdot \ldots \cdot L_{i_1,j_1}(\alpha_1) \cdot P \cdot A.$$

- Die L_{ij}-Matrizen sind alle invertierbar und somit erhalten wir

$$P \cdot A = L_{i_1,j_1}(-\alpha_1) \cdot \ldots \cdot L_{i_k,j_k}(-\alpha_k) \cdot R.$$

- Da die Matrizen $L_{i_l,j_l}(-\alpha_l)$ alle untere Dreiecksmatrizen sind, ergibt deren Produkt die untere Dreiecksmatrix L:

$$L = L_{i_1,j_1}(-\alpha_1) \cdot \ldots \cdot L_{i_k,j_k}(-\alpha_k).$$

12.1 Numerische Methoden: LR-Zerlegung

Bemerkungen:

- Im Allgemeinen gibt es für die Matrix A selbst keine LR-Zerlegung, wenn in einem Gauss-Schritt der Leitkoeffizient Null ist.
- In diesem Fall muss man Zeilenvertauschungen durchführen. Man erhält dann eine LR-Zerlegung der zeilenpermutierten Matrix $P \cdot A$.
- Ist A also invertierbar, so existiert für die (zeilenvertauschte) Matrix immer eine LR-Zerlegung.
- **Achtung!** Für eine spätere Lösung des zugehörigen LGS muss man auch die rechte Seite permutieren:
$$P \cdot Ax = P \cdot b$$
- Eine LR-Zerlegung von A bzw. $P \cdot A$ ist durch die Normierung der Hauptdiagonalelemente von L auf 1 eindeutig.

12.1 Numerische Methoden: LR-Zerlegung

Beispiel: Wir bestimmen die LR-Zerlegung der Matrix

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 3 & 1 & 4 \end{pmatrix}:$$

1. Wir addieren zur zweiten Zeile das (-2)-fache der ersten hinzu, d.h.

$$A \quad \rightarrow \quad L_{21}(-2) \cdot A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 3 & 1 & 4 \end{pmatrix}$$

2. Wir addieren zur dritten Zeile das (-3)-fache der ersten hinzu, d.h.

$$L_{21}(-2) \cdot A \quad \rightarrow \quad L_{31}(-3) \cdot L_{21}(-2) \cdot A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & -2 & 1 \end{pmatrix}.$$

12.1 Numerische Methoden: LR-Zerlegung

3. Wir addieren nun zur dritten Zeile das 2-fache der zweiten hinzu, d.h.

$$L_{31}(-3) \cdot L_{21}(-2) \cdot A \quad \to \quad L_{32}(2) \cdot L_{31}(-3) \cdot L_{21}(-2) \cdot A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & -1 \end{pmatrix} = R$$

   und haben damit die obere Dreiecksmatrix R erhalten.

4. Nun multiplizieren wir nacheinander von links mit $L_{32}(-2)$, $L_{31}(3)$ und $L_{21}(2)$:

$$A = L_{21}(2) \cdot L_{31}(3) \cdot L_{32}(-2) \cdot R = L \cdot R,$$

   womit die gesuchte untere Dreiecksmatrix L gefunden ist:

$$L = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & -2 & 1 \end{pmatrix}.$$

12.1 Numerische Methoden: LR-Zerlegung

Beispiel: Als nächstes möchten wir das zugehöriges LGS lösen:

$$\underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 3 & 1 & 4 \end{pmatrix}}_{=A} \cdot \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}}_{=x} = \underbrace{\begin{pmatrix} 2 \\ -1 \\ 13 \end{pmatrix}}_{=b}.$$

1. In $Ax = LRx = b$ setzen wir den unbekannten Vektor $y := Rx$.
2. Wir lösen $Ly = b$ durch Vorwärtssubstitution:

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & -2 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 13 \end{pmatrix}.$$

   Es ergibt sich $y_1 = 2$, $y_2 = -5$, $y_3 = -3$.

