# 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:** *(Fortsetzung 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:

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

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 $\hat{\imath} \in \{1, ..., n\}$ mit $A_i \subseteq A_{\hat{\imath}}$ 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 $\hat{\imath} = 1$ gilt $A_1 \subseteq A_{\hat{\imath}} = A_1$ ✓

Induktionsschritt: $n - 1 \mapsto n$

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

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

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 $I_m/\mathrm{Id}_m$.

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, Blatt 4 Aufgabe 1)

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

*Beweis:* (1. Übungsaufgabe)

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

2. Aus Satz 1.34 folgt, dass $g \circ f$ bijektiv ist. $\Longrightarrow (g \circ f)^{-1}$ existiert und ist eindeutig bestimmt. Es gilt

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

Analog zeigt man: $(g \circ f) \circ \left(f^{-1} \circ g^{-1}\right) = \mathrm{Id}_Y$

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

□

# 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

| $\circ$ | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $a$ | $b$ |

Man kann nachrechenen, dass $(M, \circ)$ eine Halbgruppe ist. Man 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 Existenz 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 Ring 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)

Ist $U$ nicht abgeschlossen bezüglich der Addition und der skalaren Multiplikation, dann ist $(U, +)$ keine kommutative Gruppe und $(U, \cdot)$ keine Halbgruppe. In beiden Fällen ist $(U, +, \cdot)$ dann kein Vektorraum und somit auch kein Untervektorraum von $(V, +, \cdot)$.

□

**Beispiel 2.33:**

- Jeder Vektorraum $(V, +, \cdot)$ hat die Vektorräume $(U = V, + \cdot)$ und $(U = \{0_V\}, +, \cdot)$
- Für jedes $u \in \mathbb{N}_0$ ist die Menge aller Polynome mit dem Grad kleiner gleich $n$, d.h. die Menge $P[t]_{\leq n} = \{p(t) \in P[t] \mid \text{Grad}(p) \leq n\}$ ist mit den Verknüpfungen aus Beispiel 2.28 ein Unterraum von $(P[t], +, \cdot)$

**Definition 2.34: Linearkombination**

Seien $(V, +, \cdot)$ ein $K$-Vektorraum, $n \in \mathbb{N}$ und $v_1, ..., v_n \in V$. Ein Vektor der Form

$$\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n = \sum_{i=1}^{n} \lambda_i v_i = v \in V$$

heißt **Linearkombination** von $v_1, ..., v_n \in V$ mit den Koeffizienten $\lambda_1, ..., \lambda_n \in K$. Die **lineare Hülle** / Der **Spann** von $v_1, ..., v_n \in V$ ist die Menge

$$\text{Span}\{v_1, ..., v_n\} := \left\{ \sum_{i=1}^{n} \lambda_i v_i \mid \lambda_1, ..., \lambda_n \in K \right\}$$

**Lemma 2.35:** Sei $(V, +, \cdot)$ ein $K$-Vektorraum und $v_1, ..., v_n \in V$, dann ist $(\text{Span}\{v_1, ..., v_n\}, +, \cdot)$ ein Unterraum von $(V, +, \cdot)$.

*Beweis:* Es gilt $\text{Span}\{v_1, ..., v_n\} \subseteq V$. Wegen Lemma 2.32 reicht es zu zeigen, dass $U := \text{Span}\{v_1, ..., v_n\}$ bezüglich $+$ und $\cdot$ abgeschlossen ist. Dies gilt nach der Definition der linearen Hülle.

□

**Beispiel 2.36:** Für $V = \mathbb{R}^3, K = \mathbb{R}$. Betrachte

$$M = \left\{ \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 9 \\ 0 \\ 3 \end{pmatrix} \right\}, \text{ist } \begin{pmatrix} 12 \\ 0 \\ 4 \end{pmatrix} \in \text{Span}(M)?$$

Ja, denn es gilt:

$$1 \cdot v_1 + 1 \cdot v_2 = \begin{pmatrix} 3+9 \\ 0+0 \\ 1+3 \end{pmatrix} = \begin{pmatrix} 12 \\ 0 \\ 4 \end{pmatrix}$$

Des weiteren gilt:

$$\text{Span}(M) = \left\{ \lambda \cdot \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\} = A$$

*Beweis:*

"$\subseteq$":

$$A = \left\{ \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} \cdot \lambda \mid \lambda \in \mathbb{R} \right\} \subseteq \left\{ \lambda \cdot \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 9 \\ 0 \\ 3 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\} \subseteq \text{Span}(M)$$

"$\supseteq$":

$$
\begin{aligned}
x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \operatorname{Span}(M) \iff \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &= \lambda_1 \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 9 \\ 0 \\ 3 \end{pmatrix} \\
&= \lambda_1 \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} + 3\lambda_2 \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} \\
&= (\lambda_1 + 3\lambda_2) \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} \\
\implies x = (\lambda_1 + 3\lambda_2) \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} \in A
\end{aligned}
$$

□

# 3. Basen und Dimensionen von Vektorräumen

Dieses Kapitel motiviert unter anderem die Frage, wie man Vektorräume effizient beschreiben kann.

## 3.1. Lineare Unabhängigkeit

**Definition 3.1: lineare Unabhängigkeit**

Sei $V$ ein $K$-Vektorraum. Die Vektoren $v_1, ..., v_n \in V$ heißten **linear unabhängig**, wenn aus

$$\sum_{i=1}^{n} \lambda_i v_i = 0 \qquad \text{mit } \lambda_1, ..., \lambda_n \in K$$

folgt, dass $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$ gilt. Folgt dies nicht, d.h. gilt

$$\sum_{i=1}^{n} \lambda_i v_i = 0 \qquad \text{mit } \lambda_1, ..., \lambda_n \in K$$

die nicht alle gleich 0 sind, so heißten $v_1, ..., v_n$ **linear abhängig**.

- Die leere Menge ist linear unabhängig.
- Ist $M \neq \emptyset$ eine Menge und für jedes $m \in M$ ein Vektor $v_m \in V$ gegeben, so nennt man die Menge $\{v_m\}_{m \in M}$ linear unabhängig, wenn endlich viele Vektoren immer linear unabhängig sind. Gilt dies nicht, so ist die Menge $\{v_m\}_{m \in M}$ linear abhängig.

**Bemerkung:** Nach Definition sind die Vektoren $v_1, ..., v_n$ genau dann linear unabhängig, wenn sich der Nullvektor aus ihnen nur in der Form $0 = 0 \cdot v_1 + ... + 0 \cdot v_n$ mit endlich vielen Vektoren darstellen lässt

**Beispiel 3.2:** Fortsetzung von Beispiel 2.36

Die Vektoren aus $M = \{(3, 0, 1), (9, 0, 3)\}$ sind linear abhängig, da

$$3\begin{pmatrix}3\\0\\1\end{pmatrix} - \begin{pmatrix}9\\0\\3\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix} \qquad \text{mit } \lambda_1 = 3, \lambda_2 = -1$$

Der Vektor $v_1 = (3, 0, 1)$ dagegen ist linear unabhängig, da

$$0 \cdot \begin{pmatrix}3\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix} \qquad \text{mit } \lambda_1 = 0$$

**Beispiel 3.3:** $V = \mathbb{R}^3, K = \mathbb{R}$

Betrachte $M = \{(3,0,1),(9,0,3),(0,1,1)\}$. Sind diese Vektoren linear unabhängig? Die allgemeine Vorgehensweise ist hier, ein lineares Gleichungssystem aufzustellen und zu lösen. Hat das Gleichungssystem eine Lösung $\neq 0$, dann sind die Vektoren linear abhängig.

Hier: $\Longrightarrow$ linear abhängig

**Lemma 3.4:** Sei $V$ ein $K$-Vektorraum. Dann gilt:

1. Ein einzelner Vektor ist genau dann linear unabhängig, wenn $v \neq 0_V$ gilt
2. Sind $v_1, ..., v_n \in V$ linear unabhängig und ist $\{u_1, ..., u_m\} \subseteq \{v_1, ..., v_n\}$, dann ist auch die Menge $u_1, ..., u_m$ linear unabhängig
3. Sind $v_1, ..., v_n \in V$ linear abhängig und $u_1, ..., u_m \in V$. Dann ist auch $v_1, ..., v_n, u_, ..., u_m$ linear abhängig

*Beweis:*

zu 1: Sei $v \in V, v \neq 0_V$. Es soll gelten: $\lambda v = 0 \Longrightarrow \lambda = 0$, da $v \neq 0_V$

zu 2: $v_1, ..., v_n$ sind linear unabhängig und es gilt $\{u_1, ..., u_m\} \subseteq \{v_1, ..., v_n\}$.

Damit die Vektoren $\{u_1, ..., u_m\}$ linear unabhängig sind, muss gelten

$$\lambda_1 u_1 + ... + \lambda_m u_m = 0$$

Wegen der linearen Unabhängigkeit von $\{v_1, ..., v_n\}$ gilt nach Umbennenung der Vektoren $\{u_1, ..., u_m\}$:

$$\lambda_{i_1} v_{i_1} + ... + \lambda_{i_m} + v_{i_m} + \sum_{\substack{j=1 \\ j \notin \{i_1, ..., i_m\}}}^{n} \Longrightarrow \lambda_{i_1} = ... = \lambda_{i_m} = 0$$

zu 3: $v_1, ..., v_n$ sind linear abhängig $\Longrightarrow \exists\, \lambda_i \in K$, so dass nicht alle $\lambda_i$ gleich Null sind und $\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n = 0$ gilt.

$\Longrightarrow \lambda_1 v_1 + ... + \lambda_n v_n + \mu_1 u_1 + ... + \mu_m u_m = 0 \Longrightarrow \mu_1, ..., \mu_m = 0 \Longrightarrow$ Mit Koeffizienten $\lambda_1, ..., \lambda_n, \mu_1, \mu_m$ lassen sich $v_1, ..., v_n, u_1, ..., u_m$ linear zu Null kombinieren ohne, dass alle Koeffizienten Null sind $\Longrightarrow v_1, ..., v_n, u_1, ..., u_m$ sind linear abhängig

□

Eine alternative Definition der linearen Unabhängigkeit motiviert Satz 3.5:

**Satz 3.5:** Sei $V$ ein $K$-Vektorraum. Eine Menge $M \subseteq V$ ist genau dann linear unabhängig, wenn kein Vektor $v \in V$ als Linearkombination dargestellt werden kann.

*Beweis:*

"$\Longrightarrow$": Annahme: $M \subseteq V$ sind linear unabhängig und es existiert ein Vektor $v \in M$, der als Linearkombination von endlichen Vektoren aus $M \setminus \{v\}$ dargestellt werden kann. D.h. es existieren $\lambda_1, ..., \lambda_n \in K \setminus \{0\}, n \geq 1$ und $v_1, ..., v_n \in M \setminus \{v\}$ mit

$$\sum_{i=1}^{n} \lambda_i v_i = v \Longrightarrow -v + \sum_{i=1}^{n} \lambda_i v_i = 0 \quad \lightning$$

Dies ist ein Widerspruch zur Annahme, dass die Vektoren linear unabhängig sind. Es existiert also kein Vektor, welcher als Linearkombination ausgedrückt werden kann.

"$\Longleftarrow$": Angenommen $M$ wäre linear abhängig. D.h. es existieren $n \in \mathbb{N}$ und $v_1, ..., v_n \in M, \lambda_1, ..., \lambda_n \in K$ mit $\lambda_1 \neq 0$ und $\sum_{k=1}^{n} \lambda_k v_k = 0 \Longrightarrow$

$$\sum_{k=1}^{n} \frac{\lambda_k}{\lambda_1} v_k = 0 \Longrightarrow v_1 + \sum_{k=2}^{n} \frac{\lambda_k}{\lambda_1} v_k = 0$$

$$\Longrightarrow v_1 = -\sum_{k=2}^{n} \frac{\lambda_k}{\lambda_1} v_k \quad \lightning$$

Dies ist ein Widerspruch dazu, dass man $v$ nicht als Linearkombination darstellen kann. Die Vektoren sind also linear unabhängig.

□

**Definition 3.6: Span für unendliche Mengen**

Sei $K$ ein Körper, $V$ ein $K$-Vektorraum, $M$ eine Menge und $v_m \in M \ \forall \, m \in M$ gegeben. Dann ist der Spann der Familie $\{v_m\}_{m \in M}$ gegeben durch

$$\mathrm{Span}\{v_m\}_{m \in M} := \left\{ \begin{array}{c} v \in V \mid \exists \, n \in \mathbb{N} \text{ und endliche Teilmenge } J \subset M, \\ |j| = n \text{ mit } v \in \mathrm{Span}\{v_j\}_{j \in J} \end{array} \right\}$$

**Beispiel 3.7:** $M = \mathbb{N}$, $v_m := t^m$, $t \in K$, $\mathrm{Span}\{v_m\}_{m \in M} = P[t]$

**Satz 3.8:** Sei $K$ ein Körper, $V$ ein $K$-Vektorraum und $M$ eine Menge. Dann sind folgende Aussagen äquivalent:

1. $\{v_m\}_{m \in M}$ ist linear unabhängig
2. jeder Vektor $v \in \mathrm{Span}\{v_m\}_{m \in M}$ hat eine eindeutige Darsetllung als Linearkombination

*Beweis:*

$1 \Longrightarrow 2$: Beweis per Kontraposition

Seien $I, J \subseteq M$ endlich. Sei $\lambda_K \in K, k \in I$ und $\mu_k \in K, k \in J$. Betrachte den Vektor $v \in V$. Für diesen gilt:

$$v_I = \sum_{k \in I} \lambda_k v_k \text{ und } v_J = \sum_{k \in J} \mu_k v_k$$

Überlegung: Wähle ein $k \in I \cup J$. Falls gilt $k \in I \setminus J$, setze $\lambda_k ==$. Falls gilt $k \in J \setminus I$, setze $\mu_k = 0$. Es folgt

$$\Longrightarrow 0 = \sum_{k \in I \cup J} (\lambda_k - \mu_k) v_k$$

Da die Darstellung $v_I$ und $v_J$ von $v$ unterschiedlich sind, existiert ein $k \in I \cup J$ mit $\lambda_k - \mu_k \neq 0$.

$$\Longrightarrow \{v_m\}_{m\in M} \text{ ist linear unabhängig}$$

$2 \Longrightarrow 1$: Beweis per Kontraposition

Angenommen $\{v_m\}_{m\in M}$ wäre linear unabhängig. Dann existiert ein endliches $J \subseteq M$ und $\lambda_k \in K$ für $k \in J$ mit $0 = \sum_{k\in J} \lambda_k v_k$ und mindestens ein $\lambda_k \neq 0$.

