Mathematische Grundlagen und Lineare Algebra

Hochschule
Bonn-Rhein-Sieg

Dr. Marco Hülsmann

Vorlesung WS 2025/26, Hochschule Bonn-Rhein-Sieg, FB 02

Organisatorisches

- **Modul:** Mathematische Grundlagen und Lineare Algebra
- **Dozent:** Dr. Marco Hülsmann

Kontakt

Dr. Marco Hülsmann

Lehrkraft für besondere Aufgaben
Hochschule Bonn-Rhein-Sieg
Fachbereich 02 (Informatik)
Grantham-Allee 20, 53757 Sankt Augustin

- **Büro:** C-180
- **Telefon:** 02241/865-391
- **Email:** `marco.huelsmann@h-brs.de`

Prüfung

- **Prüfungsform:** Klausur (120 min)
- **Zulassung zur Klausur:**
  keine (Freiwillige Testübungen via ACAT und freiwillige schriftiche Zusatzübungen, wahrscheinlich mit digitalen Abgaben, letztere zum Erwerb von Bonuspunkten!!!)

Weitere Informationen zur Klausur gegen Ende des Semesters!!!

Grundlagen

- Mengen
- Aussagenlogik
- Abbildungen/Funktionen
- Beweistechniken
- Algebraische Strukturen

Mengen

Definition 0.1: (Menge)

Eine *Menge* A ist eine Sammlung verschiedener Objekte, auch *Elemente* $a, b, c, d, ...$ genannt, die aus einem *Universum* $\mathcal{U}$ stammen. Man schreibt $a \in A$, wenn a ein Element der Menge A ist, andernfalls $a \notin A$.

- Aufzählende Darstellung:
  - $A = \{a, b, c, d\}$
  - $A = \{a, b, c, ..., z\}$
  - $A = \{1, 2, 3, 4, ...\}$
- Beschreibende Darstellung:
  - $A = \{x \in \mathcal{U} \mid x \text{ hat bestimmte Eigenschaft } p\}$
  - $A = \{x \in \mathcal{U} \mid x \notin B\}$

Leere Menge

Definition 0.2: (Leere Menge)

Die Menge

$$\emptyset = \{\} := \{x \mid x \neq x\}$$

heißt *leere Menge*.

Für alle Elemente x des Universums $\mathcal{U}$ gilt: $x \notin \emptyset$, d.h., die leere Menge enthält keine Elemente.

Kardinalität und Teilmengen

Definition 0.3: (Kardinalität)

Die *Kardinalität* $|A|$ einer Menge A ist die Anzahl ihrer Elemente.

Definition 0.4: (Teilmenge)

Eine Menge B ist eine *Teilmenge* der Menge A, wenn alle Elemente von B auch in A enthalten sind, wenn also für alle $x \in B$ gilt: $x \in A$. Schreibweise: $B \subseteq A$

Satz 0.1:

Falls $B \subseteq A$, so gilt $|B| \leq |A|$. Falls $B \subseteq A$ und $A \subseteq C$, so gilt auch $B \subseteq C$.

Mengengleichheit

Definition 0.5: (Gleiche Mengen)

Zwei Mengen A und B heißen *gleich*, wenn sie dieselben Elemente besitzen, wenn also aus $x \in A$ $x \in B$ folgt und umgekehrt, bzw. wenn sowohl $A \subseteq B$ als auch $B \subseteq A$ gilt.

Möchte man beweisen, daß zwei Mengen gleich sind, daß also $A = B$ gilt, so zeigt man zwei Teilmengenbeziehungen: $A \subseteq B$ und $B \subseteq A$.

Vereinigungsmenge

Definition 0.6: (Vereinigungsmenge)

Seien A und B Mengen. Dann heißt

$$A \cup B := \{x \in \mathcal{U} \mid x \in A \text{ oder } x \in B\}$$

die *Vereinigungsmenge* von A und B.

Ist $(A_i)_{i \in \mathbb{N}}$ eine Familie von Mengen, so ist deren Vereinigungsmenge gegeben durch

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$$

Schnittmenge

Definition 0.7: (Schnittmenge)

Seien A und B Mengen. Dann heißt

$$A \cap B := \{x \in \mathcal{U} \mid x \in A \text{ und } x \in B\}$$

die *Schnittmenge* von A und B.

Ist $(A_i)_{i \in \mathbb{N}}$ eine Familie von Mengen, so ist deren Schnittmenge gegeben durch

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

Komplement

Definition 0.8: (Komplement)

Die Menge $\bar{A} := \{x \in \mathcal{U} \mid x \notin A\}$ ist das *Komplement* von A. Weiterhin definiert man: $A \backslash B := \{x \in A \mid x \notin B\}$ (gesprochen: A ohne B).

Satz 0.2:

Für zwei Mengen A und B gilt

$$A \cap B = \overline{\bar{A} \cup \bar{B}}$$

$$A \subseteq B \Rightarrow \bar{B} \subseteq \bar{A} \text{ (Antitonie)}$$

Kartesisches Produkt

Definition 0.9: (Kartesisches Produkt)

Das *n-äre (binäre für $n = 2$ und ternäre für $n = 3$) kartesische Produkt* von Mengen A_i, $i = 1, ..., n$ (auch *Kreuzprodukt* genannt) ist die Menge aller Tupel der Länge n, bestehend aus Elementen der entsprechenden Mengen:

$$\bigotimes_{i=1}^{n} A_i = A_1 \times A_2 \times ... \times A_n := \{(a_1, a_2, ..., a_n) \mid a_i \in A_i,\ i = 1, ..., n\}$$

Logische Aussagen

- Eine *logische Aussage* ist ein „Satz“, dem ein sogenannter *Wahrheitswert* eindeutig zugeordnet werden kann. Die beiden Wahrheitswerte sind *wahr (w)* und *falsch (f)* (im englischen *True (T)* und *False (F)*). Sie werden vor allem in der Informatik auch oftmals als *Boolesche Variablen* **1** und **0** gekennzeichnet.
- Man kann logische Aussagen mithilfe von sogenannte *Junktoren* zu neuen logischen Aussagen verknüpfen, wie zum Beispiel **und**, **oder**, **entweder-oder** und so weiter.
- Logische Aussagen werden oft auch kurz als Aussagen bezeichnet.

Aussagenlogische Formeln

Aussagenlogische Formeln bestehen aus

- *Variablen* ($A, B, C, \ldots$ oder $p, q, r, \ldots$), die die Wahrheitswerte wahr oder falsch annehmen können sowie
- *logischen Operatoren (Junktoren)*:
  - $\wedge$: (logisches) und
  - $\vee$: (logisches) oder
  - $\oplus$: ausschließendes oder, XOR
  - $\neg$: (logische) Negation
  - $\rightarrow$, $\Rightarrow$: Subjunktion: $A \Rightarrow B$ („aus A folgt B“oder „A impliziert B“)
  - $\leftrightarrow$, $\Leftrightarrow$: Bijunktion: $A \Leftrightarrow B$: („A ist äquivalent zu B“)

Zur Strukturierung von aussagenlogischen Formeln werden runde Klammern verwendet.

Rechenregeln in der Aussagenlogik

- **Idempotenz:** $p \vee p \Leftrightarrow p$, $p \wedge p \Leftrightarrow p$
- **Doppelnegation:** $\neg(\neg p) \Leftrightarrow p$
- **Tautologien:** $1 \vee p \Leftrightarrow 1$, $p \vee \neg p \Leftrightarrow 1$
- **Unerfüllbarkeit:** $0 \wedge p \Leftrightarrow 0$, $p \wedge \neg p \Leftrightarrow 0$
- **Absorption:** $0 \vee p \Leftrightarrow p$, $1 \wedge p \Leftrightarrow p$
- **Kommutativität:** $p \vee q \Leftrightarrow q \vee p$, $p \wedge q \Leftrightarrow q \wedge p$
- **Assoziativität:**
  $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$, $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$
- **Distributivität:** $p \vee (q \wedge r) \Leftrightarrow$
  $(p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
- **de Morgan:**
  $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$, $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$
- **Subjunktion:** $p \Rightarrow q \Leftrightarrow \neg p \vee q$
- **Bijunktion:** $p \Leftrightarrow q \Leftrightarrow (p \Rightarrow q \wedge q \Rightarrow p)$

Anstelle von $q \Rightarrow p$ kann man auch $p \Leftarrow q$ schreiben.

Subjunktion bzw. Implikation

Vorsicht!

Aus $A \Rightarrow B$ folgt nicht zwangsläufig $B \Rightarrow A$

Wenn ich zu meinem Sohn sage, daß er kein Taschengeld bekommt, wenn er sich nicht benimmt, heißt das noch lange nicht, daß er welches bekommt, wenn er sich benimmt.

Was jedoch gilt:

$\neg B \Rightarrow \neg A$. Man sagt auch, B ist *notwendig*, aber nicht *hinreichend* für A. A hingegen ist hinreichend für B.

Beispiele aussagenlogischer Formeln

Wir betrachten folgende Aussagen:

- E: Es ist eiskalt.
- S : Es schneit.

Drücke die folgenden Aussagen mithilfe aussagenlogischer Formeln aus:

- Es ist eiskalt, und es schneit: $E \wedge S$.
- Es ist eiskalt, aber es schneit nicht: $E \wedge \neg S$.
- Es ist nicht eiskalt, und es schneit nicht: $\neg E \wedge \neg S$.
- Entweder es schneit, oder es ist eiskalt, oder beides: $E \vee S$.
- Es schneit, oder es ist eiskalt, aber es schneit nicht, wenn es eiskalt ist: $(E \vee S) \wedge (E \Rightarrow \neg S)$.

Wahrheitstafeln

Belegung:

Zuordnung eines Wahrheitsgehalts zu einer aussagenlogischen Variablen

- $p \vee q$ ist wahr, falls p oder q wahr ist, sonst falsch.
- $p \wedge q$ ist nur dann war, wenn beide Teilaussagen p und q wahr sind, sonst falsch.

Darstellung durch *Wahrheitstafeln:*

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Wahrheitstafeln der Subjunktion und Bijunktion

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

$\neg p$	q	$p \Rightarrow q$	$\neg p \vee q$
1	0	1	1
1	1	1	1
0	0	0	0
0	1	1	1

Also sind die Aussagen $p \Rightarrow q$ und $\neg p \vee q$ aussagenlogisch *äquivalent*. Somit gilt für die Negation:

$$\neg(p \Rightarrow q) \Leftrightarrow \neg(\neg p \vee q) \Leftrightarrow p \wedge \neg q$$

Wahrheitstafel mit drei Variablen: Das Shunting-Lemma

$$(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow ((p \wedge q) \Rightarrow r)$$

p	q	r	$q \Rightarrow r$	$p \wedge q$	$(p \Rightarrow (q \Rightarrow r))$	$((p \wedge q) \Rightarrow r)$
0	0	0	1	0	1	1
0	0	1	1	0	1	1
0	1	0	0	0	1	1
0	1	1	1	0	1	1
1	0	0	1	0	1	1
1	0	1	1	0	1	1
1	1	0	0	1	0	0
1	1	1	1	1	1	1

Schlußregeln

- **Modus ponens:**

$$p \wedge (p \Rightarrow q) \Rightarrow q$$

- **Modus tollens:**

$$(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$$

- **Abschwächung:**

$$p \wedge q \Rightarrow p$$

$$p \Rightarrow p \vee q$$

Quantoren

- $\forall_{x \in M}\ P(x)$: „Für alle x aus der Menge M gilt die Aussage $P(x)$“.
- $\exists_{x \in M}\ P(x)$: „Es existiert ein x aus der Menge M, für das die Aussage $P(x)$ gilt“.
- $\exists!_{x \in M}\ P(x)$: „Es existiert genau ein x aus der Menge M, für das die Aussage $P(x)$ gilt“.

Bei der Verneinung (Negation) von Aussagen werden sämtliche Quantoren umgedreht und die Aussage negiert.
Quantoren werden auch sehr häufig für die beschreibende Darstellung von Mengen verwendet. Menge der Quadratzahlen:

$$Q := \left\{ n \in \mathbb{N}_0 \mid \exists_{m \in \mathbb{N}_0}\ m^2 = n \right\}$$

Abbildungen/Funktionen

Definition 0.10: (Abbildung/Funktion)

Eine *Abbildung* oder *Funktion* $f : A \to B$ ist eine Teilmenge von $A \times B$ mit der zustzlichen Eigenschaft:

$$\forall_{x \in A} \; \exists!_{y \in B} \; (x, y) \in f$$

Man schreibt zumeist statt $(x, y) \in f$: $x \mapsto y$ oder $y = f(x)$.
A heißt *Definitionsbereich* und B *Wertebereich* von f.

Hintereinanderschaltung von Funktionen

Definition 0.11: (Hintereinanderschaltung/Komposition)

Seien $f : A \to B$ und $g : B \to C$ zwei Funktionen. Dann ist die *Hintereinanderschaltung* oder *Komposition*

$$h := g \circ f : A \to C$$

definiert durch

$$h(x) := g(f(x))$$

h ist ebenfalls eine Funktion. Zuerst wird auf x die Funktion f angewandt, dann wird auf das Ergebnis $f(x)$ die Funktion g angewandt.

Beweise

Beweise sind nicht jedermanns Sache, aber...

... das Nachvollziehen von Beweisen ist sehr wichtig, um zu lernen, logisch und strukturiert zu denken!

Grundbegriffe der Beweisführung:

- Voraussetzung
- Behauptung
- Folgerung / Aussage

Mathematische Aussagen werden in sogenannten **Lemmata** (Einzahl: Lemma, oftmals Hilfsaussage für einen nachfolgenden Satz), **Sätzen** oder **Korollaren** (direktes Abfallprodukt eines Satzes oder einer Definition) formuliert.

Durchführung von Beweisen

Es gibt kein allgemeines Kochrezept für Beweise!!!

Eine korrekte Beweisführung erfordert Kreativität und intensives Training.

Es muß stets die Aussage Voraussetzung $\Rightarrow$ Behauptung **bewiesen** bzw. **gezeigt** werden. Ausgehend von der Voraussetzung und evtl. anderer wahrer Aussagen folgert man die Behauptung durch **Implikation**.

Am Ende eines Beweises...

... wird die erfolgreiche Durchführung zumeist mit q.e.d. (quod erat demonstrandum) oder einem unausgefüllten Quadrat $\square$ gekennzeichnet.

Verschiedene Beweisstrukturen

Voraussetzung sei die Aussage V und die Behauptung die Aussage B. Zu beweisen sei: $V \Rightarrow B$

- **Beweis durch Kontraposition:** Man zeigt $\neg B \Rightarrow \neg V$.
- **Widerspruchsbeweis:** Nehme als sog. **Widerspruchsannahme** an, daß die Behauptung falsch ist, also $\neg B$. Stellt man nach diversen Implikationen, ausgehend von $\neg B$ fest, daß irgendeine der Voraussetzungen nicht mehr erfüllt ist oder stößt man auf eine falsche Aussage, so erhält man einen **Widerspruch**. Dies kennzeichnet man üblicherweise mit einem Blitz $\lightning$ und folgert, daß die Widerspruchsannahme falsch war. Daraus folgt, daß die Behauptung wahr ist.
  Prinzip: $(V \Rightarrow B) \Leftrightarrow ((V \wedge \neg B) \Rightarrow 0)$
- **Gegenbeispiel:** Eine Behauptung widerlegen kann man durch das Finden eines Gegenbeispiels.

Fallunterscheidungen

Beweise z.B. $A \vee B \Rightarrow C$. Dann macht man üblicherweise eine sog. **Fallunterscheidung:**

- 1. Fall: A sei wahr. Folgere daraus C.
- 2. Fall: B sei wahr. Folgere daraus ebenfalls C.

Paradebeispiel für Fallunterscheidungen sind Aussagen mit Beträgen:

- 1. Fall: Sei $x \geq 0 \Rightarrow |x| = x \Rightarrow ...$
- 2. Fall: Sei $x < 0 \Rightarrow |x| = -x \Rightarrow ...$

Beweisprinzip der vollständigen Induktion

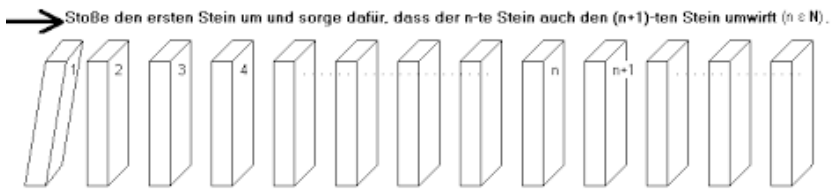
Prinzip der vollständigen Induktion

Sei $A(n)$ eine Aussage für ein $n \in \mathbb{N}$. Falls

- $A(1)$, sog. *Induktionsanfang (IA)*, und
- für alle $n \in \mathbb{N}$ gilt: $A(n) \Rightarrow A(n+1)$,

dann gilt $A(n)$ für alle $n \in \mathbb{N}$.