3. Wir lösen $Rx = y$ durch Rückwärtssubstitution:

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ -5 \\ -3 \end{pmatrix}.$$

Es ergibt sich

$$\begin{aligned} x_3 &= \tfrac{-3}{-1} = 3 \\ x_2 &= \tfrac{-5-(-1)\cdot 3}{1} = -2 \\ x_1 &= 2 - 1 \cdot (-2) - 1 \cdot 3 = 1. \end{aligned}$$

12.1 Numerische Methoden: LR-Zerlegung

Bemerkungen:

- Die Matrix L speichert einfach die notwendigen Umformungsschritte. In den Anwendungen werden die Matrizen R und L direkt in einer Matrix gespeichert (jeweils rechts oben und links unten).
- Im Allgemeinen ist das Verfahren ohne *Spaltenpivotisierung* oder *Zeilenäquilibrierung* schlecht konditioniert, d.h. eine Störung der Eingabedaten (z.B. durch Rundung) wird durch das Verfahren verstärkt und führt zu einer ungenauen oder sogar unbrauchbaren Lösung.
- Unter der **Pivotisierung** versteht man dabei die Suche nach einem von null verschiedenen Zeilen- bzw. Spaltenelement und die zugehörigen elementaren Umformungen. Dabei kann auch nach dem (betragsmäßig) größten Element gesucht werden.

12.1 Numerische Methoden: LR-Zerlegung

Bemerkungen:

- **Zeilenäquilibrierung** bedeutet die Multiplikation der Zeilen mit bestimmten Faktoren, so dass anschließend alle Zeilen bzw. Spalten die gleiche Norm besitzen. Ziel dieser Skalierung ist es, die Konditionszahl des Gleichungssystems und damit den Einfluss von Störungen der Eingabedaten auf die Lösung zu verringern.
- Die LR-Zerlegung ist ein schnelles Verfahren zur Lösung eines LGS mit bis zu $n = 10^6$ Unbekannten. Für größere LGS werden iterative Verfahren bevorzugt.
- Für symmetrische Matrizen ist die sogenannte Cholesky-Zerlegung numerisch stabil und etwa doppelt so schnell wie die LR-Zerlegung. Dabei wird die Matrix in eine untere Dreiecksmatrix und deren Transponierte zerlegt.
- In der englischen Literatur wird die LR-Zerlegung als LU-Faktorisierung (für "lower" und "upper") geführt.

12.1 Numerische Methoden: LR-Zerlegung

Beispiel: $x = (0, -1, 1)$ ist die exakte Lösung des LGS

$$\left(\begin{array}{ccc|c} 10 & -7 & 0 & 7 \\ -3 & 2.099 & 6 & 3.901 \\ 5 & -1 & 5 & 6 \end{array} \right),$$

- Bei Rechnung mit fünf Nachkommastellen erhielten wir mit der LR-Zerlegung allerdings die Lösung $\tilde{x} = (0.28, -1.4, 0.99993)$.
- Hier zeigt sich die fehlende numerische Stabilität des Verfahrens.
- Die QR-Zerlegung, welche wir im Folgenden diskutieren ist s in der nächsten Sektion diskutiert werden soll, unterlegen, allerdings ist es auch schneller!

Aufgaben:

1. Berechnen Sie (falls möglich) die LR-Zerlegung der folgenden Matrizen.

$$\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1-i & 1+i \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 4 & -2 \\ 4 & 9 & -3 \\ -2 & -3 & 7 \end{pmatrix}.$$

2. Lösen Sie für jede der jeweiligen Matrizen mittels der gewonnen LR-Zerlegung ein lineares Gleichungssystem mit erstem Einheitsvektor als rechter Seite.

12.2 Die QR-Zerlegung

12.2 Numerische Methoden: QR-Zerlegung

Lösung eines LGS durch QR-Zerlegung

Die **QR-Zerlegung** einer Matrix A ist ein Produkt aus einer **orthogonalen Matrix** Q, d.h. $Q^\top = Q^{-1}$, und einer **oberen Dreiecksmatrix** R, sodass $A = Q \cdot R$.

