OTH Regensburg
Fakultät Informatik und Mathematik
Prof. Dr. Rainer Löschel

Wintersemester 2022/2023
Informatik Bachelor IN1
Vorlesung MA1

Mathematik 1 für Informatik

Vorlesungskurzskriptum

Inhaltsverzeichnis

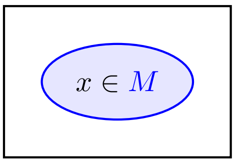
1 Logik

1.1 Mengenlehre

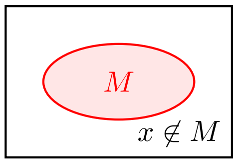
Definition 1.1.1 (Menge, Element)

Unter einer ***Menge*** versteht man die Zusammenfassung unterscheidbarer Objekte, den sog. ***Elementen***, zu einem Ganzen.

Liegt das Element x in einer Menge M, so wird dies mit $x \in M$ (oder $M \ni x$) notiert, liegt ein Objekt x nicht in M, so notiert man $x \notin M$ (oder $M \not\ni x$).



Venn-Diagramm



Unter der ***leeren Menge*** versteht man die Menge, die keine Elemente enthält,

$$\emptyset = \{\}.$$

Definition 1.1.2 (Mächtigkeit)

Die Anzahl der Elemente einer Menge M nennt man die ***Mächtigkeit*** der Menge:

$$|M| = \#M.$$

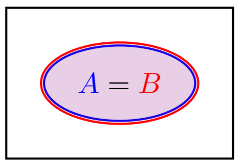
Im Fall $|M| \in \mathbb{N}_0$ spricht man von einer ***endlichen*** Menge, im Fall $|M| = \infty$ von einer ***unendlichen*** Menge.

Definition 1.1.3 (Relationen)

Relationen zwischen Mengen:

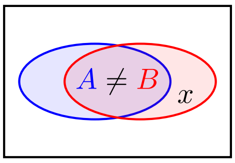
Gleichheit Zwei Mengen A und B sind gleich, wenn die beiden Mengen die selben Elemente enthalten:

$A = B$
In Worten: A gleich B



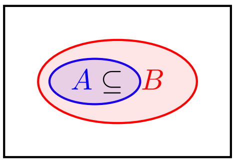
Ungleichheit Zwei Mengen A und B sind ungleich oder verschieden, wenn die beiden Mengen nicht die selben Elemente enthalten, d. h. wenn mindestens eine der Mengen ein Element x enthält, das nicht in der anderen Menge liegt:

$A \neq B$
In Worten: A ungleich B



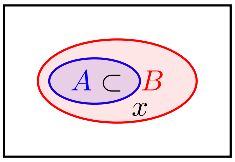
Teilmenge Eine Menge A ist eine Teilmenge einer Menge B, wenn jedes Element von A auch ein Element von B ist:

$A \subseteq B$ oder $B \supseteq A$
In Worten: A enthalten in B
B enthält A



Echte Teilmenge Eine Menge A ist eine echte Teilmenge einer Menge B, wenn jedes Element von A auch ein Element von B ist und A von B verschieden ist, also mindestens ein Element x in B existiert, das nicht in A liegt:

$A \subset B$ oder $B \supset A$
In Worten: A echt enthalten in B
B enthält A echt



Definition 1.1.4 (Potenzmenge)

Die Menge aller Teilmengen einer Menge M nennt man ***Potenzmenge*** von M:

$$\mathfrak{P}M := \{A \mid A \subseteq M\}.$$

Satz 1.1.5 (Mächtigkeit der Potenzmenge)

Die Mächtigkeit der Potenzmenge einer endlichen Menge M ist

$$|\mathfrak{P}M| = 2^{|M|}.$$

Bemerkung 1.1.6 (Notation)

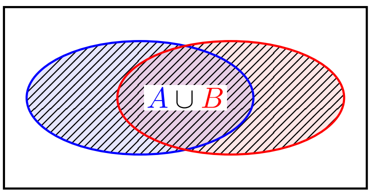
Bei einer Zuweisung, d. h. einer Definition, verwendet man die Notation $:=$ wie beispielsweise bei $\mathfrak{P}M := \{A \mid A \subseteq M\}$, bei einer Gleichheit die Notation $=$ wie bei $|\mathfrak{P}M| = 2^{|M|}$.

Definition 1.1.7 (Operationen)

Operationen auf Mengen:

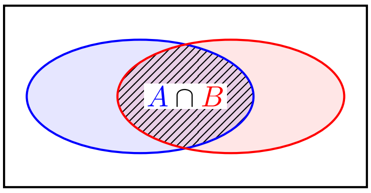
Vereinigung Die Vereinigung zweier Mengen A und B besteht aus allen Elementen, die in A oder in B (oder in beiden) liegen:

$A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$
In Worten: A vereinigt B



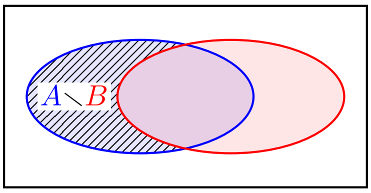
Durchschnitt Der Durchschnitt zweier Mengen A und B besteht aus allen Elementen, die sowohl in A wie auch in B liegen:

$A \cap B := \{x \mid x \in A \text{ und } x \in B\}$
In Worten: A geschnitten B



Differenz Die Differenz zweier Mengen A und B besteht aus allen Elementen, die in A, aber nicht in B liegen:

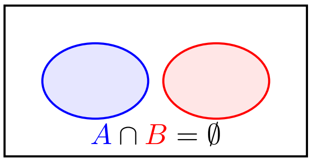
$A \setminus B := \{x \in A \mid x \notin B\}$
In Worten: A ohne B



Definition 1.1.8 (Disjunkt)

Zwei Mengen heißen ***disjunkt***, wenn sie einen leeren Durchschnitt besitzen, d. h. keine Elemente gemeinsam haben:

$A \cap B = \emptyset$
In Worten: A und B disjunkt
A disjunkt zu B
B disjunkt zu A



Bemerkung 1.1.9

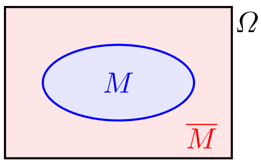
Für die Vereinigung $A \cup B$ disjunkter Mengen A und B notiert man zur Verdeutlichung $A \uplus B$. Für deren Mächtigkeit gilt stets

$$|A \uplus B| = |A| + |B|\,.$$

Definition 1.1.10 (Komplement)

Für eine Teilmenge M einer vorgegebenen Grundmenge Ω versteht man unter dem ***Komplement*** von M in Ω die Differenz

$\overline{M} := \Omega \setminus M = \{x \in \Omega \mid x \notin M\}$
Alternativ: $\complement M$, M^{c}
In Worten: Komplement von M



Satz 1.1.11 (Rechenregeln der Mengenlehre)

Für Mengen A, B, C einer Grundmenge Ω gilt:

Assoziativität $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$.

Kommutativität $A \cup B = B \cup A$, $A \cap B = B \cap A$.

Idempotenz $A \cup A = A$, $A \cap A = A$.

Verschmelzung $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$.

Null $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.

Eins $A \cup \Omega = \Omega$, $A \cap \Omega = A$.

Komplement $A \cup \overline{A} = \Omega$, $A \cap \overline{A} = \emptyset$.

Distributivität $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Dualität $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$, $\overline{\overline{A}} = A$.

Bemerkung 1.1.12 (Notation)

Aufgrund des Assoziativgesetzes können die Klammern bei Ausdrücken wie $A \cup B \cup C$ oder $A \cap B \cap C$ weggelassen werden.

Definition 1.1.13 (Kartesisches Produkt)

Unter dem ***kartesischen Produkt*** zweier Mengen A und B versteht man die Menge aller geordneten Paare

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

Speziell für zwei gleiche Mengen:

$$A^2 := A \times A = \{(a_1, a_2) \mid a_1, a_2 \in A\}.$$

Allgemeiner versteht man unter dem ***n-fachen kartesischen Produkt*** von A (mit $n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$) die Menge aller n-Tupel:

$$A^n := A \times A \times \cdots \times A = \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in A\},$$

speziell $A^0 = \{\varepsilon\}$ mit dem leeren Tupel $\varepsilon := ()$ und $A^1 = A$.

1.2 Aussagenlogik

Definition 1.2.1 (Aussage)

Unter einer ***Aussage*** $\mathcal{P}$ versteht man einen Sachverhalt, von dem eindeutig bestimmt ist, ob er ***wahr*** $\mathfrak{w}$ oder ***falsch*** $\mathfrak{f}$ ist, auch wenn der sog. ***Wahrheitswert*** nicht bekannt ist.

Definition 1.2.2 (Verknüpfungen)

Verknüpfungen zwischen Aussagen:

Negation einer Aussage $\mathcal{P}$ ist die Aussage, die genau dann wahr ist, wenn $\mathcal{P}$ falsch ist:

$\neg\mathcal{P}$
In Worten: nicht $\mathcal{P}$

$\mathcal{P}$	$\neg\mathcal{P}$
$\mathfrak{w}$	$\mathfrak{f}$
$\mathfrak{f}$	$\mathfrak{w}$

Konjunktion zweier Aussagen $\mathcal{A}$ und $\mathcal{B}$ ist die Aussage, die genau dann wahr ist, wenn beide Aussagen $\mathcal{A}$ und $\mathcal{B}$ wahr sind:

$\mathcal{A} \wedge \mathcal{B}$
In Worten: $\mathcal{A}$ und $\mathcal{B}$

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$
$\mathfrak{w}$	$\mathfrak{w}$	$\mathfrak{w}$
$\mathfrak{w}$	$\mathfrak{f}$	$\mathfrak{f}$
$\mathfrak{f}$	$\mathfrak{w}$	$\mathfrak{f}$
$\mathfrak{f}$	$\mathfrak{f}$	$\mathfrak{f}$

Disjunktion zweier Aussagen $\mathcal{A}$ und $\mathcal{B}$ ist die Aussage, die genau dann falsch ist, wenn beiden Aussagen $\mathcal{A}$ und $\mathcal{B}$ falsch sind:

$\mathcal{A} \vee \mathcal{B}$
In Worten: $\mathcal{A}$ oder $\mathcal{B}$

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$
$\mathfrak{w}$	$\mathfrak{w}$	$\mathfrak{w}$
$\mathfrak{w}$	$\mathfrak{f}$	$\mathfrak{w}$
$\mathfrak{f}$	$\mathfrak{w}$	$\mathfrak{w}$
$\mathfrak{f}$	$\mathfrak{f}$	$\mathfrak{f}$

Implikation zweier Aussagen $\mathcal{A}$ und $\mathcal{B}$ ist die Aussage, die genau dann falsch ist, wenn die Aussage $\mathcal{A}$ wahr und die Aussage $\mathcal{B}$ falsch ist:

$\mathcal{A} \Rightarrow \mathcal{B}$
In Worten: $\mathcal{A}$ impliziert $\mathcal{B}$
wenn $\mathcal{A}$, dann $\mathcal{B}$
aus $\mathcal{A}$ folgt $\mathcal{B}$
$\mathcal{A}$ ist hinreichend für $\mathcal{B}$
$\mathcal{B}$ ist notwendig für $\mathcal{A}$

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$
$\mathfrak{w}$	$\mathfrak{w}$	$\mathfrak{w}$
$\mathfrak{w}$	$\mathfrak{f}$	$\mathfrak{f}$
$\mathfrak{f}$	$\mathfrak{w}$	$\mathfrak{w}$
$\mathfrak{f}$	$\mathfrak{f}$	$\mathfrak{w}$

Äquivalenz zweier Aussagen $\mathcal{A}$ und $\mathcal{B}$ ist die Aussage, die genau dann wahr ist, wenn beide Aussagen $\mathcal{A}$ und $\mathcal{B}$ den selben Wahrheitswert aufweisen:

$\mathcal{A} \Leftrightarrow \mathcal{B}$
In Worten: $\mathcal{A}$ und $\mathcal{B}$ äquivalent
$\mathcal{A}$ äquivalent zu $\mathcal{B}$
$\mathcal{A}$ genau dann, wenn $\mathcal{B}$
$\mathcal{A}$ notwendig und hinreichend für $\mathcal{B}$

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Leftrightarrow \mathcal{B}$
$\mathfrak{w}$	$\mathfrak{w}$	$\mathfrak{w}$
$\mathfrak{w}$	$\mathfrak{f}$	$\mathfrak{f}$
$\mathfrak{f}$	$\mathfrak{w}$	$\mathfrak{f}$
$\mathfrak{f}$	$\mathfrak{f}$	$\mathfrak{w}$

Satz und Definition 1.2.3 (Kontraposition, Umkehrung)

Die Implikation $\mathcal{A} \Rightarrow \mathcal{B}$ zweier Aussagen ist äquivalent zur Verknüpfung $\mathcal{B} \vee \neg\mathcal{A}$ bzw. $\neg\mathcal{A} \vee \mathcal{B}$. Ferner versteht man unter der

Kontraposition die dazu äquivalente Aussage $\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$,

Umkehrung die (nicht dazu äquivalente) Aussage $\mathcal{B} \Rightarrow \mathcal{A}$.

