Vorlesungsskript

LinA I* WiSe 23/24

Inhaltsverzeichnis

1. Motivation und mathematische Grundlagen

Was ist lineare Algebra bzw. analytische Geometrie?

- analytische Geometrie:
  Beschreibung von geometrischen Fragen mit Hilfe von Gleichungen, Geraden, Ebenen sowie die Lösungen von Gleichungen als geometrische Form
- lineare Algebra:
  die Wissenschaft der linearen Gleichungssysteme bzw der Vektorräume und der linearen Abbildungen zwischen ihnen

Wozu braucht man das?

- mathematische Grundlage für viele mathematische Forschung z.B. in der algebraischen Geometrie, Numerik, Optimierung
- viele Anwendungen z.B. Page-Rank-Algorithmus, lineare Regression
- oder Optimierung:
  linear: Beschreibung zulässiger Punkte als Lösung von (Un)-Gleichungen
  nichtlinear: notwendige Optimalitätsbedingungen

1.1. Mengen

Der Mengenbegriff wurde von Georg Cantor (dt. Mathematiker, 1845-1918) eingeführt.

Definition 1.1: Mengen

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

Bemerkungen:

Für jedes Objekt x kann man eindeutig feststellen, ob es zu einer Menge M gehört oder nicht.

$$x \in M \to x \text{ ist Element von } M$$
$$x \notin M \to x \text{ ist nicht Element von } M$$

Beispiel 1.2: Beispiel für Mengen

- {rot, gelb, grün}
- {1, 2, 3, 4}
- $\mathbb{N} = \{1, 2, 3, ...\}, \mathbb{N}_0 = \{0, 1, 2, 3, ...\}$
- $\mathbb{Z} = \{..., -1, 0, 1, ...\}$
- $\mathbb{Q} = \left\{x \mid x = \frac{a}{b} \text{ mit } a \in \mathbb{Z} \text{ und } b \in \mathbb{N}\right\}$
- $\mathbb{R} = \{x \mid x \text{ ist reelle Zahl}\}$
- $\emptyset$ bzw. $\{\} \widehat{=}$ leere Menge

Definition 1.3: Teilmenge

Seien M, N Mengen.

1. M heißt **Teilmenge** von N, wenn jedes Element von M auch Element von N ist.
   Notation: $M \subseteq N$
2. M und N heißen gleich, wenn $M \subseteq N$ und $N \subseteq M$ gilt.
   Notation $M = N$
   Falls das nicht gilt, schreiben wir $M \neq N$

M heißt **echte Teilmenge** von N, wenn $M \subseteq N$ und $M \neq N$ gilt.
Notation: $M \subset N$

Nutzt man die Aussagenlogik, kann man diese Definitionen Umformulieren zu:

- $M \subseteq N \iff (\forall x : x \in M \implies x \in N)$
- $M = N \iff (M \subseteq N \land N \subseteq M)$
- $M \subset N \iff (M \subseteq N \land M \neq N)$

Kommentare:

- $\iff$ heißt “genau dann, wenn”
- $\forall$ heißt “für alle”
- $\land$ heißt “und”
- : heißt “mit der Eigenschaft”

Satz 1.4: Für jede Menge M gilt:

1) $M \subseteq M$ 2) $\emptyset \subseteq M$ 3) $M \subseteq \emptyset \implies M = \emptyset$

Beweis:

zu 1) Direkter Beweis (verwenden der Definitionen um Aussage zu folgern). Die Aussage:

$$x \in M \implies x \in M$$

folgt aus Def. 1.1. Daraus folgt aus Def 1.3, 1, dass $M \subseteq M$.

zu 2) Widerspruchsbeweis
Beweis der Aussage durch Annahme des Gegenteils und Herleitung eines Widerspruchs. Annahme: Es existiert eine Menge M, sodass $\emptyset \nsubseteq M$. Dann gilt: es existiert ein $x \in \emptyset$ mit $x \notin M$.

Aber: Die leere Menge enthält keine Elemente $\Longrightarrow \lightning \Longrightarrow$ Es existiert keine Menge M mit $\emptyset \not\subseteq M \Longrightarrow$ Behauptung

zu 3) Nach 2. $\emptyset \subseteq M$, wir wissen $M \subseteq \emptyset$. Nach Def. 1.3, 2 $\Longrightarrow M = \emptyset$

□

Beispiel 1.5: Ob ein Objekt ein Element oder eine Teilmenge einer Mengen ist, ist vom Kontext abhängig. Betrachten wir folgende Menge:

$$M := \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$$

D.h. die Elemente dieser Menge M sind die natürlichen, ganzen, rationalen und reellen Zahlen. Damit gilt $\mathbb{N} \in M$ aber $\mathbb{N} \subset \mathbb{Z}$ und $\mathbb{N} \subset \mathbb{Q}$.

Definition 1.6: Mengenoperationen

Seien M, N Mengen.

1. Man bezeichnet dei Menge der Elemente, die sowhol in M als auch in N enthalten sind, als **Durchschnitt** von M und N
$$M \cap N = \{x \mid (x \in M) \wedge (x \in N)\}$$
2. Man bezeichnet die Menge der Elemente, die entweder in M oder in N enthalten sind oder in beiden enthalten sind, als **Vereinigung** von M und N
$$M \cup N = \{x \mid (x \in M) \vee (x \in N)\}$$
3. Man bezeichnet die Menge der Elemente, die in M aber nicht in N enthalten sind, als **Differenz** von M und N
$$\begin{aligned} M \setminus N &= \{x \mid (x \in M) \wedge (x \notin N)\} \\ &= \{x \in M \mid x \notin N\} \end{aligned}$$

Beispiel 1.7:

Für $-\mathbb{N} := \{-n \mid n \in \mathbb{N}\}$ gilt:

- $\mathbb{N} \cup -\mathbb{N} = \mathbb{Z} \setminus \{0\}$
- $\mathbb{N} \cap -\mathbb{N} = \emptyset$

Wichtiges Beispiel für Mengen sind Intervalle reeller Zahlen

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

Dies nennt man ein abgeschlossenes Intervall (die Grenzen sind enthalten). Sei jetzt $a, b \in \mathbb{R}, a \leq b$

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

Diese Intervalle nennt man halboffene Intervalle (genau eine der Grenzen ist enthalten). Das Intervall

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

heißt offenes Intervall (keine der Grenzen ist enthalten).

Für $M := \{4, 6, 8\}$ und $N := \{8, 10\}$ gilt:

- $M \cup N = \{4, 6, 8, 10\}$
- $M \cap N = \{8\}$
- $M \setminus N = \{4, 6\}$
- $N \setminus M = \{10\}$

Satz 1.8: Für zwei Mengen M, N gelte $M \subseteq N$. Dann sind folgende Aussagen Äquivalent:

$$1)\ M \subset N \qquad\qquad 2)\ N \setminus M \neq \emptyset$$

Beweis:

Behauptung: $1) \iff 2)$

zu zeigen: $1) \implies 2)$ und $2) \implies 1)$

$1) \implies 2)$: Es gilt: $M \neq N$. Dann existiert $x \in N$ mit $x \notin M$. Dann gilt $x \in N \setminus M$. Also $N \setminus M \neq \emptyset$.

$2) \implies 1)$: Es gilt $N \setminus M \neq \emptyset$. Dann existiert ein $x \in N$ mit $x \notin M$. Daher gilt $N \neq M$. Es gilt außerdem: $M \subseteq N$. Daraus folgt $M \subset N$.

□

Satz 1.9: Seien M, N, L Mengen. Dann gelten Folgende Aussagen:

1. $M \cap N \subseteq M$ und $M \subseteq M \cup N$
2. $M \setminus N \subseteq M$
3. Kommutativgesetze:
$$M \cap N = N \cap M \text{ und } M \cup N = N \cup M$$
4. Assoziativgesetze:
$$M \cap (N \cap L) = (M \cap N) \cap L$$
$$M \cup (N \cup L) = (M \cup N) \cup L$$
5. Distributivgesetze:
$$M \cup (N \cap L) = (M \cup N) \cap (M \cup L)$$
$$M \cap (N \cup L) = (M \cap N) \cup (M \cap L)$$
$$M \setminus (N \cap L) = (M \setminus N) \cup (M \setminus L)$$
$$M \setminus (N \cup L) = (M \setminus N) \cap (M \setminus L)$$

Beweis: Es gilt $x \in M \cap N$ genau dann, wenn $x \in M \wedge x \in N$. Die Konjunktion zweier Aussagen ist symmetrisch bezüglich der Aussage. D.h. $A \wedge B \iff B \wedge A$. Es gilt also

$$(x \in M) \wedge (x \in N) \iff (x \in N) \wedge (x \in M)$$

Verwenden wir die Definition der Schnittmenge (1.6) so erhalten wir

$$(x \in N) \wedge (x \in M) \iff x \in N \cap M$$

Aus der Kette der Äquivalenzumformungen folgt $M \cap N = N \cap M$.