Bei der Lösung eines LGS $Ax = b$ mit Hilfe der QR-Zerlegung $A = Q \cdot R$ gehen wir wie folgt vor:

1. Definiere $y := Rx$, sodass das LGS zu $Ax = QRx = Qy = b$ wird.
2. Löse $Qy = b$ durch $y = Q^\top b$.
3. Löse $Rx = y$ durch Rückwärtssubstitution.

Anmerkung: Zur Bestimmung der orthogonalen Matrix Q verwenden wir sogenannte Householder Matrizen.

Definition: Householder-Matrix

Sei $v \in \mathbb{R}^n$ ein beliebiger Spaltenvektor mit $\|v\|_2 = 1$. Die zugehörige **Householder-Matrix** $H_v \in M_{n\times n}(\mathbb{R})$ ist

$$H_v := Id_n - 2v \cdot v^\top .$$

Beispiel: Die zu dem Vektor $v = (-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})^\top$ gehörige Householder-Matrix lautet

$$\begin{aligned} H_v &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - 2 \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \end{aligned}$$

Anmerkung: Hier ist $H_v \cdot x$ die Spiegelung von x an der ersten Winkelhalbierenden.

Proposition: Eigenschaften der Householder-Matrix

Sei H_v eine Householder-Matrix. Dann gilt:

1. H_v ist symmetrisch, d.h. $H_v = (H_v)^\top$.
2. H_v ist orthogonal, d.h. $(H_v)^{-1} = (H_v)^\top$.
3. H_v ist involutorisch, d.h. $H_v^2 = Id_n$.

Beweis:

1. Es gilt

$$
\begin{aligned}
(H_v)^\top &= \left(Id_n - 2 \cdot v \cdot v^\top\right)^\top = Id_n^\top - 2\left(v \cdot v^\top\right)^\top \\
&= Id_n - 2\left(v^\top\right)^\top \cdot v^\top = Id_n - 2 \cdot v \cdot v^\top = H_v.
\end{aligned}
$$

12.2 Numerische Methoden: QR-Zerlegung

2. Es gilt

$$
\begin{aligned}
H_v \cdot (H_v)^\top &= \left(Id_n - 2v \cdot v^\top\right)^2 \\
&= Id_n^2 - \mathrm{Id}_n \cdot 4v \cdot v^\top + 4v \cdot \underbrace{v^\top \cdot v}_{=\|v\|_2^2} \cdot v^\top \\
&= Id_n - 4v \cdot v^\top + 4v \cdot v^\top = Id_n.
\end{aligned}
$$

3. Die letzte Eigenschaft folgt direkt aus 1. und 2.:

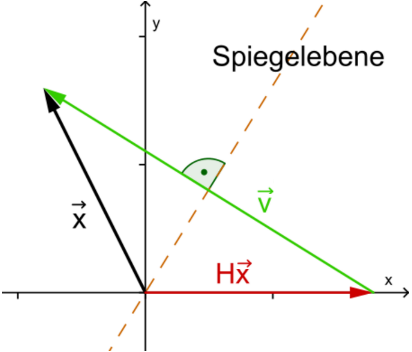
$$H_v^2 = H_v \cdot H_v = H_v \cdot H_v^\top = H_v \cdot H_v^{-1} = Id_n.$$

$\square$

12.2 Numerische Methoden: QR-Zerlegung

Interpretation:

Geometrisch gesehen ist eine Householder-Matrix eine Spiegelung. Geht man etwa von Vektoren x und $v \in \mathbb{R}^2$ aus. Dann entsteht $H_v \cdot x$ durch Spiegelung von x an der zum Vektor v orthogonalen Ursprungsgeraden.



Anmerkung:

12.2 Numerische Methoden: QR-Zerlegung

Die Multiplikation mit einer geeigneten Householder-Matrix wird ein Vektor auf ein Vielfaches eines beliebigen Vektors gespiegelt, insbesondere auf ein Vielfaches des ersten Einheitsvektors.