Umstoßen von unendlich vielen Dominosteinen:



Beispiel: Der kleine Gauß

Aufgabe: Addiere alle Zahlen von 1 bis 100.

Lösung von Gauß:

$$\begin{array}{ccccc} 1 & 2 & \cdots & 99 & 100 \\ 100 & 99 & \cdots & 2 & 1 \\ \hline 101 & 101 & \cdots & 101 & 101 \end{array}$$

Also gilt:

$$\sum_{i=1}^{100} i = \frac{100 \cdot 101}{2} = \frac{10100}{2} = 5050$$

Allgemein:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Beweis: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

- *Induktionsanfang:* Die Aussage gilt für $n = 1$, denn es gilt

$$1 = \sum_{i=1}^{1} i = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

- *Induktionsschritt:* $(n \mapsto n+1)$ Die Behauptung sei für ein beliebiges $n \in \mathbb{N}$ erfüllt. Zeige, daß sie dann auch für $n+1$ erfüllt ist. *Induktionsvoraussetzung (IV):* $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

  Zeige:

$$\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$$

Beweis: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Es gilt:

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) \overset{\text{IV}}{=} \frac{n(n+1)}{2} + (n+1)$$
$$= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Algebraische Strukturen

Eine *algebraische Struktur* $\mathcal{A} = (M, *)$ besteht aus einer *Trägermenge* M und einer *Verknüpfung* $* : M \times M \to M$.
Grundsätzlich muß $\mathcal{A} = (M, *)$ *algebraisch abgeschlossen* sein, d.h.

$$\forall_{a,b \in M} \; a * b \in M$$

Dann ist die Verknüpfung $*$ *wohldefiniert* (auch: *total definiert*).

Elemente in algebraischen Strukturen

Definition 0.12:

Sei $\mathcal{A} = (M, *)$ algebraisch abgeschlossen.

(i) $\mathcal{A}$ heißt *assoziativ*, wenn $\forall_{a,b,c \in \mathcal{A}} \ (a * b) * c = a * (b * c)$

(ii) $e \in \mathcal{A}$ heißt *Einselement* oder *neutrales Element* von $\mathcal{A}$, wenn $\forall_{a \in \mathcal{A}} \ a * e = e * a = a$

(iii) Hat $\mathcal{A}$ ein Einselement e, und falls $\forall_{a \in \mathcal{A}} \ \exists_{b \in \mathcal{A}} \ a * b = b * a = e$, dann heißt b *invers* oder *Inverses* zu a. Bez.: a^{-1}. Falls $a^{-1} = a$, dann heißt a *selbstinvers* oder *Involution*.

(iv) $\mathcal{A}$ heißt *kommutativ*, wenn $\forall_{a,b \in \mathcal{A}} \ a * b = b * a$

Gruppen

Definition 0.13: (Gruppe)

Eine algebraische Struktur $\mathcal{G} = (M, *)$ heißt *Gruppe*, falls die Verknüpfung assoziativ ist, ein Einselement besitzt und es zu jedem Element ein inverses Element gibt. Falls die Verknüpfung zusätzlich kommutativ ist, so spricht man von einer *kommutativen* oder *abelschen Gruppe*.

Eigenschaften von Gruppen

In einer Gruppe $\mathcal{G} = (M, *)$ gilt:

- Das Einselement ist eindeutig.
- Jedes inverse Element ist eindeutig.
- Für $a, b \in \mathcal{G}$ gilt: $(a * b)^{-1} = b^{-1} * a^{-1}$
- $\forall_{a,b,c \in \mathcal{G}}\ a * c = b * c \ \Rightarrow\ a = b$ (sog. *Kürzungsregel*)
- Gleichungen sind eindeutig lösbar:

$$\forall_{a,b \in \mathcal{G}}\ \exists_{x,y \in \mathcal{G}}\ a * x = b\ \wedge\ y * a = b$$

(Lösungen: $x = a^{-1} * b,\ y = b * a^{-1}$)

Ringe

Wir betrachten ab jetzt zwei Operationen $+$ und $\cdot$ für dieselbe Trägermenge M. Sei 0 das Einselement bzgl. $+$ und 1 das Einselement bzgl. $\cdot$.

Definition 0.14: (Ring)

Eine algebraische Struktur $R = (M, +, \cdot)$ heißt *Ring*, falls

1. $(M, +)$ eine abelsche Gruppe ist,
2. die Verknüpfung $\cdot$ assoziativ ist
3. ein Einselement bzgl. $\cdot$ existiert und
4. das Distributivgesetz für erfüllt ist:

$$\forall_{a,b,c \in R}\ a \cdot (b + c) = a \cdot b + a \cdot c$$

Falls die Verknüpfung $\cdot$ zusätzlich kommutativ ist, so spricht man von einem *kommutativen Ring*.

Körper

Definition 0.15: (Körper)

Eine algebraische Struktur $K = (M, +, \cdot)$ heißt *Körper*, falls

1. $(K, +, \cdot)$ ein kommutativer Ring ist und
2. jedes $x \in K \backslash \{0\}$ ein multiplikatives Inverses hat.

In Körpern sind alle bekannten Rechenregeln erlaubt.

Rechenregeln in Körpern

Satz 0.3:

Sei K ein Körper und $a, b, c, d \in K$. Dann gilt:

(i) $a \cdot 0 = 0$

(ii) $ab = 0 \Rightarrow a = 0 \vee b = 0$

(iii) $ab + (-a)b = 0$

(iv) $(-a)b = -(ab)$

(v) $(-a)(-b) = ab$

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

(vii) $(a \cdot b^{-1}) \cdot (c \cdot d^{-1}) = (a \cdot c) \cdot (b^{-1} \cdot d^{-1})$

(viii) $a \cdot b^{-1} + c \cdot d^{-1} = (a \cdot d + b \cdot c) \cdot (b \cdot d)^{-1}$

Rechenregeln in Körpern

Satz 0.3 (Fortsetzung):

Sei K ein Körper und $a, b, c, d \in K$. Dann gilt:

(ix) $\forall_{n \in \mathbb{Z}}\ a^n \cdot b^n = (ab)^n$

(x) $\forall_{n,m \in \mathbb{Z}}\ a^m \cdot a^n = a^{m+n}$

(xi) $\forall_{n,m \in \mathbb{Z}}\ (a^m)^n = a^{m \cdot n}$

(xii) $(a+b)(a-b) = a^2 - b^2$

(xiii) Die Gleichung $a + x = b$ ist eindeutig lösbar.

(xiv) Die Gleichung $ax + b = c$ mit $a \neq 0$ ist eindeutig lösbar.

(xv) Die Aussagen (i), (iii)–(v), (ix)–(xiv) gelten auch in Ringen.

Überblick I

Überblick II

Überblick I

Überblick II

Binäre Relationen

Definition 1.1: (Binäre Relation)

Eine *binäre Relation* $R : X \to Y$ zwischen zwei Mengen X und Y ist eine Teilmenge des Kreuzproduktes

$$R \subseteq X \times Y$$

Schreibweisen: $(x, y) \in R$ oder xRy $(x \in X, y \in Y)$.
Die Menge X heißt *Domäne* von R: $\mathrm{dom}(R) = X$.
Die Menge Y heißt *Kodomäne* von R: $\mathrm{cod}(R) = Y$.
Eine binäre Relation mit $\mathrm{dom}(R) = \mathrm{cod}(\mathrm{R})$ heißt *homogen* oder auch *Endorelation*.

Allgemeiner Relationsbegriff

Sei $(U_i)_{i \in \mathbb{N}}$ eine Familie von Mengen. Eine *Relation* ist eine Teilmenge des Kreuzproduktes

$$R \subseteq \bigotimes_{i \in \mathbb{N}} U_i$$

Gilt $\forall_{i,j}\ U_i = U_j$, so ist die Relation *homogen*. Für endliche Mengen $U_1, ..., U_n$ spricht man von einer *n-ären Relation*, bspw. für $n = 3$ von einer *ternären* und für $n = 4$ von einer *quaternären Relation*. Die *universelle Relation* oder *Allrelation* ist gleich dem gesamten Kreuzprodukt:

$$\top := \bigotimes_{i=1}^{n} U_i$$

Die *leere Relation* ist gleich der leeren Menge:

$$\bot := \emptyset$$

Relationen als Mengen

Was oftmals verdrängt wird:

Relationen sind Mengen!!!

Alle Mengenoperationen ($\subseteq, \cup, \cap, \setminus, \times, \ldots$) können auch auf Relationen ausgeführt werden!

Bild- und Urbildmengen

Definition 1.2: (Bild und Urbild einer Relation)

Sei $R : X \to Y$ eine binäre Relation. Seien weiterhin $U \subseteq X$ und $V \subseteq Y$. Dann heißt

(i) $R(U) := \{y \in Y \mid \exists_{x \in U}\ xRy\}$ das *Bild von* U.

(ii) $R^{-1}(V) := \{x \in X \mid \exists_{y \in V}\ xRy\}$ das *Urbild von* V.

(iii) $R(X)$ *das Bild von* R.

(iv) $R^{-1}(Y)$ *das Urbild von* R.

Komposition

Definition 1.3: (Komposition)

Seien $R : X \to Y$ und $S : Y \to Z$ zwei Relationen. Dann heißt

$$P = R \fatsemi S : X \to Z$$

mit

$$P := \{(x, z) \in X \times Z \mid \exists_{y \in Y}\ xRy \ \wedge\ ySz\}$$

die *Komposition* von R und S.

Eigenschaften der Komposition

Satz 1.1:

Seien U, V, W, X Mengen. Es gilt:

(i) Die Komposition von Relationen ist assoziativ, d.h., für drei Relationen $R : U \to V,\ S : V \to W,\ T : W \to X$ gilt

$$(R \fatsemi S) \fatsemi T = R \fatsemi (S \fatsemi T)$$

(ii) aber im allgemeinen nicht kommutativ, d.h. (selbst im Falle $U = V = W$) kann gelten:

$$R \fatsemi S \neq S \fatsemi R$$

Identitätsrelation und Konverse

Definition 1.4: (Identitätsrelation)

Es seien $x, y \in \mathcal{U}$. Die Relation

$$\mathbb{1} := \{(x, y) \mid x = y\}$$

heißt *Identitätsrelation* auf $\mathcal{U}$: $x \mathbb{1} y \Leftrightarrow x = y$

Definition 1.5: (Konverse Relation)

Für eine Relation $R : U \to V$ heißt

$$R^{\smile} := \{(y, x) \in V \times U \mid (x, y) \in R\}$$

konverse Relation oder *Konverse von* R: $x R^{\smile} y \Leftrightarrow yRx$

Relationenoperationen

Definition 1.6: (Relationenoperationen)

Es seien P, Q, R Relationen auf $\mathcal{U}$. Dann sind definiert:

(i) $x(P \cup Q)y :\Leftrightarrow (x, y) \in P \cup Q \Leftrightarrow xPy \vee xQy$

(ii) $x(P \cap Q)y :\Leftrightarrow (x, y) \in P \cap Q \Leftrightarrow xPy \wedge xQy$

(iii) $x\overline{R}y :\Leftrightarrow \neg xRy$

Rechenregeln für Relationenoperationen

Satz 1.2: (Rechenregeln für Relationenoperationen)

Es seien P, Q, R Relationen auf $\mathcal{U}$. Dann gilt:

(i) $\mathbb{1} \fatsemi R = R = R \fatsemi \mathbb{1}$ (Neutralität von $\mathbb{1}$)

(ii) $\amalg \fatsemi R = \amalg = R \fatsemi \amalg$ (Annihilation durch $\amalg$)

(iii) $R^{\smile\smile} = R$ (Konverse ist involutiv)

(iv) $\overline{R^{\smile}} = \overline{R}^{\smile}$

(v) $(P \fatsemi Q)^{\smile} = Q^{\smile} \fatsemi P^{\smile}$ (Antidistributivität)

(vi) $P \fatsemi (Q \cup R) = (P \fatsemi Q) \cup (P \fatsemi R)$ (Distributivität von $\fatsemi$ unter $\cup$)

(vii) $P \fatsemi (Q \cap R) \subseteq (P \fatsemi Q) \cap (P \fatsemi R)$
(Subdistributivität von $\fatsemi$ unter $\cap$)

(viii) $P \subseteq Q \;\Rightarrow\; P \fatsemi R \subseteq Q \fatsemi R,\; R \fatsemi P \subseteq R \fatsemi Q$ (Isotonie)

(ix) $(P \cap Q)^{\smile} = P^{\smile} \cap Q^{\smile}$, $(P \cup Q)^{\smile} = P^{\smile} \cup Q^{\smile}$

Eigenschaften von Relationen

Definition 1.7: (FLIS-Eigenschaften von Relationen)

Seien A, B Menge und $R : A \to B$ eine Relation.

(i) R heißt *funktional*, falls $\forall_{x\in A}\, \forall_{y,z\in B}\; xRy \;\wedge\; xRz \;\Rightarrow\; y = z$.

(ii) R heißt *injektiv* oder *linkseindeutig*, falls
$\forall_{x_1,x_2\in A}\, \forall_{y\in B}\; x_1Ry \;\wedge\; x_2Ry \;\Rightarrow\; x_1 = x_2$.

(iii) Das *Bild* von R ist gegeben durch
$\mathrm{Bild}(R) = \mathrm{im}\; R := \{y \in B \mid \exists_{x\in A}\; xRy\}$.

(iv) R heißt *surjektiv* oder *rechtstotal*, falls
$\forall_{y\in B}\, \exists_{x\in A}\; xRy \;\Leftrightarrow\; \mathrm{im}\; R = \mathrm{cod}(R) = B$.

(v) Das *Urbild* von R ist gegeben durch
$\mathrm{Urbild}(R) = \mathrm{im}\; R^{\smile} := \{x \in A \mid \exists_{y\in B}\; xRy\}$.

(vi) R heißt *linkstotal*, falls
$\forall_{x\in A}\, \exists_{y\in B}\; xRy \;\Leftrightarrow\; \mathrm{im}\; R^{\smile} = \mathrm{dom}(R) = A$.

Eigenschaften von Relationen

Definition 1.7: (FLIS-Eigenschaften von Relationen, Forts.: Funktionen)

Seien A, B Menge und $R : A \to B$ eine Relation.

(vii) R heißt *Funktion* oder *Abbildung*, falls R linkstotal und funktional ist, also falls $\forall_{x \in A}\ \exists!_{y \in B}\ xRy$. Man schreibt dann $y = R(x)$ anstatt xRy.

(viii) Falls R eine Funktion ist, so heißt $D(R) := \mathrm{dom}(R)$ *Definitionsmenge* von R.

(ix) Falls R eine Funktion ist, so heißt $W(R) := \mathrm{im}\ R$ *Wertemenge* von R.

Injektive und surjektive Funktionen

Für Funktionen $f : X \to Y$ haben wir die Schreibweise $y = f(x)$ für $x \in X$ und $y \in Y$.

- Die Injektivität von f wird folgendermaßen ausgedrückt:

$$\forall_{x_1, x_2 \in X} \; f(x_1) = f(x_2) \;\Rightarrow\; x_1 = x_2$$

- Die Surjektivität von f wird folgendermaßen ausgedrückt:

$$\forall_{y \in Y} \; \exists_{x \in X} \; y = f(x)$$

- Eine Funktion heißt *bijektiv*, wenn sie injektiv und surjektiv ist (das gilt übrigens auch für Relationen!). Eine bijektive Funktion nennt man auch *Bijektion*.