Sei $v \in \text{Span}\{v_m\}_{m\in M}$, d.h. es existiert ein endliches $I \subseteq M$ mit $\mu_k \in K$ für alle $k \in I$ mit

$$v = \sum_{k\in I} \mu_k v_k \Longrightarrow v + 0 = \lambda_{k\in I}\mu_k v_n + \sum_{k\in J} \lambda_k v_k = \sum_{k\in I\cup J} (\mu_k + \lambda_k) v_k$$

Es gilt wieder $\mu_k = 0$ für $k \in J \setminus I$ und $\lambda_k = 0$ für $k \in I \setminus J$. Da für mindestens ein $k \in J \cup I$, $(\mu_k + \lambda_k) \neq \lambda_k$, ist dies eine zweite Darstellung von $v$.

□

**Definition 3.9: Erzeugendensystem**

Sei $K$ ein Körper, $V$ ein $K$-Vektorraum, $M$ eine Menge und $v_m$ für $m \in M$ Vektoren in $V$. Die Menge $\{v_m\}_{m\in M}$ heißt **Erzeugendensystem** von $V$, falls

$$\text{Span}\{v_m\}_{m\in M} = V$$

**Beispiel 3.10:** Sei $K$ ein Körper, $V$ ein Vektorraum mit $V = K^n$, $n \in \mathbb{N}$

Dann ist mit

$$e_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ e_2 := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix},\ \ldots,\ e_n := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

die Menge $\{e_i\}_{\in\in\{1,\ldots,n\}}$ ein Erzeugendensystem von $K^n$.

**Definition 3.11: Basis**

Sei $K$ ein Körper, $V$ ein Vektorraum, $M$ eine Menge und $v_m$ für $m \in M$ Vektoren in von $V$. Dann heißt $\{v_m\}_{m\in M}$ **Basis** von $V$, falls sie linear unabhängig und ein Erzeugendensystem von $V$ ist.

**Beispiel 3.12:** Das Erzeugendensystem aus 3.10 ist eine Basis. Anmerkung: Basen sind nicht eindeutig. Für $K^3$ gilt etwa

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}\ v_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}\ v_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

ist ebenfalls eine Basis.

**Beispiel 3.13:** Die Familie $\{t^i\}_{i\in\mathbb{N}}$ ist ein Erzeugendensystem von $P[t]$, denn es gilt $\text{Span}\{t^i\}_{i\in\mathbb{N}} = P[t]$. Um zu prüfen, ob die Familie auch Basis von $P[t]$ muss die lineare Unabhängigkeit gerpüft werden. Sei $n \in \mathbb{N}_0,\ a_0, a_1, ..., a_n \in K$ und betrachte $p(t) = a_0 + a_1 t + ... + a_n t^n$ mit $p(t) = 0$.

Falls $a_k \neq 0$ für ein $k \in \{0, ..., n\}$ gilt, so hat $p(t)$ höchstens $n$ Nullstellen in $K$. $0 \in P[t]$ hat aber unendlich viele Nullstellen. D.h. es existiert ein $t \in K$ mit $p(t) \neq 0$ $\lightning$. Es folgt, dass die Familie $\{t^i\}_{i\in\mathbb{N}}$ linear unabhängig ist. Somit ist $\{t^i\}_{i\in\mathbb{N}}$ eine Basis von $P[t]$.

**Satz 3.14:** Sei $K$ ein Körper, $V$ ein Vektorraum und $B := \{v_1, ..., v_n\} \subseteq V$ eine Basis von $V$. Dann ist äquivalent

1. $B$ ist eine Basis
2. $B$ ist ein unverkürzbares Erzeugendensystem, d.h. $\forall r \in \{1, ..., n\}$ ist die Menge $B \setminus \{v_r\}$ kein Erzeugendensystem von $V$
3. Für alle $v \in V$ existieren eindeutige $\lambda_1, ..., \lambda_n$ mit
$$v = \sum_{k=1}^{n} \lambda_k v_k$$
4. $B$ ist unverlängerbar linear unabhängig. D.h. für alle $v \in V$ ist $B \cup \{v\}$ linear abhängig

*Beweis:* Beweis durch Kontraposition

$1 \implies 2$: Angenommen $B$ ist ein verkürzbares Erzeugendensystem. D.h. o.B.d.A $r = 1$, $B \setminus \{v_1\}$ ist auch ein Erzeugendensystem von $V$. Also existieren $\lambda_2, ..., \lambda_n \in K$ mit

$$v_1 = \sum_{k=2}^{n} \lambda_k v_k$$

Mit Satz 3.5 folgt, dass $B$ linear abhängig ist. Also ist $B$ keine Basis.

$2 \implies 3$: Beweis durch Kontraposition

Angenommen, es existiert $v \in V$, $\lambda_k, \mu_k \in K$ mit

$$v = \sum_{k=1}^{n} \lambda_K v_k \text{ und } v = \sum_{k=1}^{n} \mu_k v_k$$

o.B.d.A gilt $\mu_1 \neq \lambda_1$. Dann folgt $0 = \sum_{k=1}^{n} (\lambda_k - \mu_k) v_k$.

Weiterhin gilt

$$0 = \sum_{k=1}^{n} \frac{\lambda_k - \mu_k}{\lambda_1 - \mu_1} v_k \implies v_1 = \sum_{k=2}^{n} -\frac{\lambda_k - \mu_k}{\lambda_1 - \mu_1} v_k$$

Sei nun $w \in V$, dann existiert ein $\alpha_k \in K$ mit

$$w = \sum_{k=1}^{n} \alpha_k v_k = \alpha_1 v_1 + \sum_{k=2} \alpha_k v_k = \star$$

Wir defnieren

$$\beta_k = -\frac{\lambda_k - \mu_k}{\lambda_1 - \mu_1}$$

Dann gilt

$$\star = \sum_{k=2}^{n} (\alpha_1 \beta_k + \alpha_k) v_k$$

Also war $B$ kürzbar.

$3 \Longrightarrow 4$:

Satz 3.8 liefert, dass $B$ linear unabhängig ist. Sei $v \in V \setminus B$. Dann existieren $\lambda_1, ..., \lambda_k \in K$ mit

$$v = \sum_{k=1}^{n} \lambda_k v_k$$

Das heißt $B \cup \{v\}$ ist linear abhängig nach Satz 3.8.

$4 \Longrightarrow 1$:

Sei $B$ unverlängerbar linear abhängig. Sei $v \in V$. Dann ist $B \cup \{u\}$ linear abhängig. Also existiert $\lambda_1, ..., \lambda_n, \lambda \in K$ mit

$$0 = \sum_{k=1}^{n} \lambda_k v_k + \lambda v \text{ wobei nicht alle } \lambda_k, \lambda = 0$$

Da $B$ linear unabhängig ist folgt $\lambda \neq 0$. Daraus folgt

$$v = \sum_{k=1}^{n} -\frac{\lambda_k}{\lambda} v_k$$

Also ist $B$ ein Erzeugendensystem und somit eine Basis.

□

**Definition 3.15: endlichdimensional, unendlichdimensional**

Sei $(V, +, \cdot)$ ein $K$-Vektorraum für dein eine endliche Menge $M = \{v_1, ..., v_n\} \subset V$ existiert, so dass Span $M = V$. Dann nennt man $V$ **endlich erzeugt** und sagt $V$ ist **endlichdimensional**. Ist $V$ nicht von endlich vielen Vektoren erzeugt, nennt man $V$ **unendlichdimensional**.

**Beispiel 3.16:**

- Die Einheitsvektoren aus Beispiel 3.10 sind eine Basis des $K^n$ für einen Körper $K$. Damit ist $K^n$ endlich erzeugt.
- Der Vektorraum $P[t]$ der Polynome aus Beispiel 3.13 ist über dem Körper $K$ mit der Basis $\{t^i\}_{i\in\mathbb{N}_0}$ ist nicht endlich erzeugt.
- Sei $V$ der Vektorraum der stetigen reellwertigen Funktionen auf dem Intervall $[0,1]$. Dann ist $V$ unendlichdimensional, denn:

  Sei für $n \in \mathbb{N}$ die Funktion $f_n \in V$ definiert durch

$$f_n : [0,1] \to \mathbb{R},\ x \mapsto \begin{cases} 0, & 0 \le x \le \frac{1}{n+1} \\ 2n(n+1)x - 2n, & \frac{1}{n+1} \le x \le \frac{1}{2}\left(\frac{1}{n} + \frac{1}{n+1}\right) \\ -2(n+1)x + 2n + 2, & \frac{1}{2}\left(\frac{1}{n} + \frac{1}{n+1}\right) \\ 0, & \frac{1}{n} \le x \le 1 \end{cases}$$

  Es gilt für jede Linearkombination der $f_n$ und $j,k \in \mathbb{N}$ mit $j \le k$, dass

$$\sum_{j=1}^{k} \lambda_j f_{j\left(\frac{1}{2}\left(\frac{1}{j}+\frac{1}{j+1}\right)\right)} = \lambda_j \text{ bei } f_j = 1, \text{ sonst } 0$$

  Damit ist:

$$\sum_{i=1}^{k} \lambda_i f_{i(x)} = 0_v \in V,\ \forall x \in [0,1]$$

  nur erfüllt, wenn $\lambda_i = 0$ für alle $1 \le i \le k$. Damit sind die $f_n$ linear unabhängig. Also ist $V$ unendlichdimensional.

**Frage:** Hat jeder Vektorraum eine Basis?

Diese Frage ist relativ einfach im endlichdimensionalen Fall:

**Lemma 3.17:** Basisauswahlsatz

Ein $K$-Vektorraum $(V,+,\cdot)$ ist genau dann endlich, erzeugt, wenn er eine endliche Basis besitzt.

*Beweis:*

"$\Longleftarrow$": endliche Basis $\Longrightarrow$ endliches Erzeugendensystem $\Longrightarrow$ endlich erzeugt

"$\Longrightarrow$": Sei $V$ endlich erzeugt $\Longrightarrow \exists v_1, ..., v_n : \text{Span}\{v_1, ..., v_n\} = V$. Ist dieses Erzuegendensystem nicht minimial, d.h. linear abhängig, dann folgt mit Satz 3.5, dass ein $v_i, 1 \le i \le n$, als Linearkombation der anderen $v_j, i \ne j$ dargestellt werden kann. Entfernen des $v_i$ liefert ein kleineres Erzeugendensystem. Wiederhole $n-1$-Mal, bis die verbleibende Menge linear unabhängig ist. Soimt enthält jedes endliche Erzeugendensystem ein minimales Erzeugendensystem und somit eine Basis.

□

Für den unendlichdimensionalen Fall ist mehr Arbeit nötig:

**Satz 3.18:** Jeder $K$-Vektorraum $(V, +, \cdot)$ besitzt eine Basis (ein minimales Erzeugendensystem).

*Beweis:*

Idee: Wir wenden das zornsche Lemma auf $M = V$ und
$\mathcal{S} = \left\{A \subseteq V \mid \text{die Familie } \{v\}_{v \in A} \text{ ist linear unabhängig}\right\} \subseteq \mathcal{P}(M)$

Dazu treffen wir die Annahme, dass die Vorraussetzungen für das Zornsche Lemma gelten. Dann hat $\mathcal{S}$ ein maximales Element bezüglich der Relation $\leq$.

Da maximal linear unabhängige Familien von Vektoren aus $V$ Basen von $V$ sind (Satz 3.14), ist damit die Behauptung gezeigt.

Jetzt müssen wir die Verwednung des Zornschen Lemmas rechtfertigen.

Für $\mathcal{K} \subseteq \mathcal{S}$, $\mathcal{K}$ ist eine Kette, gilt $\bigcup_{A \in \mathcal{K}} A \in \mathcal{S}$. Sei $\mathcal{K} \subseteq \mathcal{S}$ seine Kette. zu zeigen:

$$B := \bigcup_{A \in \mathcal{K}} A \in \mathcal{S}$$

D.h. die Vektoren aus $B$ sind eine Menge von linear unabhängigen Vektoren. Seien dazu endlich viele Vektoren $v_1, ..., v_n \in B$ beliebig vorgegeben. Per Definition von $B$ existiert in der gegebenen Kette $\mathcal{K}$ für jeden Index $i \in \{1, ..., n\}$ eine Menge $A_i \in \mathcal{K}$ mit $v_i \in A_i$.