Definition 1.2.4 (Tautologie, Kontradiktion)

Eine Verknüpfung von Aussagen heißt

Tautologie, wenn sie für alle Wahrheitswerte konstant wahr ist,

Kontradiktion, wenn sie für alle Wahrheitswerte konstant falsch ist.

Definition 1.2.5 (Aussageform)

Unter einer ***Aussageform*** wie $\mathcal{P}(x)$ versteht man einen Sachverhalt, der Variablen wie x für Objekte enthält, so dass nach deren Ersetzung durch Objekte Aussagen entstehen.

Definition 1.2.6 (Quantoren)

Quantoren für Aussageformen:

Allquantor Für eine Aussageform $\mathcal{P}(x)$ ist

$\forall x : \mathcal{P}(x)$
In Worten: für alle x gilt $\mathcal{P}(x)$

die Aussage, die genau dann wahr ist, wenn $\mathcal{P}(m)$ für alle Objekte m einer gegebenen Menge M wahr ist.

Existenzquantor Für eine Aussageform $\mathcal{P}(x)$ ist

$\exists x : \mathcal{P}(x)$
In Worten: es gibt (mindestens) ein x mit $\mathcal{P}(x)$

die Aussage, die genau dann wahr ist, wenn $P(m)$ für (mindestens) ein Objekt m einer gegebenen Menge M wahr ist.

Satz 1.2.7 (Analogie zwischen Aussageformen und Mengen)

Betrachtet man für eine Menge M einer Grundmenge Ω von Objekten die Aussageform $\mathcal{M}(x)\colon x \in M$, so bestehen folgende Korrespondenzen:

$x \in A$	$\mathcal{A}(x)$
$x \in \overline{A}$	$\neg\mathcal{A}(x)$
$x \in A \cup B$	$\mathcal{A}(x) \vee \mathcal{B}(x)$
$x \in A \cap B$	$\mathcal{A}(x) \wedge \mathcal{B}(x)$
$x \in \emptyset$	$\mathfrak{f}$ Kontradiktion
$x \in \Omega$	$\mathfrak{w}$ Tautologie

Ferner gelten folgende Entsprechungen:

$A \subseteq B$	$\forall x : x \in A \Rightarrow x \in B$ $\forall x \in A : x \in B$
$A \subset B$	$\forall x : x \in A \Rightarrow x \in B \wedge \exists x : x \in B \wedge x \notin A$ $\forall x \in A : x \in B \wedge \exists x \in B : x \notin A$
$A = B$	$\forall x : x \in A \Leftrightarrow x \in B$ $\forall x \in A : x \in B \wedge \forall x \in B : x \in A$

Satz 1.2.8 (Rechenregeln der Aussagenlogik)

Für Aussagen $\mathcal{A}, \mathcal{B}, \mathcal{C}$ gilt:

Assoziativität $(\mathcal{A} \vee \mathcal{B}) \vee \mathcal{C} \Leftrightarrow \mathcal{A} \vee (\mathcal{B} \vee \mathcal{C})$, $(\mathcal{A} \wedge \mathcal{B}) \wedge \mathcal{C} \Leftrightarrow \mathcal{A} \wedge (\mathcal{B} \wedge \mathcal{C})$.

Kommutativität $\mathcal{A} \vee \mathcal{B} \Leftrightarrow \mathcal{B} \vee \mathcal{A}$, $\mathcal{A} \wedge \mathcal{B} \Leftrightarrow \mathcal{B} \wedge \mathcal{A}$.

Idempotenz $\mathcal{A} \vee \mathcal{A} \Leftrightarrow \mathcal{A}$, $\mathcal{A} \wedge \mathcal{A} \Leftrightarrow \mathcal{A}$.

Verschmelzung $\mathcal{A} \vee (\mathcal{A} \wedge \mathcal{B}) \Leftrightarrow \mathcal{A}$, $\mathcal{A} \wedge (\mathcal{A} \vee \mathcal{B}) \Leftrightarrow \mathcal{A}$.

Null $\mathcal{A} \vee \mathfrak{f} \Leftrightarrow \mathcal{A}$, $\mathcal{A} \wedge \mathfrak{f} \Leftrightarrow \mathfrak{f}$.

Eins $\mathcal{A} \vee \mathfrak{w} \Leftrightarrow \mathfrak{w}$, $\mathcal{A} \wedge \mathfrak{w} \Leftrightarrow \mathcal{A}$.

Komplement $\mathcal{A} \vee \neg\mathcal{A} \Leftrightarrow \mathfrak{w}$, $\mathcal{A} \wedge \neg\mathcal{A} \Leftrightarrow \mathfrak{f}$.

Distributivität $\mathcal{A} \vee (\mathcal{B} \wedge \mathcal{C}) \Leftrightarrow (\mathcal{A} \vee \mathcal{B}) \wedge (\mathcal{A} \vee \mathcal{C})$, $\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C}) \Leftrightarrow (\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C})$.

Dualität $\neg(\mathcal{A} \vee \mathcal{B}) \Leftrightarrow \neg\mathcal{A} \wedge \neg\mathcal{B}$, $\neg(\mathcal{A} \wedge \mathcal{B}) \Leftrightarrow \neg\mathcal{A} \vee \neg\mathcal{B}$, $\neg\neg\mathcal{A} \Leftrightarrow \mathcal{A}$.

Bemerkung 1.2.9 (Notation)

Aufgrund des Assoziativgesetzes können die Klammern bei Ausdrücken wie $\mathcal{A} \vee \mathcal{B} \vee \mathcal{C}$ oder $\mathcal{A} \wedge \mathcal{B} \wedge C$ weggelassen werden.

Satz 1.2.10 (Rechenregeln für Quantoren)

Für Aussageformen $\mathcal{A}(x), \mathcal{B}(x)$ gilt ferner:

$$\begin{aligned}
\neg(\forall x : \mathcal{A}(x)) &\Leftrightarrow \exists x : \neg\mathcal{A}(x) \\
\neg(\exists x : \mathcal{A}(x)) &\Leftrightarrow \forall x : \neg\mathcal{A}(x) \\
\forall x : \mathcal{A}(x) \wedge \mathcal{B}(x) &\Leftrightarrow \forall x : \mathcal{A}(x) \wedge \forall x : \mathcal{B}(x) \\
\exists x : \mathcal{A}(x) \vee \mathcal{B}(x) &\Leftrightarrow \exists x : \mathcal{A}(x) \vee \exists x : \mathcal{B}(x) \\
\forall x : \mathcal{A}(x) \vee \mathcal{B}(x) &\Leftarrow \forall x : \mathcal{A}(x) \vee \forall x : \mathcal{B}(x) \\
\exists x : \mathcal{A}(x) \wedge \mathcal{B}(x) &\Rightarrow \exists x : \mathcal{A}(x) \wedge \exists x : \mathcal{B}(x) \\
\forall x : \forall y : \mathcal{A}(x,y) &\Leftrightarrow \forall y : \forall x : \mathcal{A}(x,y) && \text{kurz } \forall x, y : \mathcal{A}(x,y) \\
\exists x : \exists y : \mathcal{A}(x,y) &\Leftrightarrow \exists y : \exists x : \mathcal{A}(x,y) && \text{kurz } \exists x, y : \mathcal{A}(x,y) \\
\forall x : \exists y : \mathcal{A}(x,y) &\Leftarrow \exists y : \forall x : \mathcal{A}(x,y)
\end{aligned}$$

1.3 Beweismethoden

Definition 1.3.1 (Satz, Beweis)

Unter einem mathematischen ***Satz*** versteht man eine wahre Aussage, die aus Axiomen und anderen Sätzen durch einen sog. ***Beweis*** nachvollziehbar durch korrektes logisches Schließen ableitbar ist.

Korrekte logische Schlüsse eines Beweises notiert man mit $\Longrightarrow$ bzw. $\Longleftrightarrow$:

Implikation $\mathcal{P} \Longrightarrow \mathcal{A}$

- $\mathcal{P}$ ist hinreichend für $\mathcal{A}$.
- $\mathcal{A}$ ist notwendig für $\mathcal{P}$.

Äquivalenz $\mathcal{A} \Longleftrightarrow \mathcal{B}$ d. h. $(\mathcal{A} \Longrightarrow \mathcal{B}) \wedge (\mathcal{B} \Longrightarrow \mathcal{A})$

- $\mathcal{A}$ gilt genau dann, wenn $\mathcal{B}$.
- $\mathcal{A}$ ist notwendig und hinreichend für $\mathcal{B}$.
- $\mathcal{B}$ ist notwendig und hinreichend für $\mathcal{A}$.

Definition 1.3.2 (Direkter Beweis)

Unter einem ***direkten Beweis*** einer Aussage $\mathcal{A}$ versteht man korrekte Schlussweisen der Form

$$\mathcal{P} \Longrightarrow \mathcal{A},$$

wobei $\mathcal{P}$ eine gegebene wahre Voraussetzung darstellt.

DEFINITION 1.3.3 (Indirekter Beweis durch Kontraposition)

Unter einem ***indirektem Beweis durch Kontraposition*** einer Aussage $\mathcal{A}$ versteht man korrekte Schlussweisen der Form

$$\neg\mathcal{A} \Longrightarrow \neg\mathcal{P}$$

wobei $\mathcal{P}$ eine gegebene wahre Voraussetzung darstellt.

DEFINITION 1.3.4 (Indirekter Beweis durch Widerspruch)

Unter einem ***indirektem Beweis durch Widerspruch*** einer Aussage $\mathcal{A}$ versteht man korrekte Schlussweisen der Form

$$\mathcal{P} \wedge \neg\mathcal{A} \Longrightarrow \mathfrak{f},$$

wobei $\mathcal{P}$ eine gegebene wahre Voraussetzung darstellt.

DEFINITION 1.3.5 (Induktionsbeweis)

Unter einem ***Induktionsbeweis*** einer Aussage $\mathcal{A}(n)$ für jede natürliche Zahl n versteht man die Schlussweise

$$\mathcal{A}(1) \wedge \forall n : (\mathcal{A}(n) \Longrightarrow \mathcal{A}(n+1)).$$

Der Nachweis der Aussage $\mathcal{A}(1)$ heißt ***Induktionsanfang***, der Nachweis der Implikationen $\mathcal{A}(n) \Longrightarrow \mathcal{A}(n+1)$ für alle n heißt ***Induktionsschritt*** mit ***Induktionsvoraussetzung*** $\mathcal{A}(n)$ und ***Induktionsbehauptung*** $\mathcal{A}(n+1)$.

