Mathematik für Informatik 2

Inoffizielles Skript

Marvin Borner

Vorlesung gehalten von

Peter Ochs

Sommersemester 2022

Dies ist mein Mitschrieb aus den Vorlesungen und ist demnach relativ ähnlich zum offiziellen Skript. Ich schreibe außerdem eine Klausurzusammenfassung, welche auf https://marvinborner.de/mathe2zus.pdf zu finden ist.

Inhalt

1 Logik

Aussagen werden **einem** Wahrheitswert zugeordnet: **w** für *wahr* und **f** für *falsch*. Eine Aussage, der der Wahrheitswert **w** schlicht durch Festlegung zugewiesen wurde, heißt **Axiom**.

1.1 Negation (nicht)

- Notation: $\neg X$
- Gesprochen: „nicht X“

X	$\neg X$
w	**f**
f	**w**

- $\neg\neg x \iff x$
- $\neg(\forall x : P) \iff \exists x : (\neg P)$
- $\neg(\exists x : P) \iff \forall x : (\neg P)$

1.2 Konjunktion (und)

- Notation: $X \wedge Y$
- Gesprochen: „X und Y“

Y	X	$X \wedge Y$
w	**w**	**w**
w	**f**	**f**

Y	X	$X \wedge Y$
f	**w**	**f**
f	**f**	**f**

1.3 Disjunktion (oder)

- Notation: $X \vee Y$
- Gesprochen: „X oder Y“

Y	X	$X \vee Y$
w	**w**	**w**
w	**f**	**w**
f	**w**	**w**
f	**f**	**f**

1.4 Bijunktion (Äquivalenz)

- Notation: $X \iff Y$
- Gesprochen: „X genau dann wenn Y“

Y	X	$X \iff Y$
w	**w**	**w**
w	**f**	**f**
f	**w**	**f**
f	**f**	**w**

- Alternative: $(X \implies Y) \wedge (Y \implies X)$

1.5 Subjunktion (Implikation)

- Notation: $X \implies Y$
- Gesprochen: „Aus X folgt Y“

Y	X	$X \implies Y$
w	**w**	**w**
w	**f**	**f**
f	**w**	**w**
f	**f**	**w**

- Alternative: $(\neg X) \vee Y$
- Der Wahrheitswert der Implikation $X \implies Y$ bewertet nur die Korrektheit des Schließens, nicht jedoch die Wahrheit der Aussagen X und Y

1.6 Kontraposition

- Definition: $X \implies Y \iff \neg Y \implies \neg X$

X	Y	$\neg Y$	$\neg Y$	$X \implies Y$	$\neg Y \implies \neg x$
w	**w**	**f**	**f**	**w**	**w**
w	**f**	**f**	**w**	**f**	**f**
f	**w**	**w**	**f**	**w**	**w**
f	**f**	**w**	**w**	**w**	**w**

- Die Kontraposition ist sehr hilfreich für **Widerspruchsbeweise**

1.7 Quantoren

- $\forall$: „für alle“
- $\exists$: „es existiert ein“
- $\exists!$: „es existiert genau ein“
- $\nexists$: „es existiert kein“

1.8 Präzedenz

Sortiert nach stärkster Bindung:

1. Negation ($\neg$)
2. Konjunktion ($\wedge$) und Disjunktion ($\vee$)
3. Implikation ($\iff$) und Äquivalenz ($\implies$)

1.9 Gesetze

- Absorption
  - $X \wedge w \iff X$
  - $X \wedge f \iff f$
  - $X \vee w \iff w$
  - $X \vee f \iff X$
- Assoziativität
  - $(X \vee Y) \vee Z \iff X \vee (X \vee Z)$
  - $(X \wedge Y) \wedge Z \iff X \wedge (X \wedge Z)$
- Kommutativität
  - $X \vee Y \iff Y \vee X$
  - $X \wedge Y \iff Y \wedge X$
- Distributivität
  - $X \wedge (Y \vee Z) \iff (X \wedge Y) \vee (X \wedge Z)$
  - $X \vee (Y \wedge Z) \iff (X \vee Y) \wedge (X \vee Z)$
- De Morgansche Regeln
  - $\neg(X \vee Y) \iff \neg X \wedge \neg Y$
  - $\neg(X \wedge Y) \iff \neg X \vee \neg Y$

2 Mengen

Eine *Menge* ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen. Die in einer Menge zusammengefassten Objekte heißen *Elemente* der Menge.

2.1 Notation

- Mengen angeben durch Auflisten der Elemente: $\{1, 2, 5, 3, 4, 0\}$
- Mengen angeben durch Vorschreiben einer Eigenschaft: $\{x \mid x \text{ ist eine natürliche Zahl kleiner als } 6\}$
- $x \in M$ heißt „x ist Element von M“
- $x \notin M$ heißt „x ist nicht Element von M“
- $\{\}$ und $\emptyset$ bezeichnen die *leere Menge*

2.2 Inklusionsrelationen

- $M \subset N \iff (x \in M \implies x \in N)$
- $M = N \iff (M \subset N \land N \subset M)$
- $M \neq N \iff \neg(M = N) \iff ((\exists x \in M : x \notin N) \lor (\exists x \in N : x \notin M))$
- $M \subsetneq N \iff (M \subset N \land M \neq N)$

2.3 Zahlenbereiche

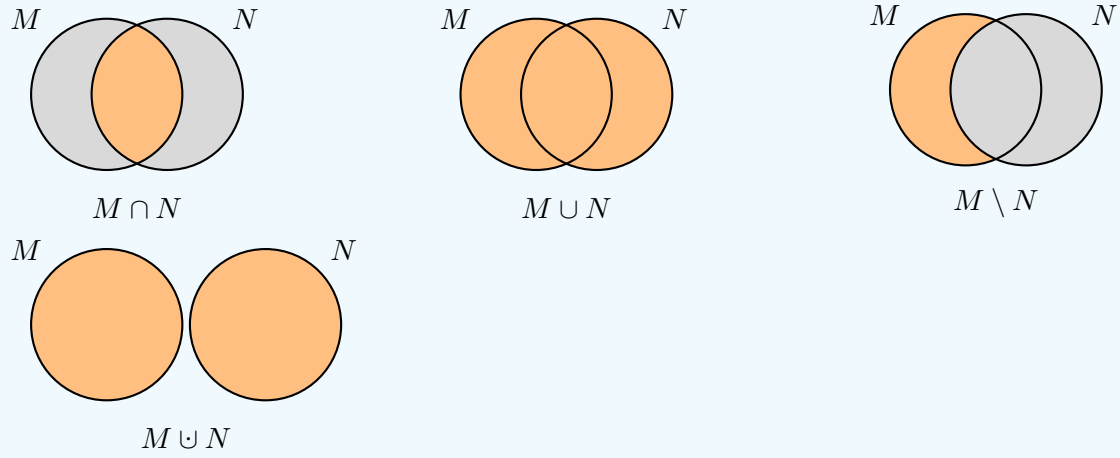
$$\mathbb{P} \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

- **Natürliche Zahlen**: $\mathbb{N} = \{0, 1, 2, 3, 4, 5, ...\}$
- **Positive natürliche Zahlen**: $\mathbb{N}_{>0} = \{1, 2, 3, 4, 5, ...\}$
- **Ganze Zahlen**: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
- **Rationale Zahlen**: $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in Z, q \neq 0\}$
- **Komplexe Zahlen**: $\mathbb{C} = 42$ TODO
- **Primzahlen**: Menge der natürlichen Zahlen p, die genau zwei positive Teiler, nämlich 1 und p, haben

2.4 Operationen von Mengen

- $M \cap N = \{x \mid x \in M \land x \in N\}$ heißt der **Durchschnitt** von M und N
- $M \cup N = \{x \mid x \in M \lor x \in N\}$ heißt die **Vereinigung** von M und N
- $M \setminus N = \{x \mid x \in M \land x \notin N\}$ heißt die **Differenzmenge** von M und N
- $M \times N = \{(x, y) \mid x \in M \land y \in N\}$ heißt das **kartesische Produkt** von M und N. Dabei ist (x, y) ein **geordnetes Paar (Tupel)**, und für zwei geordnete Paare $(x, y), (u, v) \in M \times N$ gilt:
$$(x, y) = (u, v) \iff (x = u \land y = v)$$
- M und N heißen genau dann **disjunkt**, wenn $M \cap N = \emptyset$, d.h. wenn sie kein Element gemeinsam besitzen
- $P = M \dot\cup N \iff (P = M \cup N \land M \cap N = \emptyset)$ beschreibt die **disjunkte Vereinigung**
- $\bigcap_{i \in I} M_i = \{x \mid \forall i \in I : x \in M_i\}$ heißt der **Durchschnitt** der M_i
- $\bigcup_{i \in I} M_i = \{x \mid \exists i \in I : x \in M_i\}$ heißt die **Vereinigung** der M_i
- $P = \dot\bigcup_{i \in I} M_i \iff (P = \bigcup_{i \in I} M_i \land M_i \cap M_j = \emptyset \ \forall i, j \in I \text{ mit } i \neq j)$

Visualisierung im Venn-Diagramm:



Beispiel mit den Mengen $I = \{1, 2, 3\}$, $M_1 = \{a, 1, c\}$, $M_2 = \{b, 1, e\}$ und $M_3 = \{d, 1, f\}$:

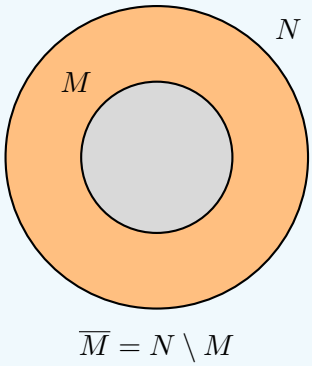
$$\bigcap_{i \in I} = \{1\} \text{ und } \bigcup_{i \in I} = \{1, a, b, c, d, e, f\}$$

2.5 Spezielle Mengen

2.5.1 Komplementärmenge

Für eine Teilmenge M einer Menge N ist $\overline{M} = N \setminus M$.

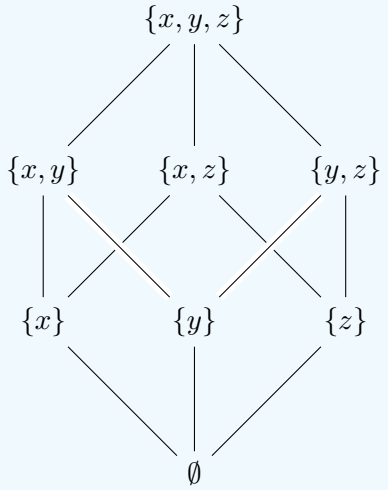
Visualisierung:



2.5.2 Potenzmenge

Für eine Menge M ist die Potenzmenge $\mathcal{P}(M) = \{A \mid A \subset M\}$.

Visualisierung:



Außerdem gilt mit der endlichen Menge M: $|\mathcal{P}(M)| = 2^{|M|}$

Beispiel mit der Menge $M = \{1, 2, 3\}$:

$$\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

sowie

$$|\mathcal{P}(M)| = 8 = 2^3 = 2^{|M|}$$

2.6 Gesetze

- Assoziativität
  - $(M \cup N) \cup P = M \cup (N \cup P)$
  - $(M \cap N) \cap P = M \cap (N \cap P)$
- Kommutativität
  - $M \cup N = N \cup M$
  - $M \cap N = N \cap M$
- Distributivität
  - $M \cap (N \cup P) = (M \cap N) \cup (M \cap P)$
  - $M \cup (N \cap P) = (M \cup N) \cap (M \cup P)$
- Identität
  - $M \cup \emptyset = M$
  - $M \subset N \implies M \cap N = M$
- Komplement
  - $M \subset N \implies M \cup (N \setminus M) = N$
  - $M \subset N \implies M \cap (N \setminus M) = \emptyset$
- De Morgansche Regeln
  - $M \setminus \bigcup_{i \in I} M_i = \bigcap_{i \in I} M \setminus M_i$
  - $M \setminus \bigcap_{i \in I} M_i = \bigcup_{i \in I} M \setminus M_i$

3 Abbildungen

Es seien M und N zwei Mengen. Eine **Abbildung** oder **Funktion** f von M nach N ist eine *eindeutige Zuordnung*, die *jedem* Element $x \in M$ *genau ein* Element $f(x) \in N$ zuweist. Man verwendet den Begriff Funktion nur dann, wenn $N = \mathbb{R}$ ist.

Man nennt M den **Definitionsbereich** von f und N den **Ziel-** oder **Wertebereich**.

Notation:

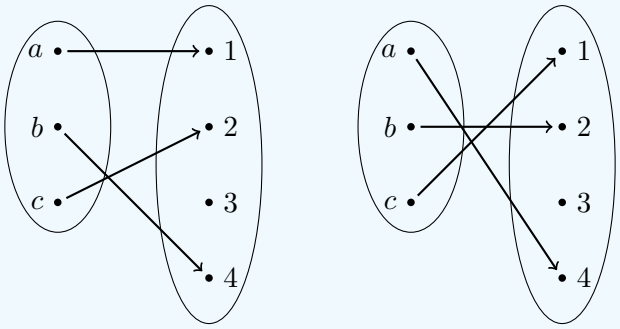
$$f : M \to N,\ x \mapsto f(x)$$

Für zwei Abbildungen $f : M \to N$ und $g : X \to Y$ gilt:

$$f = g \iff (M = X \land N = Y \land \forall x \in M : f(x) = g(x))$$

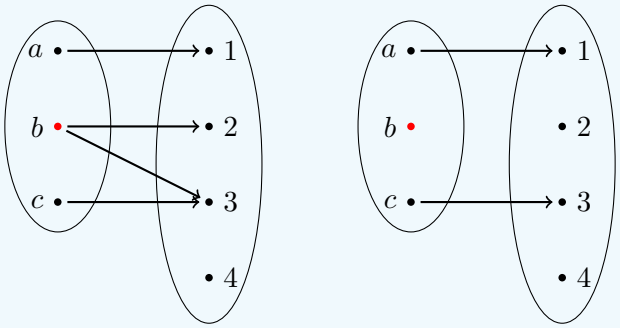
3.1 Legitime Abbildungen

Visualisierung:



3.2 Illegitime Abbildungen

Visualisierung:



3.3 Rechenregeln

Mit den Abbildungen/Funktionen $f : U \to \mathbb{R}$, $g : V \to \mathbb{R}$ und $c \in \mathbb{R}$ gilt:

$$c \cdot f : U \to \mathbb{R} \to \mathbb{R} : x \mapsto c \cdot f(x)$$
$$f + g : U \cap V \to \mathbb{R} : x \mapsto f(x) + g(x)$$
$$f - g : U \cap V \to \mathbb{R} : x \mapsto f(x) - g(x)$$
$$f \cdot g : U \cap V \to \mathbb{R} : x \mapsto f(x) \cdot g(x)$$

Falls außerdem $\forall x \in U \cap V : g(x) \neq 0$:

$$\frac{f}{g} : U \cap V \to \mathbb{R} : x \mapsto \frac{f(x)}{g(x)}$$

3.4 Selektionen

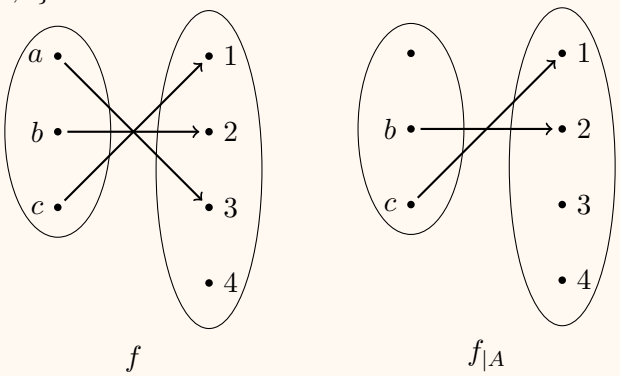
3.4.1 Einschränkung

Mit der Abbildung $f : M \to N$ und $A \subset M$, ist

$$f_{|A} : A \to N,\ x \mapsto f(x)$$

die **Einschränkung** von f auf A.