Komposition von Funktionen, Umkehrabbildung

- Seien X, Y, Z Mengen sowie $f : X \to Y$ und $g : Y \to Z$ zwei Funktionen. Anstatt $f \fatsemi g : X \to Z$ schreibt man $g \circ f : X \to Z$ (Reihenfolge brachten!).
- Ist f bijektiv, so ist f auch *umkehrbar*, d.h., es gibt eine *Umkehrabbildung* $f^{-1} : Y \to X$ mit

$$\forall_{x \in X}\ (f^{-1} \circ f)(x) = x = id_X \ \wedge\ \forall_{y \in Y}\ (f \circ f^{-1})(y) = y$$

  Dabei ist $id_M : M \to M, id_M(x) = x, x \in M$, die *Identitätsabbildung* auf M.
- Sind f und g beide umkehrbar (bijektiv), so ist auch $g \circ f$ umkehrbar mit

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Eigenschaften von Endorelationen

Definition 1.8: (Eigenschaften von Endorelationen)

Sei U ein Universum und $R : U \to U$ eine Endorelation auf U.

(i) R heißt *reflexiv*, falls $\forall_{x \in U}\ xRx$.

(ii) R heißt *symmetrisch*, falls $\forall_{x,y \in U}\ xRy \Rightarrow yRx$.

(iii) R heißt *asymmetrisch*, falls $\forall_{x,y \in U}\ xRy \Rightarrow \neg yRx$.

(iv) R heißt *antisymmetrisch*, falls $\forall_{x,y \in U}\ xRy \wedge yRx \Rightarrow x = y$.

(v) R heißt *transitiv*, falls $\forall_{x,y,z \in U}\ xRy \wedge yRz \Rightarrow xRz$.

Partielle und totale Ordnung

Sei U ein Universum und $R : U \to U$ eine Endorelation auf U.

Definition 1.9: (Ordnungen)

(i) R heißt *partielle Ordnung* oder *Halbordnung*, falls sie
- reflexiv,
- antisymmetrisch und
- transitiv

ist.

(ii) R heißt *totale Ordnung*, falls sie eine partielle Ordnung ist, bei der zusätzlich die *Vergleichbarkeit* zweier Elemente aus U erfüllt ist, d.h. $\forall_{x,y \in U}\ xRy \ \vee \ yRx$.

(iii) R heißt *streng totale Ordnung*, falls R eine transitive Relation ist, bei der zusätzlich die *Trichotomie* erfüllt ist, d.h. $\forall_{x,y \in U}\ xRy \ \vee \ yRx \ \vee x = y$.

Äquivalenzrelationen

Sei U ein Universum und $R : U \to U$ eine Endorelation auf U.

Definition 1.10: (Äquivalenzrelation)

R heißt *Äquivalenzrelation*, falls sie

- reflexiv,
- symmetrisch und
- transitiv

ist.

Äquivalenzklassen

Definition 1.11: (Äquivalenzklasse)

Sei $R : U \to U$ eine Äquivalenzrelation. Die *Äquivalenzklasse* eines Elementes $x \in U$ ist gegeben durch

$$[x] := R(x) = \{y \in U \mid xRy\}$$

Satz 1.3:

Sei $\mathcal{I}$ eine Indexmenge. Die Äquivalenzklassen $A_i,\ i \in \mathcal{I}$, einer Relation $R : U \to U$ bilden eine *Partition* auf U; d.h.

(i) $\forall_{i \neq j}\ A_i \cap A_j = \emptyset$, d.h. A_i und A_j sind *paarweise disjunkt*.

(ii) $\bigcup_{i \in \mathcal{I}} A_i = U$

(Reflexiv-)Transitive Hülle

Definition 1.12: ((Reflexiv-)Transitive Hülle)

Sei $R : U \to U$ eine Relation. Dann heißt

$$\begin{aligned} R^+ &:= R \cup R \fatsemi R \cup R \fatsemi R \fatsemi R \cup \ldots \\ &= R^1 \cup R^2 \cup R^3 \cup \ldots \\ &= \bigcup_{i \in \mathbb{N}} R^i \end{aligned}$$

transitive Hülle von R.
$R^* := R^0 \cup R^+ := \mathbb{1} \cup R^+ = \bigcup_{i \in \mathbb{N}_0} R^i$ heißt *reflexiv-transitive Hülle* von R.

Satz 1.4:

Es gilt $\forall_{i \in \mathbb{N}_0} \ (R^i)^\smile = (R^\smile)^i$.

Teilbarkeitsrelation

Definition 1.13: (Teilbarkeitsrelation)

Die Relation $R : \mathbb{N}_0 \to \mathbb{N}_0$, gegeben durch

$$\begin{aligned} xRy \;:\Leftrightarrow\; x|y \quad &:\Leftrightarrow \quad x \text{ ist Teiler von } y \\ &\Leftrightarrow \quad \exists_{k\in\mathbb{N}_0}\, y = k \cdot x \end{aligned}$$

heißt *Teilbarkeitsrelation*. $x|y$ spricht man auch x *teilt* y. Falls x kein Teiler von y ist, schreibt man auch $x \nmid y$ und spricht dann auch x *teilt nicht* y.

Satz 1.5:

Die Teilbarkeitsrelation ist eine partielle Ordnung.

Restklassen

Satz 1.6:

Für $m \in \mathbb{N}$ ist die Relation

$$\equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}$$

gegeben durch

$$a \equiv_m b \;\Leftrightarrow\; m \mid a - b,\; a, b \in \mathbb{Z}$$

eine Äquivalenzrelation.

Restklassen und Repräsentanten

Definition 1.14: (Restklasse/Repräsentant)

Für $m \in \mathbb{N}$ und $r \in \mathbb{N}_0, 0 \leq r < m$, heißt

$$r + m\mathbb{Z} := \{r + mx \mid x \in \mathbb{Z}\}$$

Restklasse modulo m. Ein Element einer Restklasse heißt *Repräsentant*.
Äquivalente Schreibweisen: $a, b \in r + m\mathbb{Z}, a \equiv b \bmod m, a \equiv b(m)$

Korollar 1.1:

Für $a, m, q \in \mathbb{N}, r \in \mathbb{N}_0$, gilt:

$$a = m \cdot q + r \;\Rightarrow\; -a = m \cdot (-(q+1)) + (m - r)$$

Modulo-Rechnung

Satz 1.7: (Rechenregeln der Modulo-Rechnung)

Für $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$ gelten die folgenden Rechenregeln:

(i) $-(b \bmod m) \equiv_m -b \bmod m$

(ii) $(a + b) \bmod m \equiv_m (a \bmod m + b \bmod m) \bmod m$

(iii) $(a - b) \bmod m \equiv_m (a \bmod m - b \bmod m) \bmod m$

(iv) $(a \cdot b) \bmod m \equiv_m (a \bmod m \cdot b \bmod m) \bmod m$

(v) $a^b \bmod m \equiv_m (a \bmod m)^b \bmod m$

Es gibt keine Aussage zur Division!

Also sind modulo-Addition und modulo-Multiplikation unabhängig vom Repräsentanten. Daher wird $\equiv_m$ auch *Kongruenzrelation* genannt (also verträglich mit Addition und Multiplikation).

Rechenstruktur der Restklassen

Addition:

$$[a]_{\equiv_m} \oplus [b]_{\equiv_m} = [a+b]_{\equiv_m} \Leftrightarrow (a+m\mathbb{Z}) \oplus (b+m\mathbb{Z}) = (a+b)+m\mathbb{Z}$$

Multiplikation:

$$[a]_{\equiv_m} \otimes [b]_{\equiv_m} = [a \cdot b]_{\equiv_m} \Leftrightarrow (a+m\mathbb{Z}) \otimes (b+m\mathbb{Z}) = (a \cdot b)+m\mathbb{Z}$$

Dies definiert eine neue Rechenstruktur $(\mathbb{Z}/m\mathbb{Z}, \oplus, \otimes)$:

$$\mathbb{Z}/m\mathbb{Z} := \{m\mathbb{Z}, 1+m\mathbb{Z}, ..., (m-1)+m\mathbb{Z}\}$$

Schreibe $[a]_{\equiv_m} = [a]_m$

Primzahlen

Definition 1.15: (Primzahl)

(i) $p \in \mathbb{N}$ heißt *Primzahl*, wenn sie genau zwei verschiedene Teiler besitzt, nämtlich 1 und sich selbst. Die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet.

(ii) $q \in \mathbb{N}$ heißt *zusammengesetzt*, falls $q \in \mathbb{N} \backslash \mathbb{P}$.

Korollar 1.2:

1 ist keine Primzahl. Die einzige gerade Primzahl ist 2.

Fermat-Zahlen

Die Zahlen

$$F_n = 2^{2^n} + 1, \ n \in \mathbb{N},$$

heißen *Fermat-Zahlen*. F_1 bis F_4 sind Primzahlen, F_5 nicht. Mithilfe der modulo-Rechnung kann man beweisen:

$$641 \mid F_5$$

Anwendung in der Geometrie: Nach Gauß kann ein regelmäßiges Polygon mit n Seiten nur dann mit Zirkel und Lineal konstruiert werden, wenn

$$n = 2^k \ \vee \ n = 2^k \cdot \prod_{i \in I} F_i, \ k \in \mathbb{N}_0, \ I \subseteq N$$

Ein Siebzehneck ist damit mit Zirkel und Lineal konstruierbar, denn es gilt $17 = F_2 = 2^0 \cdot F_2$.

Mersenne-Primzahlen

Falls $p \in \mathbb{P}$ und $2^p - 1 \in \mathbb{P}$, dann heißt $2^p - 1$ *Mersenne-Primzahl*.
Bis zum frühen Mittelalter glaubte man:

$$p \in \mathbb{P} \Rightarrow 2^p - 1 \in \mathbb{P}$$

- Erstes Gegenbeispiel: $p = 11$: $2^{11} - 1 = 2047 = 23 \cdot 89$
- Nach Fermat: $p = 23, p = 37$
- Nach Euler: $p = 29$

Größte Primzahl, die 2016 entdeckt wurde:
$2^{74\,207\,281} - 1$ ($\approx$ 22 Mio. Stellen)
21. Oktober 2024: $2^{136\,279\,841} - 1$ ($\approx$ 41 Mio. Stellen)

Weitere Darstellungsmöglichkeiten von Primzahlen

- Es gibt unendlich viele Primzahlen der Form $a^2 + b^4, \ a, b \in \mathbb{P}$.
- Vor kurzem bewiesen: Es gibt unendlich viele Primzahlen der Form $a^2 + 4b^2, \ a, b \in \mathbb{P}$.

Größter gemeinsamer Teiler

Definition 1.16: (Größter gemeinsamer Teiler)

(i) Seien $a, b \in \mathbb{Z}, a \neq 0 \ \vee \ b \neq 0$. Dann heißt $t \in \mathbb{N}$ *größter gemeinsamer Teiler (ggT)* von a und b, falls

$$t \mid a \ \wedge \ t \mid b \ \wedge \ \forall_{t' \in \mathbb{N}} \ t' \mid a \ \wedge \ t' \mid b \ \Rightarrow \ t' \mid t$$

Schreibweise: $\mathrm{ggT}(a, b), (a, b)$, Festlegung: $\mathrm{ggT}(0, 0) := 0$

(ii) Falls $\mathrm{ggT}(a, b) = 1$, so heißen a und b *teilerfremd* oder *relativ prim*.

Eigenschaften des ggT

Korollar 1.3: (Eindeutigkeit des ggT)

Der größte gemeinsame Teiler ist eindeutig bestimmt.

Korollar 1.4:

Seien $a \in \mathbb{Z}, b, c \in \mathbb{N}$ mit $\mathrm{ggT}(a, b) = 1$ und $c \mid b$. Dann gilt auch $\mathrm{ggT}(a, c) = 1$.

Euklidischer Algorithmus

Zur Bestimmung des ggT zweier ganzer Zahlen a und b wird der Euklidische Algorithmus verwendet (Beispiele an der Tafel und in den Übungen).
Dieser terminiert nach endlich vielen Schritten.

Das Lemma von Bézout

Satz 1.8 (Lemma von Bézout)

Seien $a, b \in \mathbb{Z}$. Dann gilt:

(i) $\exists_{x,y \in \mathbb{Z}}\ ax + by = \mathrm{ggT}(a, b)$

(ii) $\mathrm{ggT}(a, b) = 1 \ \Rightarrow\ \exists_{x,y \in \mathbb{Z}}\ ax + by = 1$

Erweiterter Euklidischer Algorithmus

Die Koeffizienten $x, y \in \mathbb{Z}$ erhält man mit dem sog. *erweiterten euklidischen Algorithmus* (Beispiele: Tafel und Übungen).
Der ggT zweier Zahlen ist stets eine ganzzahlige Linearkombination aus den beiden Zahlen:

$$\exists_{x,y \in \mathbb{Z}} \ \mathrm{ggT}(a, m) = ax + my$$

Im Spezialfall $\mathrm{ggT}(a, m) = 1$ gilt:

$$\begin{aligned} \exists_{x,y \in \mathbb{Z}} \ & 1 = ax + my \\ \Leftrightarrow \ & 1 \equiv ax \bmod m \\ \Leftrightarrow \ & x \equiv a^{-1} \bmod m \end{aligned}$$

In diesem Fall existiert also das modulare Inverse $a^{-1} \bmod m$.

Eigenschaften von Primzahlen

Satz 1.9: (Teiler von Primzahlen)

Für jede Zahl $a \in \mathbb{N}, a \geq 2$, gilt, daß der kleinste Teiler $p \geq 2$ eine Primzahl ist.

Satz 1.10:

Es gibt unendlich viele Primzahlen.

Der Fundamentalsatz der Zahlentheorie

Satz 1.11: (Fundamentalsatz der Zahlentheorie)

Jede natürliche Zahl $a \geq 2$ hat eine sog. *Faktorisierung* oder *Primzahlzerlegung*

$$a = \prod_{i=1}^{r} q_i, \ r \in \mathbb{N}, \ q_i \in \mathbb{P}, \ i = 1, ..., r.$$

Diese Darstellung ist bist auf die Reihenfolge der q_i eindeutig. Die Primzahlen q_i können auch mehrfach in der Zerlegung vorkommen.

Überblick I

Gruppentheorie

- Abstraktion von Rechenstrukturen (bekannt: Addition, Subtraktion, Multiplikation und Division von natürlichen, ganzen, rationalen und reellen Zahlen)
- Statt $+, -, \cdot, /$ schreiben wir allgemein $*$, und die sog. *Trägermenge* M der Rechenstruktur kann beliebig sein
- Allgemeine Verknüpfung: $* : M \times M \to M,\ (a, b) \mapsto a * b$, Rechenstruktur/algebraische Struktur $\mathcal{A} := (M, *)$
- Es wird nicht mehr zwischen $a \in M$ und $a \in \mathcal{A}$ unterschieden

Gruppe

Algebraische Struktur mit einer Verknüpfung $*$, die bzgl. $*$ ein Einselement e besitzt und bei der jedes Element a ein Inverses a^{-1} besitzt, so daß $a * a^{-1} = a^{-1} * a = e$

Verknüpfungstafeln

- Addition und Multiplikation von Bits:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- Modulo 5:

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

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Verknüpfungstafeln

- Mengen:

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a, b\}$	$\{a, b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\{b\}$	$\{a, b\}$
{a,b}	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a, b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$

Anwendungen der Gruppentheorie

- **Informatik:**
  - Modulo-Rechnung: $m = 2$ bis $m = 2^{2^{12}}$
  - Mengenoperationen: Datenbanksystem muß Mengen vereinigen/schneiden können, um Benutzerfragen zu beantworten
  - Theorie wichtig für Körper und Ringe (Kryptologie/Kodierungstheorie)
- **Chemie:** Symmetriegruppen: Drehungen und Spiegelungen von Atomen innerhalb eines Moleküls um Symmetrieebenen (dadurch Klassifizierung von Substanzen, besonders in der Kristallographie)

Lernziele

- Kennen der Definitionen von Halbgruppen, Gruppen und Elementordnung, inkl. Beispiele
- Bestimmung von Eigenschaften gegebener Rechenstrukturen
- Bestimmung von von Elementen erzeugten Untergruppen

Wichtige Begriffe: Algebraische Strukturen

Eine *algebraische Struktur* $\mathcal{A}(M, *)$ besteht aus einer *Trägermenge* M und einer *Verknüpfung* $* : M \times M \to M$.
Grundsätzlich muß $\mathcal{A}(M, *)$ *algebraisch abgeschlossen* sein, d.h.

$$\forall_{a,b \in M} \; a * b \in M$$

Dann ist die Verknüpfung $*$ *wohldefiniert* (auch: *total definiert*).

Wichtige Begriffe: Algebraische Strukturen

Definition 2.1:

Sei $\mathcal{A}(M, *)$ algebraisch abgeschlossen.