BEMERKUNG 1.3.6 (Notation)

Zur abkürzenden Notation verwendet man oft das ***Summenzeichen*** bzw. ***Produktzeichen***

$$\sum_{k=m}^{n} a_k := a_m + a_{m+1} + \cdots + a_n \qquad \text{bzw.} \qquad \prod_{k=m}^{n} a_k := a_m \cdot a_{m+1} \cdot \cdots \cdot a_n,$$

wobei für $n < m$ die (leere) Summe als 0 und das (leere) Produkt als 1 definiert wird.

2 Strukturen

2.1 Relationen

Definition 2.1.1 (Relation)

Für zwei Mengen A und B nennt man eine Teilmenge $\mathcal{R}$ des kartesischen Produkts $A \times B = \{(a,b) \mid a \in A, b \in B\}$ eine ***Relation***. Man notiert $(a,b) \in \mathcal{R}$ auch in der Form $a \; \mathcal{R} \; b$.

Eine Relation $\mathcal{R} \subseteq M \times M$ nennt man eine ***binäre Relation auf*** M.

Definition 2.1.2 (Ordnungsrelation)

Eine binäre Relation $\mathcal{R}$ auf einer Menge M heißt ***Ordnungsrelation***, wenn gilt:

Reflexiv $\forall x \in M : x \; \mathcal{R} \; x$.

Antisymmetrisch $\forall x, y \in M : x \; \mathcal{R} \; y \wedge y \; \mathcal{R} \; x \Longrightarrow x = y$.

Transitiv $\forall x, y, z \in M : x \; \mathcal{R} \; y \wedge y \; \mathcal{R} \; z \Longrightarrow x \; \mathcal{R} \; z$.

Definition 2.1.3 (Äquivalenzrelation)

Eine binäre Relation auf einer Menge M heißt ***Äquivalenzrelation***, notiert durch $\sim$, wenn gilt:

Reflexiv $\forall x \in M : x \sim x$.

Symmetrisch $\forall x, y \in M : x \sim y \Longrightarrow y \sim x$.

Transitiv $\forall x, y, z \in M : x \sim y \wedge y \sim z \Longrightarrow x \sim z$.

Definition 2.1.4 (Äquivalenzklassen)

Für eine Äquivalenzrelation $\sim$ auf einer Menge M fasst man zu $x \in M$ ***äquivalente*** Elemente zu einer ***Äquivalenzklasse*** $\overline{x}$, alternativ notiert durch $[x]$, zusammen:

$$\overline{x} := \{y \in M \mid x \sim y\}.$$

Satz 2.1.5 (Partition)

Eine Äquivalenzrelation $\sim$ auf einer Menge M liefert durch $\mathcal{P} := \{\overline{x} \mid x \in M\}$ eine ***Partition*** von M, d. h. eine Zerlegung der Menge M in ein System $\mathcal{P} \subseteq \mathfrak{P}M$ von disjunkten nichtleeren Teilmengen, die M überdecken:

$$\forall A \in \mathcal{P} : A \neq \emptyset, \qquad \bigcup_{A \in \mathcal{P}} A = M, \qquad \forall A, B \in \mathcal{P} : A \neq B \Longrightarrow A \cap B = \emptyset,$$

kurz (mit der Notation $\biguplus$ für die Vereinigung $\bigcup$ paarweise disjunkter Mengen)

$$\emptyset \notin \mathcal{P}, \qquad \biguplus_{A \in \mathcal{P}} A = M.$$

Umgekehrt liefert jede Partition $\mathcal{P}$ einer Menge M eine Äquivalenzrelation auf M durch $x \sim y :\Longleftrightarrow \exists A \in \mathcal{P} : x \in A \wedge y \in A$.

Definition 2.1.6 (Repräsentantensystem)

Eine Teilmenge $R \subseteq M$ heißt ***Repräsentantensystem*** einer Äquivalenzrelation $\sim$ auf M, wenn R mit jeder Äquivalenzklasse genau ein Element gemeinsam hat, einen sog. ausgezeichneten ***Vertreter*** oder ***Repräsentanten***, d. h.

$$M = \bigcup_{x \in M} \overline{x} = \biguplus_{x \in R} \overline{x}.$$

Definition 2.1.7 (Funktion)

Unter einer Funktion f versteht man eine ***Abbildungsvorschrift***, die jedem Element x einer ***Definitionsmenge*** D genau ein Element, den sog. ***Funktionswert*** $f(x)$, einer ***Zielmenge*** Z zuordnet:

$$\begin{aligned} f\colon D &\longrightarrow Z, \\ x &\longmapsto f(x). \end{aligned}$$

Sie heißt

injektiv, falls für $x, x' \in D$ aus $x \neq x'$ stets auch $f(x) \neq f(x')$ folgt,

surjektiv, falls für jedes $y \in Z$ ein $x \in D$ mit $f(x) = y$ existiert,

bijektiv, falls sie injektiv und surjektiv ist.

Unter dem ***Graphen*** von f versteht man die Relation

$$\mathcal{F} = \{(x, f(x)) \mid x \in D\} \subseteq D \times Z.$$

2.2 Ringe und Körper

Definition 2.2.1 (Ring)

Eine Menge R mit zwei Verknüpfungen, einer ***Addition*** und einer ***Multiplikation***,

$$\begin{aligned} +\colon R \times R &\longrightarrow R \\ (x, y) &\longmapsto x + y \end{aligned} \qquad \begin{aligned} \cdot\colon R \times R &\longrightarrow R \\ (x, y) &\longmapsto x \cdot y = xy \end{aligned}$$

heißt ***kommutativer Ring***, falls gilt:

Assoziativität $\forall x, y, z \in R : (x + y) + z = x + (y + z),\ (x \cdot y) \cdot z = x \cdot (y \cdot z).$

Neutrales Element ***(Null)*** $\exists 0 \in R : \forall x \in R : x + 0 = x = 0 + x,$
(Eins) $\exists 1 \in R \setminus \{0\} : \forall x \in R : x \cdot 1 = x = 1 \cdot x.$

Inverse Elemente ***(Negative)*** $\forall x \in R : \exists -x \in R : x + (-x) = 0 = (-x) + x.$

Kommutativität $\forall x, y \in R : x + y = y + x,\ x \cdot y = y \cdot x.$

Distributivität $\forall x, y, z \in R : x \cdot (y + z) = (x \cdot y) + (x \cdot z),\ (x + y) \cdot z = (x \cdot z) + (y \cdot z).$

Unter einem ***nichtkommutativen Ring*** versteht man einen Ring, in dem kein Kommutativgesetz bzgl. Multiplikation gilt (bzgl. der Addition aber schon).

Die Inversenbildung bezüglich der Addition induziert eine ***Subtraktion*** oder ***Differenz*** $-\colon R \times R \longrightarrow R,\ (x, y) \longmapsto x - y := x + (-y).$

Definition 2.2.2 (Körper)

Eine Menge K mit zwei Verknüpfungen, einer ***Addition*** und einer ***Multiplikation***,

$$+\colon K \times K \longrightarrow K \qquad\qquad \cdot\colon K \times K \longrightarrow K$$
$$(x, y) \longmapsto x + y \qquad\qquad (x, y) \longmapsto x \cdot y = xy$$

heißt ***Körper***, falls gilt:

Assoziativität $\forall x, y, z \in K : (x + y) + z = x + (y + z),\ (x \cdot y) \cdot z = x \cdot (y \cdot z).$

Neutrales Element ***(Null)*** $\exists 0 \in K : \forall x \in K : x + 0 = x = 0 + x,$
(Eins) $\exists 1 \in K \setminus \{0\} : \forall x \in K : x \cdot 1 = x = 1 \cdot x.$

Inverse Elemente ***(Negative)*** $\forall x \in K : \exists -x \in K : x + (-x) = 0 = (-x) + x,$
(Inverse) $\forall x \in K \setminus \{0\} : \exists x^{-1} \in K : x \cdot x^{-1} = 1 = x^{-1} \cdot x.$

Kommutativität $\forall x, y \in K : x + y = y + x,\ x \cdot y = y \cdot x.$

Distributivität $\forall x, y, z \in K : x \cdot (y + z) = (x \cdot y) + (x \cdot z),\ (x + y) \cdot z = (x \cdot z) + (y \cdot z).$

Die Inversenbildung bezüglich der Multiplikation induziert (unter Einbeziehung des Kommutativgesetzes) eine ***Division*** $\frac{-}{-}\colon K \times K \setminus \{0\} \longrightarrow K,\ (x, y) \longmapsto \frac{x}{y} := x \cdot y^{-1} = y^{-1} \cdot x.$

Bemerkung 2.2.3 (Notation)

Sowohl bei Ringen wie auch bei Körpern gilt:

- Aufgrund des Assoziativgesetzes können die Klammern bei Ausdrücken wie $x + y + z$ oder $x \cdot y \cdot z$ weggelassen werden.
- Die Multiplikation wirkt stärker als die Addition (***Punkt vor Strich***), so sich die Distributivität in der Form $x \cdot (y + z) = x \cdot y + x \cdot z$, $(x + y) \cdot z = x \cdot z + y \cdot z$ notieren lässt.

Satz 2.2.4

(a) In einem Ring R gilt für alle $x \in R$

$$x \cdot 0 = 0 = 0 \cdot x.$$

(b) In einem Körper K gilt für $x, y \in K$ stets die sog. ***Nullteilerfreiheit***

$$x \cdot y = 0 \Longrightarrow x = 0 \vee y = 0.$$

Satz 2.2.5

Für gegebenes $n \in \mathbb{N}$ stellt die Menge der Äquivalenzklassen

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots \overline{n-1}\}$$

bezüglich der Äquivalenzrelation (diese nennt man auch ***Kongruenzrelation modulo*** n)

$$x \equiv y \bmod n :\Longleftrightarrow n \text{ teilt } x - y$$

auf $\mathbb{Z}$ mit den beiden nachfolgenden Operationen ***Addition*** und ***Multiplikation***

$$+\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \qquad (\overline{x}, \overline{y}) \longmapsto \overline{x} + \overline{y} := \overline{x+y}$$

$$\cdot\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \qquad (\overline{x}, \overline{y}) \longmapsto \overline{x} \cdot \overline{y} := \overline{x \cdot y}$$

einen kommutativen Ring dar, den sog. ***Restklassenring modulo*** n .

Notation: Statt $\overline{x}$ schreibt man auch $x \bmod n$ oder oft kurz x, statt $\overline{x} = \overline{y}$ auch $x \equiv y \bmod n$ (in Worten: x ***kongruent zu*** y ***modulo*** n) oder einfach nur kurz $x = y$.

Bemerkung 2.2.6 (Verknüpfungstafeln modulo 2, modulo 3, modulo 4)

Additions- und Multiplikationstafel für Modulo-Rechnen:

- Modulo 2: Parität

+	0	1
0	0	1
1	1	0

·	1
1	1

- Modulo 3:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	1	2
1	1	2
2	2	1

- Modulo 4:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Bemerkung 2.2.7 (Verknüpfungstafel für $\mathbb{F}_4$)

Additions- und Multiplikationstafel für den Körper $\mathbb{F}_4$ mit 4 paarweise verschiedenen Elementen $0, 1, a, b$:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

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

DEFINITION 2.2.8 (Invertierbare Elemente, Inverses)

Ein Element x eines Rings R mit Einselement 1 heißt ***multiplikativ invertierbar*** oder kurz ***invertierbar***, falls ein $x^{-1} \in R$ existiert mit $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.