Nach Lemma 1.26 über endliche Teilmengen von Ketten gibt es einen Index $\tilde{i}$ mit $A_i \subseteq A_{\tilde{i}}$ für alle $i$. $\Longrightarrow$ alle Vektoren $v_1, ..., v_n \in A_{\tilde{i}} \in \mathcal{S}$. Daraus folgt, dass $\{v_1, ..., v_n\}$ linear unabhängig ist.

□

## 3.2. Basen

Man kann eine Basis als Koordinatensystem in einem Vektorraum auffassen. Wichtig ist, dass Basen nicht eindeutig sind (vergleiche Beispiel 3.12). Eine sehr wichtige Frage der linearen Algebra ist: Welche Basis wählt man?

**Beispiel 3.19:** Um aus einer im Verhältnis $1 : 1$ in Wasser gelösten System eine Lösung im Mischungsverhältnis $a : b$ zu bekommen, verdünnt man $y$ Teile der Lösung mit $x$ Teilen Wasser, so dass

$$x \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + y \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \qquad x\text{-Koordinate ist Wasser, } y\text{-Koordinate ist Substanz}$$

Eine andere Darstellung der Basis ist

$$\begin{pmatrix} 1 \\ \frac{1}{2} \end{pmatrix} = 1 \cdot e_1 + \frac{1}{2} \cdot e_2 = 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{2} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$= \frac{1}{2} v_1 + \frac{1}{2} v_2 = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Man sieht:

- 1 Parameter in $\mathbb{R}^1$
- 2 Parameter in $\mathbb{R}^2$
- 3 Parameter in $\mathbb{R}^3$

**Ziel:** Alle Basen eines endlich erzeugten Vektorraums haben gleich viele Elemente.

Das ist durchaus nicht offensichtlich**!!!**

**Beispiel 3.20:** Es gibt eine bijektive Abbildung $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Dafür kann man z.B. das Diagonalargument von Georg Cantor verwenden.

Zum Beweis der Aussage sind noch Vorarbeiten notwendig.

**Satz 3.21:** Basisergänzungssatz

Sei $(V, +, \cdot)$ eine $K$-Vektorraum,

- $\{u_i\}_{i \in I} \subseteq V$ ein linear unabhängiges System
- $\{v_j\}_{j \in J} \subseteq V$ ein Erzeugendensystem von $V$

Dann gibt es eine Teilmenge $\tilde{J} \subseteq J$ mit der Eigenschaft, dass das System

$$B := \{w_k\}_{k \in I \cup \tilde{J}} \text{ mit } w_k := \begin{cases} u_i k = i \in I \\ v_j k = j \in \tilde{J} \end{cases}$$

eine Basis von $V$ bildet.

*Beweis:* Sei $\tilde{J} \subseteq J$ eine bezüglich $\subseteq$ maximal gewählte Teilmenge mit der Eigenschaft, dass $B$ wie im Satz definiert, ein linear unabhängiges System ist. Für endliche Mengen $J$ ist das klar (siehe Lemma 3.17). Für Mengen mit unendlich vielen Elementen folgt aus dem zornschen Lemma (Satz 3.18). Damit: $B$ ist ein maximales linear unabhängiges System.

Wegen der Maximalität ist für jeden Index $j \in J \setminus \tilde{J}$ das System $B \cup \{v_j\}$ linear abhängig $\implies \exists \lambda, \lambda_i \in K, i \in I \cup \tilde{J}$ :

$$\lambda \cdot v_j + \sum_{i \in I \cup \tilde{J}} \lambda_i \cdot v_i = 0$$

wegen der linearen Unabhängigkeit der $\{v_i\}_{i \in I \cup \tilde{J}}$ muss $\lambda \neq 0$ gelten

$$\implies v_j = - \sum_{i \in I \cup \tilde{J}} \frac{\lambda_i}{\lambda} \cdot w_i \in \text{Span } B$$

Dies gilt für alle $j \in J \setminus \tilde{J} \implies v_j \in \text{Span } B \ \forall j \in J \implies B$ Basis

□

**Beispiel 3.22:** In $V = \mathbb{R}^3$ bilden die Vektoren $\{e_1, e_2, e_3\}$ die Standardbasis. Des Weiteren sind die Vektoren $u_1 = (3, 1, 0)$ und $u_2 = (1, 3, 0)$ linear unabhängig. Satz 3.21 liefert, dass $\{u_1, u_2, e_3\}$ eine Basis ist.

**Satz 3.23:** Austauschsatz von Steinitz

(Ernst Steinitz, deutscher Mathematiker, 1871 - 1928)

Sei $(V, +, \cdot)$ ein $K$-Vektorraum,

- $B = \{v_1, ..., v_n\}$ eine (endliche Basis)
- $C = \{u_1, ..., u_m\}$ eine linear unabhängige Familie

Dann ist $m \leq n$ und nach geeigneten umnummerieren der Vektoren in $B$ ist das durch austauschen der ersten $m$-Vektoren erhaltene System

$$\tilde{B} := \{u_1, ..., u_m, v_{m+1}, ..., v_n\} \text{ eine Basis von } V \text{ über } K$$

*Beweis:* Aus dem Basisergänzungssatz folgt, dass man das linear unabhängig System $u_1, ..., u_m$ zu einer Basis $u_1, ..., u_m, v_{j_1}, ..., v_{j_{k_0}}$ für ein $k_0 \geq 0$ und geeignete Indizes $j_1, ..., j_{k_0} \in \{1, ..., n\}$ erweitern kann.
Die Menge $\left\{u_1, ..., u_{m-1}, v_{j_1}, ..., v_{j_{k_0}}\right\}$ ist immer noch linear unabhängig aber kein Basis. Aus dem Basisergänzungssatz folgt wieder, dass man diese Menge zu einer Basis $\left\{u_1, ..., u_{m-1}, v_{j_1}, ..., v_{j_{k_0}}, v_{j_{k_0+1}}, ..., v_{j_{k_1}}\right\}$ für ein $k_1 > k_0$ und weitere Indizes $j_{k_0+1}, ..., v_{k_1} \in \{1, ..., n\}$. Setzt man dieses Verfahren induktiv $v$-mal fort, erhält man im $r$-ten Schritt eine Basis $\left\{u_1, ..., u_{m-r}, v_{j_1}, v_{j_2}, ..., v_{j_{k_{r-1}}}, v_{j_{k_{r-1}+1}}, ...., v_{j_{k_r}}\right\}$ für ein $k_r > k_{r-1}$ und weitere Indizes $j_{k_{r-1}+1}, ..., j_{k_r} \in \{1, ..., n\}$. Nach $m$ Schritten sind alle $u_i, 1 \leq i \leq m$ ersetzt.

Als neue Basis erhält man

$$\hat{B} := \left\{v_{j_1}, ..., v_{j_m}\right\}$$

welche ausschließlich Vektoren aus $B$ enthält. $B$ war ein minimales Erzeugendensystem. Also muss die neue Menge $\hat{B}$ bis auf die Umordnung mit der Menge $B$ übereinstimmen. Für die Menge der Indizes gilt also:

$$\hat{B} = \left\{v_{j_1}, ..., v_{j_{k_m}}\right\} = \{v_1, ..., v_n\} = B$$

Also folgt: $k_m = n$

Wir haben jeweils mindestens einen Vektor ergänzt, d.h.

$$k_m > k_{m-1} > ... > k_1 > 0 \Longrightarrow k_m \geq m \Longrightarrow n = k_m \geq m \Longrightarrow n \geq m \Longrightarrow \text{erste Aussage}$$

Dann folgt die zweite Aussage aus dem Basisergänzungssatz.

□

**Lemma 3.24:** Ist $(V, +, \cdot)$ ein von endlich vielen Vektoren erzeugter $K$-Vektorraum, so besitzt $V$ eine Basis und je zwei Basen von $V$ haben gleich viele Elemente.

*Beweis:* Sei $V = \text{Span}\{v_1, ..., v_n\}$ mit $v_1 \neq 0$. Nach Satz 3.21 kann $\{v_1\}$ durch Hinzunahme von geeigneten Elementen aus $\{v_2, ..., v_n\}$ zu einer Basis von $V$ ergänzen. Also besitzt $V$ eine Basis mit endlich vielen Elementen.

Seien $U = \{u_1, ..., u_l\}$ und $W = \{w_1, ..., w_k\}$ zwei solche Basen. Dann folgt aus dem Satz 3.23 aus Symmetrie, dass $k = l$.

□

**Ausblick:** Man kann mit Konzepten der Mengenlehre auch zeigen, dass es für unendlich erzeugte Vektorräume $V$ gilt: Für je zwei Basen $\{u_i\}_{i\in I}$ und $\{w_j\}_{i\in J}$ von $V$ existiert eine bijektive Abbildung $f : I \to J$.

Folgerung aus Satz 3.8 in Zusammenhang mit Lemma 3.24: Da für eine Basis $B := \{v_1, ..., v_n\}$ eines $K$-Vektorraums $V$ gilt, dass Span $B = V$, sind für $v \in V$ die Koeffizienten (= Koordinaten) $\lambda_1, ..., \lambda_n$ zur Darstellung von $v$ eindeutig.

**Beispiel 3.25:** für $V = \mathbb{R}^3$ sind

$$B_1 := \left\{ \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\} \text{ und } B_2 := \left\{ \begin{pmatrix}-2\\-1\\0\end{pmatrix}, \begin{pmatrix}-2\\3\\0\end{pmatrix}, \begin{pmatrix}-5\\0\\2\end{pmatrix} \right\}$$

zwei Basen. Der Vektor $v = (-5, 11, 2)$ besitzt bezüglich $B_1$ die Koordinaten $\lambda_1 = -5, \lambda_2 = 11, \lambda_3 = 2$. Was sind die Koordinaten bezüglich $B_2$? Es muss gelten:

$$a\begin{pmatrix}2\\-1\\0\end{pmatrix} + b\begin{pmatrix}-2\\3\\0\end{pmatrix} + c\begin{pmatrix}-5\\0\\2\end{pmatrix} = \begin{pmatrix}-15\\11\\2\end{pmatrix}$$

anders kann man dies notieren als

$$\begin{pmatrix}2a-2b-5c\\-a+3b+0c\\0a+0b+2c\end{pmatrix} = \begin{pmatrix}-15\\11\\2\end{pmatrix}$$

Berechnung der $a, b, c$ über ein lineares Gleichungssystem ergibt $a = 2, b = 3, c = 1$.

**Beispiel 3.26:** Für den $\mathbb{R}$-Vektorraum $P_{\leq 2}[t]$ der reellen Polynome vom Grad $\leq 2$ sind:

$$B_1 := \{1, t, t^2\} \text{ und } B_2 := \{-t, t^2 - 2, t^2 + 2\}$$

zwei Basen. Sei $p(t) = a + bt + ct^2$ ein beliebiges Polynom aus $P_{\leq 2}[t]$. Dann sind die Koeffizienten für $B_1 : \lambda_1 = a, \lambda_2 = b, \lambda_3 = c$. Für $B_2$ gilt:

$$\text{Basiswechsel, siehe Kapitel 4} \quad \begin{cases} 1 = -\frac{1}{4}(t^2-2) + \frac{1}{4}(t^2+2) \\ t = (-1)(-t) \\ t^2 = \frac{1}{2}(t^2+2) + \frac{1}{2}(t^2-2) \end{cases}$$

Es gilt

$$\begin{aligned} a1 + bt + ct^2 &= a\left(-\frac{1}{4}(t^2-2) + \frac{1}{4}(t^2+2)\right) + b(-1)(-t) + c\left(\frac{1}{2}(t^2+2) + \frac{1}{2}(t^2-2)\right) \\ &= -b(-t) + \left(-\frac{a}{4} + \frac{c}{2}\right)(t^2-2) + \left(\frac{a}{4} + \frac{c}{2}\right)(t^2+2) \end{aligned}$$

## 3.3. Dimensionen

**Definition 3.27: Dimension eines Vektorraums**

Die Dimension eines Vektorraum $(V, +, \cdot)$ über $K$ ist definiert als:

$$\dim_K(V) := \begin{cases} n & \text{falls } V \text{ eine Basis der Länge } n \text{ hat} \\ \infty & \text{sonst} \end{cases}$$

Wenn der Kontext klar ist schreibt man $\dim V$.

**Beispiel 3.28:** Sei $K$ ein Körper. Es gilt

- $\dim_K(V) = n$ genau dann, wenn $V = \{0\}$
- für $V = K^n$ folgt mit der Standardbasis, dass $\dim_K(V) = n$
- für die Dimension eines Vektorraums ist der jeweilige Grundkörper $K$ entscheident, z.B. $\mathbb{C}$ und $K = \mathbb{C}$ gilt $\dim_{\mathbb{C}} V = 1$ für $K = \mathbb{R}$ aber $\dim_{\mathbb{R}} V = 2$.
- der $K$-Vektorraum $P[t]$ ist nicht endlich erzeugt, also $\dim_K P[t] = \infty$

**Beispiel 3.29:** Sei $V = K^n$ für einen Körper $K$. Um zu prüfen, dass $n$ Vektoren aus $V$ eine Basis werden, muss nur deren lineare Unabhängigkeit geprüft werden. Seien z.B. $B$ in $V = \mathbb{R}^3$ die Vektoren

$$v_1 = \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} \; v_2 = \begin{pmatrix} -2 \\ 3 \\ 0 \end{pmatrix} \; v_3 = \begin{pmatrix} -5 \\ 0 \\ 2 \end{pmatrix}$$

gegeben. Sind diese liear unabhängig?

$$\lambda_1 \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} -2 \\ 3 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} -5 \\ 0 \\ 2 \end{pmatrix} \overset{!}{=} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Dazu wird ein lienares Gleichungssystem aufgestellt

$$\begin{pmatrix} 2a - 2b - 5c \\ -a + 3b + 0c \\ 0a + 0b + 2c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$\implies a = 0, b = 0, c = 0$.