(i) $\mathcal{A}$ heißt *assoziativ*, wenn $\forall_{a,b,c \in \mathcal{A}} \ (a * b) * c = a * (b * c)$

(ii) $e \in \mathcal{A}$ heißt *Einselement* oder *neutrales Element* von $\mathcal{A}$, wenn $\forall_{a \in \mathcal{A}} \ a * e = e * a = a$

(iii) Hat $\mathcal{A}$ ein Einselement e, und falls $\forall_{a \in \mathcal{A}} \ \exists_{b \in \mathcal{A}} \ a * b = b * a = e$, dann heißt b *invers* oder *Inverses* zu a. Bez.: a^{-1}. Falls $a^{-1} = a$, dann heißt a *selbstinvers* oder *Involution*.

(iv) $\mathcal{A}$ heißt *kommutativ*, wenn $\forall_{a,b \in \mathcal{A}} \ a * b = b * a$

Halbgruppen und Monoide

Definition 2.2: (Halbgruppen und Monoide)

(i) Eine algebraische Struktur $\mathcal{G} = (M, *)$ heißt *Halbgruppe*, falls sie assoziativ ist.
Hat sie zusätzlich auch ein Einselement, so heißt sie *Monoid*.
Falls sie kommutativ ist, so heißt sie *abelsch*.

Gruppen

Definition 2.2 (Forts.): (Gruppen)

(ii) Ein Monoid $\mathcal{G} = (M, *)$ heißt *Gruppe*, falls zu jedem Element $g \in \mathcal{G}$ ein Inverses $g^{-1} \in \mathcal{G}$ existiert.

(iii) Falls $\mathcal{U} \subseteq M$ zusammen mit der Verknpfung $*$ eine Halbgruppe, ein Monoid oder eine Gruppe bildet, so heißt $\mathcal{G}_\mathcal{U} := (\mathcal{U}, *)$ *Unterhalbgruppe*, *Untermonoid* oder *Untergruppe* von $\mathcal{G}$. Falls $\mathcal{G}_\mathcal{U}$ Untergruppe von $\mathcal{G}$ ist, so schreibt man $\mathcal{G}_\mathcal{U} \trianglelefteq \mathcal{G}$, falls sogar $\mathcal{G}_\mathcal{U} \neq G$: $\mathcal{G}_\mathcal{U} \triangleleft \mathcal{G}$.

(Element-)ordnungen

Definition 2.2 (Forts.): (Gruppen)

(iv) Ist $\mathcal{G}$ endlich, dann heißt $ord_{\mathcal{G}} := |\mathcal{G}|$ die *Ordnung* von $\mathcal{G}$.

(v) Es seien $a \in \mathcal{G}$ und e das Einselement von $\mathcal{G}$. Dann heißt $ord_{\mathcal{G}}(a) := \min\{k \in \mathbb{N} \mid a^k = e\}$ die *Ordnung* von a in $\mathcal{G}$, auch *Elementordnung* genannt. Existiert dieses Minimum nicht, so sagt man, daß a von *unendlicher Ordnung* ist.

Eigenschaften von Gruppen

Satz 2.1:

Sei $\mathcal{G} = (M, *)$ eine Gruppe mit Einselement e. Seien $a, b, c \in \mathcal{G}$. Dann gilt:

(i) e ist eindeutig.

(ii) Zu a ist a^{-1} eindeutig.

(iii) $(a^{-1})^{-1} = a$

(iv) Kürzungsregeln: $a * c = b * c \Rightarrow a = b$,
$c * a = c * b \Rightarrow a = b$

(v) $(a * b)^{-1} = b^{-1} * a^{-1}$

(vi) Die Gleichungen $a * x = b$ und $x * a = b$ mit Unbekannter x sind eindeutig lösbar.

(vii) a selbstinvers $\Leftrightarrow ord_{\mathcal{G}}(a) = 2$

Direktes Produkt von Gruppen

Definition 2.3: (Direktes Produkt von Gruppen)

Seien $\mathcal{G}_i = (M_i, *_i), 1 \leq i \leq n, n \in \mathbb{N}$, Gruppen. Dann heißt

$$\mathcal{G} := \mathcal{G}_1 \times ... \times \mathcal{G}_n = \bigotimes_{i=1}^{n} \mathcal{G}_i = (M_1 \times ... \times M_n, *) = \left(\bigotimes_{i=1}^{n} M_i, * \right)$$

mit $x * y := (x_1 *_1 y_1, ..., x_n *_n y_n)$ für $x = (x_1, ..., x_n) \in \mathcal{G}$ und $y = (y_1, ..., y_n) \in \mathcal{G}$ *direktes Produkt* der Gruppen $\mathcal{G}_1, ..., \mathcal{G}_n$.

Korollar 2.1:

Das direkte Produkt ist tatsächlich wieder eine Gruppe.

Untergruppen

Korollar 2.2:

Falls $\mathcal{G}$ eine Gruppe ist, so sind $\{e\}$ und $\mathcal{G}$ selbst triviale Untergruppen.

Satz 2.2:

Sei $\mathcal{G} = (M, *)$ eine Gruppe. Dann gilt:

(i) $U \subseteq M$ und $\mathcal{G}_\mathcal{U}$ Untergruppe $\Leftrightarrow \forall_{a,b \in \mathcal{G}_\mathcal{U}}\ a^{-1} * b \in \mathcal{G}_\mathcal{U}$

(ii) $U \subseteq M$ und $\mathcal{G}_\mathcal{U}$ Untergruppe $\Leftrightarrow \forall_{a,b \in \mathcal{G}_\mathcal{U}}\ a * b^{-1} \in \mathcal{G}_\mathcal{U}$

(iii) Für $a \in \mathcal{G}$ und $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$ ist $\langle a \rangle$ eine Untergruppe.

(iv) Für $a \in \mathcal{G}$ ist $ord_\mathcal{G}(a) = ord_{\langle a \rangle}$

Zyklische (Unter-)Gruppen

Definition 2.4: (Zyklische (Unter-)Gruppen)

Sei $\mathcal{G}$ eine Gruppe und $a \in \mathcal{G}$.

(i) $\langle a \rangle$ heißt die von a erzeugte *zyklische Untergruppe* von $\mathcal{G}$.

(ii) Falls $\langle a \rangle = \mathcal{G}$, dann heißt $\mathcal{G}$ *zyklisch*, und a *Generator* (oder *primitives Element*) von $\mathcal{G}$.

Korollar 2.3:

Jede zyklische Gruppe ist abelsch.

Ringe

Wir betrachten ab jetzt zwei Operationen $+$ und $\cdot$ für dieselbe Trägermenge M. Sei 0 das Einselement bzgl. $+$ und 1 das Einselement bzgl. $\cdot$.

Definition 2.5: (Ring)

Eine algebraische Struktur $R = (M, +, \cdot)$ heißt *Ring*, falls

1. $(M, +)$ eine abelsche Gruppe ist,
2. die Verknüpfung $\cdot$ assoziativ ist
3. ein Einselement bzgl. $\cdot$ existiert und
4. das Distributivgesetz für erfüllt ist:

$$\forall_{a,b,c \in R}\ a \cdot (b + c) = a \cdot b + a \cdot c$$

Falls die Verknüpfung $\cdot$ zusätzlich kommutativ ist, so spricht man von einem *kommutativen Ring*.

Körper

Definition 2.6: (Körper)

Eine algebraische Struktur $K = (M, +, \cdot)$ heißt *Körper*, falls

1. $(K, +, \cdot)$ ein kommutativer Ring ist und
2. jedes $x \in K \backslash \{0\}$ ein multiplikatives Inverses hat.

In Körpern sind alle bekannten Rechenregeln erlaubt.

Korollar 2.4 (Drejmol Null es Null bliev Null):

Sei R ein Ring oder auch ein Körper. Dann gilt:
$\forall_{a \in R}\ a \cdot 0 = 0 \cdot a = 0$

Ring der Matrizen

Sei $\mathcal{M}$ die Menge der Matrizen, $+$ die Matrixaddition und $\cdot$ die Matrixmultiplikation.

1. Die Matrixaddition ist assoziativ und kommutativ, da die Addition in $\mathbb{R}$ assoziativ und kommutativ ist. Das Einselement ist die Nullmatrix, und jede Matrix A hat ein additives Inverses, nämlich $-A$. $(\mathcal{M}, +)$ ist abelsche Gruppe.
2. In der Linearen Algebra beweist man, daß die Matrixmultiplikation assoziativ ist.
3. Das Einselement bzgl. $\cdot$ ist die Einheitsmatrix.
4. Ebenfalls beweist man in der Linearen Algebra, daß das Distributivgesetz erfüllt ist.
5. Nicht jede Matrix hat ein multiplikatives Inverses, und die Matrixmultiplikation ist i.A. auch nicht kommutativ.

$(\mathcal{M}, +, \cdot)$ bildet somit einen Ring, aber keinen Körper!

Ring der Polynome

Sei $\mathbb{R}[x]$ die Menge aller Polynome mit reellen Koeffizienten. Jedes Polynom ist eine Abbildung von $\mathbb{R} \to \mathbb{R}$, also $x \in \mathbb{R}$. Sei $+$ die Polynomaddition, die einfach die Koeffizienten addiert, und $\cdot$ die Polynommultiplikation.

1. Die Polynomaddition ist assoziativ und kommutativ, da die Addition in $\mathbb{R}$ assoziativ und kommutativ ist. Das Einselement bzgl. $+$ ist die konstante Nullfunktion, also das Nullpolynom. Jedes Polynom P hat ein additives Inverses, nämlich $-P$. $(\mathbb{R}[x], +)$ ist abelsche Gruppe.
2. Die Polynommultiplikation ist assoziativ und kommutativ, da die Multiplikation in $\mathbb{R}$ assoziativ und kommutativ ist.
3. Das Einselement bzgl. $\cdot$ ist die konstante Einsfunktion, also das Einspolynom.
4. Nur konstante Polynome $\neq 0$ haben multiplikative Inverse.

$(\mathbb{R}[x], +, \cdot)$ bildet somit einen komm. Ring, aber keinen Körper!

Einheiten

Definition 2.7: (Invertierbare Elemente/Einheiten)

Sei R ein Ring. Falls $a \in R$ ein multiplikatives Inverses besitzt, heißt a *invertierbar* oder *Einheit*. R^* ist die Menge aller Einheiten von R.

Satz 2.3:

R^* bildet mit $\cdot$ eine Gruppe, die sog. *Einheitengruppe* von R.

Korollar 2.5:

Sei R ein Ring mit Einselement und $|R| \geq 2$. Dann gilt $0 \notin R^*$

Nullteiler und Integritätsbereiche

Definition 2.8: (Nullteiler und Integritätsbereiche)

(i) Sei R ein Ring, $a \in R$ mit $a \neq 0$. Falls $\exists_{b \in R} a \cdot b = 0$, dann heißt a *Nullteiler* in R. Einthält R keine Nullteiler, so heißt R *nullteilerfrei*.

(ii) Ein kommutativer nullteilerfreier Ring mit Einselement heißt *Integritätsbereich I*.

Korollar 2.6:

$\mathbb{Z}$ ist nullteilerfrei.

Satz 2.4:

In Integritätsbereichen gilt die Kürzungsregel.

Nullteiler und Einheiten in endlichen Ringen

Satz 2.5:

Sei R ein endlicher Ring mit Einselement, $a \in R$ mit $a \neq 0$. Dann gilt:

(i) a invertierbar $\Rightarrow$ a kein Nullteiler

(ii) a Nullteiler $\Rightarrow$ a nicht invertierbar

(iii) a kein Nullteiler $\Rightarrow$ a invertierbar

(iv) a nicht invertierbar $\Rightarrow$ a Nullteiler

(v) a Nullteiler $\oplus$ a invertierbar

Eigenschaften von Körpern

Korollar 2.7:

Sei K ein Körper. dann gilt:

(i) $K^* = K \backslash \{0\}$

(ii) K ist nullteilerfrei

(iii) K ist Integritätsbereich

Satz 2.6:

Sei I ein endlicher Integritätsbereich. Dann ist I ein Körper.

Multiplikative Restklassengruppe modulo m

Definition 2.9: (multiplikative Restklassengruppe)

Z_m^* heißt *multiplikative Restklassengruppe modulo m*.

Satz 2.7:

Es gilt $a \in \mathbb{Z}_m^* \Leftrightarrow \operatorname{ggT}(a, m) = 1$

Korollar 2.8:

(i) $p \in \mathbb{P} \Leftrightarrow \mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$

(ii) $p \in \mathbb{P} \Leftrightarrow \mathbb{Z}_p$ Integritätsbereich

(iii) $p \in \mathbb{P} \Leftrightarrow \mathbb{Z}_p$ Körper

(iv) $p \in \mathbb{P} \Leftrightarrow$ in $\mathbb{Z}_p^*$ sind nur 1 und $p-1$ selbstinvers

Teil II: Lineare Algebra

- eines der wichtigsten Teilgebiete der Mathematik
- Entwicklung als eigenständiges Teilgebiet erst ab dem 11. Jahrhundert
- **Begründer:** Gottfried-Wilhelm Leibniz (1646–1716), Seki Takakazu (1642–1708)
- Begriff des **Vektors** erst im 19. Jahrhundert durch William Rowan Hamilton (1805–1865) eingeführt
- Begriff der **Matrix** erst seit dem 20. Jahrhundert bekannt
- **Lineare Algebra:** Grundlage vieler anwendungsbezogener Fragestellung, insbesondere in den Bereichen Numerik, Physik und Informatik
- Wichtige Anwendung von Methoden der Linearen Algebra in der **Kodierungstheorie**

Lineare Algebra in der Kodierungstheorie

(n, k)-Linearcodes

besitzen **Basisvektoren**, aus denen jedes Codewort als **Linearkombination** generiert werden kann (Zeilenvektoren einer **Generatormatrix**)

Wie funktioniert Fehlererkennung?

Ein Codewort aus einem n-dimensionalen Körper K^n wird mithilfe einer **Kontrollmatrix** H^T in einen $n-k$-dimensionalen orthogonalen **Unterraum** projiziert. Dort können sog. *Syndrome* festgestellt werden, d.h. es wird automatisch erkannt, ob ein Codewort fehlerhaft übertragen wurde oder nicht.

Was brauchen wir?

- **Vektoren** bzw. den Begriff des **Vektorraums**
- **Basis** eines Vektorraums und **Linearkombinationen**
- den Begriff der **Matrix** und Rechnen mit **Matrizen**
- **Unterräume** als orthogonale Teilräume von Vektorräumen und den Begriff der **Projektion**

Außerdem relevant:

- **Lineare (Un-)abhängigkeit** von Vektoren
- **Rang**, **Kern** und **Determinante** einer Matrix
- **Invertierbarkeit** von Matrizen, Bestimmung einer **inversen Matrix**
- Lösbarkeit und Lösung **linearer Gleichungssysteme**
- **Basiswechsel** und **Koordinatentransformation**
- **Diagonalisierung** von Matrizen
- **Eigenwerte** und **Eigenvektoren** von Matrizen

Lernziele

- Kennen, Erläuterung und sicherer Umgang mit sämtlichen auf den vorherigen Folien erwähnten Begriffen
- Vektor- und Matrizenrechnung beherrschen
- Bestimmung von Inversen, Determinanten, Eigenwerten und Eigenvektoren von Matrizen
- Lösung linearer Gleichungssysteme
- Kennen der Bedeutung der Linearen Algebra für die Kodierungstheorie und Anwendung der dafür relevanten Begriffe und Verfahren

Überblick I

Überblick II

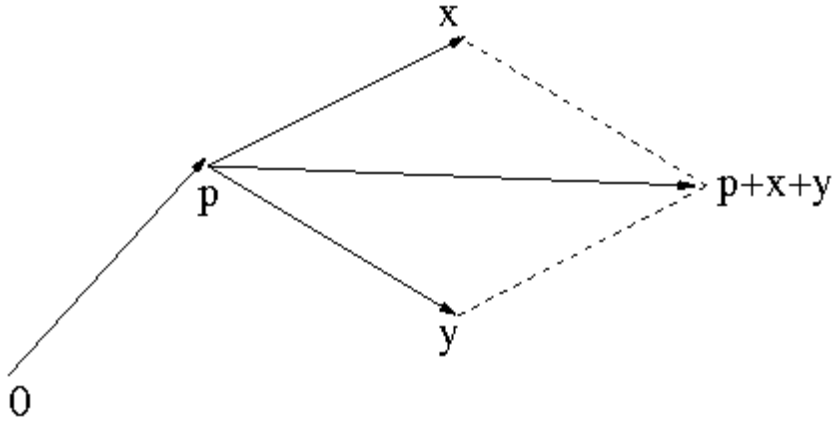
Überblick I

Überblick II

Vektorräume und Unterräume

Vektoren

Ein *Vektor* hat ursprünglich eine geometrische Bedeutung. Man betrachte einen festen Punkt p in der Ebene als *Anfangspunkt* und eine von p ausgehende Strecke zu einem anderen Punkt x (sog. *Richtung* von p nach x). Ein *Ortsvektor* zeigt vom Nullpunkt des Koordinatensystems zu einem Punkt x.