□

Etwas kompakter für das erste Distributivgesetz:

$$\begin{aligned} x \in M \cup (N \cap L) &\iff (x \in M) \vee (x \in N \cup L) \\ &\iff (x \in M) \vee ((x \in N) \wedge (x \in L)) \\ &\iff (x \in M \vee x \in N) \wedge (x \in M \vee x \in L) \\ &\iff (x \in M \cup N) \wedge (x \in M \cup L) \\ &\iff x \in (M \cup N) \cap (M \cup L) \end{aligned}$$

Damit ist $M \cup (N \cap L) = (M \cup N) \cap (M \cup L)$.

□

Die übrigen Aussagen zeigt man analog. *Übung*

Damit ist $M \cup N \cup L$ für die Mengen M, N, L wohldefiniert. Dies kann auf "viele" Mengen verallgemeinert werden:

Ist $I \neq \emptyset$ eine Menge und ist für jedes $i \in I$ eine Menge M_i gegeben, dann sind:

$$\bigcup_{i \in I} M_i := \{x \mid \exists i \in I \text{ mit } x \in M_i\}$$

$$\bigcap_{i \in I} M_i := \{x \mid \forall i \in I \text{ mit } x \in M_i\}$$

Die Menge I heißt auch **Indexmenge**. Für $I = \{1, ..., n\}$ verwendet man auch die Notation

$$\bigcup_{i=1}^{n} M_i := \{x \mid \exists i \in I \text{ mit } x \in M_i\}$$

$$\bigcap_{i=1}^{n} M_i := \{x \mid \forall i \in I \text{ mit } x \in M_i\}$$

Definition 1.10: Kardinalität, Potenzmenge

Sei M eine endliche Menge, d.h. M enthält endlich viele Elemente.

Die **Mächtigkeit** oder **Kardinalität** von M, bezeichnet mit $|M|$ oder $\#M$ ist die Anzahl von Elementen in M.

Die **Potenzmenge** von M, bezeichnet mit $\mathcal{P}(M)$ ist die Menge aller Teilmengen von M. D.h.

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Beispiel 1.11:

Die leere Menge $\emptyset$ hat die Kardinalität Null. Es gilt $\mathcal{P}(\emptyset) = \{\emptyset\}, |\mathcal{P}(\emptyset)| = 1$.

Für $M = \{2, 4, 6\}$ gilt $|M| = 3$. $\mathcal{P}(M) = \{\emptyset, \{2\}, \{4\}, \{6\}, \{2, 4\}, \{2, 6\}, \{4, 6\}, \{2, 4, 6\}\}$.

Man kann zeigen: $|\mathcal{P}(M)| = 2^{|M|}$. Deswegen wird auch die Notation 2^M für die Potenzmenge von M verwendet.

1.2. Relationen

Definition 1.12: Kartesisches Produkt

Sind M und N zwei Mengen, so heißt die Menge

$$M \times N := \{(x, y) \mid x \in M \wedge y \in N\}$$

das **kartesische Produkt** von M und N.

Sind n Mengen $M_1, ..., M_n$ gegeben, so ist deren kartesisches Produkt gegeben druch:

$$M_1 \times ... \times M_n := \{(x_1, ..., x_n) \mid x_1 \in M_1 \wedge ... \wedge x_n \in M_n\}$$

Das n-fache kartesische Produkt einer Menge von M ist:

$$M^n := M \times ... \times M := \{(x_1, ..., x_n) \mid x_i \in M \text{ für } i = 1, ..., n\}$$

Ein Element $(x, y) \in M \times N$ heißt geordnetes Paar und eine Element $(x_1, ..., x_n) \in M_1 \times ... \times M_n$ heißt **(geordnetes) n-Tupel**.

Ist mindestens eine der auftretenden Mengen leer, so ist auch das resultierende kartesische Produkt leer, d.h. die leere Menge. Das kartesische Produkt wurde nach Rene Decartes benannt. Rene Decartes war ein französische Mathematiker (1596-1650) und ein Begründer der analytischen Geometrie.

Beispiel 1.13: Das kartesische Produkt zweier Intervalle.

Seien $[a, b] \subset \mathbb{R}$ und $[c, d] \subset \mathbb{R}$ zwei abgeschlossene Intervalle von reellen Zahlen. Dann ist das kartesische Produkt beider Intervalle gegeben durch:

$$[a, b] \times [c, d] := \{(x, y) \mid x \in [a, b] \wedge y \in [c, d]\}$$

Das kartesische Produkt ist nicht kommutativ. Beweis durch Gegenbeispiel.

Definition 1.14: Relationen

Seien M und N nichtleere Mengen. Eine Menge $R \subseteq M \times N$ heißt **Relation** zwischen M und N. Ist $M = N$, so nennt man R **Relation auf** M. Für $(x, y) \in R$ schreibt man $x \sim_R y$ oder $x \sim y$, wenn die Relation aus dem Kontext klar ist. Ist mindestens eine der beiden Mengen leer, dann ist auch jede Relation zwischen den beiden Mengen die leere Menge.

Beispiel 1.15: Sei $M = \mathbb{N}$ und $N = \mathbb{Z}$. Dann ist

$$R := \{(x, y) \in M \times N \mid x + y = 1\}$$

eine Relation zwischen M und N. Es gilt

$$R = \{(1,0),(2,-1),(3,-2),...\} = \{(n,-n+1) \mid n \in \mathbb{N}\}$$

Definition 1.16: reflexiv, symmetrisch, antisymmetrisch, transitiv

Es sei M eine nicht leere Menge. Eine Relation auf M heißt:

1. **reflexiv:**
$$\forall x \in M : x \sim x$$
2. **symmetrisch:**
$$\forall x, y \in M : x \sim y \Longrightarrow y \sim x$$
3. **antisymmetrisch:**
$$\forall x, y \in M : x \sim y \wedge y \sim x \Longrightarrow x = y$$
4. **transitiv:**
$$\forall x, y, z \in M : x \sim y \wedge y \sim z \Longrightarrow x \sim z$$

Falls die Relation R reflexiv, transitiv und symmetrisch ist, so nennt man R eine **Äquivalenzrelation** auf M. Ist R reflexiv, transitiv und antisymmetrisch, so nennt man R eine **partielle Ordnung** auf M.

Beispiel 1.17: $M = \mathbb{R}$

- Die Relation $<$ auf $M = \mathbb{R}$ ist transitiv, aber weder reflexiv noch symmetrisch und auch nicht antisymmetrisch.
- Die Relation $\leq$ auf $M = \mathbb{R}$ ist reflexiv, antisymmetrisch und transitiv. Sie ist nicht symmetrisch. $\leq$ ist somit eine partielle Ordnung.
- Die Relation $=$ auf $\mathbb{R}$ ist reflexiv, symmetrisch und transitiv. Also ist $=$ eine Äquivalenzrelation. (Äquivalenzrelationen können auch antisymmetrisch sein)

Beispiel 1.18: Interpretiert man "Pfeile" als Objekte mit gleicher Orientierung und Länge, erhält man die Äquivalenzrelation

$$x \sim y :\Longleftrightarrow x \text{ und } y \text{ haben die gleiche Länge und Orientierung}$$

Auf Grund der Transitivität sind somit alle Pfeile einer vorgegebenen Orientierung und Länge äquivalent zu dem Pfeil, der im Koordinatenursprung startet und die gleiche Länge sowie Orientierung besitzt. Somit können wir Vektor $x = (x_1, x_2) \in \mathbb{R}^2$ als Repräsentant einer ganzen Klasse von Pfeilen interpretieren. Alle zueinander äquivalente Pfeile haben gemeinsam, dass die Differenz zwischen End- und Anfangspunkt genau den Vektor x ergeben.