Das Element x^{-1} heißt dann ***multiplikativ Inverses***, oder kurz ***Inverses*** von x.

SATZ 2.2.9 (Invertierbare Elemente in $\mathbb{Z}/n\mathbb{Z}$)

Im Ring $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}$ sind genau die Elemente $\overline{x}$ (multiplikativ) invertierbar, für die $x \in \mathbb{Z}$ teilerfremd zu n ist.

SATZ 2.2.10 (Endlicher Körper)

(a) Für jede Primzahl p ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein ***endlicher Körper*** mit p Elementen.

(b) Für natürliche Zahlen $n \geq 2$, die keine Primzahlen sind, ist $\mathbb{Z}/nZ$ kein Körper, sondern nur ein endlicher kommutativer nicht-nullteilerfreier Ring.

(c) Ferner gibt es für jede Primzahlpotenz $q := p^r$ mit $p \in \mathbb{P}$ und $r \in \mathbb{N}$ einen Körper $\mathbb{F}_q$ mit q Elementen. Dieser ist für $r > 1$ aber nicht durch Modulo q Rechnen konstruierbar, d. h. in diesem Fall gilt $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$.

2.3 Ergänzungen

Wichtige Beispiele von Mengen mit Strukturen sind $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$:

BEISPIEL 2.3.1

- Die Menge der ***natürlichen Zahlen***

  $$\mathbb{N} := \{1, 2, 3, \dots\}$$

  erfüllen bezüglich der üblichen Addition und Multiplikation alle Ringgesetze mit Ausnahme der Existenz der Null und der inversen Elemente.

- Die Menge der natürlichen Zahlen einschließlich der Null

  $$\mathbb{N}_0 := \{0, 1, 2, 3, \dots\}$$

  erfüllen bezüglich der üblichen Addition und Multiplikation alle Ringgesetze mit Ausnahme der Existenz der inversen Elemente.

- Die Menge der ***ganzen Zahlen***

  $$\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

  bilden bezüglich der üblichen Addition und Multiplikation einen kommutativen Ring.

- Die Menge der ***rationalen Zahlen*** (Brüche ganzer Zahlen)

  $$\mathbb{Q} := \{\frac{n}{m} \mid n \in \mathbb{Z}, m \in \mathbb{N}\}$$

  bilden bezüglich der üblichen Addition und Multiplikation

  $$\frac{n}{m} + \frac{n'}{m'} := \frac{nm' + mn'}{mm'} \qquad \frac{n}{m} \cdot \frac{n'}{m'} := \frac{nn'}{mm'}$$

  einen Körper.

  Die rationalen Zahlen entsprechen den endlichen oder schließlich periodischen Dezimalzahlen.

- Die Menge der ***reellen Zahlen*** (deren Definition nicht ganz einfach ist und deshalb hier ausgelassen wird)

  $$\mathbb{R}$$

  bilden bezüglich der Addition und Multiplikation einen Körper.

  Die reellen Zahlen entsprechen allen Dezimalzahlen (einschließlich der nichtperiodischen).

- Die ***komplexen Zahlen*** lassen sich als Ausdrücke der Form $a + b\mathrm{i}$ mit $a, b \in \mathbb{R}$ und der sog. ***imaginären Einheit*** i darstellen. Auf der Menge der komplexen Zahlen

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

  lässt sich eine Addition und eine Multiplikation definieren,

  $$\begin{aligned}(a + b\mathrm{i}) + (a' + b'\mathrm{i}) &:= \quad (a + a') + \quad (b + b')\mathrm{i},\\ (a + b\mathrm{i}) \cdot (a' + b'\mathrm{i}) &:= (aa' - bb') + (ab' + a'b)\mathrm{i},\end{aligned}$$

  die der Addition bzw. Multiplikation von Polynomen in der Variablen i unter Verwendung der Zusatzdefinition $\mathrm{i}^2 = -1$ entspricht, so dass sich ein Körper mit neutralen bzw. inversen Elementen

  $$\begin{aligned}0 &:= 0 + 0\mathrm{i} & -(a + b\mathrm{i}) &= -a - b\mathrm{i} := (-a) + (-b)\mathrm{i}\\ 1 &:= 1 + 0\mathrm{i} & \frac{1}{a + b\mathrm{i}} &= \frac{a - b\mathrm{i}}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\mathrm{i}\end{aligned}$$

  ergibt.

  Identifiziert man eine reelle Zahl a mit der komplexen Zahl $a + 0\mathrm{i}$, so lässt sich $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auffassen.

3 Lineare Gleichungssysteme

Alle Definitionen und Aussagen in diesem Kapitel lassen sich statt über den reellen Zahlen $\mathbb{R}$ analog über beliebige Körper (wie $\mathbb{F}_q$ oder $\mathbb{C}$) formulieren.

Ferner seien alle auftretenden Größen m und n natürliche Zahlen.

3.1 Äquivalenzumformungen

Definition 3.1.1 (Lineares Gleichungssystem)

- Ein reelles ***lineares Gleichungssystem*** mit m Gleichungen und n Unbekannten ist ein System der Form

$$\begin{array}{ccccccccccc} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \dots & + & a_{1,n-1}x_{n-1} & + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \dots & + & a_{2,n-1}x_{n-1} & + & a_{2,n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ a_{m,1}x_1 & + & a_{m,2}x_2 & + & \dots & + & a_{m,n-1}x_{n-1} & + & a_{m,n}x_n & = & b_m \end{array}$$

  oder kurz

$$\sum_{j=1}^{n} a_{i,j}x_j = b_i \qquad \text{für } i = 1, \dots, m$$

  mit gegebenen ***Koeffizienten*** $a_{i,j}$ und b_i (für $i = 1, \dots, m$ und $j = 1, \dots, n$) des Körpers $\mathbb{R}$.

- Das lineare Gleichungssystem heißt ***homogen***, wenn alle Koeffizienten $b_i = 0$ (für $i = 1, \dots, m$) sind, ansonsten heißt es ***inhomogen***.

- Ein Tupel $(x_1, x_2, \dots, x_{n-1}, x_n)$ des n-fachen kartesischen Produkts $\mathbb{R}^n$ heißt ***Lösung*** des linearen Gleichungssystems, wenn dieses nach Einsetzen der Werte erfüllt ist. Die Lösung $(0, 0, \dots, 0, 0)$ eines homogenen linearen Gleichungssystems nennt man auch ***triviale*** Lösung. Die Menge aller Lösungen heißt ***Lösungsmenge*** des linearen Gleichungssystems.

- Zwei lineare Gleichungssysteme heißen ***äquivalent***, wenn sie die selbe Lösungsmenge besitzen.

Definition 3.1.2 (Koeffizientenmatrix)

Für ein lineares Gleichungssystem

$$\sum_{j=1}^{n} a_{i,j}x_j = b_i \qquad \text{für } i = 1, \dots, m$$

mit m Gleichungen und n Unbekannten bezeichnet das nachfolgende rechteckige Schema die ***Koeffizientenmatrix*** bzw. die ***erweiterte Koeffizientenmatrix***:

$$\underbrace{\underbrace{\begin{matrix} a_{1,1} & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n-1} & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n-1} & a_{m,n} \end{matrix}}_{\text{Koeffizientenmatrix}} \left| \begin{matrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{matrix} \right.}_{\text{Erweiterte Koeffizientenmatrix}}$$

DEFINITION UND SATZ 3.1.3 (Elementare Zeilenumformungen)

Unter ***elementaren Zeilenumformungen*** versteht man die folgenden drei Typen von Umformungen der Zeilen einer (erweiterten) Koeffizientenmatrix bzw. der Gleichungen des zugehörigen linearen Gleichungssystems:

Typ A Addition des λ-fachen einer Zeile zu einer anderen Zeile, wobei $\lambda \in \mathbb{R}$ beliebig:

$$\begin{matrix} \text{(I)} \\ \text{(II)} \end{matrix} \quad \Longleftrightarrow \quad \begin{matrix} \text{(I)} + \lambda\text{(II)} \\ \text{(II)} \end{matrix}$$

Typ B Vertauschen zweier Zeilen:

$$\begin{matrix} \text{(I)} \\ \text{(II)} \end{matrix} \quad \Longleftrightarrow \quad \begin{matrix} \text{(II)} \\ \text{(I)} \end{matrix}$$

Typ C Multiplikation einer Zeile mit $\lambda \in \mathbb{R}$, wobei $\lambda \neq 0$:

$$\text{(I)} \quad \Longleftrightarrow \quad \lambda\text{(I)}$$

Die elementaren Zeilenumformungen sind Äquivalenzumformungen und ändern die Lösungsmenge des Gleichungssystems nicht.

3.2 Zeilenstufenform und Gaußsches Eliminationsverfahren

DEFINITION 3.2.1 (Zeilenstufenform)

- Eine (erweiterte) Koeffizientenmatrix liegt in ***Zeilenstufenform*** vor, wenn jede Nichtnullzeile mehr Anfangsnullen besitzt als die vorherige Zeile, d. h. die Anzahl der Anfangsnullen der Nichtnullzeilen mit wachsendem Zeilenindex echt zunimmt, bis am Ende ggf. nur noch Nullzeilen auftreten:

$$\begin{array}{l} \overline{0 \dots 0}\,|\, \star \;\; ? \;\dots\dots\dots\dots\dots\dots\dots\dots ? \\ 0 \dots\dots\dots\dots 0 \,|\, \star \;\; ? \;\dots\dots\dots\dots\dots ? \\ 0 \dots\dots\dots\dots\dots\dots\dots 0 \,|\, \star \;\; ? \;\dots\dots ? \\ 0 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots 0 \\ 0 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots 0 \end{array}$$

wobei ? für eine beliebige reelle Zahl und $\star$ für eine Zahl $\neq 0$ steht. Letztere nennt man auch die ***Stufen*** und die horizontalen Abstände zwischen ihnen die ***Längen*** der Stufen.

- Eine (erweiterte) Koeffizientenmatrix in Zeilenstufenform liegt in ***reduzierter Zeilenstufenform*** vor, wenn der erste Nichtnulleintrag jeder Zeile eine 1 ist und die Einträge oberhalb dieser Stufenelemente stets 0 sind:

$$\begin{array}{l}
0 \ldots 0 \;\; 1 \;\; ? \ldots ? \;\; 0 \;\; ? \ldots\ldots ? \;\; 0 \;\; ? \ldots\ldots ? \\
0 \ldots\ldots\ldots\ldots\ldots 0 \;\; 1 \;\; ? \ldots\ldots ? \;\; 0 \;\; ? \ldots\ldots ? \\
0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 \;\; 1 \;\; ? \ldots\ldots ? \\
0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 \\
0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0
\end{array}$$

  wobei ? für eine beliebige reelle Zahl steht.

Satz 3.2.2 (Gaußsches Eliminationsverfahren)

Jede Koeffizientenmatrix lässt sich durch Anwendung von elementaren Zeilenumformungen vom Typ A und B auf Zeilenstufenform und durch zusätzliche Verwendung von Typ C auf reduzierte Zeilenstufenform bringen. Die Zeilenstufenform ist i. a. nicht eindeutig, die reduzierte Zeilenstufenform hingegen ist stets eindeutig.

Erzeugung einer Zeilenstufenform:

(1) Starte mit der Koeffizientenmatrix mit m Zeilen und reellen Einträgen $a_{i,j}$.

(2) Setze Spaltenindex j auf die erste Nichtnullspalte. Falls keine solche existiert, beende Algorithmus und gib aktuelle Koeffizientenmatrix zurück.

(3) Setze Zeilenindex i auf eine Zeile, in der der Eintrag $a_{i,j}$ in der Spalte j nicht 0 ist.