Somit sind die Vektoren linear unabhängig.

**Lemma 3.30:** Sei $(V, +, \cdot)$ ein $K$-Vekorraum mit $n := \dim_K V < \infty$ und $B = \{v_1, ..., v_n\} \subset V$ eine Familie von genau $n$ Vektoren. Dann sind folgende Aussagen äquivalent:

1. $B$ ist eine Basis
2. $B$ ist linear unabhängig
3. $B$ ist ein Erzeugendensystem

*Beweis:* (Übungsaufgabe, Blatt 8, Aufgabe 1)

$1 \implies 2$ und $1 \implies 3$: Folgt direkt aus der Definition einer Basis.

$2 \implies 1$: Angenommen $B$ ist keine Basis von $V$. Da $B$ linear unabhängig ist, kann $B$ kein Erzeugendensystem von $V$ sein. Mit dem Basisergänzungssatz (Satz 3.21) lässt sich das linear unabhängige System $B$ mit Vektoren eines Erzeugendensystems von $V$, wir wählen $V$ selbst, zu einer Basis $B'$ ergänzen. Definiere die $B'$ wie folgt:

$$B' = B \cup \{v_{n+1}, ..., v_{n+k}\}, \qquad v_{n+1}, ..., v_{n+k} \in V \setminus B$$

Dann hat $B$ mit Sicherheit mehr als $n$ Elemente. Dies ist ein Widerspruch dazu, dass die Dimension des Vektorraums $n$ ist (Definition 3.27 und Lemma 3.24). Die Annahme muss also falschs sein. $\implies B$ ist eine Basis von $V$.

$3 \implies 1$: Angenommen $B$ ist keine Basis von $V$. Da $B$ ein Erzeugendensystem ist, kann $B$ nicht linear unabhängig sein. Daraus folgt, dass $B$ zu einem minimalen Erzeugendensystem, also einer Basis $B'$ verkürzbar ist. Definiere $B'$ wie folgt:

$$B' = B \setminus \left\{v_{n_0}, ..., v_{n_k}\right\}, \qquad v_{n_0}, ..., v_{n_k} \in B$$

Dann hat $B'$ mit Sicherheit weniger als $n$ Elemente. Dies ist ein Widerspruch dazu, dass die Dimension des Vektorraums $n$ ist. Die Annahme muss also falsch sein. $\implies B$ ist eine Basis von $V$.

□

**Lemma 3.31:** Sei $(V, +, \cdot)$ ein endlich erzeugter $K$-Vektorraum. Jeder Untervektorraum $W \subseteq V$ ist dann ebenfalls endlichdimensional und es gilt:

$$\dim W \leq \dim V$$

mit Gleichheit genau dann, wenn $W = V$.

*Beweis:* jede linear unabhängige Familie in $W$ ist auch linear unabhängig in $V$. Damit besteht sie nach dem Austauschsatz von Steinitz aus höchstens $\dim_K V$ Elementen. Daraus folgt, dass $W$ endlich erzeugt ist mit $\dim_K W \leq \dim_K V$. Im Fall von $\dim_K W = \dim_K V$ folgt mit Lemma 3.30, dass jede Basis von $W$ auch eine Basis von $V$ ist. $\implies V = W$

□

**Achtung:** Die letzte Aussage (d.h. $V = W$) gilt nicht für unendlich erzeugte Vektorräume. Denn der $K$-Vektorraum $P[t]$ aller Polynome hat die Basis der Monome $\{t^n\}_{n \in \mathbb{N}_0}$. Die Menge aller Polynome aus $P[t]$ mit $a_0 = 0$ ist ein Unterraum mit der Basis $\{t^n\}_{n \in \mathbb{N}}$ und wird mit $W$ bezeichnet. Dann gilt

$$\dim_K P[t] = \infty = \dim_K W, \text{aber } P[t] \neq W$$

## 3.4. Direkte Summen

Aus der Definition von Mengenoperationen aus dem ersten Kapitel folgt: sind $U_1$ und $U_2$ zwei Unterräume des $K$-Vektorraums $(V, +, \cdot)$, so gilt für ihren Durchschnitt:

$$U_1 \cap U_2 = \{u \in V \mid u \in U_1 \wedge u \in U_2\}$$

**Definition 3.32: Summe von Mengen**

Sei $(V, +, \cdot)$ ein $K$-Vektorraum für die Unterräume $U_1, ..., U_r \subseteq V$ definiert man ihre Summe als die Teilmenge

$$U_1 + U_2 + ... + U_r := \{u_1 + u_2 + ... + u_r \mid u_i \in U_i \text{ für } 1 \leq i \leq r\} \subseteq V$$

Für den Durchschnitt und die Summe von Untervektorräumen gelten folgende Regeln:

**Lemma 3.33:** Sind $U_1, U_2, U_3$ Unterräume des $K$-Vektorraums $(V, +, \cdot)$, dann gilt:

1. $U_1 \cap U_2$ und $U_1 + U_2$ sind Unterräume von $V$
2. $U_1 + (U_2 + U_3) = (U_1 + U_2) + U_3$ und $U_1 + U_2 = U_2 + U_1$
3. $U_1 + \{0\} = U_1$ und $U_1 + U_1 = U_1$
4. $U_1 \subseteq U_1 + U_2$ mit Gleichheit, d.h. $U_1 = U_1 + U_2$, wenn $U_2 \subseteq U_1$

*Beweis:* (Übungsaufgabe)

□

**Beispiel 3.34:** Sei $V := \mathbb{R}^3, U_1 := \text{Span}\{(1,0,0),(0,1,0)\}, U_2 := \{(0,1,0),(0,0,1)\}$. Dann gilt für $v \in V, v = (v_1, v_2, v_3)$

$$v = v_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + v_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + v_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Also gilt: $U_1 + U_2 = V$, insbesondere gilt auch $\dim(U_1 + U_2) = 3$, $\dim U_1 = 2 = \dim U_2$. Weiterhin gilt

$$v_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in U_1 \text{ und } v_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + v_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \in U_2$$

Aslo ist die Darstellung von $v$ als Summe **nicht** eindeutig. Insbesondere ist $\dim(U_1 \cap U_2) = 1$.

**Lemma 3.35:** Sei $V$ ein $K$-VR und $r \in \mathbb{N}$ und $U_1, ..., U_r$ Untervektorräume von $V$. Dann sind folgende Aussagen äquivalent.

1. Für $u \in \sum_{i=1}^{r} U_i$ existieren eindeutige $u_i \in U_i, i \in \{1, ..., r\}$ mit $u = \sum_{i=1}^{r} u_i$
2. Für $u_i \in U_i, i \in \{1, ..., r\}$ mit $0 = \sum u_i$ gilt
$$u_i = 0 \qquad i \in \{1, ..., r\}$$
3. Für $i \in \{1, ..., r\}$ gilt
$$U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} u_i = \{0_V\}$$

*Beweis:* (Übungsaufgabe, Blatt 9, Aufgabe 1)

$1 \implies 2$:

Eine Darstellung des Nullvektors ist $0 = 0_1 + ...0_r$ mit $0_i \in U_i$. Da jeder Vektor eine eindeutige Darstellung bestizt, folgt 2).

$2 \implies 3$: Beweis durch Kontraposition

Angenommen es gilt $U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} u_i \neq \{0_V\}$. Dann existiert ein Vektor $v$ mit $v \in U_i$ und $v \in U_1 + ... + U_{i-1} + U_{i+1} + ... + U_r$. Da $U_i$ und $U_1 + ... + U_{i-1} + U_{i+1} + ... + U_r$ Untervektorräume von $V$ bilden, gilt auch $-v \in U_i$ und $-v \in U_1 + ... + U_{i-1} + U_{i+1} + ... + U_r$. Daraus folgt

$$\sum_{j=1}^{r} u_j = v + \sum_{\substack{j=1 \\ j \neq i}}^{r} u_i = v + (-v) = 0$$

Somit gilt

$$\sum u_i = 0 \text{ aber } u_j \neq 0, j \in \{1, ..., r\}$$

$3 \implies 1$: Beweis durch Kontraposition

Angenommen ein Vektor $v \in V$ besitzt keine eindeutige Darstellung. Dann gilt für ein $u \in U_i$:

$$u = \sum_{j=1}^{r} u_j \text{ mit } u_j = 0, j \neq i \text{ und } u_j = u, j = i$$

Dann gilt $u \in U_i$ und insbesondere $u \in U_1 + ... + U_{i-1} + U_{i+1} + ...U_r$. Somit ist die Schnittmenge $U_i \cap U_1 + ... + U_{i-1} + U_{i+1} + ... + U_r \neq \{0_V\}$.

□

**Definition 3.36: Direkte Summe**

Sei $V$ ein $K$-VR und $r \in \mathbb{N}, U_1, ..., U_r$ Untervektorräume von $V$. Dann heißt die Summe $\sum U_i$ **direkt**, falls eine der Bedingungen aus Lemma 3.35 zutrifft.

Wir schreiben dann

$$U_1 \oplus U_2 \oplus ... \oplus U_r$$

**Beispiel:** Seien $V, U_1, U_2$ wie im Beispeil 3.34. Dann gilt $V = U_1 + U_2$, aber nicht $U_1 \oplus U_2$. Sei weiter $U_3 := \text{Span}\{(0,0,1)\}$. Dann gilt $V = U_1 + U_3$ und $U_1 \oplus U_3$.

**Lemma** (ohne Nummer)

Sei $V$ ein $K$-VR. Seien $U_1, U_2$ UVRs von $V$. Dann gilt

$$\dim(U_1 + U_2) \leq \dim U_1 + \dim U_2 \ (*)$$

Falls $U_1 \oplus U_2$ gilt sogar Gleichheit.

Dabei sei $\infty + \infty = \infty, \infty + n = \infty, n \leq \infty$ für $n \in \mathbb{N}$ und es gilt $\infty \leq \infty$.

*Beweis:*

**Fall 1:** $\dim U_1 = \infty$ oder $\dim U_2 = \infty$. Dann gilt $(*)$ nach den Rechenregeln der erweiterten Arithmetik.

Andernfalls existieren $m, l \in \mathbb{N}$ mit $\dim U_1 = m$ und $\dim U_2 = l$.

Sei $u_1, ..., u_m$ eine Basis von $U_1$ und $u_{m+1}, ..., u_{m+l}$ eine Basis von $U_2$. Sei weiter $u \in U_1 + U_2$, dann existieren $v \in U_1$ und $w \in U_2$, sodass $u = v + w$. Zu $v$ und $w$ existieren $\lambda_1, ..., \lambda_m \in K$ bzw. $\lambda_{m+1}, ..., \lambda_{m+l} \in K$ mit

$$v = \sum_{i=1}^{m} \lambda_i u_i \text{ und } w = \sum_{i=m+1}^{m+l} \lambda_i u_i$$

Also $u = v + w$

$$u = \sum_{i=1}^{m} \lambda_i u_i + \sum_{i=m+1}^{m+l} \lambda_i u_i = \sum_{i=1}^{m+l} \lambda_i u_i$$

Also ist $u_1, ..., u_{m+l}$ ein Erzeugendensystem von $U_1 + U_2$. Es folgt $\dim(U_1 + U_2) \leq m + l = \dim U_1 + \dim U_2$.

Sei nun $U_1 \oplus U_2$. Falls $\dim(U_1 + U_2) = \infty$ gilt $(*)$ mit Gleichheit. Andernfalls existieren $n \in \mathbb{N}$ mit $\dim(U_1 + U_2) = n$. Da $U_1$ und $U_2$ Untervektorräume von $U_1 + U_2$ sind, existieren $m, l \in \mathbb{N}$ mit $\dim U_1 = m \leq n$ und $\dim U_2 = l \leq n$. Sei wieder $u_1, ..., u_m$ eine Basis von $U_1$ und $u_{m+1}, ..., u_{m+l}$ eine Basis von $U_2$. Seien $\lambda_1, ..., \lambda_{m+l} \in K$ mit

$$0 = \sum_{i=1}^{m+l} \lambda_i u_i = \underbrace{\sum_{i=1}^{m} \lambda_i u_i}_{=v \in U_1} + \underbrace{\sum_{i=m+1}^{m+l} \lambda_i u_i}_{=w \in U_2}$$

Da $U_1 \oplus U_2$ folgt $v = 0 = w$. Da $u_i, i \in \{1, ..., m\}$ eine Basis von $U_1$ ist, folgt $0 = \lambda_i i \in \{1, ..., m\}$. Analog folgt dies für $\lambda_{m+1}, ..., \lambda_{m+l}$. Also ist $u_1, ..., u_{m+l}$ linear unabhängig.