Vektorraum

Definition 3.1: (Vektorraum)

Sei K ein Körper. Ein *K-Vektorraum* ist eine Menge V mit einer *inneren Verknüpfung (Addition)*

$$V \times V \to V,\ (a, b) \mapsto a + b$$

und einer *äußeren Verknüpfung (skalare Multiplikation)*

$$K \times V \to V,\ (\alpha, a) \mapsto \alpha \cdot a,$$

wobei

(i) $(V, +)$ abelsche Gruppe

(ii) $\forall_{\alpha,\beta \in K, a,b \in V}\ (\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a \wedge$
$\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$, d.h. sowohl Addition als auch skalare Multiplikation sind distributiv.

Vektorraum

Definition 3.1: (Vektorraum, Forts.)

(iii) $\forall_{\alpha,\beta\in K, a\in V}\ (\alpha \cdot \beta) \cdot a = \alpha \cdot (\beta \cdot a)$ (Assoziativität der skalaren Multiplikation)

(iv) $\forall_{a\in V}\ 1 \cdot a = a$, wobei $1 \in K$ das multiplikative Einselement von K ist

Wichtigster Vektorraum in dieser Vorlesung: $\mathbb{R}^n$

Unterraum

Definition 3.2: (Unterraum)

Seien K ein Körper und V ein K-Vektorraum. Eine Teilmenge $U \subseteq V$, heißt *K-Unterraum* oder *K-Untervektorraum* von V, falls

(i) $U \neq \emptyset$

(ii) $a, b \in U \Rightarrow a + b \in U$

(iii) $\alpha \in K, a \in U \Rightarrow \alpha \cdot a \in U$ Besteht U nur aus dem Nullvektor, so heißt U *Nullraum*.

Korollar 3.1: (Unterraumkriterium)

Die beiden letzten Eigenschaften lassen sich wie folgt zusammen fassen:

$$a, b \in U, \alpha, \beta \in K \Rightarrow \alpha \cdot a + \beta \cdot b \in U$$

Schnitt und Vereinigung von Unterräumen

Lemma 3.1:

Seien K ein Körper und V ein K-Vektorraum. Seien $(U_i)_{i \in I}$, I Indexmenge, eine Familie von Unterräumen von V. Dann ist auch der Schnitt $\bigcap_{i \in I} U_i$ wieder ein Unterraum.

Für die Vereinigung gilt das i.A. nicht: Bspw. bilden die Menge der Vektoren aus dem $\mathbb{R}^2$, die auf der x-Achse liegen, einen Unterraum des $\mathbb{R}^2$. Gleiches gilt für die y-Achse. Die Vereinigung ist die Menge aller Vektoren, die auf dem Koordinatenkreuz liegen. Allerdings liegt bspw. der Vektor

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

nicht auf dem Koordinatenkreuz.

Linearkombination und Spann

Definition 3.3: (Linearkombination und Spann)

Sei V ein K-Vektorraum. Sei weiterhin $A \subseteq V$.

(i) Für $r \in \mathbb{N}_0$, $a_i \in A, i = 1, ..., r$, $\alpha_i \in K, i = 1, ..., r$, heißt

$$\sum_{i=1}^{r} \alpha_i a_i$$

Linearkombination der Vektoren $a_1, ..., a_r$.

(ii) Sei $A = \{a_1, ..., a_r\}$. Die Menge $\mathrm{Span}_K\{a_1, ..., a_r\}$

$$:= \left\{ \sum_{i=1}^{r} \alpha_i a_i \;\middle|\; r \in \mathbb{N}, a_i \in A, \alpha_i \in K, i = 1, ..., r \right\}$$

heißt *Spann von A*.

Spann als kleinster Unterraum

Satz 3.1:

$\mathrm{Span}_K\{a_1, ..., a_r\}$ ist ein Unterraum, der sog. *von A erzeugte lineare Unterraum*. Es ist sogar der kleinste lineare Unterraum von V, der A enthält, genauer:

$$\mathrm{Span}_K\{a_1, ..., a_r\} \subseteq \bigcap_{U \in \mathcal{U}} U,$$

wobei $\mathcal{U}$ die Familie aller Unterräume $U \subseteq V$ ist mit $A \subseteq U$.

Lineare (Un-)Abhängigkeit

Definition 3.4: (Lineare (Un-)Abhängigkeit)

Die Vektoren $a_1, ..., a_n, n \in \mathbb{N}$, eines K-Untervektorraums V heißen *linear unabhängig (l.u.)*, falls für $\alpha_1, ..., \alpha_n \in K$ gilt:

$$\sum_{i=1}^{n} \alpha_i a_i = 0 \Rightarrow \alpha_1 = ... = \alpha_n = 0$$

Ansonsten heißen sie *linear abhängig (l.a.)*.

Lineare (Un-)Abhängigkeit

Satz 3.2:

Die Vektoren $a_1, ..., a_n$ eines K-Vektorraums V sind genau dann l.u., wenn in der Linearkombination $a = \sum_{i=1}^{n} \alpha_i a_i \in V$ für $a \in \mathrm{Span}_K\{a_1, ..., a_n\}$ die Koeffizienten $\alpha_1, ..., \alpha_n \in K$ eindeutig sind.

Die Vektoren $a_1, ..., a_n$ sind genau dann linear abhängig, wenn es mindestens einen Vektor von ihnen gibt, der sich als Linearkombination aus den anderen darstellen läßt.

Erzeugendensystem

Definition 3.5: (Erzeugendensystem)

Eine Menge A von Vektoren eines K-Vektorraums V heißen *Erzeugendensystem* von V, falls $V = \mathrm{Span}_K(A)$. V heißt *endlich erzeugt*, wenn V ein endliches EZS $\{a_1, ..., a_n\}, n \in \mathbb{N}$, besitzt.

Definition 3.6: (Einheitsvektoren)

Seien $V = K^n$ (K Körper), $1 \in K$ das Einselement von K bzgl. $\cdot$ und $0 \in K$ das Einselement bzgl. $+$. Dann heißt

$$e_i = (0 \cdots 0\ 1\ 0 \cdots 0) \in K^n,$$

wobei 1 an der i-ten Position steht, der *i-te Einheitsvektor* von K^n.

Einheitsvektoren sind stets linear unabhängig und Bilden ein EZS des Vektorraums K^n.

Basis

Definition 3.7: (Basis)

Die Vektoren $a_1, ..., a_n, n \in \mathbb{N}, \in V$ heißen *Basis* von V, falls

(i) $a_1, ..., a_n$ EZS von V

(ii) $a_1, ..., a_n$ l.u.

Satz 3.3:

Jeder endlich erzeugte K-Vektorraum hat eine Basis. Jede solche Basis ist endlich.

Dimension

Definition 3.8: (Dimension)

Sei V ein K-Vektorraum mit Basis $a_1, ..., a_n, n \in \mathbb{N}$. Dann heißt $n := \dim_K V$ die *Dimension* von V.

Satz 3.4: (Basisergänzungssatz)

Seien V ein K-Vektorraum, $a_1, ..., a_r \in V$ ein linear unabhängiges System und $b_1, ..., b_m \in V$ ein EZS ($r, m \in \mathbb{N}$). Dann läßt sich das System der $a_i, i = 1, ..., r$, durch Elemente der $b_j, j = 1, ..., m$, zu einer Basis von V ergänzen.

Korollar 3.1:

In einem K-Vektorraum gilt $\dim_K V = n$ genau dann, wenn es ein l.u. System von V von n Vektoren gibt, wobei jeweils $n + 1$ Vektoren l.a. sind.

Der Austauschsatz von Steinitz

Satz 3.5: (Austauschsatz von Steinitz)

Sei $\{b_1, ..., b_n\}$ eine Basis des K-Vektorraums V, und sei $\{a_1, ..., a_r\}$ eine linear unabhängige Teilmenge von V $(r, n \in \mathbb{N})$. Dann ist $r \leq n$, und es lassen sich r-viele Vektoren der $b_i, i = 1, ..., n$, durch die $a_j, j = 1, ..., r$, ersetzen, so daß die resultierende Menge eine Basis von V ist.

Wegen $r \leq n$ kann es höchstens so viele lineare unabhängige Vektoren wie die Anzahl an Basisvektoren geben.

Basistransformation

Man kann Vektoren als Linearkombination aus Vektoren beliebiger Basen darstellen und erhält dadurch ein neues Koordinatensystem. Einen derartigen *Basiswechsel* erhält man über eine sog. *Basistransformation*.

Lineare Abbildungen

Definition 3.9: (Lineare Abbildung)

Eine Abbildung $f : V \to V'$ zwischen zwei K-Vektorräumen V und V' heißt *K-Homomorphismus* oder *K-lineare Abbildung*, falls für $a, b \in V$, $\alpha \in K$ gilt:

(i) $f(a + b) = f(a) + f(b)$

(ii) $f(\alpha \cdot a) = \alpha \cdot f(a)$

Man kann (i) und (ii) auch zusammenfassen und direkt fordern:

$$f(\alpha \cdot a + \beta \cdot b) = \alpha \cdot f(a) + \beta \cdot f(b), \ a, b \in V, \ \alpha, \beta \in K$$

Besondere lineare Abbildungen

Definition 3.10: (Mono-/Epi-/Isomorphismus)

Eine K-lineare Abbildung $f : V \to V'$ zwischen zwei K-Vektorräumen V und V' heißt

(i) *Monomorphismus*, falls f injektiv ist

(ii) *Epimorphismus*, falls f surjektiv ist

(iii) *Isomorphismus*, falls f bijektiv ist

Satz 3.6:

Ist $f : V \to V'$ ein Isomorphismus zwischen zwei K-Vektorräumen V und V', so ist die Umkehrabbildung $f^{-1} : V' \to V$ wieder K-linear, also wieder ein Isomorphismus.

Kern und Bild linearer Abbildungen

Definition 3.11: (Kern/Bild einer linearen Abbildung)

Sei $f : V \to V'$ eine K-lineare Abbildung zwischen zwei K-Vektorräumen V und V'. Dann heißt

$$\ker f := f^{-1}(0) = \{a \in V \mid f(a) = 0\}$$

der *Kern* und

$$\operatorname{im} f := f(V) = \{f(a) \mid a \in V\}$$

das *Bild* von f.

Korollar 3.2:

$\ker f$ ist linearer Unterraum von V, und $\operatorname{im} f$ ist linearer Unterraum von V'.

Dimensionsformel

Satz 3.7:

Sei $f : V \to V'$ eine K-lineare Abbildung zwischen zwei K-Vektorräumen V und V'. Dann gilt:

(i) f injektiv $\Leftrightarrow \ker f = \{0\}$

(ii) f surjektiv $\Leftrightarrow \operatorname{im} f = V'$

Satz 3.8: (Dimensionsformel)

Sei $f : V \to V'$ eine K-lineare Abbildung zwischen zwei K-Vektorräumen V und V'. Dann gilt:

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

Überblick I

Überblick II

Matrizen

Definition 4.1: (Matrix)

Sei K ein Körper. Ein rechteckiges Schema mit m *Zeilen* und n *Spalten*, wobei $m, n \in \mathbb{N}$, sowie $m \cdot n$ *Einträgen* von Elementen in K der Form

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

heißt $m \times n$-*Matrix* über K. Es gilt $\forall_{i=1,\ldots,m;j=1,\ldots,n}\ a_{ij} \in K$.
Schreibweise: $A = (a_{ij}) = (a_{ij})_{i=1,\ldots,m;j=1,\ldots,n} \in K^{m \times n}$

Wichtige Beobachtungen

Korollar 4.1:

Die Abbildung $f : K^n \to K^m,\ x \mapsto Ax$, ist eine lineare Abbildung.

Korollar 4.2:

$K^{m \times n}$ ist ein Vektorraum über K.

Zeilen und Spalten

Definition 4.2: (Zeilen-/Spaltenvektor/Eintrag)

Sei K ein Körper und $A \in \mathbb{K}^{m \times n}$ eine Matrix wie in Def. 2.1. Ein Vektor $z_i = (a_{i1}, ..., a_{in}) \in K^n$ heißt *i-te Zeile* oder *i-ter Zeilenvektor*, ein Vektor $s_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in K^m$ heißt *j-te Spalte* oder *j-ter Spaltenvektor* der Matrix A.
Ein Element $(a_{ij})_{i=1,...,m;j=1,...,n}$ heißt *Eintrag* von A.

Definition 4.3: (Zeilen-/Spaltenraum)

(i) $\mathrm{Span}_K\{z_1, ..., z_m\}$ heißt *Zeilenraum* von A. Die Dimension des Zeilenraums heißt *Zeilenrang*.

(ii) $\mathrm{Span}_K\{s_1, ..., s_n\}$ heißt *Spaltenraum* von A. Die Dimension des Spaltenraums heißt *Spaltenrang*.

Spezielle Matrizen

Definition 4.4: (Quadratische Matrix)

Falls $m = n$, so heißt die Matrix *quadratisch*.

Definition 4.5: (Einheitsmatrix und Nullmatrix)

(i) Die sog. $n \times n$-*Einheitsmatrix* setzt sich aus den Einheitsvektoren $e_i, i = 1, ..., n$ zusammen:

$$E_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

(ii) Die sog. *Nullmatrix* besteht aus lauter Nullen.

Matrixsumme und skalare Multiplikation von Matrizen

Definition 4.6: (Matrixsumme und skalare Multiplikation von Matrizen)

Seien $A = (a_{ij})$ und $B = (b_{ij})$ Matrizen aus $K^{m \times n}$ und $\alpha \in K$.

(i) Die *Summenmatrix* $A + B$ ist gegeben durch die Summe der Einträge, $A + B = (a_{ij} + b_{ij})$. Matrizen mit ungleichem Format können nicht addiert werden!!!

(ii) Die *skalare Multiplikation von Matrizen* $\alpha \cdot A$ ist gegeben durch $\alpha \cdot A = (\alpha \cdot a_{ij})$

Matrix-Vektor-Multiplikation

Definition 4.7: (Matrix-Vektor-Multiplikation)

Seien $A \in K^{m \times n}$ mit Spaltenvektoren $s_1, ..., s_n \in K^m$ und $v = (v_1, ..., v_n) \in K^n$ ein Vektor. Dann ist das *Matrix-Vektor-Produkt* gegeben durch

$$A \cdot v = \sum_{i=1}^{n} v_i s_i \in K^m$$

(Linearkombination der Spalten von A)

Matrixprodukt

Definition 4.8: (Matrixprodukt)

Seien $A \in K^{m \times n}$ und $B \in K^{n \times \ell}$ mit $A = (a_{ij})$ und $B = (b_{jk})$,, $m, n, \ell \in \mathbb{N}$. Dann ist das *Matrixprodukt* bzw. die *Produktmatrix* $C = A \cdot B$ gegeben durch

$$C = (c_{ik}) = \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) \in K^{m \times \ell}$$

(alle *Skalarprodukte* (vgl. Abschnitt 6.1) der Zeilen von A und der Spalten von B werden gebildet)

Eigenschaften der Matrixmultiplikation

Satz 4.1:

Die Anzahl an Spalten von A muß mit der Anzahl an Zeilen von B übereinstimmen, denn ansonsten ist eine Skalarproduktbildung nicht möglich.
Die Matrixmultiplikation ist assoziativ, aber im allgemeinen nicht kommutativ.