(4) Vertausche Zeile i mit der ersten Zeile durch eine elementare Zeilenumformung vom Typ B. Die resultierende Koeffizientenmatrix hat hiernach einen Eintrag $a_{1,j} \neq 0$.

(5) Durchlaufe mit k die Zeilen ab Index 2 und addiere jeweils zur k-ten Zeile das $(-\frac{a_{k,j}}{a_{1,j}})$-fache der ersten Zeile durch eine elementare Zeilenumformung vom Typ A. Die resultierende Koeffizientenmatrix hat hiernach die Einträge $a_{k,j} = 0$ für $k \geq 2$ und Nullspalten links der j-ten Spalte.

(6) Wiederhole die Schritte (2) bis (5) rekursiv mit der Teilmatrix, die durch Weglassen der ersten Zeile aus der Koeffizientenmatrix entsteht.

Das Verfahren bricht ab, wenn es keine Nichtnullspalte in der iterativ stets um eine Zeile kleiner werdenden Teilmatrix mehr gibt, spätestens, wenn die Teilmatrix keine Zeilen mehr besitzt.

Als Ergebnis liegt die Koeffizientenmatrix in einer Zeilenstufenform vor.

Erzeugung der reduzierten Zeilenstufenform:

(1) Starte mit einer Zeilenstufenform mit m Zeilen und reellen Einträgen $a_{i,j}$.

(2) Setze Zeilenindex i auf die letzte Nichtnullzeile. Falls keine solche existiert, beende Algorithmus und gib aktuelle Koeffizientenmatrix zurück.

(3) Setze Spaltenindex j auf den ersten Nichtnulleintrag $a_{i,j} \neq 0$, d. h. auf die Stufe der Zeile i.

(4) Multipliziere die Zeile i mit dem Inversen $a_{i,j}^{-1}$ durch eine elementare Zeilenumformung vom Typ C. Die resultierende Koeffizientenmatrix hat hiernach den Eintrag 1 bei der Stufe der Zeile i.

(5) Durchlaufe mit k die Zeilen bis Index $i-1$ und addiere jeweils zur k-ten Zeile das $(-a_{k,j})$-fache der i-ten Zeile durch eine elementare Zeilenumformung vom Typ A. Die resultierende Koeffizientenmatrix hat hiernach die Einträge $a_{k,j}=0$ für $k<i$ in der j-ten Spalte oberhalb der Stufe der i-ten Zeile.

(6) Wiederhole die Schritte (2) bis (5) rekursiv mit der Teilmatrix, die durch Weglassen der Zeilen ab Index i aus der Koeffizientenmatrix entsteht.

Das Verfahren bricht ab, wenn es keine Nichtnullzeile in der iterativ stets um mindestens eine Zeile kleiner werdenden Teilmatrix mehr gibt, spätestens, wenn die Teilmatrix keine Zeilen mehr besitzt.

Als Ergebnis liegt die Koeffizientenmatrix in der eindeutig bestimmten reduzierten Zeilenstufenform vor.

Der selbe Algorithmus kann verwendet werden, um die (reduzierte) Zeilenstufenform der erweiterten Koeffizientenmatrix zu bestimmen: Die letzte Spalte mit den Einträgen b_i ist dann wie die ersten n Spalten mit den Koeffizienten $a_{i,j}$ zu behandeln.

3.3 Lösungsmethode

Definition 3.3.1

Liegt eine (erweiterte) Koeffizientenmatrix in Zeilenstufenform vor, so bezeichnet die (von der expliziten Darstellung unabhängige) Anzahl der Nichtnullzeilen ihren ***Rang***.

Satz 3.3.2 (Lösung eines linearen Gleichungssystems)

Liegt die erweiterte Koeffizientenmatrix eines lineares Gleichungssystems mit m Gleichungen und n Unbekannten in Zeilenstufenform mit Koeffizienten $a_{i,j}$ und b_i für $i=1,\dots,m$ und $j=1,\dots,n$ vor, so ergibt sich die Lösbarkeit wie folgt:

- Das Gleichungssystem ist genau dann *lösbar*, wenn der Rang der Koeffizientenmatrix mit dem Rang der erweiterten Koeffizientenmatrix übereinstimmt.
- Das Gleichungssystem ist genau dann *eindeutig lösbar*, wenn darüber hinaus der Rang mit der Anzahl der Variablen n übereinstimmt, d. h. alle Stufen in der (nicht erweiterten) Koeffizientenmatrix Länge 1 besitzen.

Im Fall der Lösbarkeit ergibt sich die Lösungsmenge wie folgt:

- Die Nichtstufen der Koeffizientenmatrix bilden die ***freien Variablen*** x_k. Diese können beliebige Werte aus $\mathbb{R}$ annehmen.
- Die Stufen der Koeffizientenmatrix bilden die ***gebundenen Variablen*** x_j. Tritt die zur gebundenen Variablen x_j zugehörende Stufe in der i-ten Zeile auf, so ergibt sich durch Auflösen der zugehörigen Gleichung $a_{i,j}x_j + a_{i,j+1}x_{j+1} + \cdots + a_{i,n}x_n = b_i$ im Falle einer beliebigen Zeilenstufenform bzw. einer reduzierten Zeilenstufenform

$$x_j = \frac{1}{a_{i,j}}\left(b_i - \sum_{k=j+1}^{n} a_{i,k}x_k\right) \qquad \text{bzw.} \qquad x_j = b_i - \sum_{k=j+1}^{n} a_{i,k}x_k.$$

Im Fall einer belieben Zeilenstufenform können in der Summe neben freien Variablen und der Stufenvariablen x_j auch weitere gebundene Variablen zu Indizes $k > j$ enthalten sein, so dass diese Gleichungen sukzessiv von unten nach oben aufgelöst und bereits berechnete gebundene Variablen eingesetzt werden müssen.
Im Fall einer reduzierten Zeilenstufenform vereinfacht sich der Vorfaktor und es treten in der Summe nur Indizes k freier Variablen auf.

4 Vektoren und Matrizen

Alle Definitionen und Aussagen in diesem Kapitel lassen sich statt über den reellen Zahlen $\mathbb{R}$ analog über beliebige Körper (wie $\mathbb{F}_q$ oder $\mathbb{C}$) formulieren.

Ferner seien alle auftretenden Größen m und n natürliche Zahlen.

4.1 Vektoren

Definition 4.1.1 (Vektor)

Ein ***Vektor*** im $\mathbb{R}^n$ ist ein Tupel reeller Zahlen, d. h. ein Element des kartesischen Produkts

$$\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \{(x_1, x_2, \ldots, x_n) \mid x_1, x_2, \ldots, x_n \in \mathbb{R}\}.$$

Notation eines Vektors $v = (v_i) = (v_i)_{i=1,\ldots,n} \in \mathbb{R}^n$ als

Spaltenvektor $v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$,

Zeilenvektor $v = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix}$.

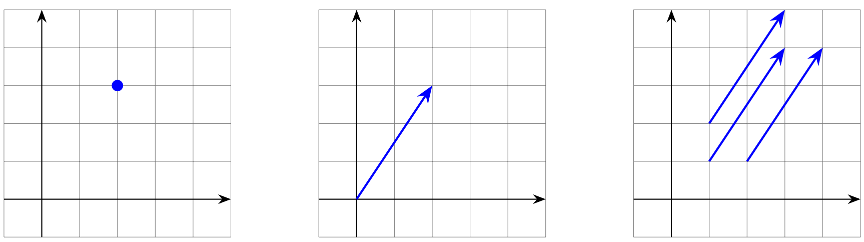
Bemerkung 4.1.2 (Geometrische Darstellung von Vektoren)

Geometrische Darstellung eines Vektors als

Punkt mit entsprechenden Koordinaten im $\mathbb{R}^n$,

Ortsvektor vom Nullpunkt zu einem Punkt (Ort) mit entsprechenden Koordinaten,

Freier Vektor wie der Ortsvektor, aber von einem beliebigen Punkt ausgehend frei im $\mathbb{R}^n$.



Punkt Ortsvektor freier Vektor

Definition 4.1.3 (Gleichheit von Vektoren)

Zwei Vektoren v und w heißen ***gleich***, wenn sie die gleiche Anzahl an Einträgen besitzen und diese ***Komponenten*** (***Koeffizienten*** oder ***Koordinaten***) paarweise übereinstimmen, d. h. für $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^n$ und $w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in \mathbb{R}^n$ gilt

$$v_i = w_i \qquad \text{für alle } i = 1, \ldots, n.$$

Definition 4.1.4 (Addition von Vektoren)

Für zwei Vektoren $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^n$ und $w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in \mathbb{R}^n$ ist die ***Addition*** definiert durch

$$v + w := \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix} \in \mathbb{R}^n.$$

Satz 4.1.5 (Rechengesetze der Vektoraddition)

Die Addition von Vektoren im $\mathbb{R}^n$ liefert eine Abbildung

$$+ \colon \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}^n \qquad (v, w) \longmapsto v + w$$

mit folgenden Eigenschaften:

Assoziativität $\forall u, v, w \in \mathbb{R}^n : (u + v) + w = u + (v + w)$.

Neutrales Element $\exists 0 \in \mathbb{R}^n : \forall v \in \mathbb{R}^n : v + 0 = v = 0 + v$, nämlich der ***Nullvektor***

$$0 := \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Inverse Elemente $\forall v \in \mathbb{R}^n : \exists -v \in \mathbb{R}^n : v + (-v) = 0 = (-v) + v$, nämlich das ***Negative***

$$-v := \begin{pmatrix} -v_1 \\ \vdots \\ -v_n \end{pmatrix} \qquad \text{zu } v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Kommutativität $\forall v, w \in \mathbb{R}^n : v + w = w + v$.

Definition 4.1.6 (Subtraktion von Vektoren)

Die Inversenbildung bezüglich Addition im $\mathbb{R}^n$ induziert die ***Subtraktion*** oder ***Differenz*** zweier Vektoren im $\mathbb{R}^n$, d. h. eine Abbildung

$$- \colon \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}^n \qquad (v, w) \longmapsto v - w := v + (-w)$$

Definition 4.1.7 (Skalarmultiplikation von Vektoren)

Für eine Zahl (einem sog. ***Skalar***) $\lambda \in \mathbb{R}$ und einen Vektor $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^n$ ist die ***Skalarmultiplikation*** definiert durch

$$\lambda v := \lambda \cdot v := \begin{pmatrix} \lambda v_1 \\ \vdots \\ \lambda v_n \end{pmatrix} \in \mathbb{R}^n.$$

Satz 4.1.8 (Rechengesetze der Skalarmultiplikation)

Die Skalarmultiplikation von Vektoren im $\mathbb{R}^n$ liefert eine Abbildung

$$\cdot : \mathbb{R} \times \mathbb{R}^n \longrightarrow \mathbb{R}^n \qquad (\lambda, v) \longmapsto \lambda \cdot v = \lambda v$$

mit folgenden Eigenschaften:

- $\forall \lambda, \mu \in \mathbb{R}, v \in \mathbb{R}^n : \lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v.$
- $\forall v \in \mathbb{R}^n : 1 \cdot v = v.$
- $\forall \lambda \in \mathbb{R}, v, w \in \mathbb{R}^n : \lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w.$
- $\forall \lambda, \mu \in \mathbb{R}, v \in \mathbb{R}^n : (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v.$

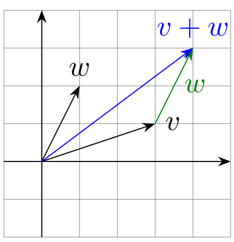
Bemerkung 4.1.9 (Geometrische Interpretation der Vektoroperationen)

Geometrische Interpretation der

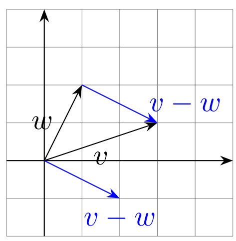
Vektoraddition Summe $v + w$ durch Aneinanderhängen der Vektoren v und w,

Subtraktion Differenz $v - w$ als Verbindungsvektor von w nach v,

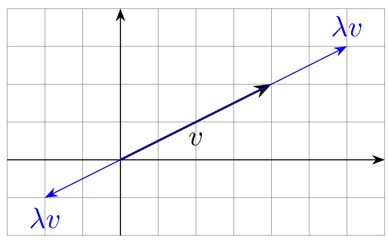
Skalarmultiplikation Streckung für $|\lambda| > 1$ oder Stauchung für $|\lambda| < 1$, mit Orientierungswechsel im Fall $\lambda < 0$.