Proposition

Sei $x \in \mathbb{R}^n$ beliebig. Für die zu $v := x - \|x\|_2 \cdot e_1$ gehörige Householder-Matrix gilt

$$H_v \cdot x = \pm \|x\|_2 \cdot e_1.$$

Beweis: Siehe Skript.

12.2 Numerische Methoden: QR-Zerlegung

Beispiel: Wir bestimmen eine QR-Zerlegung der Matrix

$$A = \begin{pmatrix} 12 & -51 & 4 \\ 6 & 167 & -68 \\ -4 & 24 & -41 \end{pmatrix}.$$

Dazu führen wir nacheinander folgende Schritte aus:

1. Wir bestimmen eine orthogonale Matrix Q_1, so dass in $Q_1 \cdot A$ nur Nullen unter dem obersten Eintrag der ersten Spalte sind.
2. Wir bestimmen eine orthogonale Matrix $Q_2 = \begin{pmatrix} 1 & 0 \\ 0 & \tilde{Q}_2 \end{pmatrix}$, sodass in $Q_2 \cdot Q_1 \cdot A$ nur Nullen unter den Hauptdiagonaleinträgen der ersten und zweiten Spalte sind. Damit haben wie gesuchten oberen Dreiecksmatrix R gefunden und erhalten die QR-Zerlegung

$$R = Q_2 \cdot Q_1 \cdot A \quad \Longleftrightarrow \quad A = Q_1^\top \cdot Q_2^\top \cdot R =: Q \cdot R.$$

1. Schritt: Wir suchen Q_1. Dazu berechnen wir den Vektor

$$w_1 = A_{*1} - \|A_{*1}\|_2 \cdot e_1 = \begin{pmatrix} 12 \\ 6 \\ -4 \end{pmatrix} - \sqrt{12^2 + 6^2 + (-4)^2} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ 6 \\ -4 \end{pmatrix}$$

und mit dessen Einheitsvektor $v_1 = \frac{1}{\sqrt{14}}(-1, 3, -2)^\top$ die orthogonale Matrix

$$Q_1 = Id_3 - 2 \cdot v_1 \cdot v_1^\top = Id_3 - 2 \cdot \frac{1}{\sqrt{14}} \begin{pmatrix} -1 \\ 3 \\ -2 \end{pmatrix} \cdot \frac{1}{\sqrt{14}}(-1, 3, -2)$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \frac{2}{14} \cdot \begin{pmatrix} 1 & -3 & 2 \\ -3 & 9 & -6 \\ 2 & -6 & 4 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 6 & 3 & -2 \\ 3 & -2 & 6 \\ -2 & 6 & 3 \end{pmatrix}.$$

Dann gilt

$$Q_1 \cdot A = \left(\begin{array}{c|cc} 14 & 21 & -14 \\ \hline 0 & -49 & -14 \\ 0 & 168 & -77 \end{array}\right).$$

2. Schritt: Wir suchen die Matrix $\tilde{Q}_2$. Dazu berechnen wir aus der 2×2-Matrix unten rechts einen Vektor w_2

$$w_2 = \tilde{A}_{*1} - \|\tilde{A}_{*1}\|_2 \cdot e_1 = \begin{pmatrix} -49 \\ 168 \end{pmatrix} - \sqrt{(-49)^2 + 168^2} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 56 \cdot \begin{pmatrix} -4 \\ 3 \end{pmatrix}$$

und dessen Einheitsvektor $v_2 = \frac{1}{5}(-4, 3)^\top$.