Als Formalisierung erhält man:

Definition 1.19: Äquivalenzklassen, Quotientenmenge

Sei $\sim$ eine Äquivalenzrelation auf einer nichtleeren Menge M. Die Äquivalenzklasse eines Element $\overline{a} \in M$ ist definiert durch:

$$[\overline{a}] := \{a \in M \mid a \sim \overline{a}\}$$

Ist die Relation nicht aus dem Kontext klar, schreibt man $[\overline{a}]_{\sim}$.

Elemente einer Äquivalenzklasse werden als **Vertreter** oder **Repräsentanten** der Äquivalenzklasse bezeichnet. Die Menge aller Äquivalenzklassen einer Äquivalenzrelation $\sim$ in einer Menge M, d.h.

$$M/\sim := \left\{[a]_{\sim} \mid a \in M\right\}$$

wird als **Faktormenge** oder **Quotientenmenge** bezeichnet.

Beispiel 1.20: *(Vortsetzung von Beispiel 1.18)*

Die Menge aller Pfeile gleicher Länge und Orientierung bilden eine solche Äquivalenzklasse, welche durch den Vektor $x = (x_1, x_2) \in \mathbb{R}^2$ repräsentiert wird. Die Menge der Vektoren $x = (x_1, x_2) \in \mathbb{R}^2$ bilden die Quotientenklasse.

Beispiel 1.21: Für eine gegebene Zahl $x \in \mathbb{N}$ ist die Menge:

$$R_n := \left\{(a, b) \in \mathbb{Z}^2 \mid a - b \text{ ist ohne Rest durch } n \text{ teilbar}\right\}$$

eine Äquivalenzrelation auf $\mathbb{Z}$, denn

- reflexiv: $a \sim a, (a, a) \in R_n :\Longleftrightarrow a - a = 0$ ✓
- symmetrie:

  $a \sim b \Longrightarrow (a, b) \in R_n \Longrightarrow a - b$ ist ohne Rest teilbar $\Longrightarrow a - b = k \cdot n$

  $\Longrightarrow b - a = -k \cdot n \Longrightarrow (b, a) \in R_n \Longrightarrow b \sim a$ ✓
- transitiv: zz: $a \sim b \wedge b \sim c \Longrightarrow a \sim c$

  $$a \sim b \Longrightarrow a - b = k \cdot n$$
  $$b \sim c \Longrightarrow b - c = l \cdot n$$

  Gleichungen addieren: $a - c = n(k + l) \Longrightarrow a \sim c$ ✓

Für a wird die Äquivalenzklasse $[a]$ auch die Restklasse von a modulo n genannt.

$$[a] = a + n \cdot z = \{a + nz \mid z \in \mathbb{Z}\}$$

Die Äquivalenzrelation R_n definiert auch eine Zerlegung der Menge $\mathbb{Z}$ in disjunkte Teilmengen, nähmlich

$$[0] \cup [1] \cup \ldots \cup [n-1] = \bigcup_{a=0}^{n-1} [a] = \mathbb{Z}$$

Es gilt allgemein: Ist $\sim$ eine Äquivalenzrelation auf M, so ist M die Vereinigung aller Äquivalenzklassen.

- "$\subseteq$":

$$M = \bigcup_{a \in M} \{a\} \subseteq \bigcup_{a \in M} [a] \checkmark$$

- "$\supseteq$":

$$[a] \subset M \Longrightarrow \bigcup_{a \in M} [a] \subseteq M \checkmark$$

□

Satz 1.22: Ist R eine Äquivalenzrelation auf der Menge M und sind $a, b \in M$, dann sind folgende Aussagen äquivalent:

$$1)\ [a] = [b] \qquad 2)\ [a] \cap [b] \neq \emptyset \qquad 3)\ a \sim b$$

Beweis: Durch Ringschluss

zu zeigen: $1 \Longrightarrow 2, 2 \Longrightarrow 3, 3 \Longrightarrow 1$

$1 \Longrightarrow 2$:

$$\text{Wegen } a \sim a \Longrightarrow a \in [a] = [b] \Longrightarrow a \in [a] \cap [b] \Longrightarrow [a] \cap [b] \neq \emptyset$$

$2 \Longrightarrow 3$:

Aus $[a] \cap [b] \neq \emptyset \Longrightarrow$ es existiert $c \in [a] \cap [b]$. Nach Definition gilt dann $c \sim a$ wegen der Symmetrie von $a \sim c$. Nach Definition auch $c \sim b$. Wegen der Transitivät der Relation gilt dann auch $a \sim b$

$3 \Longrightarrow 1$:

Es gilt $a \sim b$. Sei $c \in [a] \Longrightarrow c \sim a$. Wegen der Transitivät folgt $c \sim b \Longrightarrow c \in [b] \Longrightarrow [a] \subseteq [b]$. Analog folgt $[b] \subseteq [a]$.

□

Aus Satz 1.22 2) folgt, dass die Äquivalenzklassen eine disjunkte Zerlegung der Menge M darstellen.

Definition 1.23:

Sei M eine Menge und sei für jedes Element $m \in M$ eine weitere Menge S_m gegeben. Für $\mathcal{S} := \{S_m \mid m \in M\}$ ist die Teilmengenrelation $\subseteq$ eine partielle Ordnung. Die Menge $\mathcal{S}$ heißt dann **partiell geordnet**. Eine Menge $\hat{S} \in \mathcal{S}$ heißt **maximales Element** von $\mathcal{S}$ (bezüglich $\subseteq$), wenn aus $S \in \mathcal{S}$ und $\hat{S} \in \mathcal{S}$ folgt, dass $S = \hat{S}$ ist. Eine nichtleere Teilmenge $\mathcal{K} \subseteq \mathcal{S}$ heißt **Kette** (bezüglich $\subseteq$), wenn für alle $K_1, K_2 \in \mathcal{K}$ gilt, dass $K_1 \subseteq K_2$ oder $K_2 \subseteq K_1$. Ein Element $\widehat{K} \in \mathcal{S}$ heißt **obere Schranke** der Kette $\mathcal{K}$, wenn $K \subseteq \widehat{K}$ für alle $K \in \mathcal{K}$ gilt.

Beispiel 1.24: Sei $\mathcal{S} = P(\{2, 4, 6, 8, 10\})$

Dann ist

$$\mathcal{K} = \{\emptyset, \{2\}, \{2, 6\}, \{2, 6, 10\}\} \subseteq \mathcal{S}$$

Die Menge $K = \{2, 6, 10\}$, das maximale Elemnt von $\mathcal{S}$ ist $\hat{S} = \{2, 4, 6, 8, 10\}$.

Gibt es immer ein maximales Element?

Lemma 1.25: Zornsche Lemma

Sei M eine Menge und sei $\mathcal{S} \subseteq \mathcal{P}(M)$ eine nichtleere Menge mit der Eigenschaft, dass für jede Kette $\mathcal{K} \subseteq \mathcal{S}$ auch ihre Vereinigunsmenge in $\mathcal{S}$ liegt, d.h.

$$\bigcup_{A \in \mathcal{K}} A \in \mathcal{S}$$

Dann besitzt $\mathcal{S}$ ein maximales Element.

Beweis: Das Zornsche Lemma ist ein fundamentales Resultat aus der Mengenlehre, hier ohne Beweis

□

Lemma 1.26: Sei M eine Menge und $\mathcal{K} \subseteq \mathcal{P}(M)$ eine Kette. Dann gibt es zu je endlich vielen $A_1, ..., A_n \in \mathcal{K}$ ein $\hat{i} \in \{1, ..., n\}$ mit $A_i \subseteq A_{\hat{i}}$ für alle $i \in \{1, ..., n\}$.

Beweis: Durch vollständige Induktion über n.

Induktionsanfang: n = 1

D.h. wir haben $A_1 \in \mathcal{K}$ und für $\hat{i} = 1$ gilt $A_1 \subseteq A_{\hat{i}} = A_1$ ✓

Induktionsschritt: $n - 1 \mapsto n$

Für $A_1, ..., A_{n-1} \in \mathcal{K}$ exisitert ein $\hat{j} \in \{1, ..., n-1\}$ mit $A_i \subseteq A_{\hat{j}}$ für alle $i \in \{1, ..., n-1\}$. Mit

$$\hat{i} := \begin{cases} \hat{j} \text{ für } A_n \subseteq A_{\hat{j}} \\ n \text{ für } A_{\hat{j}} \subseteq A_n \end{cases}$$

folgt die Behautpung.