$\Longrightarrow \dim U_1 + \dim U_2 = m + l \leq \dim(U_1 + U_2)$

□

**Satz 3.38:** Sei $V$ ein $K$-VR und $U$ ein UVR von $V$. Dann existiert ein Untervektorraum $U^\top \subseteq V$ mit $V = U \oplus U^\top$ (heißt $V = U + U^\top$ und $U \oplus U \oplus U^\top$). Insbesondere gilt dann

$$\dim V = \dim U + \dim U^\top$$

*Beweis:* Sei $(u_i)_{i \in I}$ eine Basis von $U$. Nach Satz 3.21 existiert eine Menge $J$ und Vektoren $w_j, j \in J$ mit

$$I \cap J = \emptyset \text{ und } v_k := \begin{cases} u_k \, k \in I \\ w_k k \in J \end{cases} \qquad k \in I \cup J$$

ist eine Basis von $V$.

Mit $U^\top = \text{Span}\{w_j\}_{j \in J}$ gilt dann $V = U + U^\top$. Sei $v \in V$, dann existieren eindeutige $\{\lambda_i\}_{i \in I} \subseteq K$ mit

$$v = \sum_{k \in I \cup J} \lambda_k v_k = \underbrace{\sum_{k \in I} \lambda_k v_k}_{\in U} + \underbrace{\sum_{k \in J} \lambda_k v_k}_{\in U^\top}$$

die Eindeutigkeit der $\lambda_k, k \in I \cup J$ garantiert die Eindeutigkeit von $u$ und $w$. Also $U \oplus U^\top$.

□

Ein durch Satz 3.38 aus $U$ und $V$ erhaltener Untervektorraum $U^\top$ heißt **Komplement** von $U$ in $V$.

**Beispiel 3.39:** Seien $V, U_1$ und $U_3$ wie in Beispiel 3.37. Dann gilt $V = U_1 \oplus U_3$ d.h. $U_3$ ist ein Komplement von $U_1$ in $V$. Sei weiter $\widetilde{U_3} := \text{Span}\{(1, 0, 0)\}$. Dann gilt auch $V = U_1 \oplus \widetilde{U_3}$.

Insbesondere sind die Komplemente aus Satz 3.38 nicht eindeutig bestimmt.

**Satz 3.40:** Sei $V$ ein endlich erzeugter $K$-VR. Seien $U_1, U_2$ UVRs von $V$. Dann gilt

$$\dim(U_1 \cap U_2) + \dim(U_1 + U_2) = \dim U_1 + \dim U_2$$

*Beweis:* Sei $U := U_1 \cap U_2$ und für $i \in \{1, 2\}$ sei $W_i$ das Komplement von $U$ in $U_i$. Es gilt

$$U_i = U \oplus W_i, \; i \in \{1, 2\}$$

Dann gilt $U_1 + U_2 = U + W_1 + U + W_2 = U + W_1 + W_2$

$$\begin{aligned} W_1 \cap (U + W_2) &= W_1 \cap W_2 \\ &= W_1 \cap U_1 \cap U_2 (\text{da } W_1 \subseteq U_1) \\ &= W_1 \cap U \\ &= \{0_V\} \end{aligned}$$

Analog folgt $W_2 \cap (U + W_1) = \{0_V\}$. Sei $u \in U_1, w_1 \in W_1, w_2 \in W_2$ mit $0 = u + w_1 + w_2$, dann gilt

$$\begin{aligned} w_1 &= -(u + w_2) \\ w_2 &= -(u + w_1) \end{aligned}$$

Also $w_1 = 0$ und $w_2 = 0$ und damit auch $u = 0$. Also $U \oplus W_1 \oplus W_2$. Es folgt

$$\begin{aligned} \dim(U_1 + U_2) &= \dim(U + W_1) + \dim W_2 \\ &= \dim U + \dim W_1 + \dim W_2 \end{aligned}$$

Aus der Wahl von $W_i$ folgt

$$\begin{aligned} \dim U_1 &= \dim U + \dim W_1 \\ \dim U_2 &= \dim U + \dim W_2 \end{aligned}$$

durch einsetzen erhält man

$$\dim U + \dim(U_1 + U_2) = \dim U_1 + \dim U_2$$

oder (nur für endliche wegen $-\infty$)

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim U$$

□

# 4. Lineare Abbildungen

Nun behandeln wir Abbildungen, die zur Vektorstruktur "passen". Diese heißen lineare Abbildungen. Unser Ziel ist es, die Eigenschaften von linearen Abbildungen zu analysieren.

## 4.1. Definitionen und grundlegende Eigenschaften

**Definition 4.1: Lineare Abbildung**

Seien $V$ und $W$ zwei $K$-Vektorräume. Eine Abbildung $f : V \to W$ heißt **lineare Abbildung**, wenn gilt

1. $\underbrace{f(\lambda \cdot v)}_{\text{Skalarmultiplikation in } V} = \underbrace{\lambda \cdot f(v)}_{\text{Skalarmultiplikation in } W} \qquad \forall\, v \in V, \forall\, \lambda \in K$
2. $\underbrace{f(v+w)}_{\text{Addition in } V} = \underbrace{f(v) + f(w)}_{\text{Addition in } W}$

Die Menge aller linearen Abbildungen von $V$ nach $W$ bezeichnet man mit $L(V, W)$. Eine lineare Abbildung $f : V \to W$ wird auch **lineare Transformation** oder **(Vektorraum-) Homomorphismus** genannt.

Eine bijektive lineare Abbildung nennt man **(Vektorraum-) Isomorphismus**. Gibt es für zwei $K$-Vektorräume $V$ und $W$ einen Isomorphismus, so heißen die Räume $V$ und $W$ isomorph, geschrieben

$$V \cong W$$

Eine lineare Abbildung $f : V \to V$ heißt **Endomorphismus** und ein bijektiver Endomorphismus heißt **Automorhpismus**.

**Bemerkung:** Als Übungsaufgabe:

$$\text{Definition 4.1, 1) + 2)} \iff f(\lambda v + \mu w) = \lambda f(v) + \mu f(w) \qquad \forall v, w \in V, \forall \lambda, \mu \in K$$

**Beispiel 4.2:** Für $a \in \mathbb{R}$ ist $f : \mathbb{R} \to \mathbb{R}, f(x) = ax$ eine lineare Abbildung. Ihr Graph ist eine Gerade durch den Ursprung.

Betrachte eine Gerade $f(x) = ax + b$ und betrachte

$$f(x+y) = a(x+y) + b$$
$$f(x) + f(y) = a(x) + b + a(y) + b = a(x+y) + 2b$$

$f$ ist also nur eine lineare Abbildung, wenn $b = 0$ gilt. Streng genommen sind geraden der Form $f(x) = mx + n$ keine linearen Abbildung. Korrekt ist, sie als affine Abbildungen zu bezeichnen.

**Beispiel 4.3:** Für $a, b, c, d \in \mathbb{R}$ ist $f : \mathbb{R}^2 \to \mathbb{R}^2$

$$f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} \in \mathbb{R}^2$$

eine lineare Abbildung, denn

1)

$$\begin{aligned} f\left(\lambda\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) &= \begin{pmatrix} a\lambda x_1 + b\lambda x_2 \\ c\lambda x_1 + d\lambda x_2 \end{pmatrix} = \begin{pmatrix} \lambda(ax_1 + bx_2) \\ \lambda(bx_1 + cx_2) \end{pmatrix} \\ &= \lambda\begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} = \lambda f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) \checkmark \end{aligned}$$

2)

$$\begin{aligned} f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) &= f\left(\begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix}\right) = \begin{pmatrix} a(x_1 + y_1) + b(x_2 + y_2) \\ c(x_1 + y_1) + d(x_2 + y_2) \end{pmatrix} \\ &= \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} + \begin{pmatrix} ay_1 + by_2 \\ cy_1 + dy_2 \end{pmatrix} = f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) + f\left(\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) \end{aligned}$$

Damit haben wir auch bewiesen, dass für $\varphi \in \mathbb{R}$ die Abbildung

$$f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} \cos(\varphi)x_1 - \sin(\varphi)x_2 \\ \sin(\varphi)x_1 + \cos(\varphi)x_2 \end{pmatrix}$$

linear ist. Dies ist eine Drehung um den Ursprung mit dem Drehwinkel $\varphi$. Für $\varphi = 45°$

$$f\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = (\cos(45°), \sin(45°)) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

**Beispiel 4.4:** Sei $V = C^{\infty(\mathbb{R})}$ der reelle Vektorraum aller unendlichen oft differenzierbaren Funktionen $g : \mathbb{R} \to \mathbb{R}$ mit punktweisen Addition und skalaren Multiplikation. Dann ist

$$\frac{d}{dx} : V \to V, f \mapsto f' = \frac{d}{dx} f$$

eine lineare Abbildung, denn für alle $f, g \in V$ und $a, b \in \mathbb{R}$ gilt:

$$\begin{aligned} (f + g)'(x) &= f'(x) + g'(x) \qquad \forall x \in \mathbb{R} \\ (a \cdot f)'(x) &= af'(x) \qquad \forall x \in \mathbb{R} \end{aligned}$$

**Lemma 4.5:** Seien $V, W$ $K$-Vektorräume und $f : V \to W$ eine lineare Abbildung, $0_V$ der Nullvektor in $V$ und $0_W$ der Nullvektor in $W$. Dann gilt

1. $f(0_V) = 0_W$
2. $f(-x) = -f(x) \qquad \forall x \in V$

*Beweis:* Es folgt aus Definition 4.1, 1), dass

$$f(0_V) = f(0_K \cdot 0_V) = 0_K \cdot f(0_V) = 0_W$$
$$f(-x) = f((-1) \cdot x) = (-1) \cdot f(x) = -f(x)$$

□

**Lemma 4.6:** Seien $V, W$ $K$-Vektorräume. Für $f, g \in L(V, W)$ und $\lambda \in K$ seien $f + g$ und $\lambda \cdot f$ definiert durch

$$(f + g)(v) = f(v) + g(v) \qquad \forall v \in V$$
$$(\lambda \cdot f)(v) = \lambda f(v) \qquad \forall v \in V, \forall \lambda \in K$$

Dann ist $(L(V, W), +, \cdot)$ ein $K$-Vektorraum.

*Beweis:* (Übungsaufgabe)

□

**Lemma 4.7:** Sei $V$ ein $K$-Vektorraum und $B \coloneqq \{v_1, ..., v_n\} \subset V$ eine endliche Familie von Vektoren. Dann ist:

$$\Phi_B : K^n \to V, (a_i)_{i \leq i \leq n} \mapsto \sum_{i=1}^{n} a_i v_i$$

ein Homomorphimus von $K$-Vekroräumen.

*Beweis:* Seien $\lambda \in K$ und zwei Tupel $a = (a_1, ..., a_n) \in K^n$, $b = (b_1, ..., b_n) \in K^n$ gegeben. Mit der Definition der direkten Summe ist.

$$a + \lambda b = (a_i + \lambda b_i)_{1 \leq i \leq n} \in K^n$$

und deswegen gilt

$$\Phi_B(a + \lambda b) = \Phi_B(a_i + \lambda b_i)_{1 \leq i \leq n} = \sum_{i=1}^{n} \underbrace{(a_i + \lambda b_i)}_{\in K} \underbrace{v_i}_{\in V}$$
$$= \sum_{i=1}^{n} a_i v_i + \lambda \sum_{i=1}^{n} b_i v_i = \Phi_B(a) + \lambda \Phi_B(b) = \text{Def 4.1}$$

□

**Wichtig:** $B = \{v_1, ..., v_n\}$ ist endlich! Für $B$ mit unendlich vielen Elementen bräuchte man eine äußere direkte Summe.

Aus abstrakter Sicht kennen wir jetzt endlichdimensionale Vektorräume, denn: Jeder endlichdimensionaler Vektorraum ist isomorph zu einer direkten Summe von Kopien des Grundkörpers.

**Satz 4.8:** Struktursatz für Vektorräume

Sei $V$ ein $K$-Vektorraum und $B = \{v_1, ..., v_n\} \subset V$ eine Basis von $V$. Dann ist die Abbildung

$$\Phi_B : K^n \to V, (\lambda_i)_{1\leq i\leq n} \mapsto \sum_{i=1}^{n} \lambda_i v_i$$

ein Isomorphismus, d.h. $K^n \cong V$.

*Beweis:* Nach Lemma 4.7 ist $\Phi_B$ eine lineare Abbildung. Zu zeigen: $\Phi_B$ ist bijektiv

$$B \text{ Basis} \Longrightarrow \text{Span } B = V \Longrightarrow \Phi_B \text{ surjektiv}$$

$$B \text{ Basis} \Longrightarrow \text{jedes } v \in V \text{ besitzt eine eindeutige Darstellung } v = \sum_{i=1}^{n} \lambda_i v_i$$

□

Für eine gegebene Basis $B$ nenn man $\Phi_B$ auch Koordinatenabbildung.

$$\Phi \text{ bijektiv} \Longrightarrow \exists \Phi_B^{-1} \text{ als inverse Abbildung}$$

**Beispiel 4.9:** Sei $K^{n+1} = \mathbb{R}^{n+1}$ und $P_{\leq n}[t]$ der Raum der Polynome von Grad kleiner gleich $n$ für $n \in \mathbb{N}$. Eine Basis von $P_{\leq n}[t]$ ist gegeben durch $B = \{1, t, t^2, ..., t^n\}$, vergleiche Beispiel 3.13.