12.2 Numerische Methoden: QR-Zerlegung

Die Matrix $\tilde{Q}_2$ ergibt sich dann aus:

$$\tilde{Q} = Id_2 - 2 \cdot v_2 \cdot v_2^\top = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - 2 \cdot \tfrac{1}{5} \begin{pmatrix} -4 \\ 3 \end{pmatrix} \cdot \tfrac{1}{5}(-4, 3)$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \frac{2}{25} \cdot \begin{pmatrix} 16 & -12 \\ -12 & 9 \end{pmatrix} = \frac{1}{25} \begin{pmatrix} -7 & 24 \\ 24 & 7 \end{pmatrix}.$$

Dann erhalten wir mit der orthogonalen Matrix $\quad Q_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{7}{25} & \frac{24}{25} \\ 0 & \frac{24}{25} & \frac{7}{25} \end{pmatrix}.$

Dann gilt

$$Q_2 \cdot Q_1 \cdot A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{7}{25} & \frac{24}{25} \\ 0 & \frac{24}{25} & \frac{7}{25} \end{pmatrix} \cdot \begin{pmatrix} 14 & 21 & -14 \\ 0 & -49 & -14 \\ 0 & 168 & -77 \end{pmatrix} = \begin{pmatrix} 14 & 21 & -14 \\ 0 & 175 & -70 \\ 0 & 0 & -35 \end{pmatrix} = R.$$

Wir haben also die obere Dreiecksmatrix R bereits erhalten. Nun multiplizieren wir nacheinander von links mit $Q_2^\top$ und $Q_1^\top$ und erhalten $A = Q_1^\top \cdot Q_2^\top \cdot R =: Q \cdot R$. Wir berechnen noch die Matrix Q

$$Q = Q_1^\top \cdot Q_2^\top = \frac{1}{7} \begin{pmatrix} 6 & 3 & -2 \\ 3 & -2 & 6 \\ -2 & 6 & 3 \end{pmatrix} \cdot \frac{1}{25} \begin{pmatrix} 25 & 0 & 0 \\ 0 & -7 & 24 \\ 0 & 24 & 7 \end{pmatrix} = \frac{1}{175} \begin{pmatrix} 150 & 69 & -58 \\ -75 & 158 & -6 \\ 50 & 30 & 165 \end{pmatrix}$$

und haben damit die vollständige QR-Zerlegung der Matrix bestimmt.

12.2 Numerische Methoden: QR-Zerlegung

Anmerkungen:

- Alternativ zu einer Spiegelung durch eine Householder-Matrix kann man die Dreiecksmatrix R auch durch eine Drehung (Givens-Rotation) erzeugen.
- Im Gegensatz zur LR-Zerlegung hat jede Matrix eine QR-Zerlegung. Das gilt auch für nicht-quadratische Matrizen.
- Die QR-Zerlegung einer Matrix benötigt im Vergleich zur LR-Zerlegung mehr Rechenoperationen, ist aber numerisch stabiler.
- Die QR-Zerlegung hat noch weitere Anwendungen in der Eigenwertberechnung.

12.2 Numerische Methoden: QR-Zerlegung, Aufgabe

Aufgabe:
Berechnen Sie die QR-Zerlegung der folgenden Matrizen.

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -4 & 2 \\ 6 & -3 & -2 \\ 8 & 1 & -1 \end{pmatrix}.$$

12.3 Der QR-Algorithmus

12.3 Numerische Methoden: QR-Algorithmus

Vorüberlegungen:

- Wir wollen die QR-Zerlegung nutzen, um Eigenwerte und Eigenvektoren einer Matrix zu bestimmen.
- Dazu nutzen wir die bereits vorgestellte Ähnlichkeitstransformation.
- Der QR-Algorithmus versucht nun, die Matrix A durch Ähnlichkeitstransformation in Dreiecksgestalt zu bringen.
- Dann können die Eigenwerte von A auf der Hauptdiagonalen der transformierten Matrix abgelesen werden.

12.3 Numerische Methoden: QR-Algorithmus

QR-Algorithmus

Sei $A, \in M_{n\times n}(\mathbb{C})$ gegeben.