Transponierte Matrix

Definition 4.9: (Transponierte Matrix)

Sei $A \in K^{m \times n}$. Dann ist die *Transponierte* von A, $A^T \in K^{n \times m}$, gegeben durch

$$A^T = (a_{ij}^T) = a_{ji}, i = 1, ..., m; j = 1, ..., n$$

Satz 4.2:

Es gilt für $A \in K^{m \times \ell}$ und $B \in K^{\ell \times n}$: $(A \cdot B)^T = B^T \cdot A^T$

Lineare Gleichungssysteme

Definition 4.10: (Lineares Gleichungssystem)

Seien $m, n \in \mathbb{N}$. Ein *Lineares Gleichungssystem (LGS)* mit m Gleichungen und n Unbekannten $x_1, ..., x_n \in K$, wobei K ein Körper ist, ist gegeben durch

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

mit *Koeffizienzen* $a_{ij} \in K$, $i = 1, ..., m; j = 1, ..., n$, Lösungsvektor $x = (x_1, ..., x_n)$ und *Ergebnisvektor* $b = (b_1, ..., b_m)$.

LGS in Matrixschreibweise

In Matrixschreibweise lautet ein LGS

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

bzw. $A \cdot x = b$. A heißt auch *Koeffizientenmatrix*. Falls $b = 0$, so heißt das LGS *homogen*, sonst *inhomogen*.

Lösung eines Linearen Gleichungssystems

Definition 4.11: (Lösung eines Linearen Gleichungssystems)

Durch $(A|b) := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix} \in K^{m\times(n+1)}$ ist die sog. *erweiterte Koeffizientenmatrix* gegeben.

Ein LGS heißt *lösbar*, falls $\exists_{\hat{x}\in K^n}\ A \cdot \hat{x} = b$. $\hat{x}$ heißt dann *Lösung* des LGS. Falls $\hat{x}$ nicht existiert, so heißt das LGS *nicht lösbar*.

Lösbarkeit eines Linearen Gleichungssystems

Satz 4.3:

(i) Jedes homogene LGS ist lösbar.

(ii) Seien ℓ_1, ℓ_2 Lösungen und $\alpha_1, \alpha_2 \in K$. Dann ist auch die Linearkombination $\alpha_1\ell_1 + \alpha_2\ell_2$ Lösung.

(iii) Der Raum $\{x \in K^n \mid Ax = 0\}$ ist ein Vektorraum über K, genauer gesagt ein Unterraum von K^n, der sog. *Lösungsraum*.

Zeilenstufenform

Problemstellung: Sei $A \in K^{m \times n}$ eine rechteckige Matrix, d.h. $m \leq n$. Finde zu $b \in K^m$ einen Lösungsvektor $x \in K^n$ mit $Ax = b$.
Bringe A dazu auf eine sog. *Zeilenstufenform*:

$$\begin{pmatrix}
\beta_1 & x & \cdots & x & x & x & \cdots & x & x & x & \cdots & x & x & \cdots \\
 & & & & \beta_2 & x & \cdots & x & x & x & \cdots & x & x & \cdots \\
 & & & & & & & \ddots & x & \cdots & x & x & x & \cdots \\
 & & & & & & & & & & & & \beta_r & \cdots \\
 & & & & & & & & & & & & 0 & 0 \\
 & & & & & & & & & & & & \vdots & \vdots \\
 & & & & & & & & & & & & 0 & 0
\end{pmatrix}$$

mit Koeffizienten $\beta_1, ..., \beta_r \in K \backslash \{0\}, r \in \mathbb{N}$, auch *Pivotelemente* genannt.

Rang

Definition 4.11: (Rang)

Die maximale Anzahl linear unabhängiger Zeilen- bzw. Spaltenvektoren einer Matrix $A \in K^{m \times n}$ heißt *Rang* von A. Schreibweise: $rg(A)$ oder $rang(A)$.

Korollar 4.3:

Es gilt stets $rg(A) \leq \min\{m, n\} = m$

Gaußsches Eliminationsverfahren

Wende eine Folge S von Elementarmatrizen (Matrixoperationen) auf die erweiterte Koeffizientenmatrix $(A|b)$ an: $S \cdot (A|b) = (B|c)$. Es gibt drei Fälle:

(i) Es existiert keine Lösung. Dann steht in der c-Spalte von $(B|c)$ ein Pivotelement.

(ii) Es existiert genau eine Lösung. Dann muß A quadratisch sein, und die Zeilenstufenform ist eine obere Dreiecksmatrix mit Einsen auf der Diagonalen.

(iii) Es existieren mehrere verschiedene Lösungen, d.h. die Lösung ist *mehrdeutig*. Im Falle $K \in \{\mathbb{R}, \mathbb{C}\}$ gibt es sogar unendlich viele Lösungen. Dann enthält die Zeilenstufenform Nullzeilen, und man kann $|\bar{P}|$ Variablen frei wählen, wobei $\bar{P}$ die Menge der Nicht-Pivotelemente ist.

Kern einer Matrix und Dimensionsformel

Definition 4.12: (Kern einer Matrix)

Die Menge $\ker A := \{x \in K^n \mid Ax = 0\}$ heißt *Kern* von A

Satz 4.4: (Dimensionsformel)

Es gilt: $\dim(\ker A) + rg(A) = \dim(K^n) = n$

Inverse Matrizen

Definition 4.13: (Invertierbare Matrix)

Eine quadratische Matrix $A \in K^{m \times m}$ heißt *invertierbar*, falls $\exists_{B \in K^{m \times m}}\ A \cdot B = B \cdot A = E_m$. Schreibweise: $B = A^{-1}$ (inverse Matrix)

Korollar 4.4:

Sei $A \in K^{m \times m}$ eine invertierbare Matrix. Dann hat das LGS $Ax = b$, $b \in K^m$, die eindeutige Lösung $x = A^{-1}b \in K^m$.

Es sind nicht alle Matrizen invertierbar. Die Menge der Matrizen bildet mit der Matrixaddition und -multiplikation einen Ring mit Einselement.

Bestimmung der inversen Matrix

Man verwendet das Gaußsche Eliminationsverfahren mit der erweiterten Koeffizientenmatrix $(A|E_m)$ und erhält $(E_m|A^{-1})$, d.h. die inverse Matrix von A ist dann auf der rechten Seite direkt ablesbar.

Satz 4.5: (Inverse Matrix für $m = 2$)

Für $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ gilt im Falle von $ad - bc \neq 0$:

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Mithilfe der inversen Matrix kann man beweisen, daß das Gaußsche Eliminationsverfahren funktioniert! (Beweisskizze an der Tafel!)

Determinanten

Definition 4.14: (Determinante)

Sei $A \in K^{m\times m}, m \geq 2$, und $A_{ij} \in K^{(m-1)\times(m-1)}$ diejenige Matrix, die entsteht, wenn man Zeile i und Spalte j streicht. Dann heißt $\det(A) := a_{11}$ für $A \in K^{1\times 1}$ und

$$\det(A) := \sum_{i=1}^{m} (-1)^{i+1} a_{i1} \det(A_{i1})$$

die *Determinante* von A. Schreibweisen: $\det(A) = \det(a_{ij}) = |A|$

Berechnung von Determinanten

Vorzeichenschema:

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{vmatrix}, \begin{vmatrix} + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ + & - & + & - & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{vmatrix}$$

$$\det(A) = a_{11}\det(A_{11}) - a_{21}\det(A_{21}) + \ldots + (-1)^{m-1} a_{m1}\det(A_{m1})$$
$$m = 2 : \det(A) = a_{11}a_{22} - a_{21}a_{12}$$

Man muß die Determinante nicht notwendigerweise nach der ersten Spalte entwickeln. Alle Zeilen und Spalten sind erlaubt! Wähle die Zeilen/Spalten mit den meisten Nullen!

Determinanten für Dreiecks- und Diagonalmatrizen

Satz 4.6:

Sei $A = K^{m \times m}$ eine obere bzw. untere Dreiecksmatrix, d.h., alle Einträge unterhalb bzw. oberhalb der Diagonalen sind Null, oder eine Diagonalmatrix, d.h. alle Einträge außer der Diagonaleinträge sind Null. Dann ist die Determinante gleich dem Produkt der Diagonalelemente, also

$$\det(A) = \prod_{i=1}^{m} a_{ii}$$

Insbesondere gilt $\det(E_m) = 1$.

Eigenschaften von Determinanten

Satz 4.7:

Sei $A \in K^{m \times m}$ eine quadratische Matrix. Dann gilt:

(i) Vertauscht man zwei Zeilen oder Spalten von A, so ändert sich das Vorzeichen von $\det(A)$.

(ii) Multipliziert man eine Zeile oder Spalte mit einem Skalar, so wird auch $\det(A)$ mit diesem Skalar multipliziert.

(iii) Zieht man das Vielfache einer Zeile von einer anderen Zeile ab, so ändert sich die Determinante nicht.

(iv) Zwei Zeilen bzw. Spalten von A sind genau dann linear abhängig, wenn $\det(A) = 0$.

(v) $\det(A^T) = \det(A)$

Determinantenmultiplikationssatz

Satz 4.8: (Determinantenmultiplikationssatz)

Für $A, B \in K^{m \times m}$ gilt $\det(A \cdot B) = \det(A) \cdot \det(B)$

Korollar 4.5:

(i) Für $n \in \mathbb{N}$ gilt $\det(A^n) = (\det(A))^n$

(ii) Ist A invertierbar, so gilt $\det(A^{-1}) = \frac{1}{\det(A)}$

(iii) Ist $A \in K^{2 \times 2}$ gilt $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Determinantenentwicklungssatz

Satz 4.9: (Determinantenentwicklungssatz)

Es ist egal, nach welcher Zeile oder Spalte die Determinante entwickelt wird.

Man nimmt natürlich dann diejenige Zeile oder Spalte, in der die meisten Nullen stehen!

Die Cramersche Regel

Betrachte das LGS $Ax = b$ mit $A \in \mathbb{R}^{n \times n}$ mit Spaltenvektoren $a_{*1}, ..., a_{*n} \in \mathbb{R}^n$ sowie $b = (b_1, ..., b_n) \in \mathbb{R}^n$. A sei invertierbar. Dann gilt für die Lösung $x = (x_1, ..., x_n) \in \mathbb{R}^n$:

$$x_i = \frac{\det(a_{*1}, ..., b, ..., a_{*n})}{\det(A)},$$

wobei der Vektor b in der Matrix an der i-ten Position steht. D.h., um die i-te Komponente der Lösung x zu erhalten, tauscht man im Zähler den i-ten Spaltenvektor a_{*i} durch den Vektor b aus.

Ring der Matrizen

Satz 4.10:

Die Menge der Matrizen $K^{n\times n}$, bildet zusammen mit der Matrixaddition und -multiplikation einen Ring mit Einselement $E_n \in K^{n\times n}$. Da bzgl. '$\cdot$' im allgemeinen keine Kommutativität gilt und nicht alle Matrizen invertierbar sind, bildet die Menge der Matrizen keinen Körper.

Spezielle und allgemeine lineare Gruppe

Satz 4.11:

Die Abbildung $\det : (K^{n\times n}\backslash\{0\}, \cdot) \to (K\backslash\{0\}, \cdot)$ ist ein Homomorphismus. Die sog. *spezielle lineare Gruppe*

$$\mathcal{SL}_n^K := \{A \in K^{n\times n} \mid \det(A) = 1\}$$

bildet eine Untergruppe der Gruppe der invertierbaren Matrizen $\mathcal{GL}_n^K$ (sog. *allgemeine lineare Gruppe*).

Überblick I

Überblick II

Polynome

Definition 5.1:

Sei R ein Ring.

(i) Für *Koeffizienten* $a_0, ..., a_n \in R$, $n \in \mathbb{N}_0$ und $x \in R$ heißt

$$P(x) := a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1} + a_n x^n = \sum_{i=0}^{n} a_i x^i$$

Polynom über R.

Polynome

Definition 5.1 (Forts.):

Sei R ein Ring.

(ii) Falls existent, so heißt

$$a_k := a_{\max\{i \mid 0 \leq i \leq n,\ a_i \neq 0\}}$$

führender Koeffizient von P. $\operatorname{grad}(P) := k$ heißt *Grad* von P. Falls $a_k = 1$, so heißt P *normiert* oder *monisch*. Polynome vom Grad 1 heißen *linear*. Polynome mit $a_k = 1 \ \wedge \ \forall_{0 \leq i \leq k-1}\ a_i = 0$, heißen *Monome*.

(iii) Die Menge aller Polynome über R wird mit $R[x]$ bezeichnet.

Polynome

Definition 5.1 (Forts.):

Sei R ein Ring.

(iv) Seien $P, Q \in R[x]$, $P = \sum_{i=0}^{m} a_i x^i$, $Q = \sum_{i=0}^{n} b_i x^i$ zwei Polynome über R mit $\operatorname{grad}(P) = m$ und $\operatorname{grad}(Q) = n$. Dann heißt

$P + Q = \sum_{k=0}^{s} c_k x^k$ mit $s \leq \max\{m, n\}$ und

$c_k = a_k + b_k, 0 \leq k \leq \min\{m, n\}$ und

$$c_k = \begin{cases} a_k, n < k \leq m, & n < m \\ b_k, m < k \leq n, & m < n \end{cases}$$

die *Summe* von P und Q.

Polynome

Definition 5.1 (Forts.):

Sei R ein Ring.

(iv) $P \cdot Q = \sum_{i=0}^{s} d_i x^i$ mit

$d_i = \sum_{k=0}^{i} a_k b_{i-k}, 0 \leq i \leq m+n, s \leq m+n$ (Gleichheit, falls R ein Körper ist), wobei $a_k = 0$ für $k > m$ und $b_k = 0$ für $k > n$, ist das *Produkt* von P und Q.

(v) P und Q heißen *gleich*, falls Grad und Koeffizienten gleich sind.

Nullstellen und Vielfachheiten

Definition 5.2: (Nullstellen und Vielfachheiten)

Sei $P \in \mathbb{R}[x]$. $x_0 \in \mathbb{R}$ heißt *Nullstelle* von P, falls $P(x_0) = 0$.

$$\max\{k \in \mathbb{N}_0 \mid (x - x_0)^k \mid P\}$$

(der zweite senkrechte Strich ist die Teilbarkeitsrelation!) heißt *Vielfachheit* der Nullstelle x_0 in P. Ist die Vielfachheit 1, so heißt x_0 *einfache Nullstelle*. Ist die Vielfachheit 2, so heißt x_0 *doppelte Nullstelle* Ist die Vielfachheit 3, so heißt x_0 *dreifache Nullstelle* usw.

Nullstellen von Polynomen werden durch Probieren und dann durch Polynomdivision ermittelt. Die Nullstellen eines resultierenden Polynoms vom Grad 2 können schließlich via p-q-Formel berechnet werden.

Die komplexen Zahlen

Die Gleichung $x^2 = -1$ ist in $\mathbb{R}$ nicht lösbar, soll aber lösbar gemacht werden!
$\Rightarrow$ Einführung einer *imaginären Zahl* i mit $i^2 = -1$. Dann gilt auch $(-i)^2 = -1$.

Dies führt zu einem Erweiterungskörper der reellen Zahlen, dem Körper der *komplexen Zahlen*

$$\mathbb{C} := \mathbb{R}(i) = \{a + i \cdot b \mid a, b \in \mathbb{R}\}$$

(Gauß, 1831). Es gilt $\mathbb{C} \cong \mathbb{R}^2$. Isomorphismus: $\varphi(a + ib) = \begin{pmatrix} a \\ b \end{pmatrix}$

Körpereinbettung von $\mathbb{R}$ in $\mathbb{C}$: $a \mapsto (a, 0), a \in \mathbb{R}$.

Elemente in $\mathbb{C}$

Das additive Einselement ist $0 = 0 + i \cdot 0$, das multiplikative Einselement ist $1 = 1 + i \cdot 0$.

Das additive Inverse zu $a + i \cdot b \in \mathbb{C}$ ist $-a - i \cdot b \in \mathbb{C}$.

Das multiplikative Inverse zu $a + i \cdot b \in \mathbb{C}$ ist $\frac{a}{a^2+b^2} - i \cdot \frac{b}{a^2+b^2} \in \mathbb{C}$, wobei $a^2 + b^2 \neq 0$ sein muß. Durch $|a + i \cdot b| = \sqrt{a^2 + b^2}$ ist der *Betrag* einer komplexen Zahl gegeben.
(Rechenbeispiele an der Tafel!)