Dann ist:

$$\Phi_B : K^{n+1} \to P_{\leq n}[t],\ (a_i)_{0\leq i\leq n} \mapsto \sum_{i=0}^{n} a_i t^i$$

ein Isomorphismus. Weitherhin ist

$$\Phi_B^{-1} = P_{\leq n}[t] \to K^{n+1},\ p(t) = \sum_{i=0}^{n} a_i t^i \mapsto (a_i)_{0\leq i\leq n} \in K^{n+1}$$

die inverse Koordinatenabbildung.

Um eine lineare Abbildung zu definieren, reicht es ihre Werte auf einer beliebigen Basis anzugeben.

**Lemma 4.10:** Sei $V$ ein endlichdimensionaler Vektorraum über $K$ mit einer Basis $B := \{v_1, .., v_n\}$, $W$ ein beliebiger $K$-Vektorraum und $C = \{w_1, ..., w_n\}$ einer Familie von Vektoren in $W$. Dann gibt es genau eine lineare Abbildung von $f$ von $V$ nach $W$ mit

$$f(v_i) = w_i \text{ für } 1 \leq i \leq n$$

*Beweis:* zu zeigen: Existenz und Eindeutigkeit

Eindeutigkeit: Seien $f, g \in L(V, W)$ mit $f(v_i) = g(v_i) = w_i, \quad \forall i \in \{1, ..., n\}$. Sei $v \in \sum \lambda_i v_i$: Dann gilt

$$\begin{aligned} f(v) = f\Big(\sum \lambda_i v_i\Big) &= \sum_{i=1}^{n} \lambda_i f(v_i) \\ &= \sum_{i=1}^{n} \lambda_i w_i = \sum_{i=1}^{n} \lambda_i g(v_i) = g(v) \\ &\Longrightarrow f(x) = g(x) \ \forall v \in V \\ &\Longrightarrow f \text{ ist eindeutig bestimmt} \end{aligned}$$

Existenz: $B$ Basis $\Longrightarrow$ Span $B = V \Longrightarrow$ zu $v \in V$ existieren nach Satz 3.8 eindeutige Koordinaten

$$\lambda_i^v, 1 \leq i \leq n \text{ mit } v = \sum_{i=1}^{n} \lambda_i^v v_i$$

Definiere $f : V \to W, \ f(v) = \sum_{i=1}^{n} \lambda_i^v w_i \in W \Longrightarrow f(v_i) = w_i$

Ist $f$ linear?

Für jedes $\mu \in K$ gilt:

$$\begin{aligned} \mu_v = \sum_{i=1}^{n} (\mu \lambda_i^v v_i) \Longrightarrow f(\mu_v) &= f\left(\sum_{i=1}^{n} (\mu \lambda_i^v w_i)\right) \\ = \mu \sum \lambda_i^v w_i = \mu f(v) &\qquad \text{erste Eigenschaft } \checkmark \end{aligned}$$

Sei $u = \sum_{i=1}^{n} \lambda_i^u v_i \Longrightarrow$

$$\begin{aligned} f(v+u) = f\left(\sum_{i=1}^{n} \lambda_i^v v_i + \sum_{i=1}^{n} \lambda_i^u v_i\right) &= f\left(\sum_{i=1}^{n} (\lambda_i^v + \lambda_i^u) v_i\right) \\ = \sum_{i=1}^{n} (\lambda_i^v + \lambda_i^u) w_i = \sum_{i=1}^{n} \lambda_i^v w_i + \sum_{i=1}^{n} \lambda_i^u w_i & \\ = f(v) + f(w) &\qquad \text{zweite Eigenschaft } \checkmark \\ \Longrightarrow f \text{ linear} & \end{aligned}$$

□

## 4.2. Kern, Bild und Rang von linearen Abbildungen

Kern und Bild wurden bereits im Kapitel 2 behandelt. Hier behandeln wir die Konzepte im Kontext linearer Abbildungen.

**Definition 4.11: Kern, Bild**

Es seien $V$ und $W$ $K$-Vektorräume sowie $f : V \to W$ eine lineare Abbildung. Die Menge

$$\ker(f) := \{v \in V \mid f(v) = 0\}$$

heißt **Kern** der linearen Abbildung $f$.

Die Menge

$$\mathrm{im}(f) := f(V) = \{w \in W \mid \exists v \in V : w = f(v)\}$$

heißt **Bild** der linearen Abbildung $f$.

**Beispiel 4.12:**

1. Für den Isomorphismus aus Beispiel 4.9 gilt:

   $$\Phi_B : K^{n+1} \to P_{\leq n}[t]$$

   mit

   $$\ker(\Phi_B) = \{0_{K^{n+1}}\}$$

   denn nur $0 \in K^{n+1}$ wird auf das Nullpolynom abgebildet.
2. Fortsetzung von Beispiel 4.3 (Drehungsmatrizen)

   Für $a = 0 = b, c, d \in \mathbb{R}, c \neq 0$ und damit

   $$f : \mathbb{R}^2 \to \mathbb{R}^2,\ f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} = \begin{pmatrix} 0 \\ cx_1 + dx_2 \end{pmatrix}$$

   gilt:

   $$\ker(f) = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \mid x_1 = -\frac{dx^2}{c} \right\},$$

   $$\mathrm{im}(f) = \left\{ \begin{pmatrix} 0 \\ x \end{pmatrix} \mid x \in \mathbb{R} \right\} \subset \mathbb{R}^2$$

   weil $x = cx_1 + dx_2$ für jedes $x \in \mathbb{R}$ lösbar ist ($c \neq 0$).

**Lemma 4.13:** Es seien $V$ und $W$ zwei $K$-Vektorräume und $f : V \to W$ eine lineare Abbildung. Dann gilt :

1. $\ker(f) \subseteq V$ ist ein Untervektorraum von $V$
2. $\mathrm{im}(f) \subseteq W$ ist ein Untervektorraum von $W$

*Beweis:*

zu 1) $0_V \in \ker(f) \Longrightarrow \ker(f) \neq \emptyset$. Weitherhin ist $\ker(f)$ abgeschlossen bezüglich Addition und Multiplikation, denn sei $x, \tilde{x} \in \ker(f), \lambda, \mu \in K$.

Zu zeigen: $\lambda x + \mu \tilde{x} \in \ker(f)$

$$f(\lambda x + \mu\tilde{x}) = \lambda f(x) + \lambda f(\tilde{x}) = 0_W$$
$$\Longrightarrow \text{Abgeschlossenheit in } V$$

Daraus folgt auch mit $\tilde{x} = 0_V$ die Abgeschlossenheit bezüglich der Multiplikation.

$\Longrightarrow \ker(f)$ Unterraum ✓

zu 2) $f(0_V) = 0_W \in \text{im}(f) \neq \emptyset$

zu zeigen: $\text{im}(f)$ abgeschlossen bezüglich $+$ und $\cdot$. Seien $y, \tilde{y} \in \text{im}(f), \lambda, \mu \in K$

$\Longrightarrow x, \tilde{x} \in V : f(x) = y \wedge f(\tilde{x} = \tilde{y})$. Dann gilt für $\lambda x + \mu\tilde{x}$, dass

$$f(\lambda x + \mu\tilde{x}) = \lambda f(x) + \mu f(\tilde{x}) = \lambda y + \mu\tilde{y}$$
$$\Longrightarrow \lambda x + \mu\tilde{x} \text{ ist das Urbild von } \lambda y + \mu\tilde{y}$$
$$\Longrightarrow \lambda y + \mu\tilde{y} \in \text{im}(f)$$

□

**Definition 4.14: Rang einer Abbildung**

Es seien $V$ und $W$ zwei $K$-Vektoräume und $f : V \to W$ eine lineare Abbildung. Der **Rang** der linearen Abbildung $f$ ist definiert als

$$\text{rg}(f) := \dim_K(\text{im}(f))$$

**Lemma 4.15:** Es seien $V$ und $W$ zwei $K$-Vektorräume und $f \in L(V, W)$, $W$ sei endlichdimensional. Dann gilt

1. $f$ surjektiv $\iff \text{rg}(f) = \dim W$
2. $f$ injektiv $\iff \dim(\ker(f)) = 0$

*Beweis:*

zu 1) "$\Longrightarrow$": Sei $f$ surjektiv. Dann gilt $W = f(v) = \text{im}(f)$ und damit auch

$$\text{rg}(f) = \dim(\text{im}(f)) = \dim W$$

"$\Longleftarrow$": Es gilt $\text{rg}(f) = \dim(\text{im}(f)) = W$. Nach Lemma 4.13 ist $\text{im}(f)$ ein Vektorraum. Da $W$ endlichdimensional ist, folgt mit Lemma 3.31

$$\Longrightarrow \text{im}(f) = W, \ f \text{ surjektiv}$$

zu 2) "$\Longrightarrow$": Sei $f$ injektiv. Wir wissen $f(0_V) = 0_W$.

$$\Longrightarrow \ker(f) = \{v \in V \mid f(v) = 0\} = \{0_V\} \Longrightarrow \dim(\ker(f)) = 0$$

"$\Longleftarrow$": Es gilt $\dim(\ker(f)) = 0 \Longrightarrow \ker(f) = \{0_V\}$. Damit erhält man für $x, \tilde{x} \in V$ wegen der Linearität in $f$:

$$f(x) = f(\tilde{x}) \iff f(x) - f(\tilde{x}) = 0 \iff f(x - \tilde{x}) = 0 \in \ker(f)$$
$$\iff x - \tilde{x} \in \ker(f) \iff x - \tilde{x} = 0 \iff x = \tilde{x} \ f \text{ injektiv}$$

□

**Satz 4.16:** Dimensionsformel

Seien $V$ und $W$ zwei endlichdimensionale $K$-Vektorräume und $f \in L(V, W)$. Dann gilt

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

*Bewei:* Mit $r := \dim(\ker(f)), n := \dim V$ gilt

$$v < \infty \text{ und } r < \infty \text{ sowie } r \leq n$$

Sei $\tilde{B} := \{v_1, ..., v_r\}$ eine Basis von $\ker(f)$. Mithilfe des Austauschsatzes von Steinitz (3.23) kann $\tilde{B}$ zu einer Basis $B = \{v_1, ..., v_r, v_{r+1}, ..., v_n\}$ von $V$ ergänzt werden.

zu zeigen: $C = \{f(v_{r+1}), ..., f(v_n)\}$ ist eine Basis von $\mathrm{im}(f)$.

1) Erzeugendensystem

$f$ linear $\Longrightarrow$ Span $C \subset \mathrm{im}(f)$. Sei $y \in \mathrm{im}(f) \Longrightarrow \exists x \in V : f(x) = y$.

$B$ ist eine Basis von $V \Longrightarrow$ es existiert eine eindeutige Darstellung

$$x = \sum_{i=1}^{n} \lambda_i v_i$$

Mit der Linearität von $f$ folgt:

$$f(x) = f\left(\sum_{i=1}^{n} \lambda_i v_i\right) = \sum_{i=1}^{n} \lambda_i f(v_i) =$$

$$v_1, ..., v_r \in \ker(f) \Longrightarrow y = f(x) = \sum_{i=1}^{n} \lambda_i f(v_i)$$

$$\Longrightarrow \mathrm{im}(f) \subseteq \text{Span } C$$

$$\Longrightarrow \mathrm{im}(f) = \text{Span } C$$

$$\checkmark$$

lineare Unabhängigkeit: Sei

$$\sum_{i=r+1}^{n} \lambda_i f(v_i) = 0$$

zu zeigen: $x_i = 0$ für $r + 1 \leq i \leq n$

$$f \text{ linear} \Longrightarrow 0 = \sum_{i=r+1}^{n} \lambda_i f(v_i) = f\left(\sum_{i=r+1}^{n} \lambda_i v_i\right)$$

$$\Longrightarrow \sum_{i=r+1}^{n} \lambda_i v_i \in \ker(f)$$

$\Longrightarrow$ es existieren eindeutige Koeffizienten $\mu_i \in K, 1 \leq i \leq r$

$$\sum_{i=r+1}^{n} \lambda_i v_i = \sum_{i=1}^{n} \mu_i v_i \Longrightarrow \sum_{i=r+1} 1n\lambda_i v_i - \sum_{i=1}^{n} \mu_i v_i = 0$$

$\{v_1, ..., v_n\}$ sind Basis von $V$. $\Longrightarrow$ $\mu_i = ... = \mu_r = \lambda_{r+1} = ... = \lambda_n = 0$. $\Longrightarrow$ $f(v_{n+1}), ..., f(v_n)$ sind linear unabhängig $\Longrightarrow$ $C$ ist Basis von $\text{im}(f)$

$$\Longrightarrow \dim(\text{im}(f)) = n - r$$

□

**Beispiel 4.17:** Fortsetzung von Beispiel 4.12.

zu 1)

$\Phi_B : K^{n+1} \to P_{\leq n}[t]$

Es gilt $\ker(\Phi_B) = \{0\} \Longrightarrow \dim(\ker(f)) = 0$

$\Longrightarrow \dim(P_{\leq n}[t]) = n + 1$

zu 2)

$f : \mathbb{R}^2 \to \mathbb{R}^2,\ a = b = 0, c \neq 0, c, d \in \mathbb{R}$

Es gilt

$$\dim(\ker(f)) = \dim\left(\left\{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid s_1 = \frac{dx_2}{c}\right\}\right) = 1$$

$$\dim(\text{im}(f)) = \dim\left(\left\{\begin{pmatrix} 0 \\ x \end{pmatrix} \mid x \in \mathbb{R}\right\}\right) = 1$$

$$\dim(\ker(f)) + \dim(\text{im}(f)) = \dim(\mathbb{R}^2) = 2$$

**Beispiel 4.18:** Sei $V = \mathbb{R}^3, W = \mathbb{R}^3$ und $f : V \to W$

$$f\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = \begin{pmatrix} x_1 - x_2 + 2x_3 \\ x_1 + x_2 + x_3 \\ 0x_1 + 3x_2 + 0x_3 \end{pmatrix}$$

gegeben. Damit ist $f$ linear. Nach Lemma 4.10 wird das Bild $\text{im}(f)$ durch die Bilder $f(e_1), f(e_2)$ und $f(e_3)$ erzeugt.

$$\Longrightarrow \text{im}(f) = \text{Span}\left\{\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}\right\}$$

$$\Longrightarrow \text{rg}(f) = \dim(\text{im}(f)) = 2$$

Aus der Dimensionsformel folgt

$$\dim(\ker(f)) = \dim(V) - \dim(\text{im}(f)) = 3 - 2 = 1$$

$$\Longrightarrow \{0_{\mathbb{R}^3}\} \subset \ker(f)$$

**Lemma 4.19:** Zwei endlichdimensionale $K$-Vektorräume $V$ und $W$ sind genau dann isomorph, wenn

$$\dim(V) = \dim(W)$$

*Beweis:*

"$\Longrightarrow$": Gilt $V \cong W$, so existiert ein Isomorphismus $f \in L(V, W)$.