1. Setze $A_0 := A$ und zerlege in $A_0 = Q_0 \cdot R_0$.
2. Setze $A_1 := R_0 \cdot Q_0$ und zerlege A_1 in $A_1 = Q_1 \cdot R_1$.

Wiederhole das Verfahren bis A_k annähernd obere Dreiecksgestalt hat und lese die **Eigenwerte** auf der Hauptdiagonalen ab.

Die **Eigenvektoren** stehen für große k approximativ in den Spalten von

$$Q_0 \cdot Q_1 \cdot \ldots \cdot Q_k.$$

Anmerkung:

- Das Verfahren funktioniert, da $Q_k^\top = Q^{-1}$, sodass gilt
  $$A_{k+1} = R_k \cdot Q_k = \underbrace{Q_k^\top Q_k}_{=\mathrm{Id}_n} R_k \cdot Q_k = Q_k^\top \underbrace{Q_k R_k}_{=A_k} \cdot Q_k = Q_k^{-1} A_k Q_k.$$
  Damit ist A_{k+1} ähnlich zu A_k und alle Matrizen A_k haben dieselben Eigenwerte.
- Wenn A komplexe Eigenwerte hat, so treten diese in Form eines 2×2-Blockes auf der Hauptdiagonalen in den Iterierten auf.
- In den Anwendungen wird die Matrix A zunächst auf so genannte Hessenberg-Form gebracht (Dreiecksmatrix mit einer Nebendiagonalen). Der QR-Algorithmus respektiert diese Form während den einzelnen Schritten. Dies minimiert die Anzahl auszuführender Rechenoperationen.
- Um die Konvergenzgeschwindigkeit zu erhöhen werden die Matrizen *geshiftet*, d.h. zu den Hauptdiagonalelementen wird ein Wert μ addiert.

12.3 Numerische Methoden: QR-Algorithmus

Beispiel: Wir berechnen die Eigenwerte der Matrix

$$A = \begin{pmatrix} 2 & -1 \\ -1 & 4 \end{pmatrix}$$

mit dem QR-Algorithmus. Die exakten Eigenwerte sind

$$\begin{aligned} \lambda_1 &= 3 + \sqrt{2} \approx 4.41421\ldots, \\ \lambda_2 &= 3 - \sqrt{2} \approx 1.58578\ldots. \end{aligned}$$

Nun wenden wir den QR-Algorithmus an.

1. Zunächst berechnen wir die QR-Zerlegung von $A_0 = A$. Man erhält

$$A_0 = Q_0 R_0 = \begin{pmatrix} -0.8944 & 0.4472 \\ 0.4472 & 0.8944 \end{pmatrix} \begin{pmatrix} -2.2361 & 2.6833 \\ 0 & 3.1305 \end{pmatrix}.$$

12.3 Numerische Methoden: QR-Algorithmus

2. Wir berechnen
$$A_1 = R_0 \cdot Q_0 = \begin{pmatrix} 3.2 & 1.4 \\ 1.4 & 2.8 \end{pmatrix}$$
und machen die QR-Zerlegung von A_1. Es ergibt sich
$$A_1 = Q_1 R_1 = \begin{pmatrix} -0.9162 & -0.4008 \\ -0.4008 & 0.9162 \end{pmatrix} \begin{pmatrix} -3.4928 & 2.4049 \\ 0 & 2.0041 \end{pmatrix}.$$
3. Wiederholt man das Verfahren so erhält man nach zehn Schritten
$$A_{10} = \begin{pmatrix} 4.4142 & -0.0002 \\ -0.0002 & 1.5858 \end{pmatrix}.$$
Da die Matrix annähernd in Dreiecksgestalt ist, kann man die Eigenwerte von A_{10} (und damit von A) nun auf der Hauptdiagonalen approximativ ablesen.

12.3 Numerische Methoden: QR-Algorithmus, Aufgabe

Aufgabe:
Führen Sie mit der folgenden Matrix zwei Schritte des QR-Algorithmus aus und geben Sie (approximativ) die Eigenwerte der Matrix an:

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$