Beispiel mit $A = \{b, c\}$:



f $f_{|A}$

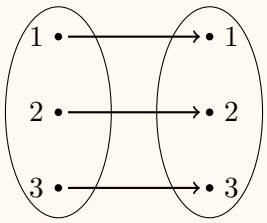
3.4.2 Identität

Mit der Menge M ist die Abbildung

$$\mathrm{id}_M : M \to M,\ x \mapsto x$$

die **Identität** auf M.

Beispiel mit $M = \{1, 2, 3\}$:



id_M

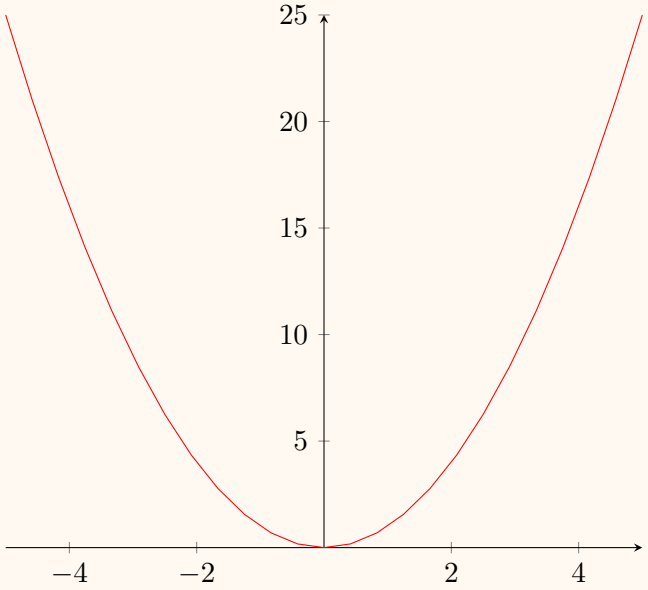
3.4.3 Graph

Mit der Abbildung $f : M \to N$ ist

$$\mathrm{Graph}(f) = \{(x, f(x)) \mid x \in M\} \subset M \times N$$

der **Graph** von f.

Beispiel mit Abbildung $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$:



- Für zwei Abbildungen $f : M \to N$ und $g : P \to N$ gilt:

$$f = g \iff \text{Graph}(f) = \text{Graph}(g)$$

- Ist $\Gamma \subset M \times N$ so, dass

$$\forall x \in M\ \exists!\ y \in N : (x, y) \in \Gamma,$$

dann gibt es eine Abbildung $f : M \to N$ mit $\Gamma = \text{Graph}(f)$

3.4.4 Bild

Mit der Abbildung $f : M \to N$ und $A \subset M$ ist

$$f(A) = \{f(x) \mid x \in A\} \subset N$$

das **Bild** von A *unter* f.

Beispiel mit $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ und $A = \{-2, -1, 0, 1, 2\} \subset M$:

$$f(A) = \{0, 1, 4\}$$

$\text{im}(f) = f(M) \subset N$ heißt das **Bild** von f. Umgangssprachlich bezeichnet das die Menge des getroffenen Zielbereichs.

Mit vorigem **Beispiel**: $\text{im}(f) = \{x \in \mathbb{R} \mid x \geq 0\}$.

3.4.5 Urbild

Mit der Abbildung $f : M \to N$ und $B \subset N$ ist

$$f^{-1}(B) = \{x \in M \mid f(x) \in B\} \subset M$$

das **Urbild** von B unter f.

Beispiel mit $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ und $B = \{0, 1, 4\} \subset N$:

$$f^{-1}(B) = \{-2, -1, 0, 1, 2\}$$

Ist $y \in N$ und $x \in M$ mit $f(x) = y$, so nennt man x **ein Urbild** von y unter f.

3.5 Nachfolgerfunktion

Die Abbildung

$$\mathrm{nf} : \mathbb{N} \to \mathbb{N},\ x \mapsto x + 1$$

nennt man **Nachfolgerfunktion**. Es gilt

$$\mathrm{im}(\mathrm{nf}) = \mathbb{N} \setminus \{0\}$$

und

$$\forall y \in \mathrm{im}(f) : \mathrm{nf}^{-1}(\{y\}) = \{y - 1\}$$

3.6 Eindeutigkeiten

3.6.1 Injektivität (linkseindeutig)

Mit Abbildung $f : M \to N$:

$$f \text{ ist injektiv} \iff \forall x, x' \in M : f(x) = f(x') \implies x = x'$$

oder

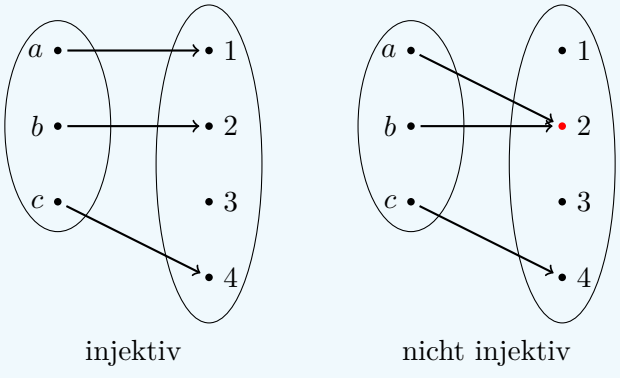
$$f \text{ ist injektiv} \iff \text{jedes } y \in N \text{ hat höchstens ein Urbild}$$

oder

$$f \text{ ist injektiv} \iff f \text{ ist linksinvertierbar}$$

Es gilt: Bei injektivem f gibt es eine oder keine Lösungen für $f(x) = y$.

Visualisierung:



injektiv nicht injektiv

3.6.2 Surjektivität (rechtstotal)

Mit Abbildung $f : M \to N$:

$$f \text{ ist surjektiv} \iff \forall y \in N\ \exists x \in M : f(x) = y$$

oder

$$f \text{ ist surjektiv} \iff \text{im}(f) = N$$

oder

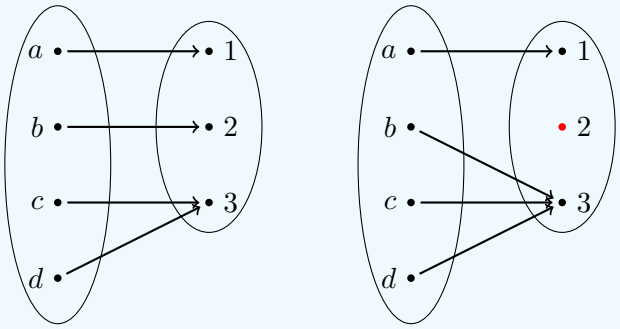
$$f \text{ ist surjektiv} \iff \text{jedes } y \in N \text{ hat mindestens ein Urbild}$$

oder

$$f \text{ ist surjektiv} \iff f \text{ ist rechtsinvertierbar}$$

Es gilt: Bei surjektivem f gibt es eine oder mehrere Lösungen für $f(x) = y$.

Visualisierung:



3.6.3 Bijektivität (eineindeutig)

Mit Abbildung $f : M \to N$:

$$f \text{ ist bijektiv} \iff f \text{ ist injektiv und surjektiv}$$

oder

$$f \text{ ist bijektiv} \iff g : N \to M \text{ existiert} : (g \circ f = \text{id}_M) \wedge (f \circ g = \text{id}_N)$$

oder

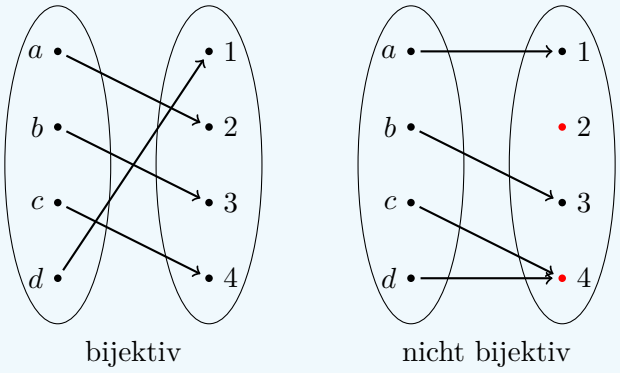
$$f \text{ ist bijektiv} \iff \text{jedes } y \in N \text{ hat genau ein Urbild}$$

oder

$$f \text{ ist bijektiv} \iff f \text{ ist invertierbar}$$

Es gilt: Bei bijektivem f gibt es genau eine Lösung für $f(x) = y$.

Visualisierung:



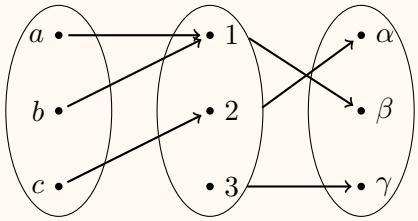
3.7 Komposition

Mit den Abbildungen $f : M \to N$ und $g : N \to P$, ist

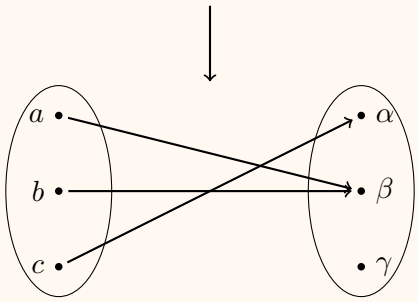
$$g \circ f : M \to P,\ x \mapsto g(f(x))$$

die **Komposition** oder **Verkettung** von f und g.

Beispiel:



$f : M \to N\ \ g : N \to P$



$g \circ f : M \to P$

3.7.1 Assoziativität

Mit den Abbildungen $f : M \to N$, $g : N \to P$ und $h : P \to Q$ gilt:

$$(h \circ g) \circ f = h \circ (g \circ f),$$

weshalb man auch kurz $h \circ g \circ f$ schreibt.

3.7.2 Eindeutigkeiten unter Komposition

Mit den Abbildungen $f : M \to N$ und $g : N \to P$ gilt:

- Sind f und g injektiv, so ist $g \circ f$ injektiv.
- Sind f und g surjektiv, so ist $g \circ f$ surjektiv.
- Sind f und g bijektiv, so ist $g \circ f$ bijektiv.

4 Vollständige Induktion

Sei $\mathcal{A}(n)$ eine Aussageform mit zulässigen Werten $n \in \mathbb{N}$. Falls $\mathcal{A}(0)$ wahr ist und $\mathcal{A}(n) \implies \mathcal{A}(n+1)$ wahr ist, so ist $\mathcal{A}(n)$ wahr für alle $n \in \mathbb{N}$.

- „$\mathcal{A}(0)$ wahr“ nennt man den *Induktionsanfang*
- „$\mathcal{A}(n)$ wird als wahr vorausgesetzt“ nennt man die *Induktionsvoraussetzung*
- „$\mathcal{A}(n) \implies \mathcal{A}(n+1)$“ nennt man den *Induktionsschluss*

5 Mächtigkeit von Mengen

- Eine Menge M ist **endlich**, wenn sie nur endlich viele Elemente enthält. In diesem Fall bezeichnet man mit $\#M = |M|$ die Anzahl an Elementen in M und nennt die Zahl die **Mächtigkeit/Kardinalität** von M. Enthält M unendlich viele Elemente, so nennt man M **unendlich** und setzt $\#M = |M| = \infty$.
- Zwei Mengen M und N heißen **gleichmächtig**, wenn es eine bijektive Abbildung $f : M \to N$ gibt.
- Eine Menge heißt **abzählbar unendlich**, wenn sie gleichmächtig zu $\mathbb{N}$ ist.
- Eine Menge heißt **überabzählbar**, wenn sie weder endlich noch abzählbar unendlich ist.
- Für $m, n \in \mathbb{Z}$ bezeichnet man mit

  $$\{m, ..., n\} = \{k \in \mathbb{Z} \mid m \leq k \leq n\}$$

  die Menge der ganzen Zahlen zwischen m und n.

5.1 Eigenschaften endlicher Mengen

- Ist eine Menge endlich und enthält genau n Elemente, so kann man die Elemente in M mit $x_1, x_2, x_3, ..., x_n$ abzählen und man erhält eine bijektive Abbildung

  $$f : \{1, ..., n\} \to M : i \mapsto x_i.$$

  Umgekehrt erlaubt eine solche Abbildung, die Elemente von M abzuzählen und man erhält $|M| = n$. Damit sieht man, dass eine Menge genau dann endlich von Mächtigkeit n ist, wenn es eine Bijektion von $\{1, ...n\}$ nach M gibt.
- Ist die Menge M endlich und $A \subset M$, so ist auch A endlich und $|A| \leq |M|$.
- Ist $M = A \cup B$ eine endliche Menge, so gilt $|M| = |A| + |B|$.

Zusammenhang zwischen Mächtigkeit und Abbildung:

Mit den nicht-leeren endlichen Mengen M und N gilt:

- $|M| \leq |N| \iff$ eine injektive Abbildung $f : M \to N$ existiert
- $|M| \geq |N| \iff$ eine surjektive Abbildung $f : M \to N$ existiert
- $|M| = |N| \iff$ eine bijektive Abbildung $f : M \to N$ existiert

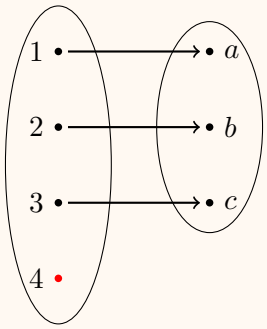
5.2 Schubfachprinzip

Aus dem Zusammenhang zwischen Mächtigkeit und Abbildung folgt

$$f : M \to N \text{ ist eine Abbildung und } |M| > |N| \implies f \text{ ist nicht injektiv.}$$

Diese Kontraposition nennt man auch das **Schubfachprinzip**. Umgangssprachlich heißt das: Wenn man $m > n$ Gegenstände auf n Schubfächer verteilen möchte, dann muss man in mindestens ein Schubfach zwei legen.