Der Fundamentalsatz der Algebra

Satz 5.1: (Fundamentalsatz der Algebra)

Jedes nichtkonstante Polynom $P \in \mathbb{C}[x]$ hat in $\mathbb{C}$ genau $\operatorname{grad}(P)$ Nullstellen. Diese müssen nicht paarweise verschieden sein und sind mit ihren Vielfachheiten gezählt. Falls die Koeffizienten von P reell sind und $z = a + i \cdot b$ Nullstelle ist, dann auch die sog. *konjugiert-komplexe Zahl* $\bar{z} = a - i \cdot b$.

Eigenwerte und Eigenvektoren

Definition 5.3: (Eigenwerte und Eigenvektoren)

Sei $A \in K^{m \times m}$ eine quadratische Matrix. Ein Skalar $\lambda \in K$ heißt *Eigenwert* von A zum *Eigenvektor* $v \in K^m \backslash \{0\}$ von A, falls

$$A \cdot v = \lambda \cdot v$$

Es gilt $A \cdot v = \lambda \cdot v \Leftrightarrow (A - \lambda \cdot E_m) \cdot v = 0$. Die Matrix $A - \lambda \cdot E_m$ ist nicht regulär (nicht invertierbar, Beweis in den Übungen!). D.h., die Lösung des LGS ist mehrdeutig, und somit gibt es unendlich viele Eigenvektoren. Der Nullvektor ist per Definition als Eigenvektor ausgeschlossen!

Charakteristisches Polynom

Definition 5.4: (Charakteristisches Polynom)

Das Polynom $\chi_A(\lambda) := \det(A - \lambda \cdot E_m)$ heißt *charakteristsiches Polynom* von A.

Die Eigenwerte sind genau die Nullstellen von χ_A. Nach dem Fundamentalsatz der Algebra exisiteren stets m Eigenwerte (mit Vielfachheiten gezählt), die auch komplex sein können. Falls $\lambda \in \mathbb{C}$ Eigenwert einer reellen Matrix A ist, dann auch der dazu konjugiert-komplexe Eigenwert $\bar{\lambda}$.

Diagonalisierbarkeit

Definition 5.5: (Ähnliche Matrizen)

Zwei Matrizen $A, B \in \mathbb{R}^{n \times n}$ heißen *ähnlich*, wenn es eine invertierbare Matrix $S \in \mathbb{R}^{n \times n}$ gibt mit $B = S^{-1} \cdot A \cdot S$ bzw. $S \cdot B = A \cdot S$.

Definition 5.6: (Diagonalisierbarkeit)

Eine Matrix $A \in \mathbb{R}^{n \times n}$ heißt *diagonalisierbar*, wenn sie zu einer Diagonalmatrix ähnlich ist.

Diagonalisierung

Satz 5.2:

Eine Matrix $A \in \mathbb{R}^{n \times n}$ ist genau dann diagonalisierbar, wenn sie eine Basis V aus Eigenvektoren besitzt. Die Diagonalisierung lautet

$$D = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix} = V^{-1} \cdot A \cdot V, \text{ wobei } \lambda_1, ..., \lambda_n \in \mathbb{R}$$

die Eigenwerte von A sind und V als Spalten die Eigenvektoren $v_1, ..., v_n \in \mathbb{R}^n$ von A enthält.

Korollar 5.1:

Ähnliche Matrizen haben dieselben Eigenwerte. Die Determinante einer Matrix ist gleich dem Produkt ihrer Eigenwerte.

Eigenraum

Satz 5.3:

Sei $A \in \mathbb{R}^{n \times n}$ eine Matrix mit Eigenwerten $\lambda_1, ..., \lambda_n \in \mathbb{R}$ und Eigenvektoren $v_1, ..., v_n \in \mathbb{R}^n$. Sei $r \in \mathbb{N}$ so, daß $\lambda_1, ..., \lambda_r \in \mathbb{R}$ paarweise verschieden sind. Dann sind die zugehörigen Eigenvektoren $v_1, ..., v_r \in \mathbb{R}^n$ linear unabhängig.

Definition 4.7: (Eigenraum)

Sei $\lambda \in \mathbb{R}$ ein Eigenwert einer Matrix $A \in \mathbb{R}^{n \times n}$. Dann heißt

$$\mathcal{U}_\lambda := \ker(A - \lambda E_n) = \{v \in \mathbb{R}^n \mid A \cdot v = \lambda \cdot v\}$$

Eigenraum zum Eigenvektor λ.

Wichtige Äquivalenzen in der Linearen Algebra

Satz 5.4:

Es seien $A \in \mathbb{R}^{n \times n}$ und $b \in \mathbb{R}^n$. Dann sind folgende Aussagen äquivalent:

(i) Die Lösung des LGS $(A|b)$ ist eindeutig.

(ii) $\ker A = \{0\}$, d.h. der Kern von A besteht nur aus dem Nullvektor.

(iii) A ist invertierbar.

(iv) $\det(A) \neq 0$.

(v) $rg(A) = n$.

(vi) $\lambda = 0$ ist kein Eigenwert von A.

Definitheit von Matrizen

Definition 5.8: (Definitheit)

Sei A eine $n \times n$-Matrix.

(i) A heißt *positiv definit (pd)*, falls $\forall_{x \in \mathbb{R}^n \setminus \{0\}} \ \langle x, Ax \rangle > 0$.

(ii) A heißt *positiv semidefinit (psd)*, falls $\forall_{x \in \mathbb{R}^n \setminus \{0\}} \ \langle x, Ax \rangle \geq 0$.

(iii) A heißt *negativ (semi-)definit (nd/nsd)*, falls $-A$ positiv (semi-)definit ist.

(iv) A heißt *indefinit*, falls $\exists_{x,y \in \mathbb{R}^n} \ \langle x, Ax \rangle > 0 \ \wedge \ \langle y, Ay \rangle < 0$.

Eigenwerte und Eigenvektoren symmetrischer Matrizen

Satz 5.7: (Eigenwerte und Eigenvektoren symmetrischer Matrizen)

Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch. Dann gilt:

(i) A hat nur reelle Eigenwerte.

(ii) A hat eine Orthonormalbasis aus Eigenvektoren.

Korollar 5.3:

Falls $A \in \mathbb{R}^{n \times n}$ symmetrisch und $\lambda \in \mathbb{R}$ ein Eigenwert mit Vielfachheit k ist, so hat λ auch einen k-dimensionalen Eigenraum.

Satz 5.8: (Definitheit symmetrischer Matrizen)

Eine symmetrische Matrix $A \in \mathbb{R}^{n \times n}$ ist genau dann positiv definit, wenn alle ihre Eigenwerte echt positiv sind.

Hauptminoren

Definition 5.9: (Hauptminor)

Die Determinante der linken oberen $k \times k$-Untermatrix einer symmetrischen Matrix heißt der k-te *Hauptminor*, Bezeichnung: M_k.

Satz 5.9: (Sylvester)

Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch. Dann gilt:

(i) A pd $\Leftrightarrow \forall_{k=1,\ldots,n}\ M_k > 0$

(ii) A nd $\Leftrightarrow \forall_{k=1,\ldots,n}\ (-1)^k M_k > 0$

(iii) $\forall_{k=1,\ldots,n-1}\ M_k > 0\ \wedge\ M_n = \det(A) = 0\ \Rightarrow\ A$ psd

(iv) $\forall_{k=1,\ldots,n-1}\ (-1)^k M_k > 0\ \wedge\ M_n = \det(A) = 0\ \Rightarrow\ A$ nsd

Hauptminoren und Definitheit

Satz 5.9: (Sylvester, Forsetzung)

(v) $M_n \neq 0$, aber weder (i) noch (ii) trifft zu $\Rightarrow$ A indefinit

(vi) A hat mindestens ein echt positives und ein echt negatives Diagonalelement $\Rightarrow$ A indefinit

Vorgehensweise zur Definitheitsprüfung

1. Hat A Diagonalgestalt? Falls ja, lese Eigenwerte auf Diagonalen ab und entscheide die Definitheit direkt.
2. Falls nein, bestimme die Hauptminoren von A.
3. Sind alle Hauptminoren echt positiv, so ist A pd.
4. Ist der erste Hauptminor echt negativ und danach liegen wechselnde Vorzeichen vor (keine 0 erlaubt!), so ist A nd.
5. Ist der letzte Hauptminor, also die Determinante, gleich 0? Falls ja, prüfe ggf. auf positive/negative Semidefinitheit gemäß Satz 5.9 (iii)/(iv).
6. Falls nein und es konnte bislang noch keine Entscheidung getroffen werden, so liegt Indefinitheit vor.

Hinweis: Aussage (vi) von Satz 5.9 ist auch sehr nützlich, um direkt auf Indefinitheit zu entscheiden.

Definitheit von A^{-1}, AA^T und A^TA

Satz 5.10: (Definitheit der Inversen)

Sei $A \in \mathbb{R}^{n\times n}$ positiv definit. Dann ist A invertierbar, und A^{-1} ist auch positiv definit.

Satz 5.11: (Definitheit von AA^T und A^TA)

Sei $A \in \mathbb{R}^{n\times n}$. Dann gilt:

(i) A und A^T haben dieselben Eigenwerte.

(ii) AA^T und A^TA haben dieselben Eigenwerte. Ist v Eigenvektor von AA^T (A^TA), so ist A^Tv (Av) Eigenvektor von A^TA (AA^T).

(iii) AA^T und A^TA sind positiv semidefinit. Falls A invertierbar, so sind sie positiv definit. Sie sind symmetrisch und haben somit reelle Eigenwerte. Diese sind positiv und echt positiv, falls A invertierbar.

Anwendung in der Informatik: Bildverarbeitung

Bei Gesichtserkennungen in der Bildverarbeitung werden relevante Informationen zu einer bestimmten Klasse von bekannten Objekten ermittelt (Mustererkennung). Dabei werden Bilder als sog. *Pixelvektoren* des $\mathbb{R}^n$ aufgefaßt. Die Bilder sind also Punkte $b_1, ..., b_M \in \mathbb{R}^n$, wobei $n \in \mathbb{N}$ die Anzahl an Pixeln und $m \in \mathbb{M}$ die Anzahl an Bildern ist.

Frage:

Kann man den Raum der Gesichtsbilder als Unterraum des Bilderraums repräsentieren und das Auftreten neuer/ähnlicher Gesichter erkennen?

Antwort:

Ja, und zwar durch die Bestimmung der Kovarianzmatrix der Gesichtsbildvektoren (Abweichungen vom Durchschnittsbild). Die Eigenvektoren dieser Matrix spannen den gesuchten Unterraum auf.

Anwendung in der Informatik: Page-Ranking

Das sog. *PageRank-Verfahren* nach Larry Page modelliert das Verhalten eines Internetbenutzers, der über Links verbundene Webseiten aufruft.

Hauptanwendung: Seitenbewertung für Google.

Prinzip: Das Gewicht einer Seite (PageRank) soll umso höher sein, je mehr Seiten mit möglichst hohem Eigengewicht auf die Seite verlinken.

Definition: PageRank einer Webseite a:

$$PR(a) = \frac{q}{T} + (1-q)\sum_{i=1}^{n}\frac{PR(p_i)}{L(p_i)},$$

- $p_1, ..., p_n$: Anzahl Seiten, die auf a verlinken,
- T: Gesamtzanzahl an Seiten
- $L(p)$: Anzahl Seiten, auf die die Webseite p verlinkt,
- $q \in [0,1]$: Wahrscheinlichkeit eines zufälligen Seitenwechsels,
- $1-q \in [0,1]$: Wahrscheinlichkeit der Benutzung eines Links.

Google-Matrix

- **Normierte Adjazenzmatrix** A: $a_{ij} = 1$ falls Seite i und j durch Link verbunden sind, sonst 0,
- **Linkmatrix** L**:**

$$L_{ij} := \begin{cases} \frac{1}{L(p_i)}, & a_{ij} = 1, \\ 0 & \text{sonst} \end{cases},$$

- **Dangling-Nodes-Vektor** w**:**

$$w_i = \begin{cases} 1, & L(p_i) = 0 \\ 0 & \text{sonst} \end{cases},$$

- **Einsvektor** e: $e = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \in \mathbb{R}^T$.

Google-Matrix: Eigenwertproblem des PageRanks-Verfahrens

$$P := (1-d)\left(L + \frac{1}{T}we^T\right) + \frac{d}{T}ee^T.$$

sog. **Google-Matrix.**

Der **PageRank-Vektor** PR ist Eigenvektor von P^T zum Eigenwert 1:

$$P^T(PR) = PR.$$

Überblick I

Überblick II

Bilinearform

Definition 6.1: (Bilinearform)

Sei V ein K-Vektorraum. Eine Abbildung $\Phi : V \times V \to K$ heißt *Bilinearform*, falls für $x, x_1, x_2, y, y_1, y_2 \in V$ und $\alpha \in K$ gilt:

(i) $\Phi(x_1 + x_2, y) = \Phi(x_1, y) + \Phi(x_2, y)$

(ii) $\Phi(\alpha x, y) = \alpha \Phi(x, y)$

(iii) $\Phi(x, y_1 + y_2) = \Phi(x, y_1) + \Phi(x, y_2)$

(iv) $\Phi(x, \alpha y) = \alpha \Phi(x, y)$,

also wenn sie linear in beiden Argumenten ist. Φ heißt *symmetrisch*, falls $\Phi(x, y) = \Phi(y, x)$ für $x, y \in V$, und *nicht ausgeartet* (oder *nicht entartet*), falls

$$\forall_{y \in V}\ \Phi(x, y) = 0 \ \Rightarrow\ x = 0 \ \wedge\ \forall_{x \in V}\ \Phi(x, y) = 0 \ \Rightarrow\ y = 0$$

Positive (Semi-)Definitheit und Skalarprodukt

Definition 6.2: (positiv (semi-)definite Bilinearform)

Eine symmetrische Bilinearform $V \times V \to K$ heißt *positiv semidefinit (psd)*, falls $\forall_{x \in V}\ \Phi(x,x) \geq 0$. Gilt sogar $\forall_{x \in K \setminus \{0\}}\ \Phi(x,x) > 0$, so heißt sie *positiv definit (pd)*.

Definition 6.3: (Skalarprodukt)

Sei Φ eine symmetrische und positiv definite Bilinearform. Dann heißt Φ auch *Skalarprodukt* auf dem K-Vektorraum V.
Bezeichnung: $\Phi(\cdot,\cdot) = \langle \cdot,\cdot \rangle : V \times V \to K$

Definition 6.4: (euklidischer/unitärer Vektorraum)

Sei V ein K-Vektorraum und $\langle \cdot,\cdot \rangle$ ein Skalarprodukt auf V. Dann heißt das Paar $(V, \langle \cdot,\cdot \rangle)$ für $K = \mathbb{R}$ *euklidischer* und für $K = \mathbb{C}$ *unitärer Vektorraum*.

Das Skalarprodukt

Satz 6.1:

Sei K ein Körper und $V = K^n, n \in \mathbb{N}$. Die Abbildung $\langle \cdot, \cdot \rangle : V \times V \to K$ mit

$$\langle x, y \rangle := \sum_{i=1}^{n} x_i y_i$$

für $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in K^n$ ist ein nicht-entartetes Skalarprodukt, in dieser Vorlesung <u>das</u> Skalarprodukt.

Das Skalarprodukt induziert eine Norm $||x|| := \sqrt{\langle x, x \rangle} = \sqrt{\sum_{i=1}^{n} x_i^2}$

(die sog. *euklidische Länge* eines Vektors x).

Winkel zwischen zwei Vektoren

Der Winkel $\omega \in [0, \pi)$ zwischen zwei Vektoren $x, y \in \mathbb{R}^n$ ist gegeben durch die Formel

$$\cos(\omega) = \frac{\langle x, y \rangle}{||x|| \cdot ||y||}$$

Das Skalarprodukt ist somit eine Art *Ähnlichkeitsmaß* für Vektoren.