□

1.3. Abbildungen

Definition 1.27: Abbildungen

Es Seien X und Y beliebig, nichtleere Mengen. Eine **Abbildung** von X nach Y ist eine Vorschrift f, die jedem Element $x \in X$ genau ein Element $f(x) \in Y$ zuordnet. Man schreibt

$$f : X \to Y, \ x \mapsto y = f(x)$$

Die Menge X heißt **Definitionsbereich** von f, die Menge Y heißt **Wertebereich** von f

Achtung: Jede Abbildung besteht aus drei "Teilen". Angabe des Definitionsbereichs, Angabe des Wertebereichs, Angabe der Zuordnungsvorschrift.

Beispiel 1.28: Sei M eine nichtleere Menge. Dann ist

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

eine Abbildung f **Identität** von M mit der Notation I_m/Id_m.

Sei $X = Y = \mathbb{R}$, dann ist $f : \mathbb{R} \to \mathbb{R},\ x \mapsto f(x) := 7x + 2$ eine Abbildung.

Definition 1.29: Bild, Urbild

Seien X, Y beliebige nichtleere Mengen und $f : X \to Y$. Es gelte $M \subseteq X$ und $N \subseteq Y$. Dann heißen die Mengen:

$$f(M) := \{f(x) \in Y \mid x \in M\} \subseteq Y \text{ das } \textbf{Bild} \text{ von } M \text{ unter } f.$$
$$f^{-1}(N) := \{x \in X \mid f(x) \in N\} \subseteq X \text{ das } \textbf{Urbild} \text{ von } N \text{ under } f.$$

Ist $\emptyset \neq M \subseteq X$, dann heißt $f_{|M} : M \to Y,\ x \mapsto f(x)$, die **Einschränkung** von f auf M.

Beispiel 1.30: Sei $X = Y = \mathbb{R}$ und $x \mapsto f(x) = x^4$. Dann ist $\mathbb{R}$ Definitions- und Wertebereich von f.

- $f(\mathbb{R}) = \mathbb{R}_+ := [0, \infty[$ das Bild von f
- $f([0, 2]) = [0, 16]$
- $f^{-1}([16, 81]) = [-3, -2] \cup [2, 3]$ das Urbild des Intervalls $[16, 81]$ unter f.

Definition 1.31: injektiv, surjektiv, bijektiv

Seien X, Y zwei beliebige, nichtleere Mengen und $f : X \to Y$ eine Abbildung. Dann heißt f:

- **injektiv:** falls für alle $x, \tilde{x} \in X$ gilt:
$$f(x) = f(\tilde{x}) \Longrightarrow x = \tilde{x}$$
- **surjektiv:** falls für jedes $y \in Y$ gilt:
$$\exists\, x \in X : f(x) = y$$
- **bijektiv:** falls f injektiv und surjektiv ist

Man kann sich anhand der Definition leicht überlegen, dass eine Abbildung $f : X \to Y$ genau dann bijektiv ist, wenn es für jedes $y \in Y$ genau ein $x \in X$ gibt, sodass $f(x) = y$ gilt.

Beispiel 1.32: Betrachte die Funktion $f : \mathbb{R} \to \mathbb{R},\ x \mapsto \max(0, x)$

- $f : \mathbb{R} \to \mathbb{R}$, f ist weder injektiv noch surjektiv
- $f : \mathbb{R} \to \mathbb{R}_+$, f ist surjektiv, aber nicht injektiv
- $f : \mathbb{R}_+ \to \mathbb{R}_+$, f ist injektiv aber nicht surjektiv
- $f : \mathbb{R}_+ \to \mathbb{R}_+$, f ist bijektiv

Definition 1.33: Komposition

Seien X, Y, Z nichtleere Mengen und die Abbildungen $f : X \to Y,\ x \mapsto f(x)$ sowie $g : Y \to Z,\ y \mapsto g(y)$ gegeben. Dann ist die **Komposition** oder **Hintereinanderausführung** von f und g die Abbildung

$$g \circ f : X \to Z,\ x \mapsto g(f(x)) \in Z$$

Satz 1.34: Seien W, X, Y und Z nichtleere Mengen, und die Abbildungen $f : W \to X$, $g : X \to Y$, $h : Y \to Z$ gegeben. Dann gilt:

1. $h \circ (g \circ f) = (h \circ g) \circ f$, d.h. die Komposition von Abbildungen ist Assoziativ
2. Sind beide Abbildungen f und g injektiv/surjektiv/bijektiv, dann ist auch die Komposition $g \circ f$ injektiv / surjektiv / bijektiv.
3. Ist $g \circ f$ injektiv, dann ist f injektiv
4. Ist $g \circ f$ surjktiv, dann ist g surjektiv

Beweis: (Übungsaufgabe)

1. $h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$
2. Für jedes $x_1, x_2 \in X$ folgt aus g injektiv: $g(f(x_1)) = g(f(x_2)) \implies f(x_1) = f(x_2)$. Aus f injektiv folgt widerum: $f(x_1) = f(x_2) \implies x_1 = x_2$. Also gilt $g(f(x_1)) = g(f(x_2)) \implies x_1 = x_2$. Somit ist $g \circ f$ injektiv.

   Für jedes $z \in Z$ folgt aus g surjektiv: $\exists\, y \in Y : f(y) = z$. Für jedes $y \in Y$ folgt aus f surjektiv widerium: $\exists\, x \in X : f(x) = y$. Also folgt $\forall\, z \in Z\, \exists\, x \in X : g(f(x)) = z$. Somit ist $g \circ f$ surjektiv.

   Sind f und g bijektiv, folgt aus den obigen Beweisen, dass $g \circ f$ injektiv und surjektiv ist. Somit ist $g \circ f$ auch bijektiv.
3. Ist f nicht injektiv, dann existieren $x_1, x_2 \in X$ mit $f(x_1) = f(x_2)$ aber $x_1 \neq x_2$. Wegen $g \circ f$ injektiv gilt $g(f(x_1)) = g(f(x_2)) \implies x_1 = x_2$. Damit $g(f(x_1)) = g(f(x_2))$ gilt, muss auch $f(x_1) = f(x_2)$ gelten, dann gilt aber auch $f(x_1) = f(x_2) \implies x_1 = x_2$. Dies ist ein Widerspruch $\lightning$. f ist also injektiv.
4. Ist g nicht surjektiv, dann existiert ein $z \in Z$ für das kein $y \in Y$ mit $g(y) = z$ existiert. Wegen $g \circ f$ surjektiv gilt $\forall\, z \in Z\, \exists\, x \in X : g(f(x)) = z$. Dann gilt auch $g(f(x)) = g(y) = z,\ y \in Y$, also existiert ein $y \in Y$ mit $g(y) = z$. Dies ist ein Widerspruch $\lightning$. Also ist g surjektiv.

□

Satz 1.35: Seien X, Y nichtleere Mengen und $f : X \to Y$ eine Abbildung. Die Abbildung ist genau dann bijektiv, wenn es eine Abbildung $g : Y \to X$ existiert, so dass $g \circ f = \mathrm{Id}_X$ und $f \circ g = \mathrm{Id}_Y$ gilt.

Beweis:

"$\implies$"

Zu jedem $y \in Y$ existiert genau ein $x_y \in X$ mit $f(x_y) = y$. Damit kann man eine Abbildung g definieren durch:

$$g : Y \to X,\ g(y) = x_y$$

Für $y \in Y$ folgt dann $(f \circ g)(y) = f(g(y)) = f(x_y) = y \Longrightarrow f \circ g = \mathrm{Id}_Y$. Sei $x \in X \Longrightarrow f(x) = y \in Y$. Wegen der Bijektivität von f folgt $x = x_y \in X$

Dann gilt:

$$(g \circ f)(x) = g(f(x)) = g(y) = x_y = x \Longrightarrow g \circ f = \mathrm{Id}_X$$

"$\Longleftarrow$":

Es gilt: $g \circ f = \mathrm{Id}_X, \mathrm{Id}_X$ ist injektiv. Wegen Satz 1.34, 3) ist dann auch f injektiv. Des weiteren gilt $f \circ g = \mathrm{Id}_Y$ ist surjektiv. Wegen 1.34, 4) ist dann auch f surjektiv $\Longrightarrow f$ ist bijektiv

Frage: Gibt es eine weitere Abbildung, $\tilde{g} : Y \to X$ mit den gleichen Eigenschaften wie im letzten Satz? Wegen Satz 1.34, 1) gilt:

$$\tilde{g} = \mathrm{Id}_X \circ \tilde{g} = (g \circ f) \circ \tilde{g} = g \circ (f \circ \tilde{g}) = g \circ \mathrm{Id}_Y = g$$

Definition 1.36: inverse Abbildung / Umkehrabbildung

Seien X, Y zwei nichtleere Mengen und $f : X \to Y$ eine Abbildung. Ist f bijektiv, dann heißt die in Satz 1.35 definierte, eindeutige Abbildung $g : Y \to X$ **inverse Abbildung** oder **Umkehrabbildung** von f und wird f^{-1} bezeichnet.