Beispiel des Versuchs einer Konstruktion einer injektiven Abbildung trotz $|M| > |N|$ mit $M = \{1, 2, 3, 4\}$ und $N = \{a, b, c\}$:



Injektivität nicht möglich

6 Äquivalenzrelationen

Mit den Mengen M und N, ist jede Teilmenge $R \subset M \times N$ eine **Relation** zwischen M und N. Für $x \in M$ und $y \in N$ schreibt man auch xRy statt $(x, y) \in R$, wenn x in Relation zu y bezüglich R steht.

Für die Äquivalenzrelation R auf die Menge M gilt die Notation:

$$x \sim y \iff (x, y) \in R.$$

6.1 Axiome

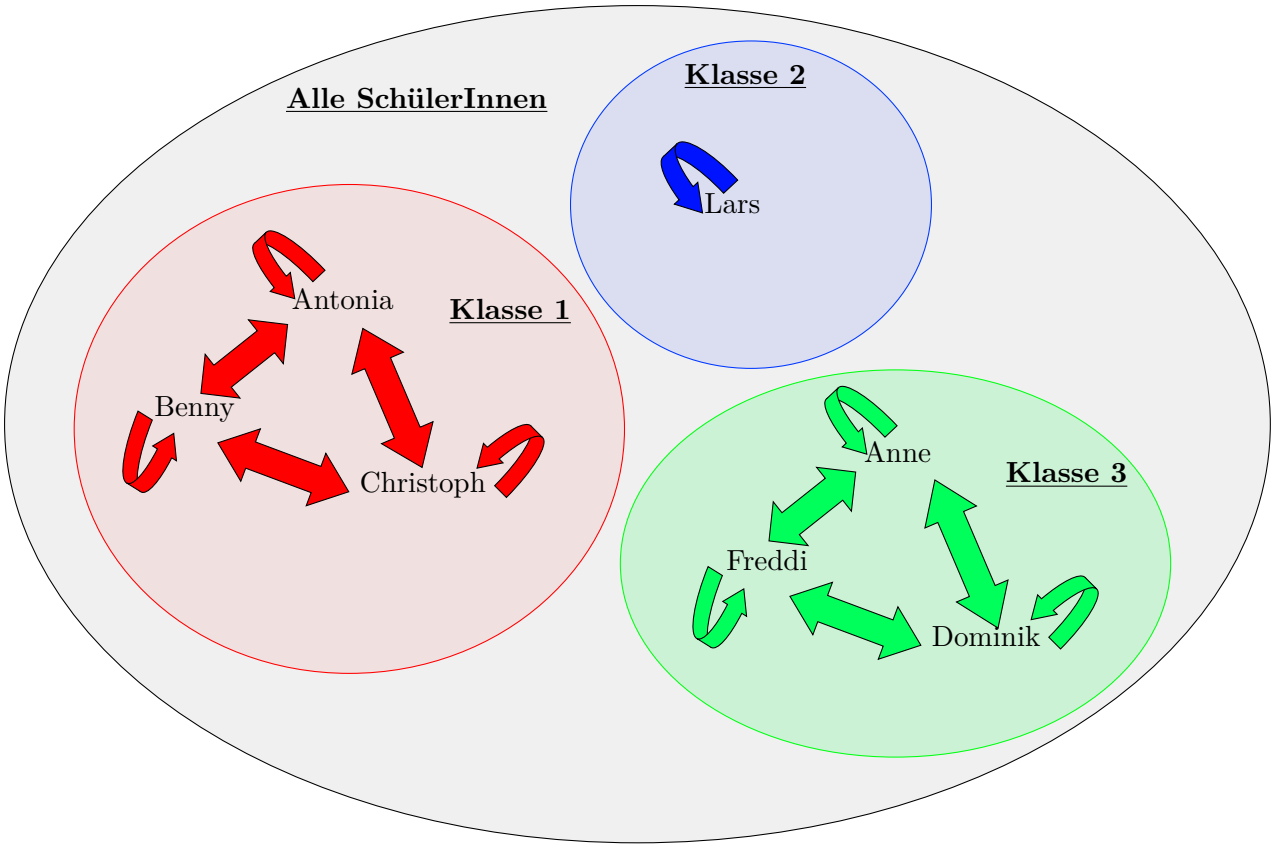
1. *Reflexivität*: $x \sim x$
2. *Symmetrie*: $x \sim y \implies y \sim x$
3. *Transitivität*: $x \sim y \wedge y \sim z \implies x \sim z$

Beispiel einer abstrakten Alltagssituation: In einer Schule werden SchülerInnen klassisch in Schulklassen unterteilt. Übertragen sind die Axiome dann für die Schüler Alfred, Ben und Christoph:

1. Alfred gehört zu einer Schulklasse: Er ist in derselben Schulklasse wie er selbst.
2. Wenn Alfred in derselben Schulklasse ist wie Ben, dann ist Ben auch in derselben Schulklasse wie Alfred.
3. Wenn Alfred in derselben Schulklasse ist wie Ben und wenn zugleich Ben in derselben Schulklasse ist wie Christoph, dann ist auch Alfred in derselben Schulklasse wie Christoph.

In diesem Fall ist dann die Relation „SchülerIn x ist in derselben Schulklasse wie SchülerIn y“ die *Äquivalenzrelation*, die SchülerInnen derselben Schulklasse *äquivalent* und die Schulklassen die *Äquivalenzklassen*.

Visualisierung zu vorigem Beispiel (wunderschön):



6.2 Äquivalenzklassen

Mit der Menge M und der Äquivalenzrelation $\sim$ auf M, heißt für $x \in M$ die Menge

$$[x] = \{y \in M \mid y \sim x\}$$

die **Äquivalenzklasse** von x. Jedes $y \in [x]$ heißt ein **Repräsentant** der Klasse $[x]$.

Mit dem vorigen **Beispiel** gilt:

$$[\text{Alfred}] = \{\text{Alfred, Ben, Christoph}\},$$

sowie

$$[\text{Alfred}] = [\text{Ben}] = [\text{Christoph}].$$

Mit

$$M/\sim = \{[x] \mid x \in M\}$$

bezeichnet man die Menge der **Äquivalenzklassen modulo der Äquivalenzrelation** $\sim$.

Mit dem vorigen **Beispiel** gilt:

$$M/\sim = \{[\text{Alfred}], [\text{Ben}], [\text{Christoph}], [\text{Philipp}], [\text{Anne}], [\text{Dominik}], [\text{Freddi}]\}.$$

6.3 Disjunkte Zerlegung

Ist $(M_i)_{i\in I}$ eine disjunkte Zerlegung der Menge M und die Relation auf M

$$x \sim y \iff \exists i \in I : x, y \in M_i,$$

dann ist $\sim$ eine Äquivalenzrelation auf M.

Ist $\sim$ eine Äquivalenzrelation auf der Menge M, dann bilden die Äquivalenzklassen eine disjunkte Zerlegung von M, d.h. jedes $x \in M$ liegt in genau einer Äquivalenzklasse. Insbesondere gilt für Äquivalenzklassen $[x]$ und $[y]$ entweder $[x] = [y]$ oder $[x] \cap [y] = \emptyset$.

Voriges **Beispiel** der Schulklassen ist hilfreich um zu sehen, dass kein Repräsentant in zwei Äquivalenzklassen gleichzeitig sein kann und damit eine disjunkte Zerlegung der SchülerInnen vorliegen muss.

6.4 Kongruenz modulo n

Mit $n \in \mathbb{Z}_{>0}$ und $a, b \in \mathbb{Z}$ wird die Äquivalenzrelation $\equiv$ definiert:

$$a \equiv b \pmod{n} \iff n \mid a - b$$

Das heißt, die Reste der ganzzahligen Division von a mit n, sowie von b mit n, müssen gleich sein. Zwei äquivalente Zahlen a und b werden dann auch **kongruent modulo** n genannt.

Beispiel mit $5 \equiv 11 \pmod{3}$:
Die Aussage ist wahr, da $\frac{5}{3} = 1$ Rest 2 und $\frac{11}{3} = 3$ Rest 2 die gleichen Reste besitzen bzw. auch $3 \mid (11 - 5) = 3 \mid 6$ wahr ist.

Man bezeichnet die Äquivalenzklasse von $a \in \mathbb{Z}$ mit

$$[a] = \{a + kn \mid k \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$$

Die Menge der Äquivalenzklassen ist

$$\mathbb{Z}/n\mathbb{Z} = \{[a] \mid a \in \mathbb{Z}\}$$

und es gilt $|\mathbb{Z}/n\mathbb{Z}| = n$.

6.4.1 Teilbarkeit in Kongruenz

Mit $a \in \mathbb{Z}$ und $n > 1$ ist die Kongruenz

$$ax \equiv b \pmod{n}$$

genau dann für alle $b \in \mathbb{Z}$ lösbar, wenn $\mathrm{ggT}(a, n) = 1$ gilt, also wenn

$$ax \equiv 1 \pmod{n}$$

lösbar ist.

Beispiel mit $n = 27$ und $a = 5$: Es gilt $\text{ggT}(5, 27) = 1$. Dann ist

$$5 \cdot z \equiv b \pmod{27}$$

lösbar für jedes $b \in \mathbb{Z}$. Es gilt

$$5 \cdot 11 \equiv 1 \pmod{27}$$

und allgemein für $z = 11 \cdot b$:

$$5 \cdot (11 \cdot b) \equiv (5 \cdot 11) \cdot b \equiv b \pmod{27}.$$

Als direkte Konsequenz gilt dann: Mit $a \in \mathbb{Z}$, $n > 1$ und $[a] \in \mathbb{Z}/n\mathbb{Z}$ gilt

$$[a] \text{ ist invertierbar in } \mathbb{Z}/n\mathbb{Z} \quad \Longleftrightarrow \quad \text{ggT}(a, n) = 1$$

Jene invertierbaren Restklassen in $\mathbb{Z}/n\mathbb{Z}$ bezeichnet man dann als **prime Restklassen** modulo n und die Menge der Restklassen (modulo n) als **prime Restklassengruppe** $(\mathbb{Z}/n\mathbb{Z})^*$) (modulo n). Außerdem wird die **Euler'sche φ-Funktion** für $n \in \mathbb{N}$ definiert durch

$$\varphi(n) := \begin{cases} 1, & \text{wenn } n = 1 \\ \#(\mathbb{Z}/n\mathbb{Z})^*, & \text{wenn } n > 1 \end{cases}$$

wobei

$$\#(\mathbb{Z}/n\mathbb{Z})^* = \#\{i \in \mathbb{N} \mid i < n \text{ und } \text{ggT}(i, n) = 1\}.$$

Beispiel:

$$\varphi(p) = p - 1 \quad \text{für } p \in \mathbb{P}$$

$$\varphi(12) = 4 \text{ und } (\mathbb{Z}/n\mathbb{Z})* = \{1, 5, 7, 11\}$$

7 Primzahlen

- Zu jeder Zahl $a \in \mathbb{Z}$ und $b \in \mathbb{N}_{>0}$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

  $$a = qb + r, \quad 0 \leq r < b.$$

  Dabei ist q der **Quotient** und r der **Rest der Division** von a und b.
- Für eine Primzahl $p \in \mathbb{P}$ gilt mit $a, b \in \mathbb{Z}$:

  $$p \mid a \cdot b \implies p \mid a \vee p \mid b.$$

- Die Menge $\mathbb{P}$ der Primzahlen ist unendlich.

7.1 Fundamentalsatz der Arithmetik

Jedes $n \in \mathbb{N} \setminus \{0; 1\}$ hat eine eindeutige Zerlegung

$$n = p_1^{v_1} \cdot p_2^{v_2} \cdot ... \cdot p_r^{v_r}$$

mit Primzahlen $p_1 < p_2 < ... < p_r$ und $v_1, ..., v_r \in \mathbb{N}_{>0}$. Diese Zerlegung nennt man die **Primfaktorzerlegung** von n.

TODO: Erathostenes, ggT, euklidischer Algorithmus

8 Gruppen

Eine **Gruppe** ist ein Paar $(G, *)$ bestehend aus einer *nicht-leeren* Menge G und einer zweistelligen Operation „$*$“, d.h. einer Abbildung

$$* : G \times G \to G : (g, h) \mapsto g * h,$$

sodass folgende *Gruppenaxiome* gelten:

1. *Assoziativgesetz*: $(g * h) * k = g * (h * k)\ \forall g, h, k \in G$
2. *Existenz eines Neutralen*: $\exists e \in G : \forall g \in G : e * g = g$
3. *Existenz von Inversen*: $\forall g \in G : \exists g^{-1} \in G : g^{-1} * g = e$

Eine Gruppe $(G, *)$ heißt **abelsch** oder **kummutativ**, wenn $(G, *)$ zudem noch dem folgenden Axiom genügt:

4. *Kommutativgesetz*: $g * h = h * g\ \forall g, h \in G$

8.1 Eigenschaften

- Aufgrund der Axiome erhält man folgende Eigenschaften für eine Gruppe $(G, *)$:
  - Das neutrale Element $e \in G$ ist eindeutig bestimmt und hat die Eigenschaft

    $$e * g = g * e = g \quad \forall g \in G$$

  - Mit $g \in G$ ist das inverse Element g^{-1} zu g eindeutig bestimmt und hat die Eigenschaft

    $$g^{-1} * g = g * g^{-1} = e$$

  - Für $g, h \in G$ gelten $(g^{-1})^{-1} = g$ und $(g * h)^{-1} = h^{-1} * g^{-1}$
- Häufig wird „$*$“ die **Gruppenmultiplikation** genannt.
- Ist $(G, *)$ eine Gruppe mit endlich vielen Elementen $n \in \mathbb{N}$, so bezeichnet man mit $\#G = |G| = n$ die **Ordnung** der Gruppe.