Lemma 4.15:

$$\ker(f) = \{0\} \qquad (f \text{ injektiv})$$
$$\operatorname{im}(f) = W \qquad (f \text{ surjektiv})$$

Satz 4.16:

$$\begin{aligned}\dim(V) &= \dim(\ker(f)) + \dim(\operatorname{im}(f)) \\ &= 0 + \dim(W) \\ &= \dim(W) \checkmark\end{aligned}$$

"$\Longleftarrow$": $\dim(V) = \dim(W) < \infty$

Seien $\{v_1, ..., v_n\}$ und $\{w_1, ..., w_n\}$ Basen von $V$ bzw. $W$. Nach Lemma 4.10 gibt es genau eine Abbildung $f \in L(V, W)$ mit

$$f(v_i) = w_i, \qquad 1 \leq i \leq n$$

Ist $v = \lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n \in \ker(f)$. Dann gilt $0 = f(v) = f(\lambda_1 v_1 + ... + \lambda_n v_n)$ $\underset{f \in L(V,W)}{=}$ $\lambda_1 f(v_1) + ... + \lambda_n f(v_n) = \lambda_1 w_1 + ... + \lambda_n w_n \overset{4.15}{,} w_1, ..., w_n$ linear unabhängig $\Longrightarrow$ $\lambda_1 = \lambda_2 = ... = \lambda_n = 0 \Longrightarrow v = 0 \Longrightarrow \ker(f) = \{0_V\} \Longrightarrow f$ injektiv Mit der Dimensionsformel folgt

$$\begin{aligned}&\dim(V) = 0 + \dim(\operatorname{im}(f)) \\ &\dim(W)\end{aligned}$$

$$\Longrightarrow \text{mit} \dim(\operatorname{im}(f)) \leq W \Longrightarrow \operatorname{im}(f) = W \Longrightarrow f \text{ surjektiv}$$

□

Was passiert bei Verknüpfungen von linearen Abbildungen?

**Satz 4.20:** Seien $V, W$ und $X$ drei endlichdimensionale $K$-Vektorräume sowie $f \in L(V, W)$ und $g \in L(W, X)$. Dann gilt

$$g \circ f \in L(V, X) \text{ und}$$
$$\dim(\operatorname{im}(g \circ f)) = \dim(\operatorname{im}(f)) - \dim(\operatorname{im}(f) \cap \ker(g))$$

*Beweis:* 1) $g \circ f \in L(V, X)$: Für $u, v \in V$ und $\lambda, \mu \in K$ erhält man:

$$\begin{aligned}(g \circ f)(\lambda u + \mu v) &= g(f(\lambda u + \mu v)) \\ &= g(\lambda f(u) + \mu f(u)) = \lambda g(f(u)) + \lambda g(f(v)) \\ &= \lambda(g \circ f)(u) + \mu(g \circ f)(v) \checkmark\end{aligned}$$

2) Betrachte $\tilde{g} := g_{|\operatorname{im}(f)}$. Die Dimensionsformel liefert

$$\dim(\mathrm{im}(f)) = \dim(\mathrm{im}(\tilde{g})) + \dim(\ker(\tilde{g}))$$

Des weiteren gilt: $\mathrm{im}(\tilde{g}) := \{g(v) \in X \mid v \in \mathrm{im}(f)\} = \mathrm{im}(g \circ f)$

$$\ker(\tilde{g}) = \{v \in \mathrm{im}(f) \mid \tilde{g}(v) = 0\} = \mathrm{im}(f) \cap \ker(g)$$

□

**Lemma 4.21:** Sei $K$ ein Körper. Die linearen Abbildungen $f : K^n \to K^m$ sind genau die Abbildungen der Form:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \to \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + ... + a_{mn}x_n \end{pmatrix}$$

mit Koeffizienten $a_{ij} \in K$ für $1 \leq i \leq m$ und $1 \leq j \leq n$.

*Beweis:* "$\Longleftarrow$": Die Dimensionen passen aufgrund der Definitionen. Die Linearität $f$ folgt aus den Rechengesetzen im Körper.

"$\Longrightarrow$": Sei $f \in L(K^n, K^m)$. Zu zeigen: $f$ ist in angegebener Form darzustellen.

**Beobachtung:** Wenn $f$ so darstellbar ist, haben alle Bilder der Standardbasis $e_1, ..., e_n$:

$$f(e_i) = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix} \in K^m$$

Deswegen definieren wir

$$\begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix} := f(e_i) \in K^m$$

Jetzt definieren wir $g \in L(K^n, K^m)$ durch

$$g\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = \begin{pmatrix} a_{11}x_1 + ... + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n \end{pmatrix}$$

Per Konstruktion gilt $f(e_i) = g(e_i)$.

Mit Lemma 4.10 folgt $f = g$.

□

Dieses Resultat motiviert das nächste Kapitel:

# 5. Matrizen

James Sylvester (brit. Mathematiker, 1814 - 1897) erfand den Begriff der Matrix im Jahr 1850. Die im folgenden definierte Matrixoperationen führte Arthur Cayley (brit. Mathematiker, 1821 - 1895) im Jahr 1858 ein.

## 5.1. Definitionen und Basisoperationen

Wir nehmen für dieses Kapitel an: $R$ ist ein Ring mit $1 \neq 0$.

**Definition 5.1: Matrix**

Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins und seien $n, m \in \mathbb{N}_0$. Ein rechteckiges Schema der Form

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

mit $a_{ij} \in K$ für $1 \leq i \leq m$ und $1 \leq j \leq n$ heißt **(m $\times$ n) Matrix** mit den Einträgen in $R$. Die Einträge nennt man auch Koeffizienten. Die Menge aller $(m \times n)$ Matrizen nennt man $R^{m \times n}$.

**Bemerkungen:**

- Rein formal erlaubt diese Definition $n = 0$ oder $m = 0$. Dann erhält man Matrizen der Form $0 \times n$, $m \times 0$ oder $0 \times 0$.

  Diese leeren Matrizen werden in manchen Beweisen aus technischen Gründen benötigt. In der Regel gilt aber $n, m \geq 1$.
- Die Nullmatrix in $R^{m \times n}$ ist die Matrix, bei der alle Einträge gleich 0 sind. Sie wird mit $0^{m \times n}$ bezeichnet
- Ist $m = n$, so nennt man $A \in R^{m \times n}$ quadratisch bzw. eine quadratische Matrix
- Ist $A \in R^{n \times n}$ heißen die Einträge $a_{jj}$ für $1 \leq j \leq n$ **Diagonaleinträge** von

$$A = \begin{pmatrix} a_{11} & \dots & \dots \\ \vdots & \ddots & \vdots \\ \dots & \dots & a_{nn} \end{pmatrix}$$

- Die Kronecker-Delta Funktion $\delta_{ij}$ für $i \in I$ und $j \in J$, $I$ und $J$ sind Indexmengen, ist benannt nach Leopold Kronecker (1823 - 1891) und gegeben durch

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 \text{ sonst} \end{cases}$$

  Damit definiert man die Einheitsmatrix $I_n \in R^{n \times n}$ durch

$$I_n := [\delta_{ij}] = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$$

  Man verwendet $I$, wenn $n$ aus dem Kontext klar ist.
- Die $i$-te Zeile von $A \in R^{m \times n}$ ist

$$(a_{i1}, \dots, a_{in}) \in R^{1 \times n} \text{ für } i = 1, \dots, m \text{ ist ein Zeilenvektor}$$

  Die $j$-te Spalte von $A \in R^{m \times n}$ ist

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in R^{m \times 1} \text{ für } i = 1, \dots, n \text{ ist ein Spaltenvektor}$$

  Diese sind selbst wieder Matrizen.
- Sind $m_1, m_2, n_1, n_2 \in \mathbb{N}_0$ und $A_{ij} \in R^{m,n}$ für $ij = 12$ gegeben, definieren diese eine sogenannte **Blockmatrix** der Form

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \in R^{m_1 + m_2, n_1 + n_2}$$

**Beispiel 5.2:** Für

$$A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & 6 \end{pmatrix} \in \mathbb{Z}^{2,3} \quad \text{und} \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \\ 1 & -1 \end{pmatrix} \in \mathbb{Z}^{3,2}$$

ist $a_{23} = 6$, $(1, -2, 3) \in \mathbb{Z}^{1,3}$ die erste Zeile von $A$ und $b_{22} = 1$ und

$$\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \in \mathbb{Z}^{3,1}$$

die zweite Spalte von $B$. Keine dieser Matrizen inst quadratisch.

**Definition 5.3: Addition von Matrizen**

Seien $A, B \in R^{m,n}$ zwei Matrizen. Dann ist $C = A + B \in R^{m,n}$ definiert durch

$$C := A + B = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

Die Addition in $R^{m,n}$ erfolgt also komponentenweise basieren auf der Addition auf $R$.

**Achtung:** Die Addition ist nur für Matrizen gleicher Größe / Dimension definiert.

**Definition 5.4: Multiplikation einer Matrix mit einem Skalar**

Sei $A \in R^{m,n}$ eine Matrix und $\lambda \in R$. Dann ist $C = \lambda \cdot A \in R^{m,n}$ definiert durch

$$C = \lambda A = \lambda \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} \lambda a_{11} & \dots & \lambda a_{1n} \\ \vdots & \ddots & \vdots \\ \lambda a_{m1} & \dots & \lambda a_{mn} \end{pmatrix}$$

Die Multiplikation einer Matrix mit einem Skalar aus $R$ erfolgt komponentenweise basierend auf der Multiplikation in $R$.

**Definition 5.5: Multiplikation von Matrizen**

Seien $A \in R^{m,n}$ und $B \in R^{n,l}$ zwei Matrizen. Dann ist $C = A \cdot B \in R^{m,l}$ definiert durch

$$C := A \cdot B = \begin{pmatrix} c_{11} & \dots & c_{1l} \\ \vdots & \ddots & \vdots \\ c_{m1} & \dots & c_{ml} \end{pmatrix} \quad \text{mit} \quad c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$$

für $i = 1, \dots, m$ und $j = 1, \dots, l$

**Bemerkung:** Um das Produkt $A \cdot B$ berechnen zu können **muss** die Anzahl der Spalten von $A$ gleich der Anzahl von Zeilen in $B$ sein.

**Merkregel:**

$$c_{ij} = i\text{-te Zeile von } A \text{ mal } j\text{-t Spalte von } B$$

Oder Zeile “mal” Spalte. (“mal” $\widehat{=}$ Skalarprodukt)

**Beispiel 5.6:** Für die Matrizen

$$A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & 6 \end{pmatrix} \in \mathbb{Z}^{2,3}, \; B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \\ 1 & -1 \end{pmatrix} \in \mathbb{Z}^{3,2} \quad \text{und} \quad C = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix} \in \mathbb{Z}^{3,2}$$

gilt:

$A + B$ geht nicht

$$B + C = \begin{pmatrix} 0 & 2 \\ 3 & 5 \\ 6 & 5 \end{pmatrix} \in \mathbb{Z}^{3,2} \qquad 3 \cdot A = \begin{pmatrix} 3 & -6 & 9 \\ -12 & 15 & 18 \end{pmatrix} \in \mathbb{Z}^{2,3}$$

$$A \cdot B = \begin{pmatrix} 2 & -5 \\ 10 & -1 \end{pmatrix} \in \mathbb{Z}^{2,2} \qquad B \cdot A = \begin{pmatrix} -1 & 2 & -3 \\ -4 & 5 & 6 \\ 5 & -7 & -3 \end{pmatrix} \in \mathbb{Z}^{3,3}$$

Also $A \cdot B$ und $B \cdot A$ sind für dieses Beispiele definiert, aber $A \cdot B \neq B \cdot A$. Damit ist die Multiplikation von Matrizen nicht kommutativ. Dies gilt auch für gleichgroße Matrizen:

$$D = \begin{pmatrix} 1 & -2 \\ -4 & 5 \end{pmatrix} \in \mathbb{Z}^{2,2} \ , \ E = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}^{2,2} \Longrightarrow$$

$$D \cdot E = \begin{pmatrix} -1 & -2 \\ 4 & 5 \end{pmatrix} \ \neq \ \begin{pmatrix} -1 & 2 \\ -4 & 5 \end{pmatrix} = E \cdot D$$

**Lemma 5.7:** Für $A, \tilde{A} \in R^{m,m}$ $B, \tilde{B} \in R^{m,l}$, $C \in R^{l,k}$ sowie $\lambda, \mu \in R$ gelten

- Assoziativgesetze, d.h.