Beispiel 1.37: Die Abbildung $f : \mathbb{R} \to \mathbb{R},\ f(x) = 3x - 5$ ist bijektiv. Die zu f inverse Abbildung erhält man durch Umformung.

$$y = 3x - 5 \Longleftrightarrow y + 5 = 3x \Longleftrightarrow x = \frac{1}{3}(y + 5)$$

Also $f^{-1} : \mathbb{R} \to \mathbb{R},\ y \mapsto \frac{1}{3}(y + 5)$

Achtung: $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$ ist nicht bijektiv.

$$\tilde{f} : \mathbb{R} \to \mathbb{R}_+,\ \tilde{f}(x) = x^2 \qquad \tilde{f}^{-1}(y) = \sqrt{y}$$

Achtung: Die Notation f^{-1} ist doppelt Belegt! Zum einen für die Notation der Umkehrabbildung und zum Anderen für die Notation des Urbilds.

Satz 1.38: Seien X, Y und Z nichtleere Mengen und die Abbildungen $f : X \to Y$ sowie $g : Y \to Z$ bijektiv.

Dann gilt:

1. f^(-1) ist bijektiv $\qquad \left(f^{(-1)^{-1}}\right) = f$
2. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Beweis: (1. Übungsaufgabe)

1.
$$\begin{aligned} f &= f \circ \mathrm{Id}_X \\ &= f \circ \left(f^{-1} \circ (f^{-1})^{-1} \right) \\ &= (f \circ f^{-1}) \circ (f^{-1})^{-1} \\ &= \mathrm{Id}_Y \circ (f^{-1})^{-1} \\ &= (f^{-1})^{-1} \end{aligned}$$

2. Aus Satz 1.34 folgt, dass $g \circ f$ bijektiv ist. $\Longrightarrow (g \circ f)^{-1}$ existiert und ist eindeutig bestimmt. Es gilt
$$\begin{aligned} (f^{-1} \circ g^{-1}) \circ (g \circ f) & \\ &= f^{-1} \circ ((g^{-1} \circ g) \circ f) \\ &= f^{-1} \circ (\mathrm{Id}_Y \circ f) \\ &= f^{-1} \circ f = \mathrm{Id}_X \end{aligned}$$
Analgog ziegt man: $(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{Id}_Y$
$$\Longrightarrow (g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

□

2. Algebraische Strukturen

Algebraische Strukturen sind Mengen und Verknüpfungen, die auf den Elementen der Menge definiert sind. Ein Beispiel dafür ist die Menge aller ganzen Zahlen mit der Addition als Verknüpfung.

Algebraische Strukturen besitzen wichtige Eigenschaften:

- Die Summe zweier ganzer Zahlen ist wieder eine ganze Zahl $\widehat{=}$ Abgeschlossenheit der Menge bezüglich der Verknüpfung
- Es gibt die ganze Zahl 0, sodass für jede ganze Zahl $a \in \mathbb{Z}$ gilt: $0 + a = a$. Dieses Element nennt man das neutrale Element
- Für jede ganze Zahl $a \in Z$ gibt es ein $-a \in \mathbb{Z}$, sodass gilt: $(-a) + a = 0$. Dieses Element nennt man das inverse Element von a

Algebraische Strukturen erlauben es uns, abstrakte Konzepte aus konkreten Beispielen zu extrahieren und später komplexe Zusammenhänge mit diesen Konzepten zu analysieren und Stück für Stück zu erweitern.

2.1. Gruppen

Definition 2.1: innere Verknüpfung, Halbgruppe

Sei M eine nichtleere Menge. Eine Abbildung $\circ : M \times M \to M,\ (a, b) \mapsto a \circ b$ heißt **(innere) Verknüpfung** auf M. Gilt: $(a \circ b) \circ c = a \circ (b \circ c)$, dann heißt die Verknüpfung **assoziativ** und $(M, \circ)$ eise **Halbgruppe**. Gilt für eine Halbgruppe, dass $a \circ b = b \circ a$, so heißt die Halbgruppe **abelsch** oder **kommutativ**.

Je nach Kontext kann die Notation einer Verknüpfung variieren. ($a \circ b$, $a \cdot b$, ab)

Beispiel 2.2:

- $(\mathbb{N}, +)$ und $(\mathbb{N}, *)$ sind kommutative Halbgruppen
- Sei X eine nichtleere Menge. Dann ist $M := \mathrm{Abb}(X, X)$ $= \{\text{Abbildungen } f : X \to X\}$ eine Halbgruppe mit der Verknüpfung $\circ$ als Komposition von Abbildungen (Def. 1.33). Diese Halbgruppe ist nicht abelsch.

  Beweis durch Gegenbeispiel:

  Sei $a, b, c \in X, a \neq b, a \neq c, b \neq c$. Definiere $f, g \in M$ mit

$$f(x) := \begin{cases} b \text{ für } x = a \\ a \text{ für } x = b \\ x \text{ sonst} \end{cases} \qquad g(x) := \begin{cases} c \text{ für } x = a \\ a \text{ für } x = c \\ x \text{ sonst} \end{cases}$$

Dann folgt:

$$(f \circ g)(a) = f(g(a)) = f(c) = c$$
$$(g \circ f)(a) = g(f(a)) = g(b) = b$$
$$\checkmark$$

Die Halbgruppe ist ein relativ "schwaches" Konzept. Deswegen braucht man weitere Eigenschaften:

Definition 2.3: neutrales Element

Sei M eine nichtleere Menge und $\circ$ eine innere Verknüpfung auf M. Existiert ein Element $e \in M$ mit

$$a \circ e = e \circ a = a \qquad \forall\, a \in M$$

so heißt e **neutrales Element** für die Verknüpfung $\circ$.

Eine Halbgruppe, die ein neutrales Element besitzt heißt **Monoid**.

Beispiel 2.24: Kein Monoid

Gegeben sei die Menge $M = \{a, b\}$ und die folgende Verknüfung

$\circ$	a	b
a	a	b
b	a	b

Mann kann nachrechenen, dass $(M, \circ)$ eine Halbgruppe ist. Mann kann auch prüfen, dass a linksneutral aber nicht rechtsneutral ist, sowie dass b rechtsneutral aber nicht linksneutral ist. Somit besitzt die Halbgruppe kein neutrales Element, $(M, \circ)$ ist also kein Monoid.

Bemerkung: In der Definition eines Monoids wird nur die Existens aber nicht die Eindeutigkeit des neutralen Elements gefordert. Ist dies sinnvoll?

Lemma 2.5: Sei $(M, \circ)$ ein Monoid und $e_1, e_2 \in M$ neutrale Elemente, dann gilt

$$e_1 = e_2$$

Beweis:

$$\begin{aligned} e_1 &= e_1 \circ e_2 \\ &= e_2 \end{aligned}$$

□

Beispiel 2.6:

- $(\mathbb{N}, +)$ ist kein Monoid, da kein neutrales Element existiert ($0 \notin \mathbb{N}$ in LinA)
- $(\mathbb{N}, \cdot)$ ist ein Monoid mit dem neutralen Element $e = 1$
- Für $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ ist $(\mathbb{N}_0, +)$ ein Monoid mit dem neutralen Element $e = 0$

Definition 2.7: Gruppen

Ein Monoid $(M, \circ)$ ist eine **Gruppe**, wenn für jedes $a \in M$ ein $b \in M$ existiert, so dass

$$a \circ b = b \circ a = e$$

wobei e das neutrale Element des Monoids ist. Wir nennen b das **inverse Element** zu dem gegebenen Element a und bezeichnen es mit $a^{-1} = b$.