8.2 Kürzungsregeln

Für die Gruppe $(G, *)$ gilt mit $g, a, b \in G$:

- $g * a = g * b \implies a = b$
- $a * g = b * g \implies a = b$

8.3 Multiplikative Gruppe

Wird die Gruppenoperation als Multiplikation und mit „$\cdot$“ bezeichnet, so schreibt man

- für das Neutrale Element 1_G bzw. 1
- für das Inverse zu g g^{-1} oder $\frac{1}{g}$
- häufig das Multiplikationszeichen nicht, wenn die Bedeutung klar ersichtlich ist (z.B. gh statt $g \cdot h$)
- für das Produkt von $g1, ..., g_n \in G$

$$\prod_{i=1}^{n} g_i = g_1 \cdot g_2 \cdot ... \cdot g_n$$

Außerdem gelten normale multiplikative Potenzgesetze. Allerdings gilt

$$(g \cdot h)^n = g^n \cdot h^n$$

nicht in nicht-abelschen Gruppen, da z.B. mit $n = 4$ Kommutativität notwendig ist:

Beispiel:

$$\begin{aligned} & (g \cdot h)^n = g^n \cdot h^n \\ \Longrightarrow\ & (g \cdot h)^4 = g^4 \cdot h^4 \\ \Longrightarrow\ & (g \cdot h) \cdot (g \cdot h) \cdot (g \cdot h) \cdot (g \cdot h) = (g \cdot g \cdot g \cdot g) \cdot (h \cdot h \cdot h \cdot h) \\ \Longrightarrow\ & g \cdot h \cdot g \cdot h \cdot g \cdot h \cdot g \cdot h = g \cdot g \cdot g \cdot g \cdot h \cdot h \cdot h \cdot h \end{aligned}$$

8.4 Additive Gruppe

Wird die Gruppenoperation als Addition und mit „+“ bezeichnet, so schreibt man

- für das Neutrale Element meist 0_G bzw. 0
- für das Inverse zu g meist $-g$ und meist $g - h$ statt $g + (-h)$
- für die Summe von $g1, ..., g_n \in G$

$$\sum_{i=1}^{n} g_i = g_1 + g_2 + ... + g_n$$

Außerdem gelten normale additive Rechenregeln. Insbesondere muss man bei Rechnungen aufpassen, die je nach Variablen unterschiedliche Operationen mit gleichem Symbol nutzen. **Beispiel** mit $g, h \in G$ und $m, n \in \mathbb{Z}$:

- $\underbrace{(m+n)}_{\text{Add. in } \mathbb{Z}} g = \underbrace{mg + ng}_{\text{Add. in } G}$
- $n \cdot \underbrace{(m+n)}_{\text{Add. in } G} = \underbrace{ng + nh}_{\text{Add. in } G}$
- $0_{\mathbb{Z}} \cdot g = 0_G$
- $n \cdot 0_G = 0_G$

8.5 Permutationsgruppe

Eine **Permutation** ist eine bijektive Abbildung einer endlichen Menge auf sich selbst. Für ein $n \in \mathbb{N}$ verwendet man im Allgemeinen die Menge $\{1, ..., n\}$ und schreibt die Permutation

$$\begin{array}{rccc} \sigma: & \{1, ..., n\} & \to & \{1, ..., n\} \\ & i & \mapsto & \sigma(i) \end{array}$$

als Tabelle

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}.$$

Beispiel mit $n = 4$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Die Permutation (bijektive Abbildung (!)) ist dann

$$\begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 3 \\ 3 &\mapsto 1 \\ 4 &\mapsto 4 \end{aligned}$$

8.6 Symmetrische Gruppe

Die **Menge aller Permutationen** von $\{1, ..., n\}$ wird mit S_n bezeichnet und bildet mit der Komposition "$\circ$" von Abbildungen als Gruppenoperation ("Gruppenmultiplikation")

$$\begin{aligned} \circ : \quad S_n \times S_n &\to S_n \\ (\sigma, \tau) &\mapsto \sigma \circ \tau \end{aligned}$$

eine Gruppe $(S_n, \circ)$ die für $n > 2$ nicht abelsch ist. Diese Gruppe nennt man die **Permutationsgruppe** oder die **Symmetrische Gruppe der Ordnung** n. Es gilt $S_n = \mathrm{Sym}(\{1, ..., n\})$.

Eine Permutation, die nur zwei Elemente vertauscht, heißt **Transposition** (2-Zykel).

Beispiel 1:

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 7 & 6 \end{pmatrix}$ Zykelschreibweise: $\sigma = (1,2,3)(4)(5)(6,7) = (1,2,3)(6,7)$

Beispiel 2:

$$\sigma = (1,2,3)(6,7) = (1,2)(2,3)(6,7)$$

Dann ist

$$\begin{aligned} \sigma(7) &= 6 \\ \sigma(6) &= 7 \\ \sigma(4) &= 4 \\ \sigma(5) &= 5 \\ \sigma(1) &= 2 \\ \sigma(2) &= 3 \\ \sigma(5) &= 1 \end{aligned}$$

Hat $\sigma \in S_n$ zwei Zerlegungen in Transpositionen $\sigma_1, ..., \sigma_k \in S_n$ und $\tau_1, ..., \tau_l \in S_n$, d.h.

$$\sigma = \sigma_1 ... \sigma_k = \tau_1 ... \tau_l,$$

dann gilt $k \equiv l \pmod 2$ und man bezeichnet die **Signatur** von σ mit

$$\mathrm{sign}(\sigma) = (-1)^{\text{Anzahl von Transpositionen in einer Darstellung von } \sigma}.$$

Man nennt eine Permutation σ **gerade**, wenn $\mathrm{sign}(\sigma) = 1$ und **ungerade**, wenn $\mathrm{sign}(\sigma) = -1$ ist.

8.7 Untergruppen

Mit der Gruppe $(G, *)$ mit neutralem Element $e \in G$, heißt die Teilmenge $U \subset G$ **Untergruppe** von G, wenn gilt:

1. $e \in U$
2. $g, h \in U \implies g * h \in U$
3. $g \in U \implies g^{-1} \in U$

Beispiel: Die Menge der Vielfache einer Zahl n, d.h. die Menge $n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$, bildet eine Untergruppe von $(\mathbb{Z}, +)$.

8.8 Nebenklassen

8.8.1 Motivation

$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, ...\}$, dann ist $\{..., -3, 0, 3, 6, ...\} = 3\mathbb{Z}$ eine Untergruppe von Z. $\{..., -2, 1, 4, 7, ...\} = 1 + 3\mathbb{Z}$ sowie $\{..., -1, 2, 5, 8, ...\} = 2 + 3\mathbb{Z}$ sind allerdings keine Untergruppen, aber **Nebenklassen**.

8.8.2 Definition

Mit der Untergruppe $U \subset G$ und $g \in G$, ist die **Linksnebenklasse** von g bezüglich U in G die Menge

$$g * U = \{g * u \mid u \in U\}.$$

Die **Menge der Linksnebenklassen** ist dann

$$G/U = \{g * U \mid g \in G\}.$$

Die **Rechtsnebenklasse** von g bezüglich U in G ist die Menge

$$U * g = \{u * g \mid u \in U\}.$$

Die **Menge der Rechtsnebenklassen** ist analog enstprechend

$$U\backslash G = \{U * g \mid g \in G\}.$$

Mit der Untergruppe $U \subset G$ und $g, h \in G$ gilt:

1. $g * U = h * U \quad \iff \quad h^{-1} * g \quad \in U.$

   Beispiel: $1 + 3\mathbb{Z} = 10 + 3\mathbb{Z} \implies (-10) + 1 \quad \in 3\mathbb{Z}.$

2. Je zwei verschiedene Nebenklassen sind disjunkt.
3. Die Abbildung $f : U \to g * U$ mit $f(u) = g * u$ ist eine Bijektion.
4. Die Anzahl der Linksnebenklassen von U in G ist gleich der Anzahl der Rechtsnebenklassen von U in G. Diese Anzahl heißt **Index**

   $$[G : U] := |G/U| = |U\backslash G|$$

   von U in G.

8.8.3 Satz von Lagrange

Mit der Untergruppe $U \subset G$ gilt

$$|G| = |U| \cdot [G : U].$$

Es folgt, dass *die Ordnung einer jeden Untergruppe die Gruppenordnung teilen muss.*

Beispiel bei Primzahlen: Mit $p \in \mathbb{P}$ gilt: Wenn -1 ein Quadrat in $Z/p\mathbb{Z}$ ist, so ist $p-1$ durch 4 teilbar.

Beweis. Mithilfe des Satz von Lagrange:
$\exists i \in \mathbb{Z}/p\mathbb{Z} : \ i^2 = -1$. Dann ist $U = \{1, -1, i, -i\} \subset (Z/p\mathbb{Z})^*$ mit $|U| = 4$. Es gilt demnach:

$$p - 1 = |(\mathbb{Z}/p\mathbb{Z})^*| = |U| \cdot [(\mathbb{Z}/p\mathbb{Z})^* : U]$$

und deshalb $4 \mid (p-1)$. □

8.9 Zyklische Gruppen

Mit der Gruppe $S \subset G$ ist das **Erzeugnis** von S bzw. die von S **erzeugte Untergrupppe** definiert mit

$$\langle S \rangle = \bigcap \{U \subset G \mid U \text{ ist Untergruppe von } G \text{ mit } S \subset U\}.$$

Ist $S = \{g_1, g_2, ...\}$ gegeben, schreibt man

$$\langle g_1, g_2, ... \rangle = \bigcap \{U \subset G \mid U \text{ ist Untergruppe von } G, \text{ die } g_1, g_2, ... \text{ enthält}\}.$$

Insbesondere für $g \in G$ ist $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ die von g **erzeugte zyklische Untergruppe**. Die **Ordnung** von g ist die Ordnung von $\langle g \rangle$.

Allgemein: Ist $G = \langle g \rangle$ für ein $g \in G$, dann heißt G zyklisch.

Beispiel:
1. $(\mathbb{Z}, +)$: $\mathbb{Z} = \langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\}$.
2. $(\mathbb{Z}/n\mathbb{Z}, +)$ ist eine zyklische Gruppe.
3. $((\mathbb{Z}/5\mathbb{Z})^*, \cdot) \ni [1]$: $\langle [1] \rangle = \langle 1_{(\mathbb{Z}/5\mathbb{Z})^*} \rangle = \langle 1 \rangle = \{[1]^k \mid k \in \mathbb{Z}\} = \{[1^k] \mid k \in \mathbb{Z}\} = \{[1]\}$.

$$\langle [2] \rangle = \{[2]^0, [2]^1, [2]^2, [2]^3, [2]^4\}$$

$$\implies |\langle [2] \rangle| = 4 \mid (5-1) = |(\mathbb{Z}/5\mathbb{Z})^*|$$

Mit der endlichen Gruppe G und $g \in G$ gilt:

$$|\langle g \rangle| \mid |G|.$$

Außerdem gilt mit der Gruppe G und $g \in G$: Die Ordnung von g ist unendlich und die kleinste positive ganze Zahl k mit $g^k = e$, wobei e das neutrale Element der Gruppe ist. Demnach folgt:

8.9.1 Kleiner Satz von Fermat

Ist G eine endliche Gruppe, so gilt für alle Elemente $g \in G$:

$$g^{|G|} = e.$$

8.9.2 Satz von Euler

Mit $n \in \mathbb{N}_{>0}$ und $a \in \{1, 2, ..., n-1\}$ gilt: Ist a teilerfremd zu n, so gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Ist $n = p$ eine Primzahl, so gilt

$$a^{p-1} \equiv 1 \pmod{p}.$$

8.10 Klassifikation von zyklischen Gruppen

Mit den Gruppen G, H heißt die Abbildung $f : G \to H$ **Homomorphismus** (der Gruppen G und H), wenn gilt

$$\forall g, g' \in G : f(g *_G g') = f(g) *_H f(g').$$

Ein **Isomorphismus** ist ein bijektiver Homomorphismus. Wenn es einen Isomorphismus auf zwei Gruppen G und H gibt, heißen diese **isomorph** und werden geschrieben als $G \cong H$.

Für eine zyklische Gruppe G gilt:

$$(G, *) \cong (\mathbb{Z}, +) \quad \text{oder} \quad (G, *) \cong (\mathbb{Z}/n\mathbb{Z}, +) \text{ mit } n = |G|.$$

Ein **Automorphismus** ist ein Isomorphismus einer Gruppe auf sich selbst. TODO?

9 Ringe und Körper

Ein **Ring** ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R zusammen mit zwei zweistellgen Operationen

$$+ : R \times R \to R : (g, h) \mapsto g + h \quad \text{„Addition“}$$

und

$$\cdot : R \times R \to R : (g, h) \mapsto g \cdot h \quad \text{„Multiplikation“}$$

sodass folgende Axiome erfüllt sind:

1. $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0_R.
2. R zusammen mit der Multiplikation „$\cdot$“ erfüllt die Axiome
   a. *Assoziativgesetz*: $(g \cdot h) \cdot k = g \cdot (h \cdot k) \quad \forall g, h, k \in R$
   b. *Existenz eines Neutralen*: $\exists 1_R \in R : \forall g \in R : 1_R \cdot g = g$
3. *Zwei Distributivgesetze*: $\forall g, h, k \in R$:
   a. $(g + h) \cdot k = g \cdot k + h \cdot k$
   b. $g \cdot (h + k) = g \cdot h + g \cdot k$
4. $0_R \neq 1_R$

Ein Ring $(R, +, \cdot)$ heißt **kommutativ**, wenn zudem noch die Multiplikation dem folgenden Axiom genügt:

5. *Kommutativgesetz*: $g \cdot h = h \cdot g \quad \forall g, h \in R$

Ein kommutativer Ring $(R, +, \cdot)$ heißt **Körper**, falls zusätzlich gilt

6. $(R \setminus \{0_R\}, \cdot)$ eine abelsche Gruppe mit 1_R

TODO: Unterschied Ring Körper 9.3

Beispiele:
- $\mathbb{Z}/n\mathbb{Z}$ ist ein kommutativer Ring.
- $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper für $p \in \mathbb{P}$.

9.1 Rechenregeln

Mit Körper K, $x, y, z \in K$ und $u, v \in K \setminus \{0\}$ gilt:

- $-(-x) = x$
- $x + y = z \iff x = z - y$
- $-(x + y) = -x - y$
- $0 \cdot x = x \cdot 0 = 0$
- $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$
- $(-x) \cdot (-y) = x \cdot y$
- $x \cdot (y - z) = x \cdot y - x \cdot z$
- $(x^{-1})^{-1} = x$, für $x \neq 0$
- $x \cdot y = 0 \iff x = y$ oder $y = 0$
- $z \cdot x = z \cdot y,\ z \neq 0 \implies x = y$
- $\frac{x}{u} \cdot \frac{y}{v} = \frac{x \cdot y}{u \cdot v}$
- $\frac{x}{u} + \frac{y}{v} = \frac{x \cdot v + y \cdot u}{u \cdot v}$

9.2 Unterringe

Sei $(R, +, \cdot)$ ein Ring und $S \subset R$. Dann ist $(S, +, \cdot)$ ein **Unterring**, wenn folgende Unterringkriterien erfüllt sind:

1. $(S, +)$ ist eine Untergruppe von $(R, +)$.
2. $1_R \in S$.
3. $g, h \in S \implies g \cdot h \in S$.