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \ \text{ und } (\lambda\mu) \cdot A = \lambda \cdot (\mu \cdot A)$$

- Distributivitätsgesetze , d.h.

$$\left(A + \tilde{A}\right) \cdot B = A \cdot B + A \cdot B$$
$$A \cdot \left(B + \tilde{B}\right) = A \cdot B + A \cdot \tilde{B}$$
$$(\lambda \cdot \mu) \cdot A = \lambda \cdot A + \mu \cdot A$$
$$\lambda \cdot \left(A + \tilde{A}\right) = \lambda \cdot A + \lambda \cdot \tilde{A}$$
$$\lambda \cdot (A \cdot B) = A \cdot (\lambda \cdot B)$$

- und mit

$$I_n = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} \in R^{n,n} \ \text{ bzw. } I_m \in R^{m,m}$$

  gilt

$$I_n \cdot A = A = A \cdot I_m$$

*Beweis:* Nachrechnen

□

**Definition 5.8: Transposition von Matrizen**

Sei

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in R^{m \times n}$$

eine Matrix. Dann ist die zu $A$ **Transponierte** Matrix $A^\top$ definert durch

$$A^\top := \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{mn} \end{pmatrix} \in R^{n \times m}$$

**Beispiel 5.9:** Die zu

$$A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & 6 \end{pmatrix} \in \mathbb{Z}^{2,3}$$

tranponierte Matrix ist

$$A^\top = \begin{pmatrix} 1 & -4 \\ -2 & 5 \\ 3 & 6 \end{pmatrix} \in \mathbb{Z}^{3,2}$$

**Lemma 5.10:** Für $A, \tilde{A} \in R^{m,n},\ B \in R^{n,l}$ und $\lambda \in R$ gilt

1. $\left(A^\top\right)^\top = A$
2. $\left(A + \tilde{A}\right)^\top = A^\top + \tilde{A}^\top$
3. $(\lambda \cdot A)^\top = \lambda \cdot A^\top$
4. $\underbrace{\underbrace{A \cdot B}_{\in R^{m,l}}^\top}_{\in R^{l,m}} = \underbrace{\underbrace{B^\top}_{\in R^{m,l}} \cdot \underbrace{A^\top}_{\in R^{n,m}}}_{\in R^{l,m}})$

*Beweis:* Nachrechnen.

□

**Zur Notation:**

$$R^n,\ v \in R^n,\ v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in R^{n,1}$$

d.h. $v$ wird immer als Spaltenvektor interpretiert.

Für Zeilenvektor:

$$w \in R^{1,n} \text{ gilt } w^\top \in R^{n,1} \cong R^n$$

**Beobachtung:** Alle Operationen, die wir für Matrizen definiert haben, sind konsistent mit den Vektoroperationen, wenn diese im obigen Sinn als Matrizen interpretiert werden.

## 5.2. Matrizengruppen und -ringe

**Lemma 5.11:** Mit den angegebenen Rechenregeln gilt

1. $(R^{m,n}, +)$ ist eine kommutative Gruppe mit dem neutralen Element $0 \in R^{m,n}$, d.h. der Nullmatrix und dem zu $A \in R^{m,n}$ inversen Element $-A = (-a_{ij}) \in R^{m,n}$. Manschreibt statt $A + (-B) = A - B$.
2. Ist $R$ ein Körper, so ist $R^{m,n}$ ein $R$-Vektorrau der Dimension $m \cdot n$.

*Beweis:*

1) Folgt durch Nachrechnen unter Ausnutzung der Eigenschaften von $R$.

2) Aufgrund der Rechenregeln ist $R^{m,n}$ abgeschlossen bezüglich der

$$+ : R^{m,n} \times R^{m,n} \to R^{m,n} \quad \text{und} \quad \cdot : R \times R^{m,n} \to R^{m,n}$$

Zur Dimension: $A \in R^{m,n}$ kann dargestellt werden durch

$$a_{11} \cdot \begin{pmatrix} 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} + a_{12} \cdot \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$$\Longrightarrow \text{Erzeugendensystem} + \text{linear unabhägnig} \Longrightarrow \text{Basis}$$

□

Aufgrund der Eigenschaft 2 aus Lemma 5.10 ist die Transposition von Matrizen ein Homomorphismus (vlg. Definition 2.11) der Gruppen $(R^{m,n}, +)$ und $(R^{n,m}, +)$

**Lemma 5.12:** Sei $n \in \mathbb{N}$. Die Menge der quadratischen Matrizen $R^{n,n}$, d.h. $(R^{n,n}, +, \cdot)$, ist ein Ring mit Eins, welche durch die Einheitsmatrix $I_n$ gegeben ist. Dieser Ring ist kommutativ.

*Beweis:* Lemma 5.11: $(R^{n,n}, +)$ ist eine kommutative Gruppe mit neutralem Element $0 \in R^{n,n}$. Lemma 5.7: Assoziativität, Distributivitätsgesetze, Einselement $I_n$. $\Longrightarrow$ Ring mit $1$ ✓

$n = 1$: Kommutativität folgt aus Eigenschaften von $R$. Für $n = 2$ gilt mit

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \text{dass}$$

$$A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = B \cdot A$$

□

Aus dem Beispiel im letzten Satz folgt auch, dass $A, B \in R^{n,n}$ mit

- $A \neq 0 \in R^{n,n}$, $B \neq 0 \in R^{n,n}$
- $A \cdot B = 0$

existiert. Damit besitzt $R^{n,n}$ sogenannte nichttriviale Nullteiler. Mit $R = \mathbb{R}$ gilt dies auch wenn $R$ ein Körper ist.

Weitere wichtige Eigenschaft:

Invertierbarkeit bezüglich der Multiplikation!

**Frage:** Gibt es für jede Matrix $A \in R^{n,n}$ eine Matrix $A^{-1}$, so dass $A \cdot A^{-1} = I - n = A^{-1} \cdot A$? Wenn dies gilt, dann müsste $A^{-1}$ existieren, so dass für

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ gilt } A \cdot A^{-1} = I = A^{-1} \cdot A$$

$$A \cdot A^{-1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Für das erste Element der Matrix folgt

$$0 \cdot a + 0 \cdot c = \underbrace{0 \neq 1}_{\text{Ring mit } 0 \neq 1} \quad \lightning$$

**Folgerung:** Nicht alle quadratischen Matrizen sind invertierbar.

**Beispiel 3.13:** Die Matrix

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \in \mathbb{Z}^{2,2}$$

ist damit über $R = \mathbb{Z}$ nicht invertierbar. Es gilt

$$\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ -\frac{2}{3} & \frac{1}{3} \end{pmatrix}}_{A^{-1} \in \mathbb{Q}^{2,2}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

Ist $A \in \mathbb{Q}^{2,2}$, dann ist $A$ invertierbar. Also: Invertierbarkeit hängt vom Ring $R$ ab!

---

**Lemma 5.14:** Sind $A, B \in R^{n,n}$ zwei invertierbare Matrizen. D.h. es existieren $A^{-1}, B^{-1} \in R^{n,n}$ mit $A \cdot A^{-1} = I = A^{-1} \cdot A$ und $B \cdot B^{-1} = I = B^{-1} \cdot B$, so gilt:

- $A \cdot B$ ist invertierbar und es ist
$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$$
- $A^\top$ ist invertierbar und es ist $\left(A^\top\right)^{-1} = \left(A^{-1}\right)^\top = A^{-\top}$

*Beweis:*

1. Aussage: Folgt aus der allgemeinen Aussage für Ringe mit Eins im Satz 2.13.
2. Aussage: Regel 4 aus Lemma 5.10:
$$\left(A^{-1}\right)^\top \cdot A^\top = \left(A \cdot A^{-1}\right)^\top = \left(I_n\right)^\top = I_n = \left(I_n\right)^\top = \left(A^{-1} \cdot A\right)^\top = A^\top \cdot \left(A^{-1}\right)^\top$$

□

**Lemma 5.15:** Die Menge $\mathrm{GL}_n(R) := \{A \in R^{n,n} \mid A \text{ invertierbar}\}$ bilden mit der Matrixmultiplikation eine Gruppe.

*Beweis:* Lemma 5.14, 1. Aussage: Abgeschlossenheit bezüglich $\cdot$. Lemma 5.7: Assoziativität + neutrale Element $I_n$. Mit $\left(A^{-1}\right)^{-1} = A$ ist auch $A^{-1}$ invertierbar $\Longrightarrow A^{-1} \in \mathrm{GL}_n(R)$.

□

*Hinweis:* $\mathrm{GL}_n(R)$ = General linear Group

Matrixmultiplikation: $A \in R^{m,n}, v \in R^{n,1} = R^n$

$$\begin{pmatrix} a_{11} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} v_{11} \\ \vdots \\ v_{n1} \end{pmatrix} = A \cdot v$$

definiert damit auch die Matrix-Vektor-Multiplikation.

Diese Beobachtung motiviert:

## 5.3. Matrizen und lineare Abbildungen

**Beispiel 5.16:** Fortsetzung von Beispiel 4.3.

Die lineare Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$,

$$y = f(x) = f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix}$$

mit $a, b, c, d \in \mathbb{R}$ wird beschrieben duch

$$y = f(x) = \underbrace{\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\in R^{2,2}} \cdot \underbrace{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}}_{\in R^{2,1}}}_{\in R^{2,1}} = A \cdot x \quad \text{mit } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Die Kombination mit Lemma 4.21 liefert:

**Satz 5.17:** Sei $K$ ein Körper. Zu jeder linearen Abbildung $f : K^n \to K^m$, $y = f(x)$, existiert eine Matrix $A \in K^{m,n}$, so dass gilt

$$y = f(x) = A \cdot x$$

*Beweis:* Nach Lemma 4.21 besitzt jede lineare Abbildung $f : K^n \to K^m$ die Form

$$y = f(x) = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + x_{m2}x_2 + \dots + a_{mn}x_n \end{pmatrix}$$

mit Koeffizienten $a_{ij} \in K$, $i = 1, ..., m$, j = 1, ..., $n$. Mit den Rechenregeln für Matrizen inklusive dem Spezialfall der Vektoren folgt

$$y = f(x) = A \cdot x \quad \text{mit} \quad A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

□

Was gilt für allgemeine Basen?

**Satz 5.18:** Seien $V$ und $W$ zwei $K$-Vektorräume mit den Basen $B = \{v_1, ..., v_n\}$ von $V$ und $C = \{w_1, ..., w_m\}$ von $W$ und $f : V \to W$ eine lineare Abbildung. Dann gibt es eine eindueitg bestimmte Matrix $\left(A_f\right)^{B,C} = \left(a_{ij}\right) \in K^{m,n}$ so, dass

$$W \ni f(v_j) = \sum_{i=1}^{m} a_{ij} w_i \qquad j = 1, ..., n$$

gilt. Die Abbildung $F : L(V, W) \to K^{m,n}$ mit $F(f) = \left(A_f\right)^{B,C}$ ist ein Isomorphismus zwischen zwei $K$-Vektorräumen.

*Beweis:* Da $C$ eine Basis von $W$ ist, besitzt jedes $w \in W$ eine eindeutige Darstellung als Linearkombination der Vektoren $\{w_1, ..., w_m\}$. Damit besitzt auch für jedes $f \in L(V, W)$ die Vektoren $f(v_1), ..., f(v_n)$ eine eindeutige Darstellung. Die Koeffizienten dieser Linearkombinationen bestimmen eindeutig die Matrix $\left(A_f\right)^{B,C}$.

zu zeigen: $F$ ist ein Isomorphismus.

$F$ ist linear: Seien $f, g \in L(V, W)$ mit den zugehörigen Matrizen $\left(A_f\right)^{B,C}$ bzw. $\left(A_f\right)^{B,C}$ mit

$$\left(A_f\right)^{B,C} = \left(a_{ij}\right), \left(A_g\right)^{B,C}, \left(A_f\right)^{B,C} \in K^{m,n}, \left(A_g\right)^{B,C} \in K^{m,n}$$

Für $\lambda, \mu \in K$ gilt

$$\begin{aligned}(\lambda f + \mu g)(v_j) = \lambda f(v_j) + \mu g(v_j) &= \lambda \sum_{i=1}^{m} a_{ij} w_i + \mu \sum_{i=1}^{m} b_{ij} w_i \\ &= \sum_{i=1}^{m} \underbrace{\left(\lambda a_{ij} + \mu b_{ij}\right)}_{\text{Matrix für } \lambda + \mu g} w_i\end{aligned}$$

Also ist

$$F(\lambda f + \mu g) = \lambda F(f) + \mu F(g)$$

$\Longrightarrow F$ linear