Bemerkung: Für $\circ = +$, d.h. additiv geschriebene Gruppen schreibt man auch $-a := b$.

Beispiel 2.8:

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind kommutative Gruppen
- $(\mathbb{N}, +)$ ist keine Gruppe, da kein neutrales Element und keine inversen Elemente existieren
- Rechnen mit binären Zahlen

  Betrachtet wird $\mathbb{F}_2 = \{0, 1\}$ und die Verknüpfungen

$+$	0	1
0	0	1
1	1	0

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

  Anhand der Verknüpfungstabellen erkennt man, dass $(\mathbb{F}_2, +)$ mit dem neutralen Element $e = 0$ eine abelsche Gruppe ist. Jedoch ist $(\mathbb{F}_2, \cdot)$ keine Gruppe, da zwar ein neutrales Element $e = 1$, aber das Element 0 kein inverses Element besitzt.

Satz 2.9: Sei $(M, \circ)$ eine Gruppe, dann gilt:

1. Es gibt **genau ein** neutrales Element in M.
2. Jedes Element der Menge M besitzt **genau ein** inverses Element.
3. Jedes linksinverse Element ist gleichzeitig auch rechtsinvers.
4. Jedes linksneutrale Element ist gleichzeitig auch rechtsneutral.

Beweis:

1. Folgt aus Lemma 2.5, da $(M, \circ)$ nach Definition ein Monoid ist.
2. Annahme: Seien $b \in M$ und $\tilde{b} \in M$ inverse Elemente zu $a \in M$.

   zu zeigen: $z = \tilde{z}$

   Dann gilt:

$$\begin{aligned} b &= b \circ e \\ &= b \circ \left(a \circ \tilde{b}\right) \\ &= (b \circ a) \circ \tilde{b} \\ &= e \circ \tilde{b} \\ &= \tilde{b} \end{aligned}$$

3. Es sei $b \in M$ ein linksinverses Element zu $a \in M$. D.h. $b \circ a = e$. Sei $\tilde{b} \in M$ ein linksneutrales Element zu $b \in M$. D.h. $\tilde{b} \circ b = e$.

$$\begin{aligned} a \circ b &= e \circ (a \circ b) \\ &= \tilde{b} \circ b \circ (a \circ b) \\ &= \tilde{b} \circ (b \circ a) \circ b \\ &= \tilde{b} \circ e \circ b \\ &= \tilde{b} \circ b \\ &= e \end{aligned}$$

4. Es gelte $e \circ a = a$ und $b \circ a = a \circ b = e$

   Dann gilt: $(a \circ b) \circ a = a \circ (b \circ a) = a \circ e = a$ ✓

Lemma 2.10: Sei $(M, \circ)$ eine Gruppe. Gilt für ein $a \in M$, dass $c \circ a = a$ für ein $c \in M$; dann ist c das neutrale Element der Gruppe.

Beweis: Sei e das neutrale Element (es gibt genau 1) der Gruppe $(M, \circ)$ und für $a, c \in M$ gelte: $c \circ a = a$. Sei b das inverse Element zu a.

$$\begin{aligned} c &= c \circ e \\ &= c \circ (a \circ b) \\ &= (c \circ a) \circ b \\ &= a \circ b \\ &= e \end{aligned}$$

□

Besonders wichtig in der linearen Algebra sind Abbildungen zwischen Gruppen, die bezüglich der Verknüpfung "kompatibel" sind.

Definition 2.11: Homomorphismus

Seien $(M, \circ)$ und $(N, \oplus)$ Gruppen. Eine Abbildung $f : M \to N$ heißt **Homomorphismus** (oder **Gruppenhomomorphismus**) falls:

$$f(x \circ y) = f(x) \oplus f(y) \qquad \forall\, x, y \in M$$

Ein Homomorphismus heißt **Isomorphismus**, wenn er bijektiv ist.

Beispiel 2.12: Die Abbildung $f : \mathbb{R} \to \mathbb{R}_{>0}$ mit $f(x) = e^{2x}$ ist ein Homomorphismus zwischen $(\mathbb{R}, +)$ und $(\mathbb{R}_{>0}, \cdot)$ mit $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$ denn

$$f(x + y) = e^{2(x+y)} = e^{2x} \cdot e^{2y} = f(x) \cdot f(y)$$

Satz 2.13: Sei $f : M \to N$ für die Gruppen $(M, \circ)$ und $(N, \oplus)$ ein Homomorphismus sowie e_M und e_N jeweils die neutralen Elemente. Dann gilt $f(e_M) = e_N$.

Beweis: Sei $a \in M$ beliebig gewählt, dann folgt

$$f(a) = f(e_M \circ a) = f(e_M) \oplus f(a) = e_N \oplus f(a)$$
$$\overset{2.10}{\Longrightarrow} f(e_M) \text{ ist ein neutrales Element } \overset{2.9}{\Longrightarrow} f(e_M) = e_N$$

□

Homomorphismen bilden das neutrale Element im Definitionsbereich immer auf das neutrale Element des Wertebereichs ab. Später werden wir sehen, dass wenn der Homomorphismus nicht bijektiv ist, noch mehr Elemente auf das neutrale Element im Wertebereich e_N abgebildet werden können. Dies motiviert folgende Definition:

Definition 2.14: Kern

Ist $f : (M, \circ) \to (N, \oplus)$ ein Homomorphismus, so nennt man:

$$\ker(f) := \{a \in M \mid f(a) = e_N\}$$

den **Kern** von f.

2.2. Ringe

Ringe sind eine Erweiterung der algebraischen Strukturen von einer auf zwei Verknüpfungen.

Definition 2.15: Ring

Seien R eine Menge und "$+$" sowie "$\cdot$" zwei Verknüpfungen auf R. Das Tripel $(R, +, \cdot)$ heißt **Ring**, falls gilt:

1. $(R, +)$ ist eine kommutative Gruppe, deren neutrales Element wir mit 0 bezeichnen.
2. $(R, \cdot)$ ist eine Halbgruppe, d.h. es gilt das Assoziativgesetz.
3. Es gelten die Distributivgesetze: $\forall a, b, c \in R$

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

Ein Ring heißt kommutativ, wenn $\cdot$ kommutativ ist. D.h. $a \cdot b = b \cdot a, \ \forall\, a, b \in R$. Ein Element $1 \in R$ heißt **Einselement**, wenn es das neutrale Element bezüglich der Multiplikation ist. Das heißt wenn für alle $a \in R$ gilt: $1 \cdot a = a \cdot 1 = a$.

Achtung: Die Formulierung der Distributivitätsgesetze impliziert, dass die Multiplikation stärker bindet als die Addition ("Punkt vor Strich").

Beispiel 2.16:

- $(\mathbb{N}, +, \cdot)$ ist kein Ring
- $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement

- $(\mathbb{F}_2, +, \cdot)$ ist ein kommutativer Körper mit Einselement, denn
  - das neutrale Element bezüglich der Addition ist die 0, denn $0+0=0$, $0+1=1, 1+0=0$
  - das additive inverse Element zu 0 ist 0 und zu 1 die 1, denn $1+1=0$
  - die Addition ist kommutativ
  - die Addition ist assoziativ, zeigt man durch nachrechnen für alle 8 Möglichkeiten
  - das neutrale Element für die Multiplikation ist 1, denn $0 \cdot 1 = 0$ und $1 \cdot 1 = 1$
  - die Multiplikation ist kommutativ
  - die Multiplikation ist assoziativ, zeigt man durch nachrechnen
  - die Distributivgesetze gelten, zeigt man durch nachrechnen

In Ringen gelten die "üblichen" Rechenregeln, z.B.:

$$0 \cdot a = 0$$

Beweis:

$$\begin{aligned} 0 \cdot a &= 0 \cdot a + 0 \cdot a - 0 \cdot a = (0+0) \cdot a - 0 \cdot a \\ &= 0 \cdot a - 0 \cdot a = 0 \end{aligned}$$

oder auch

$$(-1) \cdot a = -a$$

Beweis:

$$\begin{aligned} &a + (-1) \cdot a = 0, \text{denn} \\ &a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0 \end{aligned}$$

analog zeigt man $a \cdot 0 = 0$ und $a \cdot (-1) = -a$

Bemerkung: Wenn in einem Ring die Gleichung $1 = 0$ gilt, folgt

$$a = a \cdot 1 = a \cdot 0 = 0$$

Somit muss R der Nullring sein, $R = \{0\}$.