9.3 Unterkörper/Teilkörper

Sei $(K, +, \cdot)$ ein Körper und $L \subset K$. Dann ist L ein **Teilkörper/Unterkörper**, von K, wenn folgende Bedingungen erfüllt sind:

1. $g, h \in L \implies g + h, g \cdot h \in L$.
2. $0, 1 \in L$.
3. $g \in L \implies -g \in L$.
4. $g \in L, g \neq 0 \implies g^{-1} \in L$.

9.4 Chinesischer Restsatz

9.4.1 Ziel

Sei $m, n \geq 1$ und $a, b \in \mathbb{Z}$. Finde $x \in \mathbb{Z}$:

$$x \equiv a \pmod{n}$$

$$x \equiv b \pmod{m}$$

Beispiele:

$$x \equiv 4 \pmod 7$$

$$x \equiv 2 \pmod 6$$

Schreibe: $x = 4 \cdot ?_1 + 2 \cdot ?_2 \equiv 4 \cdot 1 + 2 \cdot 0 \pmod 4 \equiv 4 \cdot 0 + 2 \cdot 1 \pmod 6$
Demnach:
Für $?_1$ finde $k \in \mathbb{Z} : 6 \cdot k \equiv 1 \pmod 7 \implies 6^{-1} = 6$.
Für $?_2$ finde $k \in \mathbb{Z} : 7 \cdot l \equiv 1 \pmod 6 \implies 7^{-1} = 1$.

9.4.2 Definition

Seien $m_1, ..., m_r > 1$ paarweise teilerfremde Zahlen, $r > 1$ und $a_1, ..., a_r \in \mathbb{Z}$ beliebig. Dann existiert ein $x \in \mathbb{Z}$ mit

$$x \equiv a_1 \pmod{m_i} \quad \forall i = 1, ..., r$$

und je zwei Lösungen x, x' dieser Kongruenzen erfüllen

$$x \equiv x' \pmod m, \quad m := \prod_{i=1}^{r} m_i.$$

Beweis. Zunächst wird die *Existenz* bewiesen. Es sei $n_i := \frac{m}{m_i} = m_1 \cdot ... \cdot m_{i-1} \cdot m_{i+1} \cdot ... \cdot m_r$. Dann ist $\text{ggT}(m_i, n_i) = 1$ und nach 8.19 existiert n_i^*, sodass $[n_i^*] := [n_i]^{-1} \in \mathbb{Z}/m_i\mathbb{Z}$ ist, d.h. $n_i^* \cdot n_i \equiv 1 \pmod{m_i}$. Wenn nun $x := a_1 n_1 n_1^* + a_2 n_2 n_2^* + ... + a_r n_r n_r *$, gilt nach Konstruktion $m_i \mid n_j$ für $i \neq j$ und damit $a_j n_j n_j^* \equiv 0 \pmod{m_i}$ und daher

$$x \equiv a_i n_i n_i^* \pmod{m_i} \equiv a_i \pmod{m_i}.$$

Um die *Eindeutigkeit* zu zeigen, seien x, x' Lösungen der Kongruenzen (9.1). Dann gilt $x \equiv x' \pmod{m_i}$ für alle $i = 1, ..., r$ und daher auch $m_i \mid (x - x')$. Da dies für alle i erfüllt ist, gilt auch $m \mid x$, woraus die Behauptung bewiesen ist. □

Beispiel:

$$x \equiv 6 \pmod{30}$$
$$x \equiv 2 \pmod{7}$$

Anwendung des chinesischen Restsatzes: Setze $m_1 = \frac{m_1 m_2}{m_1} = m_2 = 7$ und $m_2 = \frac{m_1 m_2}{m_2} = m_1 = 30$.

- Bestimme Inverse von n_1 und n_2:

$$\begin{aligned} 30 &= 4 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

und Rückeinsetzen:

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3 \cdot (30 - 4 \cdot 7) \\ &= 13 \cdot 7 - 3 \cdot 30 \end{aligned}$$

Also $13 \cdot 7 \equiv 1 \pmod{30}$.

- Lösung:

$$x = a_1 n_1 n_1^* + a_2 n_2 n_2^* = a_1 \cdot 7 \cdot 13 + a_2 \cdot 30 \cdot 4 = 6 \cdot 7 \cdot 13 + 2 \cdot 4 \cdot 30.$$

Demnach:

$$x \equiv 156 \pmod{210},$$

d.h. der nächste Vollmond am Sonntag ist in 156 Tagen und wiederholt sich dann alle 210 Tage.

10 Körper der komplexen Zahlen

Motivation: Lösung für $x^2 = -1$ mit $x = i$ und $i^2 = -1$. Also: Konstruktion von i, damit dies erfüllt ist.
Man kann den Körper der komplexen Zahlen konstruieren, indem man den Körper $\mathbb{R}$ der reelen Zahlen und die Menge $C := \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$ betrachtet mit den folgenden Operationen:

$$\begin{aligned} + : \quad C \times C \quad &\to \quad C \\ ((a, b), (c, d)) &\mapsto (a, b) + (c, d) := (a + c, b + d) \end{aligned}$$

und

$$\begin{aligned} \cdot : \quad C \times C \quad &\to \quad C \\ ((a, b), (c, d)) &\mapsto (a, b) \cdot (c, d) := (ac - bd, ad + bc). \end{aligned}$$

Also definiert man:

$$\begin{aligned} (x, 0), \quad x \in \mathbb{R} &:= x \\ (0, 1) &:= i, \end{aligned}$$

da dann gilt:

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1.$$

Für $z = (x, y) \in C$ gilt:

$$z = (x, 0) + (0, 1)(y, 0) = x + iy.$$

Außerdem gilt in $\mathbb{C}$:

$$(x + iy)(u + iv) = (xu + i^2yv) + i(xv + yu) = (xu - yv) + i(xv + yu).$$

Das multiplikative Inverse von $x + iy$ ist demnach:

$$u + iv = \frac{x}{x^2 + y^2} - \frac{iy}{x^2 + y^2}.$$

10.1 Operationen

1. **Betragsfunktionen**:

$$\begin{aligned} |\cdot| : \quad \mathbb{C} \quad &\to \quad \mathbb{R}_{\geq 0} \\ x + iy &\mapsto \sqrt{x^2 + y^2} \end{aligned}$$

2. **Komplexe Konjugation**:

$$\begin{aligned} \bar{\cdot} : \quad \mathbb{C} \quad &\to \quad \mathbb{C} \\ z = x + iy &\mapsto \bar{z} := x - iy. \end{aligned}$$

3. **Realteil**:

$$\begin{aligned} \mathrm{Re} : \quad \mathbb{C} \quad &\to \quad \mathbb{R} \\ x + iy &\mapsto \quad x. \end{aligned}$$

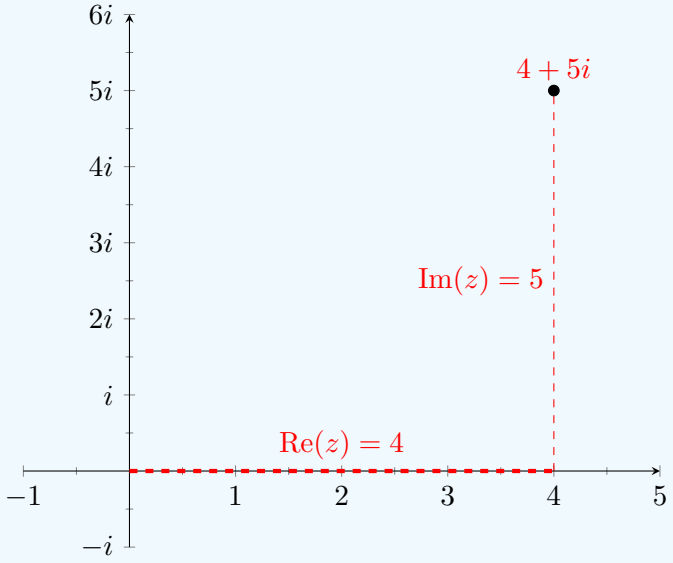
4. **Imaginärteil**:

$$\begin{aligned} \mathrm{Im} : \quad \mathbb{C} \quad &\to \quad \mathbb{R} \\ x + iy &\mapsto \quad y. \end{aligned}$$

10.2 Geometrische Deutung

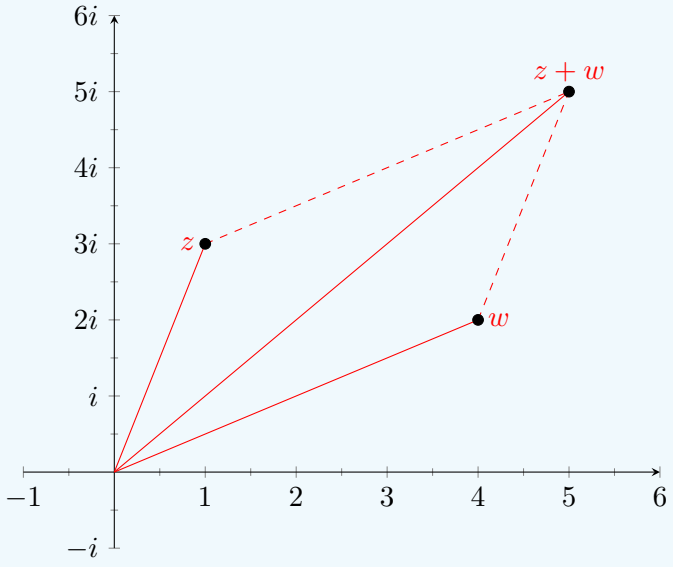
10.2.1 Graph von z

Mit $z = x + yi = 4 + 5i$:



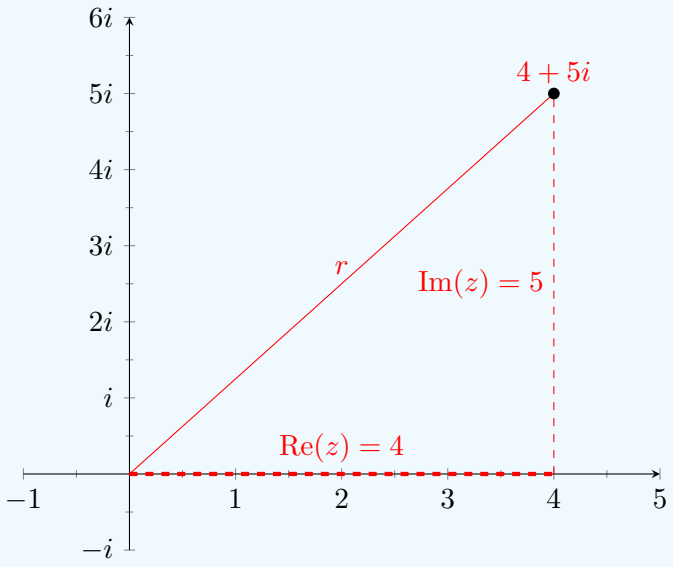
10.2.2 Vektoraddition

Mit $z = x + yi = 1 + 3i$ und $w = u + vi = 4 + 2i$ und $z + w = 5 + 5i$:



10.2.3 Betrag

Mit $z = x + iy = 4 + 5i$, entspricht der Betrag $|z| = \sqrt{x^2 + y^2} = \sqrt{4^2 + 5^2} \approx 6.4 = r$ der euklidischen Länge des Vektors z:



10.2.4 Einheitskreis

$$z = \cos(\alpha) + i\sin(\alpha)$$

TODO. Tikz weird af

Euler-Formel:

$$\mathbb{C} \ni e^{i\alpha} = \cos(\alpha) + i\sin(\alpha)$$

mit α als Winkel im Bogenmaß, sowie

$$|e^{i\alpha}| = 1, \quad \forall \alpha \in \mathbb{R}.$$

10.2.5 Polarkoordinaten

Mit dem Punkt $z' = \frac{z}{|z|}$ gilt:

$$z = x + iy = |z| \cdot \frac{z}{|z|} = |z| \cdot z' = |z| \cdot e^{i\alpha}.$$

Polarkoordinatendarstellung: $z = r \cdot e^{i\alpha} = r(\cos(\alpha) + i\sin(\alpha))$

TODO: Tikz Darstellung der Multiplikation

$$\begin{aligned}(r \cdot e^{i\alpha})(r' \cdot e^{i\alpha'}) &= r \cdot r'(\cos(\alpha) + i\sin(\alpha))(\cos(\alpha') + i\sin(\alpha')) \\ &= \dots \\ &= r \cdot r' \cdot e^{i(\alpha+\alpha')}\end{aligned}$$

10.3 Gleichungen in $\mathbb{C}$

10.3.1 Lineare Gleichung

Finde $z \in \mathbb{C}$ mit $u, v \in \mathbb{C}$ und $u \neq 0$:

$$\begin{aligned} & uz + v = 0 \\ \iff & z = -u^{-1} \cdot v \end{aligned}$$

Ist $u = a + ib$ und $v = c + id$ mit $a, b, c, d \in \mathbb{R}$, dann ist

$$z = -\frac{v}{u} = -\frac{c+id}{a+ib} \cdot \frac{a-ib}{a-ib} = -\frac{(ac+bd) - i(bc-ad)}{a^2+b^2} = -\frac{ac+bd}{a^2+b^2} + i\frac{bc-ad}{a^2+b^2}$$

10.3.2 Quadratische Gleichungen

Finde $z \in \mathbb{C}$ mit Koeffizienten $a, b, c \in \mathbb{R}, \quad a \neq 0$, sodass

$$\begin{aligned} & az^2 + bz + c = 0 \\ \iff & a(z^2 + \frac{b}{a} \cdot z + \frac{z}{a}) = 0 \\ \iff & {}^{a\neq 0} z^2 + \frac{b}{a} \cdot z + \frac{b^2}{4a^2} = \frac{b^2}{4a^2} - \frac{c}{a} \\ \iff & (z + \frac{b}{za})^2 = \frac{b^2 - 4ac}{4a^2} \\ \iff & z_{1,2} = \pm\sqrt{\frac{b^2-4ac}{4a^2}} - \frac{b}{2a} \\ & = \frac{-b \pm \sqrt{b^2-4ac}}{2a} \end{aligned}$$

$$z_{1,2} = \begin{cases} -\frac{b}{2a} \in \mathbb{R}, & \text{wenn } \Delta = 0 \\ \frac{-b \pm \sqrt{b^2-4ac}}{2a} \in \mathbb{R}, & \text{wenn } \Delta > 0 \\ \frac{-b \pm i\sqrt{4ac-b^2}}{2a} = \frac{-b}{2a} \pm i\frac{\sqrt{4ac-b^2}}{2a}, & \text{wenn } \Delta < 0 \end{cases}$$

10.3.3 Einheitswurzeln

Sei $0 \neq \omega = r \cdot e^{i\alpha} \in \mathbb{C}$ und $n \in \mathbb{N}$. Finde $z \in \mathbb{C}$ mit

$$z^n = \omega.$$

Polarkoordinatendarstellung: Betrag und Argument von z^n gleich r und α. Sei $z = s \cdot e^{i\beta}$, dann sucht man (s, β), sodass

$$z^n = s^n \cdot e^{i(n\beta)} = r \cdot e^{i\alpha} = \omega$$

also $s^n = r$ und $n\beta = \alpha + 2\pi k$ mit $k \in \mathbb{Z}$. **Also**: $s = \sqrt[n]{r}$ und $\beta_k \frac{\alpha + 2\pi k}{n}$ mit $k = 0, ..., n-1$. Es gibt also n Lösungen $z_k = \sqrt[n]{r} \cdot e^{i\beta k}, \quad k = 0, ..., n-1$.