Vektoraddition



Subtraktion



Skalarmultiplikation

Definition 4.1.10 (Reeller Vektorraum)

Eine Menge V mit zwei Verknüpfungen, einer Addition und einer Skalarmultiplikation, die den Gesetzen der Sätze 4.1.5 und 4.1.8 genügen, nennt man einen ***reellen Vektorraum***.

Die ***Addition***

$$+ : V \times V \longrightarrow V \qquad (v, w) \longmapsto v + w$$

erfüllt somit:

Assoziativität $\forall u, v, w \in V\colon (u+v)+w = u+(v+w)$.

Neutrales Element $\exists 0 \in V : \forall v \in V : v + 0 = v = 0 + v$.

Inverse Elemente $\forall v \in V : \exists -v \in V : v + (-v) = 0 = (-v) + v$.

Kommutativität $\forall v, w \in V\colon v + w = w + v$.

Für die ***Skalarmultiplikation***

$$\cdot\colon \mathbb{R} \times V \longrightarrow V \qquad\qquad (\lambda, v) \longmapsto \lambda \cdot v = \lambda v$$

gilt ferner:

- $\forall \lambda, \mu \in \mathbb{R}, v \in V\colon \lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$.
- $\forall v \in V\colon 1 \cdot v = v$.
- $\forall \lambda \in \mathbb{R}, v, w \in V\colon \lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$.
- $\forall \lambda, \mu \in \mathbb{R}, v \in V\colon (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$.

Satz 4.1.11

Die Menge der Vektoren des $\mathbb{R}^n$, versehen mit Addition und Skalarmultiplikation, bilden einen reellen Vektorraum.

4.2 Matrizen

Definition 4.2.1 (Matrix)

Eine ***Matrix*** über $\mathbb{R}$ der Größe $m \times n$ ist ein rechteckiges Schema von doppelt indizierten Einträgen $a_{i,j} \in \mathbb{R}$, d. h. von der Form

$$A = (a_{i,j}) = (a_{i,j})_{\substack{i=1,\dots,m\\ j=1,\dots,n}} = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n-1} & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \dots & \dots & a_{i,j} & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n-1} & a_{m,n} \end{pmatrix}$$

Die Menge der reellen $(m \times n)$-Matrizen bezeichnet man mit $\mathrm{M}_{m,n}(\mathbb{R})$, und für $m = n$ die Menge der ***quadratischen*** $(n \times n)$-Matrizen mit $\mathrm{M}_n(\mathbb{R})$.

Notation in

Spaltendarstellung als Matrix bestehend aus Spaltenvektoren:

$$A = (a_j)_{j=1,\dots,n} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \qquad \text{mit } a_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{m,j} \end{pmatrix} \text{ für } j = 1, \dots, n,$$

Zeilendarstellung als Matrix bestehend aus Zeilenvektoren

$$A = (a^i)_{i=1,\dots,m} = \begin{pmatrix} a^1 \\ a^2 \\ \vdots \\ a^m \end{pmatrix} \qquad \text{mit } a^i = \begin{pmatrix} a_{i,1} & \cdots & a_{i,n} \end{pmatrix} \text{ für } i = 1, \dots, m.$$

Definition 4.2.2 (Gleichheit von Matrizen)

Zwei Matrizen A und B heißen ***gleich***, wenn sie die gleiche Anzahl an Zeilen sowie die gleiche Anzahl an Spalten besitzen und die ***Komponenten*** (***Koeffizienten***) paarweise übereinstimmen, d. h. $A = (a_{i,j}) \in \mathrm{M}_{m,n}(\mathbb{R})$ und $B = (b_{i,j}) \in \mathrm{M}_{m,n}(\mathbb{R})$ mit

$$a_{i,j} = b_{i,j} \qquad \text{für alle } i = 1, \ldots, m \text{ und } j = 1, \ldots, n.$$

Definition 4.2.3 (Addition von Matrizen)

Für zwei Matrizen $A = (a_{i,j}) \in \mathrm{M}_{m,n}(\mathbb{R})$ und $B = (b_{i,j}) \in \mathrm{M}_{m,n}(\mathbb{R})$ ist die ***Addition*** definiert durch

$$A + B := (a_{i,j} + b_{i,j}) \in \mathrm{M}_{m,n}(\mathbb{R}).$$

Satz 4.2.4 (Rechengesetze der Matrizenaddition)

Die Addition von Matrizen aus $\mathrm{M}_{m,n}(\mathbb{R})$ liefert eine Abbildung

$$+\colon \mathrm{M}_{m,n}(\mathbb{R}) \times \mathrm{M}_{m,n}(\mathbb{R}) \longrightarrow \mathrm{M}_{m,n}(\mathbb{R}) \qquad (A, B) \longmapsto A + B$$

mit folgenden Eigenschaften:

Assoziativität $\forall A, B, C \in \mathrm{M}_{m,n}(\mathbb{R}) : (A + B) + C = A + (B + C)$.

Neutrales Element $\exists 0 \in \mathrm{M}_{m,n}(\mathbb{R}) : \forall A \in \mathrm{M}_{m,n}(\mathbb{R}) : A + 0 = A = 0 + A$, nämlich die ***Nullmatrix***

$$0 := \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix}.$$

Inverse Elemente $\forall A \in \mathrm{M}_{m,n}(\mathbb{R}) : \exists -A \in \mathrm{M}_{m,n}(\mathbb{R}) : A + (-A) = 0 = (-A) + A$, nämlich das ***Negative*** $-A := (-a_{i,j})$ zu $A = (a_{i,j})$.

Kommutativität $\forall A, B \in \mathrm{M}_{m,n}(\mathbb{R}) : A + B = B + A$.

Definition 4.2.5 (Subtraktion von Matrizen)

Die Inversenbildung bezüglich Addition in $\mathrm{M}_{m,n}(\mathbb{R})$ induziert die ***Subtraktion*** oder ***Differenz*** zweier Matrizen in $\mathrm{M}_{m,n}(\mathbb{R})$, d. h. eine Abbildung

$$-\colon \mathrm{M}_{m,n}(\mathbb{R}) \times \mathrm{M}_{m,n}(\mathbb{R}) \longrightarrow \mathrm{M}_{m,n}(\mathbb{R}) \qquad (A, B) \longmapsto A - B := A + (-B)$$

Definition 4.2.6 (Skalarmultiplikation von Matrizen)

Für eine Zahl (einem Skalar) $\lambda \in \mathbb{R}$ und eine Matrix $A = (a_{i.j}) \in \mathrm{M}_{m,n}(\mathbb{R})$ ist die ***Skalarmultiplikation*** definiert durch

$$\lambda A := \lambda \cdot A := (\lambda a_{i,j}) \in \mathrm{M}_{m,n}(\mathbb{R}).$$

Satz 4.2.7 (Rechengesetze der Skalarmultiplikation)

Die Skalarmultiplikation bei Matrizen im $\mathrm{M}_{m,n}(\mathbb{R})$ liefert eine Abbildung

$$\cdot\colon \mathbb{R} \times \mathrm{M}_{m,n}(\mathbb{R}) \longrightarrow \mathrm{M}_{m,n}(\mathbb{R}) \qquad (\lambda, A) \longmapsto \lambda \cdot A = \lambda A$$

mit folgenden Eigenschaften:

- $\forall \lambda, \mu \in \mathbb{R}, A \in \mathrm{M}_{m,n}(\mathbb{R}) : \lambda \cdot (\mu \cdot A) = (\lambda \cdot \mu) \cdot A$.
- $\forall A \in \mathrm{M}_{m,n}(\mathbb{R}) : 1 \cdot A = A$.
- $\forall \lambda \in \mathbb{R}, A, B \in \mathrm{M}_{m,n}(\mathbb{R}) : \lambda \cdot (A + B) = (\lambda \cdot A) + (\lambda \cdot B)$.
- $\forall \lambda, \mu \in \mathbb{R}, A \in \mathrm{M}_{m,n}(\mathbb{R}) : (\lambda + \mu) \cdot A = (\lambda \cdot A) + (\mu \cdot A)$.

Korollar 4.2.8 (Vektorraum der Matrizen)

Die Menge der Matrizen $M_{m,n}(\mathbb{R})$, versehen mit Addition und Skalarmultiplikation, bilden einen reellen Vektorraum.

Definition 4.2.9 (Multiplikation von Matrizen)

Für eine Matrix $A = (a_{i,k}) \in \mathrm{M}_{m,r}(\mathbb{R})$ und eine Matrix $B = (b_{k,j}) \in \mathrm{M}_{r,n}(\mathbb{R})$ ist die ***Multiplikation*** definiert durch

$$AB := A \cdot B := (c_{i,j}) \in \mathrm{M}_{m,n}(\mathbb{R}) \qquad \text{mit} \qquad c_{i,j} := \sum_{k=1}^{r} a_{i,k} b_{k,j}.$$

d. h. anschaulich

$$\underbrace{\begin{pmatrix} \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{i,1} & \cdots & a_{i,k} & \cdots & a_{i,r} \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}}_{m \times r} \cdot \underbrace{\begin{pmatrix} \vdots & b_{1,j} & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & b_{k,j} & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & b_{r,j} & \vdots & \vdots \end{pmatrix}}_{r \times n} = \underbrace{\begin{pmatrix} \cdots & \vdots & \cdots & \cdots \\ \cdots & c_{i,j} & \cdots & \cdots \\ \cdots & \vdots & \cdots & \cdots \end{pmatrix}}_{m \times n}$$

Satz 4.2.10 (Rechengesetze der Matrizenmultiplikation)

Die Multiplikation von Matrizen aus $\mathrm{M}_{m,r}(\mathbb{R})$ und $\mathrm{M}_{r,n}(\mathbb{R})$ liefert eine Abbildung

$$\cdot : \mathrm{M}_{m,r}(\mathbb{R}) \times \mathrm{M}_{r,n}(\mathbb{R}) \longrightarrow \mathrm{M}_{m,n}(\mathbb{R}) \qquad (A, B) \longmapsto A \cdot B = AB$$

mit folgenden Eigenschaften:

Assoziativität $\forall A \in \mathrm{M}_{m,r}(\mathbb{R}), B \in \mathrm{M}_{r,s}(\mathbb{R}), C \in \mathrm{M}_{s,n}(\mathbb{R}) : (A \cdot B) \cdot C = A \cdot (B \cdot C)$.

Neutrales Element ***(rechtsneutral)*** $\exists E_n \in \mathrm{M}_{n,n}(\mathbb{R}) : \forall A \in \mathrm{M}_{m,n}(\mathbb{R}) : A \cdot E_n = A$,
(linksneutral) $\exists E_m \in \mathrm{M}_{m,m}(\mathbb{R}) : \forall A \in \mathrm{M}_{m,n}(\mathbb{R}) : A = E_m \cdot A$,
nämlich die ***Einheitsmatrix*** passender Größe

$$E_k := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} = (\delta_{i,j}) \in \mathrm{M}_{k,k}(\mathbb{R}) = \mathrm{M}_k(\mathbb{R})$$

mit $\delta_{i,j} = 1$ für $i = j$ und $\delta_{i,j} = 0$ für $i \neq j$.