Beispiel 2.17: Ring der Polynome

Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Ein Polynom mit Koeffizienten in R und der Unbekannten $t \in R$ (kurz Polynom über R) ist gegeben durch

$$p(t) = a_0 \cdot t^0 + a_1 \cdot t^1 + ... + a_n \cdot t^n, \qquad a_0, a_1, ..., a_n \in R$$

Die Menge aller Polynome über R wird mit $P[t]$ bezeichnet.

Betrachte zwei Polynome $p, q \in P[t]$ mit

$$p(t) = a_0 + a_1 t + ... + a_n t^n \text{ und } q(t) = b_0 + b_1 t + b_m t^m$$

mit $n \geq m$. Ist $n > m$, so setzen wir $b_j = 0$ für $j = m+1, ..., n$. $p(t)$ und $q(t)$ sind gleich, wenn $a_j = b_j$ für alle $j \in \{1, ..., n\}$ gilt.

Aufgrund der Eigenschaften von R gilt

$$a_0 + a_1 t + ... + a_{n-1} t^{n-1} + a_n t^n = a_n t^n + a_{n-1} t^{n-1} + ... + a_1 t + a_0$$

Der Grad eines Polynoms $p(t) \in P[t]$ ist definiert als der größte Index j für den $a_j \neq 0$ gilt. Gibt es keinen solchen Index, ist $p(t)$ das Nullpolynom, d.h. $p(t) = 0$ für alle $t \in R$ und man definiert den Grad von $p(t)$ als $-\infty$.

Sind zwei Polynome $p, q \in P[t]$ wie oben definiert, und setzen wir wieder $b_j = 0$ für alle $j \in \{m+1, ..., n\}$, dann sind die Verknüpfungen "$+$" und "$\cdot$" wie folgt definiert:

$$p(t) + q(t) = (a_0 + b_0) + (a_1 + b_1)t + ... + (a_n + b_n)t^n \text{ und}$$
$$p(t) \cdot q(t) = c_0 + c_1 t + ... + c_{n+m} t^{n+m}, \qquad c_k := \sum_{i+k=k} a_i \cdot b_j$$

Mit dem Nullpolynom definiert wie oben und dem Einspolynom definiert als $p(t) := 1$ kann man nachrechnen, dass $(P[t], +, \cdot)$ ein kommutativer Ring ist.

Definition 2.18: invertierbar

Es sei $(R, +, \cdot)$ ein Ring mit Eins und $a \in R$ gegeben. Ein Element $b \in R$ heißt **invers** (bezüglich $\cdot$) zu a, wenn gilt:

$$a \cdot b = b \cdot a = 1$$

Existiert zu $a \in R$ ein inverses Element, so heißt a **invertierbar**.

Satz 2.19: Es sei $(R, +, \cdot)$ ein Ring mit Eins. Dann gilt:

1. Existiert zu $a \in R$ ein inverses Element bezüglich $\cdot$, so ist dies eindeutig bestimmt. Dies wird mit a^{-1} gekennzeichnet.
2. Wenn $ab \in R$ invertierbar sind, dann ist auch $a \cdot b$ invertierbar und es gilt:

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

Beweis: Siehe oben im Abschnitt zu Abbildungen.

□

2.3. Körper

Eine knappe Definition eines Körpers:

Ein kommutativer Ring mit Eins heißt Körper, falls $0 \neq 1$ gilt (der Nullring wird ausgeschlossen) und jedes Element $a \in R \setminus \{0\}$ invertierbar ist.

Es folgt eine äquivalente und formalere Definition:

Definition 2.20: Körper

Eine Menge K mit zwei Verknüpfungen

$$+ : K \times K \to K,\ (a,b) \mapsto a+b \qquad \text{Addition}$$
$$\cdot : K \times K \to K,\ (a,b) \mapsto a \cdot b \qquad \text{Multiplikation}$$

heißt **Körper**, wenn gilt:

- $(K, +)$ ist eine kommutative Gruppe
- $(K \setminus \{0\}, \cdot)$ ist auch eine kommutative Gruppe
- Es gelten die Distributivgesetze

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

Lemma 2.21: Sei $(K, +, \cdot)$ ein Körper. Gilt für $a, b \in K$, dass $a \cdot b = 0$, so ist mindestens eins davon die 0.

Beweis:

Fall 1: $a = b = 0$

Fall 2: o.B.d.A: $a \neq 0 \Longrightarrow \exists\, a^{-1} : a \cdot a^{-1} = 1$

$$b = 1 \cdot b = \left(a^{-1} \cdot a\right) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$$

□

Diese Eigenschaft nennt man Nullteilerfreiheit.

Beispiel 2.22:

- $(\mathbb{R}, +, \cdot)$ ist ein Körper
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper, da die multiplikativ inversen Elemente in $\mathbb{Q}$, aber nicht immer in $\mathbb{Z}$ liegen

Beispiel 2.23: komplexe Zahlen

Die Menge der komplexen Zahlen ist definiert als:

$$\mathbb{C} := \{(x, y) \mid x, y \in \mathbb{R}\}$$

d.h. $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. Die zwei Verknüpfungen Addition und Multiplikation werden wie folgt definiert:

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C},\ (a,b) + (c,d) = (a+c, b+d)$$
$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C},\ (a,b) \cdot (c,d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c)$$

Wir verwenden impliziet die Operationen auf den reellen Zahlen, $+, -, \cdot$. Dann sieht man:

- Das neutrale Element in $\mathbb{C}$ bezüglich $+$ ist die $0_{\mathbb{C}} = (0,0)$
- Das neutrale Element in $\mathbb{C}$ bezüglich $\cdot$ ist die $1_{\mathbb{C}} = (1,0)$

Man rechnet nach, dass

- Das inverse Element bezüglich $+$ in $\mathbb{C}$ definiert ist mit
$$-(x,y) = (-x,-y) \in \mathbb{C} \qquad \forall\,(x,y) \in \mathbb{C}$$
- Das inverse Element bezüglich $\cdot$ in $\mathbb{C}$ definiert ist mit
$$(x,y)^{-1} = \left(\frac{x}{x^2+y^2}, \frac{y}{x^2+y^2}\right) \in \mathbb{C} \qquad \forall\,(x,y) \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}$$

Das Überprüfen der Rechengesetze zeigt, dass $\mathbb{C}$ ein Körper ist.

Für die Teilmenge
$$M := \{(x,0) \mid x \in \mathbb{R}\} \subset \mathbb{C}$$
kann man jedes Element der reellen Zahlen mit einem Element der Menge M mit der bijektiven Abbildung
$$\mathbb{R} \to M,\ x \mapsto (x,0)$$
identifizieren. Mit $0_{\mathbb{R}} \mapsto (0,0) = 0_{\mathbb{C}}$, $1_{\mathbb{R}} \mapsto (1,0) = 1_{\mathbb{C}}$ kann man M als Teilkörper von $\mathbb{C}$ auffassen. Es gilt jedoch auch $\mathbb{R} \not\subseteq \mathbb{C}$ (zummindest in LinA).

Eine besondere komplexe zahl ist die imaginäre Einheit $(0,1)$, für die gilt:
$$(0,1) \cdot (0,1) = (-1,0) \mathrel{\widehat{=}} -1$$
Dabei wird $(-1,0) \in \mathbb{C}$ mit $-1 \in \mathbb{R}$ über die oben genannte bijetkive Abbildung identifiziert. Mit der Definition $i := (0,1)$ folgt
$$i \cdot i = -1$$
Mit dieser Notation und Identifikation kann man eine komplexe Zahl $z \in \mathbb{C}$ beschreiben mit
$$\begin{aligned} z = (x,y) &= (x,0) + (0,y) = (x,0) + (0,1)\cdot(y,0) \\ &= x + iy \end{aligned}$$
Man schreibt $\mathrm{Re}(z) = x$ als **Realanteil** von z und $\mathrm{Im}(z) = y$ als **Imaginäranteil** von z.