11 Polynomringe

Sei R ein kommutativer Ring.

1. Ein **Polynom** über dem Ring R in der Unbestimmten X ist ein Ausdruck der Form
$$f = f(x) = \alpha_n X^n + \alpha_{n-1} X^{n-1} + ... + \alpha_0 X^0 = \sum_{i=0}^{n} \alpha_i X^i$$
mit $n \in \mathbb{N}$ und **Koeffizienten** $\alpha_i \in R,\ i = 0, ..., n$. Genauer ist α_i der **Koeffizient von f zum Grad i**. Ist $a_n = 1$, so nennt man das Polynom f **normiert**.
2. Ist $\alpha_n \neq 0$, so ist n der **Grad** $\text{grad}(f)$ des Polynoms f. Man definiert den Grad des **Nullpolynoms** $f = 0$ als $\text{grad}(0) = -\infty$.
3. Ist $\text{grad}(f) = 2$, dann nennt man $f(X) = \alpha_2 X^2 + \alpha_1 X + \alpha_0$ auch **quadratische Polynome**. Ist $\text{grad}(f) = 1$, dann spricht man auch von **linearen Polynomen** $f(X) = \alpha_1 X + \alpha_0$, und für $\text{grad}(f) = 0$ von den **konstanten Polynomen** $f(X) = \alpha_0$.

Ein **Polynomring** $R[X]$ ist dann die Menge aller Polynome in der Unbestimmten X mit Koeffizienten in einem Ring R, weshalb dieser auch die Ringaxiome erfüllt.

$R[X]$ besitzt die folgenden Operationen:

1.
$$\left(\sum_{i\in\mathbb{N}} \alpha_i X^i\right) + \left(\sum_{i\in\mathbb{N}} \beta_i X^i\right) = \sum_{i\in\mathbb{N}} (\alpha_i + \beta_i) X^i$$

2.
$$\left(\sum_{i\in\mathbb{N}} \alpha_i X^i\right) \cdot \left(\sum_{i\in\mathbb{N}} \beta_i X^i\right) = \sum_{i\in\mathbb{N}} \left(\sum_{k+l=i} (\alpha_k + \beta_l) X^i\right)$$

Für $f, g \in R[X]$ gilt:
$$\text{grad}(f + g) \leq \max(\text{grad}(f), \text{grad}(g))$$
$$\text{grad}(f \cdot g) \leq \text{grad}(f) + \text{grad}(g)$$

Ist $R = K$ ein Körper, so gilt sogar:
$$\text{grad}(f \cdot g) = \text{grad}(f) + \text{grad}(g)$$

11.1 Polynomdivision

Von nun an ist $R = K$ ein beliebiger Körper.

Seien $f, g \in K[X]$ und $g \neq 0$ Polynome mit Koeffizienten in K. Dann existieren eindeutig bestimmte Polynome $q, r \in K[X]$ mit
$$f = q \cdot g + r \quad \text{mit } \text{grad}(r) < \text{grad}(g).$$

Man nennt q den **Quotienten** und r den **Rest der Division** von f durch g.

Beispiel:

$$\begin{array}{r} \left(X^4 + 2X^3 \qquad - X \;\; + 2 \right) \div \left(3X^2 - 1 \right) = \frac{1}{3}X^2 + \frac{2}{3}X + \frac{1}{9} + \frac{-\frac{1}{3}X + \frac{19}{9}}{3X^2 - 1} \\ \underline{-X^4 \qquad + \frac{1}{3}X^2} \\ 2X^3 + \frac{1}{3}X^2 \;\; - X \\ \underline{-2X^3 \qquad + \frac{2}{3}X} \\ \frac{1}{3}X^2 - \frac{1}{3}X \;\; + 2 \\ \underline{-\frac{1}{3}X^2 \qquad + \frac{1}{9}} \\ -\frac{1}{3}X + \frac{19}{9} \end{array}$$

Mit $f, g \in K[X]$, definiert man g **teilt** f oder g **ist ein Teiler von** f, wenn

$$g \mid f \quad :\Longleftrightarrow \quad \exists q \in K[X] : f = g \cdot q.$$

Falls g kein Teiler von f ist, so schreibt man $g \nmid f$.

Beispiel: Das Polynom $X + 1$ ist ein teiler von $X^2 - 1$ in $\mathbb{R}[x]$, da

$$X^2 - 1 = (X + 1)(X - 1) = X^2 - X + X - 1.$$

Ein Polynom $f \in K[X]$ heißt **reduzibel**, wenn es nicht-konstante Polynome $g, h \in K[X]$ gibt, sodass $f = g \cdot h$ gilt. Andernfalls heißt f **irreduzibel**.

Beispiel: $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$, aber reduzibel in $\mathbb{C}[x]$, da $X^2 + 1 = (X - i)(X + i)$ gilt.

11.2 Euklidischer Algorithmus

Ein Polynom $p \in K[X]$ ist **gemeinsamer Teiler** von Polynomen $f, g \in K[X]$, wenn p ein Teiler von f und ein Teiler von g ist. Wir nennen

$$p = \mathrm{ggT}(f, g)$$

einen **größten gemeinsamen Teiler** von f und g, falls p durch jeden gemeinsamen Teiler von f und g teilbar ist. Man nennt p den **normierten größten gemeinsamen Teiler**, wenn $p = \mathrm{ggT}(f, g)$ normiert ist.

Seien $f, g \in K[X]$, $g \neq 0$ und $\mathrm{grad}(f) \geq \mathrm{grad}(g)$. Setze man $r_0 = f$ und $r_1 = g$ und berechne für $j = 0, 1, ...$ die Division von r_j durch r_{j+1} mit Rest r_{j+2} bis $r_{j+2} = 0$ gilt, d.h. finde $q_j \in K[X]$ so, dass

$$r_j = q_j r_{j+1} + r_{j+2} \quad (\text{mit } 0 \leq \mathrm{grad}(r_{j+2}) < \mathrm{grad}(r_{j+1}))$$

erfüllt ist. Ist $n = j + 1 \in \mathbb{N}$ gefunden mit $r_{n+1} = 0$, dann gilt $r_n = \mathrm{ggT}(f, g)$.

TODO: Beispiel

Jedes nicht-konstante Polynom $f \in K[X]$ lässt sich als Produkt irreduzible Polynome aus $K[X]$ darstellen. Diese Darstellung ist bis auf die Reihenfolge und die Multiplikation mit konstanten Polynomen eindeutig.

11.3 Nullstellen von Polynomen

Ist $f \in K[X]$ ein Polynom mit **Nullstelle** $x_0 \in K$, d.h. $f(x_0) = 0$, so ist das Polynom (auch **Linearfaktor** genannt) $g(X) = (X = x_0)$ ein Teiler von f.

Sei $0 \neq f \in K[X]$, dann besitzt f nur endlich viele paarweise verschiedenen Nullstellen $\alpha_1, ..., \alpha_r \in K$, wobei $r \leq \text{grad}(f)$ gilt. Weiter existieren $n_1, ..., n_r \in \mathbb{N}_{>0}$ sowie ein Polynom $g \in K[X]$ ohne Nullstellen in K mit

$$f = \prod_{i=1}^{r} (X - a_i)^{n_i} \cdot g.$$

Dabei sind die Exponenten n_i sowie das Polynom g eindeutig durch f bestimmt. Wir nennen n_i die **Vielfachheit** der Nullstelle a_i.

11.3.1 Anzahl der Nullstellen

Ein Polynom $f \in K[X]$ vom Grad $\text{grad}(f) = n \geq 0$ hat höchstens n Nullstellen.

11.3.2 Fundamentalsatz der Algebra

Jedes Polynom $f \in \mathbb{C}[X]$ zerfällt in Linearfaktoren, d.h. es lässt sich als Produkt von Linearfaktoren schreiben.

12 Vektorräume

1. Ein **K-Vektorraum** ist eine Menge V, auf der eine (innere) Verknüpfung

$$\begin{array}{rccc} + : & V \times V & \to & V \\ & (u, v) & \mapsto & u + v \end{array}$$

   und eine **skalare Multiplikation** (äußere Verknüpfung)

$$\begin{array}{rccc} \cdot : & K \times V & \to & V \\ & (\lambda, v) & \mapsto & \lambda \cdot v \end{array}$$

   definiert sind, sodass folgende **Vektorraumaxiome** erfüllt sind:
   1. $(V, +)$ ist eine abelsche Gruppe
   2. *Assoziativgesetz*: $\forall \lambda, \gamma \in K \wedge v \in V : \lambda(\gamma \cdot v) = (\lambda \cdot \gamma)v$
   3. *Neutrales Element*: $\forall v \in V : 1 \cdot v = v$
   4. *Distributivgesetze*:
      1. $\forall \lambda \in K \wedge u, v \in V : \lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$
      2. $\forall \lambda, \gamma \in K \wedge u \in V : (\lambda + \gamma) \cdot u = \lambda \cdot u + \gamma \cdot u$
2. Die Elemente von V heißen **Vektoren** und die Elemente in K **Skalare**. Das neutrale Element der Gruppe $(V, +)$ nennt man den **Nullvektor** 0.
3. Für $K = \mathbb{R}$ spricht man von einem **reelen Vektorraum** und für $K = \mathbb{C}$ von einem **komplexen Vektorraum**.

Beispiele:

1. $\mathbb{R}^n$: n-dimensionaler euklidischer Raum, welcher alle n-Tupel der reelen Zahlen enthält. $\mathbb{R}^2$ ist entsprechend der klassische zweidimensionale Raum mit Vektor $(x, y)^\top$; analog $\mathbb{R}^3$ mit Vektor $(x, y, z)^\top$. $\mathbb{R}^n$ ist erweiterbar zu $\mathbb{C}^n$ und enthält entsprechend zusätzlich die komplexen Zahlen.
2. Funktionenräume: Die Menge aller K-wertigen Abbildungen $\mathrm{Abb}(X, K) = \{f : X \to K\}$. Dann gilt:
$$(f + g)(x) = f(x) + g(x), \quad \forall x \in X,$$
$$(\lambda \cdot f)(x) = \lambda \cdot f(x), \quad \forall x \in X.$$
3. Der Polynomring $K[X]$ über einem Körper K ist ein K-Vektorraum. Die Ringeigenschaften von $K[X]$ liefern eine Addition, die man als Vektoraddition interpretieren kann. Die skalare Multiplikation mit $\lambda \in K$ lässt sich als Multiplikation in $K[X]$ definieren, indem man den Skalar λ als konstantes Polynom mit dem Wert λ identifiziert (d.h. als Polynom $\lambda X^0 = \lambda \in K[X]$).

12.1 Unterräume

12.1.1 Untervektorraum

Mit dem K-Vektorraum V und $U \subset V$ ist U ein K-**Untervektorraum** von V, wenn folgende Axiome erfüllt sind:

1. $U \neq \emptyset$
2. $u, v \in U \quad \Longrightarrow \quad u + v \in U$
3. $u \in U,\ \lambda \in K \quad \Longrightarrow \quad \lambda u \in U$

Kurz spricht man auch von einem **Unterraum** U von V.

Beispiele:

1. Jeder K-Vektorraum V hat die trivialen Unterräume $\{0\}$ und V.
2. Die Menge aller Polynome vom Grad kleiner gleich $n \in \mathbb{N}$
$$K[X]_{\leq n} = \{f \in K[X] \mid \mathrm{grad}(f) \leq n\}$$
ist ein Unterraum von $K[X]$. Die Addition und Multiplikation können jeweils den Grad nicht gehören und der Raum ist somit abgeschlossen.

12.2 Familie von Vektoren

Eine Familie ist eine geordnete Ansammlung von Elementen. TODO: Mehr.

Mit der Familie von Untervektorräumen von V namens $(U_i)_{i \in I}$ ist auch

$$\bigcap_{i \in I} U_i \text{ ein Untervektorraum von } V.$$

TODO: (Generell) TikZ aus Gekritzel?

12.3 Lineare Hülle

Mit der Familie von Vektoren in V $\mathcal{F} = (v_i)_{i \in I}$ ist eine **Linearkombination** von $\mathcal{F}$ (oder über $\mathcal{F}$) ein Element der Form

$$\sum_{i \in I} \lambda_i v_i \in V, \quad \text{wobei } \lambda_i \in K \text{ und } \lambda_i \neq 0 \text{ für höchstes endlich viele } i \in I.$$

Die Menge aller Linearkombinationen von $\mathcal{F}$ in V wird als **Erzeugnis** (**lineare Hülle**, **Spann**) von $\mathcal{F}$ bezeichnet und mit

$$\text{Lin}(\mathcal{F}) = \text{Lin}((v_i)_{i \in I}) = \left\{ v \in V \;\middle|\; v \text{ ist Linearkombination über } \mathcal{F} \right\}$$

notiert. Dabei nennt man $\mathcal{F} = (v_i)_{i \in I}$ ein **Erzeugendensystem** von $\text{Lin}(\mathcal{F})$. Es gilt außerdem $\text{Lin}() = \{0\}$.