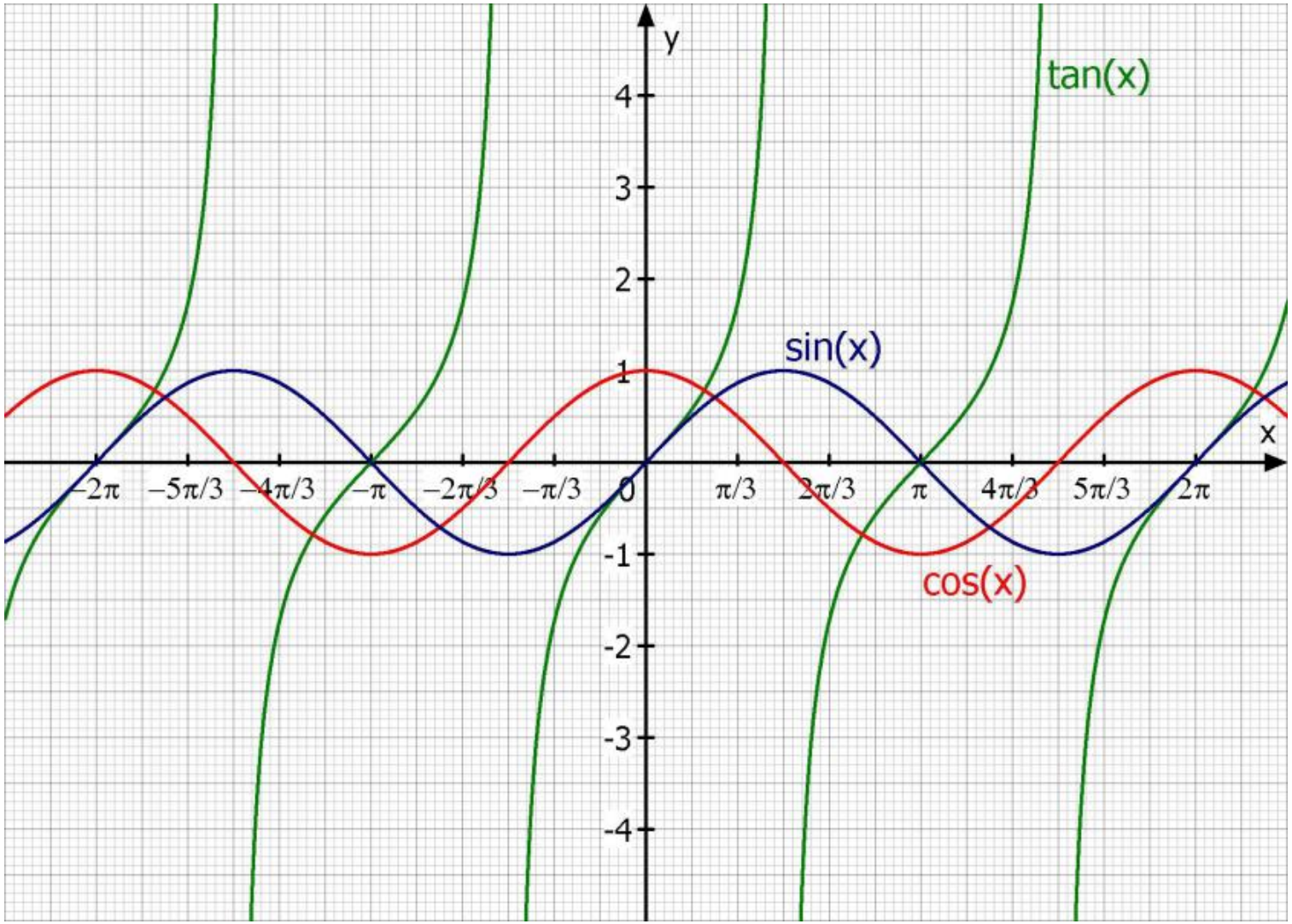
Wichtige sin- und cos-Werte:

ω	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	2π
$\sin(\omega)$	0	$\frac{1}{2}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}\sqrt{3}$	1	0	0
$\cos(\omega)$	1	$\frac{1}{2}\sqrt{3}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}$	0	-1	1

Man beachte auch die Symmetrien:

- sin ist achsensymmetrisch bei $\frac{\pi}{2}$ und punktsymmetrisch bei 0
- cos ist punktsymmetrisch bei $\frac{\pi}{2}$ und achsensymmetrisch bei 0

Verlauf der trigonometrischen Funktionen



Die Cauchy-Schwarzsche Ungleichung

Satz 6.2: (Cauchy-Schwarzsche Ungleichung)

Es gilt:

$$\forall_{x,y\in\mathbb{R}^n}\ \langle x,y\rangle^2 \leq \langle x,x\rangle \cdot \langle y,y\rangle$$

mit Gleichheit genau dann, wenn x und y linear abhängig sind.

Beachte:

$$\begin{aligned} & \langle x,y\rangle^2 \leq \langle x,x\rangle \cdot \langle y,y\rangle \\ \Leftrightarrow \quad & \langle x,y\rangle^2 \leq ||x||^2 \cdot ||y||^2 \\ \Leftrightarrow \quad & |\langle x,y\rangle| \leq ||x|| \cdot ||y|| \end{aligned}$$

Orthogonalität und Orthonormalität

Definition 6.5: (Orthogonalität)

Sei $\langle \cdot, \cdot \rangle$ eine symmetrische Bilinearform auf einem K-Vektorraum V, insbesondere das Skalarprodukt aus Satz 6.1. Zwei Vektoren $x, y \in V$ heißen *orthogonal* bzw. *stehen senkrecht aufeinander*. falls $\langle x, y \rangle = 0$. Schreibweise: $x \perp y$

Definition 6.6: (Orthonormalität)

Zwei orthogonale Vektoren $x, y \in V$ heißen *orthonormal*, falls zusätzlich $\langle x, x \rangle = \langle y, y \rangle = 1$ gilt. Ein System $x_1, ..., x_n \in V, n \in \mathbb{N}$, heißt *Orthonormalsystem*, falls

$$\forall_{i,j=1,...,n} \langle x_i, x_j \rangle = \delta_{ij} := \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

(sog. *Kronecker-Delta*)

Norm

Definition 6.7: (Norm)

Sei V ein K-Vektorraum. Eine Abbildung $||\cdot|| : V \to K$ heißt *Norm*, falls für alle $x, y \in V$ und $\alpha \in K$ gilt:

(i) $||x|| > 0$ für $x \in \mathbb{R}^n \backslash \{0\}$, $||x|| = 0 \Leftrightarrow x = 0$ (Definitheit)

(ii) $||\alpha x|| = |\alpha| \cdot ||x||$ für $\alpha \in \mathbb{R}$, $x \in \mathbb{R}^n$ (Homogenität)

(iii) $||x + y|| \leq ||x|| + ||y||$ für $x, y \in \mathbb{R}^n$ (Dreiecksungleichung)

Korollar 6.1:

Jedes Skalarprodukt $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ induziert eine Norm $||\cdot|| : V \to \mathbb{R}$ mit

$$||x|| = \sqrt{\langle x, x \rangle}, \ x \in V$$

Orthogonalraum

Definition 6.8: (Orthogonalraum)

Sei V ein K-Vektorraum. Sei $\langle \cdot, \cdot \rangle : V \times V \to K$ eine symmetrische Bilinearform, insbesondere das Skalarprodukt aus Satz 3.1. Sei weiterhin U ein Unterraum von V. Dann heißt

$$U^{\perp} := \{v \in V \mid \langle u, v \rangle = 0,\ u \in U\}$$

der *Orthogonalraum* von U.

Satz 6.2:

Der Orthogonalraum $U^{\perp}$ ist ein Unterraum von V.

Dimensionsformel und Selbstorthogonalität

Satz 6.3:

Sei U ein Unterraum von $K^n, n \in \mathbb{N}$, K Körper. Dann gilt:

(i) $\dim(U) + \dim(U^\perp) = \dim(K^n) = n$

(ii) $(U^\perp)^\perp = U$

(iii) $(K^n)^\perp = \{0\}$

Gibt es selbstorthogonale Vektoren?

In unserer Definition nicht, da sonst die positive Definitheit des Skalarprodukts verletzt wäre und das Skalarprodukt dann keine Norm induzieren würde. In der Kodierungstheorie darf man strenggenommen kein Skalarprodukt zugrundelegen, sondern nur eine symmetrsiche Bilinearform!

Ebenen

Die Parameterdarstellung einer Ebene im $\mathbb{R}^3$ lautet

$$x = a + \lambda u_1 + \mu u_2, \ \lambda, \mu \in \mathbb{R},$$

wobei $a \in \mathbb{R}^3$ ein Ortsvektor ist, der zu einem Punkt auf der Ebene zeigt, und u_1, $u_2 \in \mathbb{R}^3$ die sog. *Richtungsvektoren* sind.
Eine Koordinatendarstellung erreicht man mit dem sog. *Normalenvektor* $n \in \mathbb{R}^3 \backslash \{0\}$, der senkrecht auf der Ebene bzw. auf beiden Richtungsvektoren steht (auch *Normalform* genannt):

$$\langle n, x \rangle = c, \ c \in \mathbb{R} \ \Leftrightarrow \ n_1 x_1 + n_2 x_2 + n_3 x_3 = c$$

wobei $n = (n_1, n_2, n_3)^T$ und $x = (x_1, x_2, x_3)^T$.

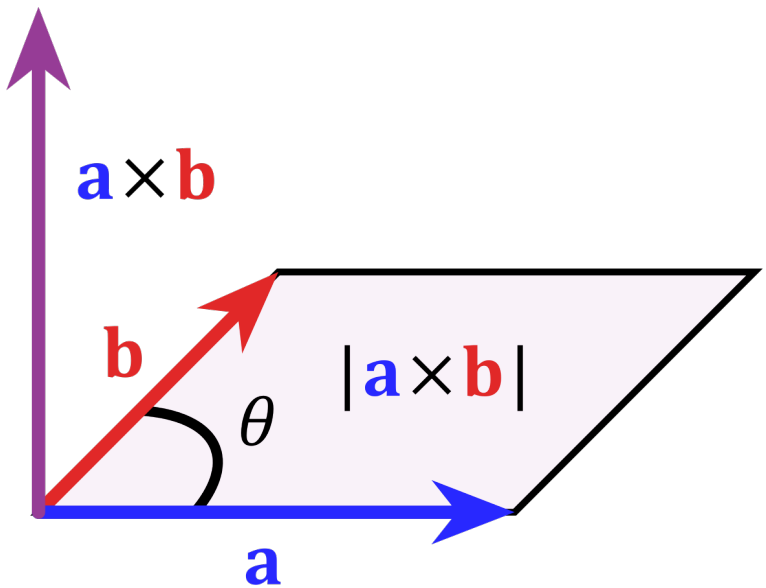
Vektorprodukt

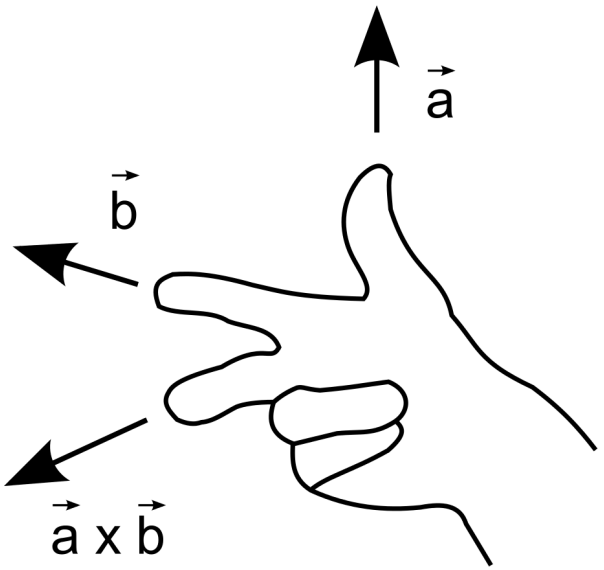
Das sog. *Vektorprodukt* zweier Vektoren $a = (a_1, a_2, a_3)^T, y = (b_1, b_2, b_3)^T$, auch *vektorielles* oder *äußeres Produkt* oder *Kreuzprodukt* genannt, ist gegeben durch

$$a \times b := \begin{pmatrix} \begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix} \\ -\begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} \\ \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \end{pmatrix}$$

und ergibt den Vektor, der auf a und b senkrecht steht. a, b und c bilden ein sog. *Rechtssystem*.

Geometrische Bedeutung des Vektorprodukts





Die Norm des Vektorprodukts ist gleich dem Flächeninhalt des Parallelogramms, welches von a und b aufgespannt wird. Somit ergibt sich der Winkel θ zwischen a und b gemäß $||a \times b|| = ||a||||b|| \sin(\theta)$.

Hessesche Normalform

Mithilfe des Vektorprodukts läßt sich der Normalenvektor einer Ebene aus den beiden Richtungsvektoren bestimmen. Dividiert man die Ebenengleichung durch dessen Norm, so erhält man die sog. *Hessesche Normalform*

$$\langle n_0, x \rangle = d$$

mit $n_0 := \frac{n}{||n||}$. $d = \frac{c}{||n||}$ ist der Abstand der Ebene zum Koordinatenursprung. n_0 heißt *Normaleneinheitsvektor*.

Orthogonale Matrizen

Definition 6.9: (Orthogonale Matrix)

Eine Matrix $Q \in \mathbb{R}^{n \times n}$ heißt *orthogonal*, falls $Q^T Q = E_n$, d.h., die Spaltenvektoren bilden eine Orthonormalbasis:
$\langle q_i, q_j \rangle = \delta_{ij}, \;\; i, j = 1, ..., n.$

Korollar 6.2:

(i) Q orthogonal $\Rightarrow$ Q invertierbar mit $Q^{-1} = Q^T$

(ii) Q orthogonal $\Rightarrow$ Q^T orthogonal mit $Q^T Q = Q Q^T = E_n$

Eigenschaften orthogonaler Matrizen

Satz 6.4: (Eigenschaften orthogonaler Matrizen)

Sei $Q \in \mathbb{R}^{n \times n}$ orthogonal. Dann gilt:

(i) $\det(Q) \in \{-1, 1\}$

(ii) $\forall_{x,y \in \mathbb{R}^n} \langle Qx, Qy \rangle = \langle x, y \rangle$ und
$\forall_{x \in \mathbb{R}^n} ||Qx|| = ||x||$ (euklidische Norm), d.h. die Abbildung $x \mapsto Qx$ ist winkel- und längentreu.

Drehungen und Spiegelungen

Die orthogonale Matrix

$$Q = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

beschreibt im $\mathbb{R}^2$ eine Drehung um den Winkel $\varphi \in [0, 2\pi)$.
Die orthogonale Matrix

$$H = E_n - 2n_0 n_0^T$$

beschreibt eine Spiegelung um eine Ebene mit Normaleneinheitsvektor n_0. Dabei ist $E_n - n_0 n_0^T$ die sog. *Projektionsmatrix* auf die Ebene (orthogonale Projektion).

Drehmatrizen im $\mathbb{R}^3$:

- um die x-Achse: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\varphi) & -\sin(\varphi) \\ 0 & \sin(\varphi) & \cos(\varphi) \end{pmatrix}$
- um die y-Achse: $\begin{pmatrix} \cos(\varphi) & 0 & \sin(\varphi) \\ 0 & 1 & 0 \\ -\sin(\varphi) & 0 & \cos(\varphi) \end{pmatrix}$
- um die z-Achse: $\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Literatur: Mathematische Grundlagen

[MG1] G. Teschl, S. Teschl: *Mathematik für Informatiker*, Band 1: Diskrete Mathematik und Lineare Algebra, Springer-Verlag Berlin Heidelberg (2008), 3. Auflage

[MG2] A. Beutelspacher, M.-A. Zschiegner: *Diskrete Mathematik für Einsteiger* – Mit Anwendungen in Technik und Informatik, Springer Vieweg Wiesbaden (2011), 4. Auflage

[MG3] K.-U. Witt: *Mathematische Grundlagen für die Informatik* – Mengen, Logik, Rekursion, Springer Vieweg Wiesbaden (2013)

[MG4] S. Lipschutz, M. Lipson: *Schaum's Outline of Discrete Mathematics*, McGraw Hill (2007), 3. Auflage

[MG5] K.-U. Witt: *Algebraische und zahlentheoretische Grundlagen für die Informatik* – Gruppen, Ringe, Körper, Primzahltests, Verschlüsselung, Springer Vieweg Wiesbaden (2014)

Literatur: Lineare Algebra

[LA1] K.-U. Witt: *Lineare Algebra für die Informatik* – Vektorräume, Gleichungssysteme, Codierung, Quantenalgorithmen, Springer Vieweg Wiesbaden (2013)

[LA2] G. Strang: *Introduction to Linear Algebra*, Cambridge University Press (2023), 6. Auflage

[LA3] G. Fischer: *Lineare Algebra* – Eine Einführung für Studienanfänger, Springer Spektrum Wiesbaden (2014), 12. Auflage

[LA4] S. Bosch: *Lineare Algebra*, Springer Berlin-Heidelberg (2001)