Man definiert zu $(x,y) \in \mathbb{C}$ die **konjugiert komplexe Zahl** durch
$$\overline{z} = (x,-y) \in \mathbb{C}$$
Damit erhält man für ein $z = (x,y) \in \mathbb{C}$:
$$\begin{aligned} |z| := \sqrt{z \cdot \overline{z}} &= \sqrt{(x+iy)\cdot(x-iy)} \\ &= \sqrt{x^2 - ixy + ixy - i^2y^2} \\ &= \sqrt{x^2+y^2} \end{aligned}$$

2.4. Vektorräume

Beispiel 2.24: Kräfeparallelogramm

Betrachten wir einige Gesetze aus der Mechanik:

Je zwei am selben Punkt angreifende Kräfte können durch eine einzige Kraft ersetzt werden. Diese resultierende Kraft (= Gesamtkraft) hat die gleiche Wirkung wie die Einzelkräfte.

$$F = F_1 + F_2 \qquad \text{die Kräfte können als Vektoren betrachtet werden}$$

- Ein Vektor hat eine Länge und eine Richtung
- Vektoren kann man addieren
- Vektoren können mit einer reellen Zahl multipliziert werden

Beispiel 2.25: Interpolationsproblem

Gegeben sind reelle Zahlen $a, b, c \in \mathbb{R}$. Gesucht ist ein Polynom zweiten Grades $p(t) \in P[t]$ mit

$$p(1) = a \qquad p(2) = b) \qquad p(3) = c$$

für ein $p(t) = a_0 + a_1 t + a_2 t^2$. D.h. es muss gelten:

$$\begin{aligned} p(1) &= a_0 + a_1 \cdot 1 + a_2 \cdot 1 = a \\ p(2) &= a_0 + a_1 \cdot 2 + a_2 \cdot 4 = b \\ p(3) &= a_0 + a_1 \cdot 3 + a_2 \cdot 9 = c \end{aligned}$$

Diese Gleichung hat genau eine Lösung.

$$p(t) = (3a - 3b + c) + \left(-5\frac{a}{2} + 4b - 3\frac{c}{2}\right)t + \left(\frac{a}{2} - b + \frac{c}{2}\right)t^2$$

Eine alternative Darstellung ist

$$p_1(t) = \frac{1}{2}(t-2)(t-3) \qquad p_2(t) = -(t-1)(t-3) \qquad p_3(t) = \frac{1}{2}(t-1)(t-2)$$

für die gilt:

$$p_{i(k)} = \begin{cases} 1 \text{ für } i = k \\ 0 \text{ sonst} \end{cases}$$

Dann ist $p(t)$ gegeben durch:

$$p(t) = ap_1(t) + bp_2(t) + cp_3(t)$$

Beobachtung: Die additive Verknüpfung zweier Elemente gleicher Art und Multiplikation mit einer reellen Zahl ($\widehat{=}$ Skalar).

Solch eine algebraische Sturktur wollen wir beschreiben:

Definition 2.26: Vektorraum

Sei K ein Körper. Ein Vektorraum über K, kurz K-Vektorraum, ist eine Menge V mit zwei Abbildungen:

- Addition
$$+ : V \times V \to V,\ (v, w) \mapsto v + w$$
- skalare Multipliktation
$$\cdot : K \times V \to V,\ (\lambda, v) \mapsto \lambda v$$

für die folgendes gilt:

- $(V, +)$ ist eine kommutative Gruppe
- Für alle $v, w \in V$ und $\lambda, \mu \in K$ gilt:
  1. $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$
  2. $1 \cdot v = v$
  3. $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$
  4. $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$

Ein Element $v \in V$ nennen wir **Vektor**, ein $\mu \in K$ nenn wir einen **Skalar**.

Beobachtung: Für einen Vektorraum sind die Operatinen $+$ und die skalare Multiplikation $\cdot$ abeschlossen.

Beispiel 2.27: Für einen Körper K ist der Standartvektorraum gegeben durch die Menge $V = K^n$ für ein $n \in \mathbb{N}$. Die n-Tupel werden geschrieben als

$$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \text{ mit } v_1, v_2, ..., v_n \in K$$

Die Addition und die skalare Multiplikation ist komponentenweise definiert.

$$v + w = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \\ \vdots \\ v_n + w_n \end{pmatrix}$$

$$\lambda \cdot w = \lambda \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} \lambda \cdot w_1 \\ \lambda \cdot w_2 \\ \vdots \\ \lambda \cdot w_n \end{pmatrix}$$

Damit ist der Vektorraum $V = K^n$ ein K-Vektorraum. Der Nullvektor $\vec{v_0}$ ist definiert durch

$$\vec{0} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Das additiv inverse Element ist gegeben durch

$$-v = -\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} -v_1 \\ -v_2 \\ \vdots \\ -v_n \end{pmatrix} \text{ für } v_1, v_2, ..., v_n \in K$$

Da K ein Körper ist, ist die so definierte skalare Multiplikation assoziativ, distributiv und mit $1 \in K$ kompatibel ($1 \cdot v = v$).

Beispiel 2.28: Polynome

Die Menge $P[t]$ aller Polynome über einen Körper K mit der Unbekannten t bilden einen K-Vektorraum, wenn die Addition von Polynomen wie in Beispiel 2.17 definiert ist nd die skalare Multiplikation für ein $p(t) = a_0 + a_1 t + ...a_n t^n \in P[t]$ definiert ist durch:

$$\cdot : K \times P[t] \to P[t]$$

$$\lambda \cdot p(t) = (\lambda a_0) + (\lambda a_1)t + ... + (\lambda a_n)t^n$$

Beispiel 2.29: Abbildungen

Die Menge $V = \text{Abb}(\mathbb{R}, \mathbb{R})$ der Abbildungen $f : \mathbb{R} \to \mathbb{R}$ bilden einen Vektorraum über den Körper $\mathbb{R}$ mit den Verknüpfungen

$$+ : V \times V \to V,\ (f, g) \mapsto f + g \qquad (f + g)(x) := f(x) + g(x)$$

und

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

Das Gleiche gilt für

$$V := \{\text{stetige Abbildungen } f : \mathbb{R} \to \mathbb{R}\}$$
$$V := \{\text{differenzierbare Abbildungen } f : \mathbb{R} \to \mathbb{R}\}$$

Lemma 2.30: Für den K-Vektorraum $(V, +, \cdot)$ mit dem Nullement 0_K des Körpers und 0_V des Vektorraums. Dann gilt

1. $0_K \cdot v = 0_V$
2. $\lambda \cdot 0_V = 0_V$
3. $-(\lambda \cdot v) = (-\lambda) \cdot v = \lambda \cdot (-v) \qquad \forall\, \lambda \in K, \forall\, v \in V$

Beweis:

zu 1) $\forall\, v \in V$ gilt

$$
\begin{aligned}
0_K \cdot v = (0_K + 0_K) \cdot v = 0_K \cdot v + 0_K \cdot v \qquad & | - (0_K \cdot v) \\
0_V = 0_K \cdot v + 0_V = 0_K \cdot v & \\
0_V = 0_K \cdot v &
\end{aligned}
$$

zu 2) $\forall\, \lambda \in K$ gilt

$$
\begin{aligned}
\lambda \cdot 0_V = \lambda \cdot (0_V + 0_V) = \lambda \cdot 0_V + \lambda \cdot 0_V \qquad & | - (\lambda \cdot 0_V) \\
0_V = \lambda \cdot 0_V &
\end{aligned}
$$

zu 3) $\forall\, \lambda \in K, \forall\, v \in V$ gilt

$$
\begin{aligned}
\lambda \cdot v + ((-\lambda) \cdot v) = (\lambda - \lambda) \cdot v = 0_K \cdot v = 0_V \ \checkmark \\
\lambda \cdot v + (\lambda \cdot (-v)) = (\lambda \cdot (v - v)) = \lambda \cdot 0_V = 0_V \ \checkmark
\end{aligned}
$$

□

Definition 2.31: Untervektorraum

Sei $(V, +, \cdot)$ ein K-Vektorraum und sei $U \subseteq V$. Dann ist $(U, + \cdot)$ ein **Untervektorraum**, kurz **Unterraum** von $(V, +, \cdot)$.

Lemma 2.32: Sei $(V, +, \cdot)$ ein K-Vektorraum und $U \subseteq V$. Dann ist $(U, +, \cdot)$ genau dann ein Unterraum von V, wenn gilt:

1. $u + w \in U \qquad \forall\, u, w \in U$
2. $\lambda u \in U \qquad \forall\, \lambda \in U, \forall\, u \in U$

Beweis: (Übung)