Eine **Linearkombination** von einer Familie von Vektoren $\mathcal{F} = (v_1, ..., v_n)$ in V ist ein Element der Form

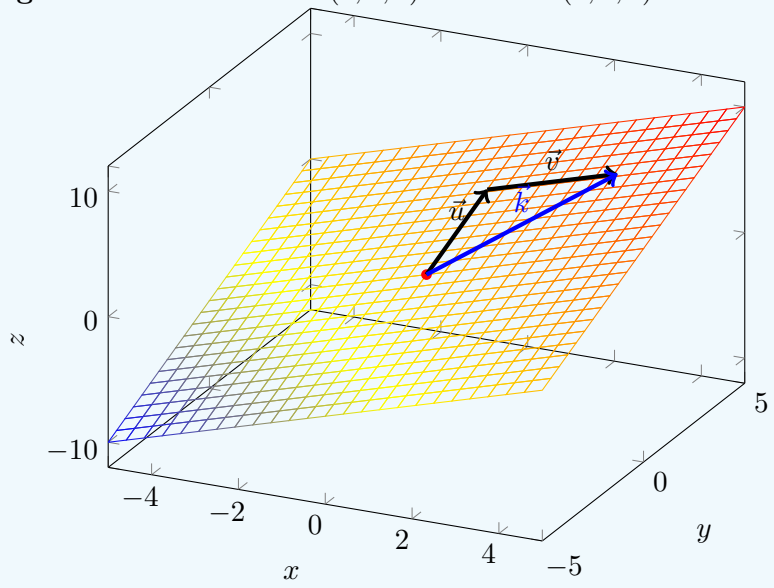
$$\text{Lin}(\mathcal{F}) = \text{Lin}(v_1, ..., v_n) = \left\{ \sum_{i=1}^{n} \lambda_i v_i \;\middle|\; \lambda_i \in K, i \in I \right\}.$$

Beispiele:

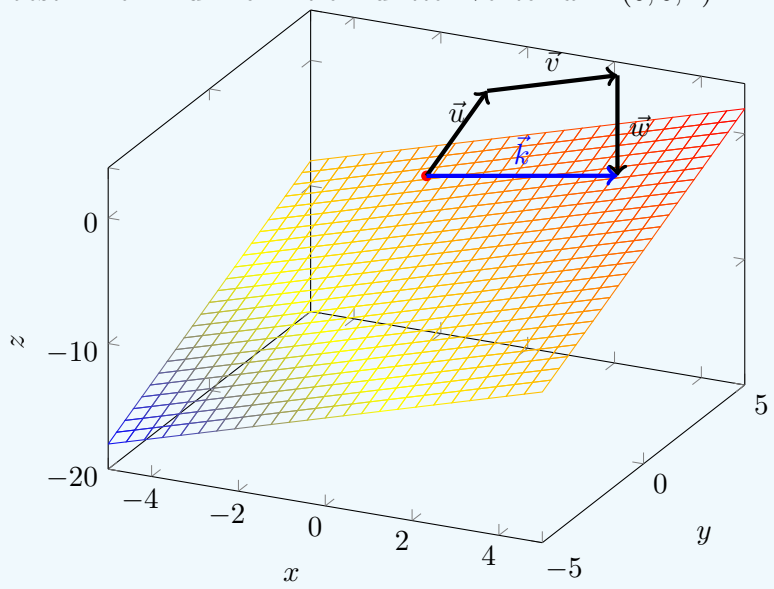
1. Die lineare Hülle der n Koordinateneinheitsvektoren (Basisvektoren) von $\mathbb{R}^n$ ist gerade wieder $\mathbb{R}^n$.
2. Die lineare Hülle von den Vektoren $(1,2)^\top$, $(3,6)^\top$ und $(-2,-4)^\top$ ist die Gerade $\{\vec{r} \mid \vec{r} = t(1,2)^\top, t \in \mathbb{R}\}$ da diese Gerade durch jeden Vektor verläuft (bzw. Ergebnis einer Linearkombination ist).
3. Ist V ein $\mathbb{R}$-Vektorraum $\mathbb{R}^3$ und $\mathcal{F} = (v_1, v_2)$ mit $v_1 = (1,1,0)$ und $v_2 = (1,0,0)$ in $\mathbb{R}^3$, gilt

$$\text{Lin}(\mathcal{F}) = \text{Lin}(v_1, v_2) = \{(\lambda_1 + \lambda_2, \lambda_1, 0) \mid \lambda_1, \lambda_2 \in \mathbb{R}\} = \{(\lambda_1', \lambda_2', 0) \mid \lambda_1', \lambda_2' \in \mathbb{R}\}.$$

Visualisierung in $\mathbb{R}^3$. Zuerst mit $\vec{u} = (0,1,1)^\top$ und $\vec{v} = (1,0,1)^\top$:



Es entsteht ein linearkombinierter Vektor (in diesem Fall $\vec{k} = 3\vec{u} + 3\vec{v} = (3,3,6)^\top$). Durch diesen Vektor lässt sich entsprechend jeglicher Punkt auf der entstandenen Ebene (= lineare Hülle) bestimmen. Nun kommt ein dritter Vektor $\vec{w} = (0,0,1)$ hinzu:



$\vec{w}$ dient nun also als „Veschiebungs“-Vektor, welcher die Ebene in z-Richtung verschieben kann (im Bild mit Faktor -8). Damit ergibt sich, dass die lineare Hülle der drei Vektoren nun den ganzen Raum $\mathbb{R}$ umfasst.

Ist $\mathcal{F} = (v_i)_{i \in I}$ eine Familie von Vektoren in V, dann ist $\mathrm{Lin}(\mathcal{F})$ ein Untervektorraum von V und es gilt

$$\forall i \in I : v_i \in \mathrm{Lin}(\mathcal{F}).$$

Ist $\mathcal{F} = (v_i)_{i \in I}$ eine Familie von Vektoren in V und $M = \{v_i \mid i \in I\}$ die Menge der Vektoren aus $\mathcal{F}$, dann gilt

$$\mathrm{Lin}(\mathcal{F}) = \bigcap_{\substack{M \subset U \subset V \\ U \text{ Unterraum von } V}} U.$$

Existiert für einen Unterraum $U \subset V$ eine Familie von Vektoren $\mathcal{F} = (v_i)_{i \in I}$, sodass $U = \text{Lin}(\mathcal{F})$ gilt, dann nennt man $\mathcal{F}$ ein **Erzeugendensystem** von U, bzw. U **wird von** $\mathcal{F}$ **erzeugt**. Ist $\mathcal{F}$ endlich, so ist U **endlich erzeugt** (von $\mathcal{F}$).

12.4 Lineare Unabhängigkeit

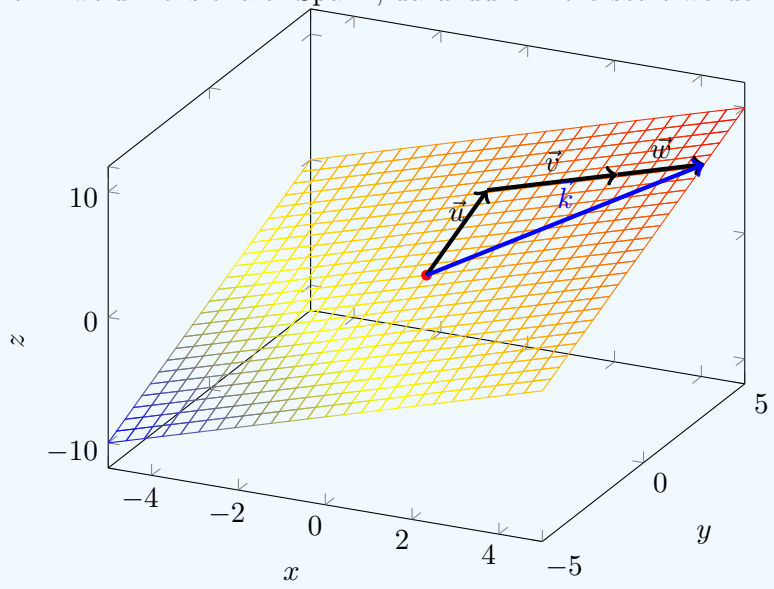
1. Eine Familie $\mathcal{F} = (v_i)_{i \in I}$ in V heißt genau dann **linear abhängig**, wenn eine Linearkombination mit mindestens einem Koeffizienten ungleich 0 existiert, sodass mit $J \subset I$ gilt
$$\sum_{i \in J} \lambda_i v_i = 0, \quad \exists i \in J : \lambda_i \neq 0.$$
2. Dieselbe Familie $\mathcal{F}$ heißt genau dann **linear unabhängig**, wenn diese nicht linear abhängig ist - also wenn jede Darstellung der 0 mittels einer Linearkombination ausschließlich triviale Koeffizienten besitzt:
$$\sum_{i \in J} \lambda_i v_i = 0 \quad \Longrightarrow \quad \forall i \in J : \lambda_i = 0.$$
3. Dieselbe Familie $\mathcal{F}$ ist außerdem ganau dann linear unabhängig, wenn sich jeder Vektor $v \in \text{Lin}(\mathcal{F})$ in eindeutiger Weise als Linearkombination aus Vektoren von $\mathcal{F}$ schreiben lässt.

Beispiele bzw. vereinfachte Erklärung:

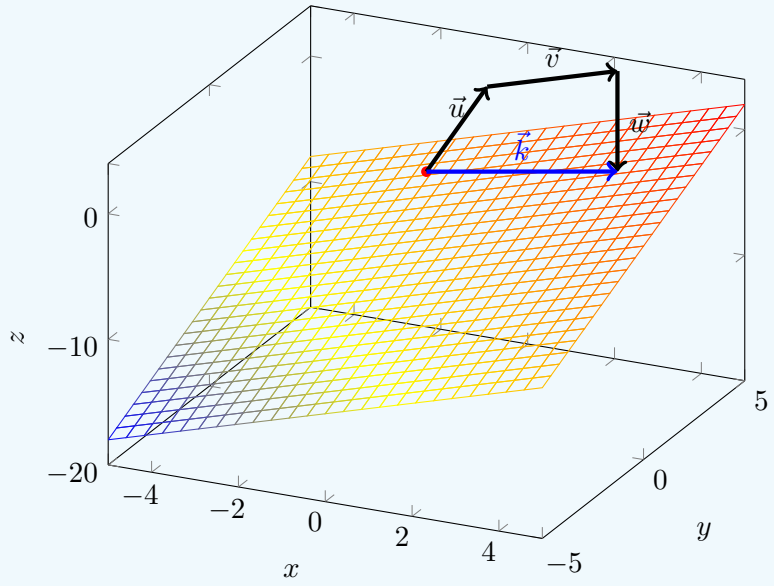
1. Eine Vektorfamilie ist **linear abhängig**, wenn mindestens ein Vektor bereits durch eine Linearkombination eines oder mehrerer anderen Vektoren der Familie ersetzt werden könnte (er ist also redundant für den linearen Spann). Das heißt der lineare Spann verändert sich nicht, wenn man diesen Vektor entfernen würde.
2. Wenn hingegen jeder Vektor tatsächlich eine neue Dimension zum linearen Spann hinzufügt, ist die Vektorfamilie **linear unabhängig**.

Visualisierung in $\mathbb{R}^3$.

1. Mit linear abhängigen Vektoren $\vec{u} = (0,1,1)^\top$, $\vec{v} = (1,0,1)^\top$ und $\vec{w} = (2,0,2)^\top$ entsteht ein zweidimensionaler Spann, da $\vec{w}$ durch $2\vec{v}$ ersetzt werden kann:



2. Mit linear unabhängigen Vektoren $\vec{u} = (0,1,1)^\top$, $\vec{v} = (1,0,1)^\top$ und $\vec{w} = (0,0,1)^\top$ entsteht ein dreidimensionaler Spann, da keiner der Vektoren durch eine Linearkombination anderer Vektoren dargestellt werden kann (siehe auch Kapitel *Lineare Hülle)*:



12.5 Basis

Eine **Basis** $\mathcal{B}$ für V ist ein linear unabhängiges Erzeugendensystem für V, d.h. es gilt

$$\text{Lin}(\mathcal{B}) = V \quad \wedge \quad \mathcal{B} \text{ ist linear unabhängig.}$$

Sie ist also eine Familie an linear unabhängigen Vektoren, die einen Raum aufspannen.

Beispiele:
1. Die Koordinateneinheitsvektoren $e_1 = (1, 0, ..., 0)^\top$, $e_2 = (0, 1, 0, ..., 0)^\top$ bis $e_n = (0, 0, 0, ..., 1)^\top$ sind eine Basis des n-dimensionalen Raumes $\mathbb{R}^n$
2. Die Monome $1, x, x^2, x^3, ...$ bilden eine Basis des unendlichdimensionalen Raumes aller Polynome.

Eigenschaften:

1. Aus jedem endlichen Erzeugendensystem eines Vektorraums kann man eine Basis auswählen.
2. Jeder endlich erzeugte Vektorraum hat eine endliche Basis.
3. Jeder Vektorraum besitzt eine Basis.
4. Hat V eine endliche Basis von n Vektoren, so hat jede Basis von V genau n Vektoren.
5. Jede linear unabhängige Familie von $n = \dim(V)$ Vektoren ist eine Basis von V.

TODO: 11.24?

12.5.1 Steinitzsches Austauschlemma

Mit der endlichen Basis $\mathcal{B} = (b_1, ..., b_n)$ von V und $V \ni b \neq 0$ existiert $i \in \{1, ..., n\}$, sodass $\mathcal{B}' = (b_1, ..., b_{i-1}, b, b_{i+1}, ..., b_n)$ eine Basis von V ist.

12.5.2 Steinitzscher Austauschsatz

Mit der endlichen Basis $\mathcal{B} = (b_1, ..., b_n)$ von V und der linear unabhängigen Familie $\mathcal{F} = (b'_1, ..., b'_m)$ ist $m \leq n$ und es gibt $J \subset \{1, ..., n\}$ derart, sodass man nach Austausch von $(b_i)_{i \in J}$ gegen $\mathcal{F}$ wieder eine Basis von V erhält.

12.6 Dimension

Die **Dimension** $\dim_K(V)$ eines Vektorraums V entspricht der Anzahl der Vektoren einer Basis von V, sofern diese endlich ist, und $\dim_K(V) = \infty$, wenn es keine endliche Basis von V gibt. Wenn aus dem Kontext klar wird, über welchem Körper der Vektorraum gebildet ist, dann schreibt man auch $\dim(V) = \dim_K(V)$.

Zusammenfassend gilt:

V ist n-dimensional
$\iff$ Je n linear unabhängige Vektoren bilden eine Basis.
$\iff$ Eine (und damit jede) Basis hat n Elemente.
$\iff$ Es gibt n linear unabhängige Vektoren mit $V = \text{Lin}(v_1, ..., v_n)$.
$\iff$ Es gibt n linear unabhängige Vektoren, aber jeweils $n + 1$ Vektoren sind linear abhängig.

Beispiele:
1. $\dim_K(K^n) = n$.
2. $\dim_{\mathbb{R}}(\mathbb{R}) = 1$, $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$.
3. $\dim_{\mathbb{R}}(\mathbb{C}) = 2$.

13 Lineare Abbildungen

TUDU.

14 Matrizen

TUDU.