Skalare $\forall A \in \mathrm{M}_{m,r}(\mathbb{R}), B \in \mathrm{M}_{r,n}(\mathbb{R}), \lambda \in \mathbb{R} : (\lambda \cdot A) \cdot B = A \cdot (\lambda \cdot B) = \lambda \cdot (A \cdot B)$.

Satz 4.2.11 (Ringstruktur für quadratische Matrizen)

Die quadratischen Matrizen $\mathrm{M}_n(\mathbb{R})$ bilden mit der Addition und der Multiplikation einen Ring, den ***Matrizenring***. Im Fall $n = 1$ ist dieser kommutativ, im Fall $n \geq 2$ ist er ***nicht-kommutativ***. Die Verknüpfungen

$$+\colon\ \mathrm{M}_n(\mathbb{R}) \times \mathrm{M}_n(\mathbb{R}) \longrightarrow \mathrm{M}_n(\mathbb{R}) \qquad (A,B) \longmapsto A+B$$

$$\cdot\colon\ \mathrm{M}_n(\mathbb{R}) \times \mathrm{M}_n(\mathbb{R}) \longrightarrow \mathrm{M}_n(\mathbb{R}) \qquad (A,B) \longmapsto A \cdot B = AB$$

erfüllen also folgende Eigenschaften:

Assoziativität $\forall A,B,C \in \mathrm{M}_n(\mathbb{R})$: $(A+B)+C = A+(B+C)$, $(A\cdot B)\cdot C = A\cdot(B\cdot C)$.

Neutrales Element ***(Nullmatrix)*** $\exists 0 \in \mathrm{M}_n(\mathbb{R}) : \forall A \in \mathrm{M}_n(\mathbb{R}) : A + 0 = A = 0 + A$,
(Einheitsmatrix) $\exists E \in \mathrm{M}_n(\mathbb{R}) : \forall A \in \mathrm{M}_n(\mathbb{R}) : A \cdot E = A = E \cdot A$.

Inverse Elemente ***(Negative)*** $\forall A \in \mathrm{M}_n(\mathbb{R}) : \exists -A \in \mathrm{M}_n(\mathbb{R}) : A+(-A) = 0 = (-A)+A$.

Kommutativität $\forall A,B \in \mathrm{M}_n(\mathbb{R}) : A+B = B+A$, für $n = 1$ auch $A \cdot B = B \cdot A$, für $n \geq 2$ i. a. aber nicht.

Distributivität $\forall A,B,C \in \mathrm{M}_n(\mathbb{R}) : A\cdot(B+C) = A\cdot B + A\cdot C$, $(A+B)\cdot C = A\cdot C + B\cdot C$.

Definition 4.2.12 (Multiplikation von Matrix mit Vektor)

- Interpretiert man einen Spaltenvektor als Matrix mit genau einer Spalte, so ergibt sich durch die Matrizenmultiplikation eine ***Multiplikation einer*** $(m \times n)$***-Matrix mit einem Spaltenvektor*** des $\mathbb{R}^n$, wobei das Ergebnis ein Spaltenvektor des $\mathbb{R}^m$ ist:

$$\cdot\colon\ \mathrm{M}_{m,n}(\mathbb{R}) \times \mathbb{R}^n \longrightarrow \mathbb{R}^m \qquad (A,x) \longmapsto A\cdot x = Ax$$

- Interpretiert man einen Zeilenvektor als Matrix mit genau einer Zeile, so ergibt sich durch die Matrizenmultiplikation eine ***Multiplikation eines Zeilenvektors*** des $\mathbb{R}^m$ ***mit einer*** $(m \times n)$***-Matrix***, wobei das Ergebnis ein Zeilenvektor des $\mathbb{R}^n$ ist:

$$\cdot\colon\ \mathbb{R}^m \times \mathrm{M}_{m,n}(\mathbb{R}) \longrightarrow \mathbb{R}^n \qquad (x,A) \longmapsto x\cdot A = xA$$

Bemerkung 4.2.13

Interpretiert man ein Skalar als Matrix mit genau einer Zeile und einer Spalte, so lässt sich die Skalarmultiplikation mit einem Zeilenvektor bzw. einem Spaltenvektor auch als Multiplikation einer (1×1)-Matrix von links bzw. von rechts darstellen:

$$\lambda \cdot \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix} = (\lambda) \cdot \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}, \qquad \lambda \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot (\lambda).$$

4.3 Linearkombinationen und lineare Unabhängigkeit

Definition 4.3.1 (Linearkombination)

- Ein Vektor $w \in \mathbb{R}^n$ heißt ***Linearkombination*** der Vektoren $v_1, \ldots, v_k \in \mathbb{R}^n$ mit $k \in \mathbb{N}$, falls Skalare $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ existieren, auch ***Koeffizienten*** genannt, so dass

$$w = \lambda_1 v_1 + \cdots + \lambda_k v_k = \sum_{i=1}^{k} \lambda_i v_i.$$

- Unter einer ***Linearkombination der Null*** versteht man eine Linearkombination des Nullvektors $0 \in \mathbb{R}^n$, d. h. eine Darstellung

$$\lambda_1 v_1 + \cdots + \lambda_k v_k = 0.$$

- Eine Linearkombination heißt ***trivial***, wenn alle zugehörigen Koeffizienten 0 sind, $\lambda_1 = 0, \ldots, \lambda_k = 0$. Andernfalls heißt sie ***nichttrivial***, d. h. mindestens einer der Koeffizienten ist ungleich 0.

Definition 4.3.2 (Lineare Unabhängigkeit, Lineare Abhängigkeit)

Vektoren $v_1, \ldots, v_k \in \mathbb{R}^n$ mit $k \in \mathbb{N}$ heißen ***linear unabhängig***, wenn eine der folgenden äquivalenten Bedingungen gilt:

- Es gibt nur die triviale Linearkombination der Null aus den Vektoren $v_1, \ldots, v_k$.
- Die Linearkombination der Null aus den Vektoren $v_1, \ldots, v_k$ ist eindeutig.
- Mit $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ folgt aus $\lambda_1 v_1 + \cdots + \lambda_k v_k = 0$, dass alle Koeffizienten gleich 0 sind: $\lambda_1 = 0 \wedge \cdots \wedge \lambda_k = 0$.

Andernfalls heißen die Vektoren $v_1, \ldots, v_k$ ***linear abhängig***, d. h. wenn eine der folgenden äquivalenten Bedingungen gilt:

- Es gibt eine nichttriviale Linearkombination der Null aus den Vektoren $v_1, \ldots, v_k$.
- Die Linearkombination der Null aus den Vektoren $v_1, \ldots, v_k$ ist nicht eindeutig.
- Es gibt $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ mit $\lambda_1 v_1 + \cdots + \lambda_k v_k = 0$, wobei nicht alle Koeffizienten gleich 0 sind, also mindestens einer davon ungleich 0 ist: $\lambda_1 \neq 0 \vee \cdots \vee \lambda_k \neq 0$.

Im Fall $k = 0$, d. h. einer leeren Menge von Vektoren, spricht man stets von linear unabhängig.

Satz 4.3.3 (Lineare Abhängigkeit)

Vektoren $v_1, \ldots, v_k \in \mathbb{R}^n$ mit $k \in \mathbb{N}$ sind genau dann linear abhängig, wenn mindestens einer dieser Vektoren eine Linearkombination der restlichen ist.

Bemerkung 4.3.4 (Spezialfälle von linearer Abhängigkeit bzw. Unabhängigkeit)

Lineare Abhängigkeit von Vektoren liegt insbesondere in folgenden Fällen vor:

- Einer der Vektoren ist der Nullvektor.
- Ein Vektor kommt mindestens zweimal vor.
- Ein Vektor ist ein Vielfaches eines anderen Vektors.

Lineare Unabhängigkeit von Vektoren liegt insbesondere in folgenden Fällen vor:

- Die Anzahl der betrachteten Vektoren ist 0.
- Die Anzahl der betrachteten Vektoren ist 1, und dieser Vektor ist nicht der Nullvektor.
- Die Anzahl der betrachteten Vektoren ist 2, und keiner der beiden Vektoren ist ein Vielfaches des anderen.

4.4 Lineares Gleichungssystem als Matrixgleichung

Satz 4.4.1 (Lineares Gleichungssystem als Matrixgleichung)

Das lineare Gleichungssystem

$$\sum_{j=1}^{n} a_{i,j} x_j = b_i \qquad \text{für } i = 1, \dots, m$$

mit m Gleichungen und n Unbekannten entspricht der Gleichung

$$A \cdot x = b \qquad \text{mit } A = (a_{i,j}) \in \mathrm{M}_{m,n}(\mathbb{R}) \text{ und } b = (b_i) \in \mathbb{R}^m.$$

Lösungstupel $(x_1, \dots, x_n) \in \mathbb{R} \times \dots \times \mathbb{R}$ entsprechen hierbei Spaltenvektoren $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$.

Die Einträge der Lösungsvektoren x der Gleichung $A \cdot x = b$ mit Matrix A in Spaltendarstellung,

$$A \cdot x = \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 a_1 + \dots + x_n a_n,$$

ergeben sich aus den Koeffizienten der Linearkombinationen von b aus den Spaltenvektoren $a_1, \dots, a_n \in \mathbb{R}^m$ der Matrix A.

Insbesondere ergeben sich die Lösungen der Gleichung $A \cdot x = 0$ durch die Linearkombinationen des Nullvektors aus den Spaltenvektoren der Matrix A.

Korollar 4.4.2 (Lösung eines homogenen linearen Gleichungssystems)

Für ein homogenes lineares Gleichungssystem der Form $A \cdot x = 0$ mit $A \in \mathrm{M}_{m,n}(\mathbb{R})$ gilt:

(a) Es gibt stets die Lösung $x = 0$.

(b) Es ist genau dann eindeutig lösbar, wenn die Spalten der Matrix A linear unabhängig sind.

(c) Sind $u_1, \dots, u_k \in \mathbb{R}^n$ Lösungen, dann ist auch jede Linearkombination $\lambda_1 u_1 + \dots + \lambda_k u_k$ mit $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ eine Lösung.

Korollar 4.4.3 (Lösung eines inhomogenen linearen Gleichungssystems)

Für ein inhomogenes lineares Gleichungssystem der Form $A \cdot x = b$ mit $A \in \mathrm{M}_{m,n}(\mathbb{R})$ und $0 \neq b \in \mathbb{R}^m$ gilt:

(a) Es ist genau dann lösbar, wenn b Linearkombination der Spalten von A ist.

(b) Es ist genau dann eindeutig lösbar, wenn b eindeutige Linearkombination der Spalten von A ist.

(c) Ist v_0 eine fixierte Lösung des inhomogenen Gleichungssystems und u eine beliebige Lösung des zugehörigen homogenen Gleichungssystems $A \cdot x = 0$, dann ist $v_0 + u$ eine weitere Lösung des inhomogenen Systems, und umgekehrt ergibt sich im Falle der Lösbarkeit jede Lösung des inhomogenen Systems auf diese Weise:

$$L_{\text{inhom}} = v_0 + L_{\text{hom}} := \{v_0 + u \mid u \in L_{\text{hom}}\}, \qquad \text{falls } v_0 \in L_{\text{inhom}} \neq \emptyset.$$

Bemerkung 4.4.4 (Verfahren zum Lösen einer Matrixgleichung)

Vorgehensweise zur Bestimmung der Lösungsmenge L der Matrixgleichung $Ax = b$ mit $x \in \mathbb{R}^n$ für $A \in \mathrm{M}_{m,n}(\mathbb{R})$ und $0 \neq b \in \mathbb{R}^m$:

(1) Überführen der erweiterten Koeffizientenmatrix $A|b$ in (reduzierte) Zeilenstufenform.