14.1 Blockmatrizen

Eine $m \times n$-**Blockmatrix** M über K mit Blöcken (Untermatrizen) $A_{ij} \in K^{m_i \times n_i}$ für $i = 1, ..., k$ und $j = 1, ..., l$, sodass $m_1 + ... + m_k = m$ und $n_1 + ... + n_l = n$ ist, ist ein rechteckiges Schema der Form

$$M = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1l} \\ A_{21} & A_{22} & \dots & A_{2l} \\ \vdots & \vdots & & \vdots \\ A_{k1} & A_{k2} & \dots & A_{kl} \end{pmatrix} \in K^{m \times n}$$

Beispiel:

$$K^{n \times n} \ni M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

TODO: Elemente klassifizieren

Mit

$$K^{n \times n} \ni M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

und

$$K^{n \times n} \ni M \ = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$$

gilt

$$MM' = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} = \begin{pmatrix} AA' + BC' & AB' + BD' \\ CA' + DC' & CB' + DD' \end{pmatrix}$$

Mit

$$K^{n \times n} \ni M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

und $A \in K^{r \times r}$ und $C = 0$ gilt:

$$M \text{ ist invertierbar } \iff A \text{ und } D \text{ sind invertierbar.}$$

Ist dies der Fall, dann ist

$$M^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{pmatrix}$$

Die Menge aller invertierbaren Matrizen der Form $\mathrm{GL}(n, K) \ni \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ mit A, B, D wie zuvor ist eine Untergruppe von $\mathrm{GL}(n, K)$.

Sei $A \in K^{n\times n}$ eine **(obere) Dreiecksmatrix**, d.h.

$$A = (a_{ij})_{ij} = 1, ..., n \text{ und } a_{ij} = 0 \text{ für } i > j.$$

Genau dann ist A invertierbar, wenn alle $a_{ii} \neq 0, i = 1, ..., n$ sind.

Explizit geschrieben wird eine solche Matrix wie folgt:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{mn} \end{pmatrix}$$

Da A invertirebar ist genau dann, wenn $A^\top$ invertierbar ist, gilt die Aussage des vorigen Korollars auch für eine **(untere) Dreiecksmatrix**, also der Transponierten der oberen Dreiecksmatrix.

Eine Diagonalmatrix $D = \text{diag}(d_{11}, ..., d_{nn}) \in K^{n\times n}$ ist genau dann invertierbar, wenn $d_{ii} \neq 0$ für alle $i = 1, ..., n$ gilt. In diesem Fall ist

$$D^{-1} = \text{diag}()$$

TUDU: REST

TODO: Lückenhaft

14.2 Elementare Zeilen- und Spaltenoperationen

Eine Matrix $A \in K^{m\times n}$ besitzt **Zeilenstufenform**, wenn A folgende Form hat:

$$A = \begin{pmatrix} 0 & \dots & 0 & a_{1j_1} & * & \dots & * & * & * & \dots & * & * & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & a_{2j_2} & * & \dots & * & * & * & \dots & * \\ & \vdots & & & & \vdots & & & & \ddots & & & & \vdots & \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & a_{rj_r} & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ & \vdots & & & & \vdots & & & & \vdots & & & & \vdots & \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

wobei $j_1 < j_2 < ... < j_r$ und $0 \neq a_{kj_k} \in K$ für $k = 1, ..., r$ gilt und $*$ für ein beliebiges Element in K steht. Die Einträge $a_{1j_1}, ..., a_{rj_r}$ sind die **Pivoteinträge**. Man sagt, dass A **normierte Zeilenstufenform** hat, wenn sie Zeilenstufenform mit Pivoteinträgen $a_{1j_1} = ... = a_{rj_r} = 1$ besitzt.

Mit der Matrix $a \in K^{m\times n}$ mit Zeilenvektoren $z_1, ..., z_m \in K^{1\times n}$. Man unterscheidet drei Typen von **elementaren Zeilenoperationen** der Matrix A:

1. Addition des λ-fachen der j-ten Zeile zur i-ten Zeile wobei $i \neq j$ und $\lambda \in K$:

$$Z_{\lambda;j,i} : \begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ z_j \\ \vdots \\ z_m \end{pmatrix} \mapsto \begin{pmatrix} z_1 \\ \vdots \\ z_i + \lambda z_j \\ \vdots \\ z_j \\ \vdots \\ z_m \end{pmatrix}$$

2. Vertauschen der i-ten mit der j-ten Zeile:

$$Z_{i,j} : \begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ z_j \\ \vdots \\ z_m \end{pmatrix} \mapsto \begin{pmatrix} z_1 \\ \vdots \\ z_j \\ \vdots \\ z_i \\ \vdots \\ z_m \end{pmatrix}$$

3. Multiplikation der i-ten Zeile von A mit $0 \neq \lambda \in K$:

$$Z_{\lambda;i} : \begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ z_m \end{pmatrix} \mapsto \begin{pmatrix} z_1 \\ \vdots \\ \lambda \cdot z_i \\ \vdots \\ z_m \end{pmatrix}$$

Dieselben Regeln gelten analog auch für Spaltenvektoren und Spaltenoperationen.

Mit der Matrix $A \in K^{m \times n}$ gelten folgende Aussagen:

1. Man kann A durch endlich viele elementaren Zeilenoperationen vom Typ (i) und (ii) in Zeilenstufenform bringen.
2. Beistzt A Zeilenstufenform, so kann man A durch endlichviele elementaren Zeilenoperationen vom Typ (iii) in normierte Zeilenstufenform bringen.

14.3 Gaußsches Eliminationsverfahren

Sei $0 \neq A \in K^{m \times n}$.

1. Finde die kleinste Zahl $0 \leq j_1 \leq n$, sodass die j_1-te Spalte von A keine Nullspalte ist.
2. Wähle $0 \leq i_1 \leq m$ mit $a_{i_1 j_1} \neq 0$ und vertausche die i_1-te und die 1-te Zeile, d.h. wende Z_{1,i_1} auf A an. Die so erhaltene Matrix $B = Z_{1,i_1}(A)$ hat die Form

$$B = (b_{ij}) = \begin{pmatrix} 0 & \dots & 0 & a_{i_1 j_1} & * & \dots & * \\ 0 & \dots & 0 & * & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & * & * & \dots & * \end{pmatrix}$$

   wobei „$*$“ für ein beliebiges Element in K steht.

3. Für $i = 2, ..., m$ addiere man das $-\frac{b_{ij_1}}{a_{i_1 j_1}}$-fache der ersten Zeile zur i-ten Zeile, d.h. wende $Z_{\lambda_i;1,i}$ mit $\lambda_i = -\frac{b_{ij_1}}{a_{i_1 j_1}}$ für $i = 2, ..., m$ sukzessive an. Dadurch ergibt sich eine Matrix $C = (Z_{\lambda_m;1,m} \circ \cdots \circ Z_{\lambda_2;1,2})(B)$ der Form

$$C = (c_{ij}) = \begin{pmatrix} 0 & \dots & 0 & a_{i_1 j_1} & * & \dots & * \\ 0 & \dots & 0 & 0 & \bullet & \dots & \bullet \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \bullet & \dots & \bullet \end{pmatrix}$$

wobei „$*$“ für das gleiche Element wie in der Matrix B steht und TODO für ein beliebiges Element in K steht. Damit hat man für die erste Zeile den gewünschten Zustand erreicht.

4. Wiederhole Algorithmus auf $D = (c_{(i_1)j})_{i=1,...,m-1;j=1,...,n}$ an.

TODO: Beispiel Algorithmus Treppenform

Sei $A \in K^{m \times n}$ eine Matrix in Zeilenstufenform mit r Pivotspalten. Dann kann A mittels endlich vieler elementarer Spaltenoperationen vom Typ (i) und vom Typ (ii) auf folgende Gestalt bringen

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

wobei D eine $r \times r$-Diagonalmatrix ist. Durch Spaltenoperationen vom Typ (iii) erreicht man weiter, dass $D = E_r$ gilt.

14.4 Elementarmatrizen

Die elementaren Zeilenoperationen lassen sich als Matrix-Matrix Produkte mit sogenannten **Elementarmatrizen** auffassen.

1. Es gilt:

$$Z_{\lambda;i,j}(A) = \underbrace{\begin{pmatrix} 1 & 0 & & & & & 0 \\ 0 & \ddots & & & & & \\ & & 1 & & \lambda & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & 0 \\ 0 & & & & & 0 & 1 \end{pmatrix}}_{=:E_{m;\lambda_i j,i} \in K^{m \times m}} \cdot A$$

2. Es gilt:

$$Z_{ij}(A) = \underbrace{\begin{pmatrix} 1 & 0 & & & & & 0 \\ 0 & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & 0 \\ 0 & & & & & 0 & 1 \end{pmatrix}}_{=:E_{m;i,j} \in K^{m \times m}}$$

3. Es gilt:

$$Z_{\lambda;i}(A) = \underbrace{\begin{pmatrix} 1 & 0 & & & & & 0 \\ 0 & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & 0 \\ 0 & & & & & 0 & 1 \end{pmatrix}}_{=:E_{m;\lambda_i j,i} \in K^{m \times m}}$$

(TUDU: nicht ganz fertig)

Die elementaren Spaltenoperationen lassen sich auch als Matrix-Matrix Produkte mit **Elementarmatrizen** auffassen. Operationen der Spalten erfordern die Multiplikation mit Matrizen vonrechts, anstatt von links. Sei $B \in K^{m \times n}$, dann gilt:

1. $S_{\lambda;i,j}(B) = B \cdot E_{n;\lambda;i,j}$
2. $S_{ij}(B) = B \cdot E_{n;i,j}$
3. $S_{\lambda;i}(B) = B \cdot E_{n;\lambda;i}$

Sei $A \in K^{m \times n}$. Dann gelten folgende Aussagen:

1. Es gibt Elementarmatrizen $S_1, ..., S_k \in K^{m \times m}$, sodass

$$S_k ... S_1 \cdot A$$

   normierte Zeilenstufenform besitzt.
2. Besitzt A Zeilenstufenform mit r Pivotspalten, so gibt es Elementarmatrizen $T_1, ..., T_l \in K^{n \times n}$ mit

$$A \cdot T_1 ... T_l = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

3. Es gibt Elementarmatrizen $S_1, ..., S_k \in K^{m \times m}$ und $T_1, ..., T_l \in K^{n \times n}$ mit

$$S_k ... S_1 \cdot A \cdot T_1 ... T_l = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

Beispiel: Bestimmen der Matrizen S und T.

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \in \mathbb{Q}^{2\times 3}$$

Nun führt man folgende Schritte durch:

$$\left(\begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)$$
$$\rightsquigarrow \left(\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)$$
$$\rightsquigarrow \left(\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)$$

TU DU

15 Der Rang einer Matrix

Sei $A \in K^{m\times n}$.

1. Der **Spaltenraum** von A ist der durch die Spalten $s_1, ..., s_n$ von A erzeugte Untervektorraum $\mathrm{Lin}(s_1, ..., s_n)$ von K^m.
2. Der **Spaltenrang** von A ist die Dimension des Spaltenraums von A:

$$\mathrm{rank}_S(A) = \dim(\mathrm{Lin}(s_1, ..., s_n))$$

Beispiele:

1. Der Spaltenrang der Einheitsmatrix in K^n ist $\mathrm{rank}_S E_n = n$. Allgemeiner gilt
$$\mathrm{rank}_S \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = r.$$
2. Mit der Matrix $\begin{pmatrix} 1 & 3 & 3 \\ 2 & 6 & 2 \\ 3 & 9 & 1 \end{pmatrix}$ gilt $\mathrm{Lin} = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \right) = \mathrm{Lin} \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \right)$ TU-DU: Gekritzel

---

Mit Matrix $A \in K^{m\times n}$ mit Spalten $s_1, ..., s_n$ und $\varphi_A : K^n \to K^m, v \mapsto Av$ gilt

$$\mathrm{im}(\varphi_A) = \mathrm{Lin}(s_1, ..., s_n) \quad \text{und} \quad \dim(\mathrm{im}(\varphi_A)) = \mathrm{rank}_S(A)$$

Mit Matrix $A \in K^{m\times n}$ gilt:

1. Ist $T \in K^{n\times n}$ invertierbar, so gilt $\mathrm{rank}_S(AT) = \mathrm{rank}_S(A)$.

2. Ist $S \in K^{m\times m}$ invertierbar, so gilt $\text{rank}_S(SA) = \text{rank}_S(A)$.

Mit Matrix $A \in K^{m\times n}$ und $r \in \mathbb{N}$ sind folgende Aussagen äquivalent:

1. $\text{rank}_S(A) = r$.
2. Es existieren Elementarmatrizen $S_1, ..., S_K \in K^{m\times m}$ und $T_1, ..., T_1 \in K^{n\times n}$ mit

$$S_k...S_1 \cdot A \cdot T_1...T_l = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

Sei $A \in K^{m\times n}$. Dann gilt:

1. Der **Zeilenraum** von A ist der durch die Zeilen $z_1, ..., z_m$ von A erzeugte Untervektorraum $\text{Lin}(z_1, ..., z_m)$ von K^n.
2. Der **Zeilenrang** von A ist die Dimension des Zeilenraums von A:

$$\text{rank}_Z(A) = \dim(\text{Lin}(z_1, ..., z_m)).$$

Sei $A \in K^{m\times n}$. Dann stimmen Zeilen- und Spaltenrang der Matrix A überein und man bezeichnet diesen als **Rang** von A:

$$\text{rank}(A) = \text{rank}_Z(A) = \text{rank}_S(A).$$

Für eine Matrix $A \in K^{n\times n}$ sind folgende Aussagen äquivalent:

1. Die Spalten von A bilden eine Basis des K^n.
2. Die Zeilen von A bilden eine Basis des K^n.
3. Es gilt $\text{rank}(A) = n$.
4. A ist ein Produkt von Elementarmatrizen.
5. A ist invertierbar. Insbesondere wird die Gruppe $\text{GL}(n, K)$ von den Elementarmatrizen erzeugt.

Beispiel: Bestimmen dse Inversen zu

$$A = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}.$$

Dazu bildet man das Tupel (A, E_3): TUDU: Annotationen

$$\begin{aligned} \left(\begin{pmatrix} 0 & 0 & 1 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) &\rightsquigarrow \left(\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\right) \\ &\rightsquigarrow \left(\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\right) \\ &\rightsquigarrow \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 \\ -1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right) \end{aligned}$$

Damit erhält man

$$A^{-1} = \begin{pmatrix} -1 & 0 & 1 \\ -1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

16 Lineare Gleichungssysteme

Ein **lineares Gleichungssystem** über K in den Variablen $x_1, ..., x_n$ ist ein Gleichungssystem der Form

$$\begin{aligned} a_{11}x_1 + ... + a_{1n}x_n &= b_1, \\ &\vdots \\ a_{m1}x_1 + ... + a_{mn}x_n &= b_m, \end{aligned}$$

mit Koeffizienten $a_{ij}, b_i \in K$. Man nennt das Gleichungssytem **homogen**, falls $b_1 = ... = b_m = 0$ gilt, und sonst nennt man es **inhomogen**.
Eine **Lösung** des Gleichungssystems ist ein Vektor $u \in K^n$, der alle Gleichungen erfüllt. Das System heißt **lösbar**, wenn eine Lösung existiert.