(2) Lösbarkeit ablesen: Genau dann lösbar, wenn der Rang der Koeffizientenmatrix r mit dem Rang der erweiterten Koeffizientenmatrix übereinstimmt. Ansonsten Algorithmus beenden mit $L = \emptyset$.

(3) Lösungsmenge $L_{\text{hom}} = \{\sum_{i=1}^{s} \lambda_i v_i \mid \lambda_1, \ldots, \lambda_s \in \mathbb{R}\}$ des homogenen Gleichungssystems $Ax = 0$, wobei die $s := n - r$ linear unabhängigen Vektoren $v_1, \ldots, v_s$ wie folgt gewählt werden:

   (i) Freie Variablen jeweils genau eine auf 1, restlichen auf 0 setzen.

   (ii) Gebundene Variablen aus der Zeilenstufenform zu A des homogenen Systems (ohne Verwendung des Vektors b) bestimmen.

   Für $s = 0$ ergibt sich insbesondere die triviale Lösungsmenge $L_{\text{hom}} = \{0\}$.

(4) Spezielle Lösung v_0 des inhomogenen Gleichungssystems $Ax = b$:

   (i) Freie Variablen alle auf 0 setzen.

   (ii) Gebundene Variablen aus der Zeilenstufenform zu $A|b$ des inhomogenen Systems (unter Verwendung des Vektors b) bestimmen.

(5) Lösungsmenge $L = L_{\text{inhom}} = v_0 + L_{\text{hom}}$ des inhomogenen Gleichungssystems als Ergebnis des Algorithmus im Falle der Lösbarkeit: $L = \{v_0 + \sum_{i=1}^{s} \lambda_i v_i \mid \lambda_1, \ldots, \lambda_s \in \mathbb{R}\}$. Für $s = 0$ ergibt sich insbesondere die einelementige Lösungsmenge $L = \{v_0\}$.

Im homogenen Fall $b = 0$ lässt sich der selbe Algorithmus durchführen, es vereinfachen sich hierbei einige Schritte:

(1) Es genügt, die Koeffizientenmatrix A in (reduzierte) Zeilenstufenform zu überführen.

(2) Es gilt stets die Lösbarkeit. (Dieser Punkt kann somit übersprungen werden.)

(3) Bei der Berechnung von L_{hom} vereinfacht sich nichts.

(4) Eine spezielle Lösung von $Ax = b$ ist hier nicht nötig (bzw. es kann stets der triviale Lösungsvektor $v_0 = 0$ gewählt werden). (Dieser Punkt kann somit übersprungen werden.)

(5) Die Lösungsmenge ist $L = L_{\text{hom}} = \{\sum_{i=1}^{s} \lambda_i v_i \mid \lambda_1, \ldots, \lambda_s \in \mathbb{R}\}$. Für $s = 0$ ergibt sich insbesondere die einelementige Lösungsmenge $L = \{0\}$.

5 Vektorräume

5.1 Unterräume

Alle Definitionen und Aussagen in diesem Abschnitt lassen sich statt für den Vektorraum $\mathbb{R}^n$, wobei n stets eine natürliche Zahl darstellt, analog einerseits für beliebige reelle Vektorräume andererseits über beliebige Körper (wie $\mathbb{F}_q$ oder $\mathbb{C}$) formulieren.

Definition 5.1.1 (Unterraum)

Eine Teilmenge U des $\mathbb{R}^n$ heißt ***Unterraum***, wenn gilt

- $0 \in U$,
- $\forall u, u' \in U : u + u' \in U$,
- $\forall \lambda \in \mathbb{R}, u \in U : \lambda u \in U$.

Satz 5.1.2 (Unterraum)

Eine Teilmenge U des $\mathbb{R}^n$ ist genau dann ein Unterraum, wenn U mit den induzierten Operationen ein reeller Vektorraum ist.

Satz und Definition 5.1.3 (Spann, Erzeugendensystem)

Für gegebene Vektoren $u_1, \ldots, u_k \in \mathbb{R}^n$ mit $k \in \mathbb{N}_0$ ist die Menge der Linearkombinationen

$$\operatorname{span}(u_1, \ldots, u_k) := \left\{ \sum_{i=1}^{k} \lambda_i u_i \mid \lambda_1, \ldots, \lambda_k \in \mathbb{R} \right\}$$

ein Unterraum des $\mathbb{R}^n$, der von den Vektoren $u_1, \ldots, u_k$ ***aufgespannte Unterraum***, kurz ***Spann*** oder auch ***lineare Hülle*** von $u_1, \ldots, u_k$ genannt.

Spannen Vektoren $u_1, \ldots, u_k$ einen Unterraum U auf, so nennt man diese Vektoren ein ***Erzeugendensystem*** von U.

Für $k = 0$ ergibt sich der Spann $\{0\}$ aus der leeren Summe.

Lemma 5.1.4

Bilden Vektoren $u_1, \ldots, u_k \in \mathbb{R}^n$ mit $k \in \mathbb{N}$ ein linear abhängiges Erzeugendensystem eines Unterraums $U \subseteq \mathbb{R}^n$, dann kann dieses echt verkleinert werden, ohne den Spann zu ändern. Insbesondere lassen sich aus $u_1, \ldots, u_k$ linear unabhängige Vektoren auswählen, die den selben Spann besitzen.

Lemma 5.1.5

Für ein linear unabhängiges Erzeugendensystem $u_1, \ldots, u_k \in \mathbb{R}^n$ mit $k \in \mathbb{N}_0$ eines Unterraums $U \subseteq \mathbb{R}^n$ und einen Vektor $v \in \mathbb{R}^n$ gilt: Der Vektor v liegt genau dann im Unterraum U, wenn die Vektoren $u_1, \ldots, u_k$ nach Hinzunahme von v linear abhängig werden. Anders formuliert: Die Vektoren $v, u_1, \ldots, u_k$ sind genau dann linear unabhängig, wenn v nicht im Spann der Vektoren $u_1, \ldots, u_k$ liegt.

5.2 Basis und Dimension

Alle Definitionen und Aussagen in diesem Abschnitt lassen sich statt für den Vektorraum $\mathbb{R}^n$, wobei n stets eine natürliche Zahl darstellt, analog einerseits für beliebige endlich-dimensionale reelle Vektorräume andererseits über beliebige Körper (wie $\mathbb{F}_q$ oder $\mathbb{C}$) formulieren.

Definition 5.2.1 (Basis)

Ein linear unabhängiges Erzeugendensystem eines Unterraums nennt man eine ***Basis*** des Unterraums, d. h. Vektoren $b_1, \ldots, b_k \in \mathbb{R}^n$ mit $k \in \mathbb{N}_0$ bilden eine Basis eines Unterraums $U \subseteq \mathbb{R}^n$, wenn gilt:

- $\operatorname{span}(b_1, \ldots, b_k) = U$,
- $b_1, \ldots, b_k$ sind linear unabhängig.

Satz 5.2.2 (Charakterisierung einer Basis)

Vektoren $b_1, \ldots, b_k \in \mathbb{R}^n$ mit $k \in \mathbb{N}_0$ bilden genau dann eine Basis eines Unterraums $U \subseteq \mathbb{R}^n$, wenn sich jeder Vektor $u \in U$ aus diesen ***eindeutig linear kombinieren*** lässt, d. h. die Gleichung $u = \lambda_1 b_1 + \cdots + \lambda_k b_k$ stets eine eindeutige Lösung mit $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ besitzt.

Bemerkung 5.2.3

Bei einer Basis eines Unterraums $U \subseteq \mathbb{R}^n$ handelt es sich um ein

(a) ***minimales Erzeugendensystem*** von U, d. h. die Vektoren spannen den Unterraum U auf und es darf keiner der Vektoren weggelassen werden (sonst spannen diese nicht mehr ganz U auf),

(b) ***maximal linear unabhängiges System*** von Vektoren aus U, d. h. die Vektoren sind linear unabhängig und es darf kein weiterer Vektor aus U hinzugefügt werden (sonst sind diese Vektoren nicht mehr linear unabhängig).

Lemma 5.2.4

Ist $b_1, \ldots, b_k$ mit $k \in \mathbb{N}_0$ eine Basis eines Unterraums $U \subseteq \mathbb{R}^n$, dann sind mehr als k Vektoren aus U stets linear abhängig. Anders formuliert: Dann sind höchstens k Vektoren aus U linear unabhängig, d. h. für m lineare unabhängige Vektoren $u_1, \ldots, u_m \in U$ mit $m \in \mathbb{N}_0$ folgt stets $m \leq k$.

Satz und Definition 5.2.5 (Dimension)

Für einen Unterraums $U \subseteq \mathbb{R}^n$ ist die Anzahl der Elemente einer Basis stets gleich. Diese Anzahl heißt ***Dimension*** des Unterraums, notiert als

$$\dim(U) \in \mathbb{N}_0.$$

Satz 5.2.6

Für einen Unterraum $U \subseteq \mathbb{R}^n$ der Dimension d gilt:

(a) Mehr als d Vektoren des Unterraums U sind stets linear abhängig.

(b) Weniger als d Vektoren erzeugen nie den Unterraum U.

Korollar 5.2.7

Für den Vektorraum $\mathbb{R}^n$ gilt:

(a) Die Dimension ist $\dim(\mathbb{R}^n) = n$.

(b) Mehr als n Vektoren im $\mathbb{R}^n$ sind stets linear abhängig.

(c) Weniger als n Vektoren im $\mathbb{R}^n$ erzeugen nie den $\mathbb{R}^n$.

Satz 5.2.8 (Existenz einer Basis)

Jeder Unterraum U des $\mathbb{R}^n$ besitzt eine Basis, wobei die Anzahl der Basisvektoren $\dim(U)$ aus $\{0, 1, \dots, n\}$ ist.

Satz 5.2.9 (Dimensionen von Unterräumen)

Für zwei Unterräume $U \subseteq W$ des $\mathbb{R}^n$ gilt stets $\dim(U) \leq \dim(W)$. Gleichheit der Dimension gilt hierbei genau dann, wenn $U = W$.

Korollar 5.2.10

(a) Jeweils n linear unabhängige Vektoren des $\mathbb{R}^n$ erzeugen stets den $\mathbb{R}^n$.

(b) Erzeugen n Vektoren den $\mathbb{R}^n$, dann sind sie auch linear unabhängig.

In beiden Fällen liegt dann sogar eine Basis des $\mathbb{R}^n$ vor.

Bemerkung 5.2.11 (Lineare Gleichungssysteme)

Für die Lösungsmengen linearer Gleichungssysteme ergibt sich:

(a) Die Lösungsmenge L_{hom} eines homogenen linearen Gleichungssystems mit n Unbekannten ist stets ein Unterraum des $\mathbb{R}^n$.

Die Dimension ist $\dim(L_{\text{hom}}) = s := n - r$, die Anzahl der freien Variablen, wobei r den Rang der Koeffizientenmatrix darstellt.

Die s Vektoren $v_1, \dots, v_s$ aus Bemerkung 4.4.4 bilden stets eine Basis des Lösungsraums L_{hom}.

(b) Die Lösungsmenge L_{inhom} eines inhomogenen linearen Gleichungssystems ist niemals ein Unterraum, sondern entweder leer, $L_{\text{inhom}} = \emptyset$, oder ein verschobener Unterraum (man sagt auch affiner Unterraum), nämlich der um einen beliebigen Lösungsvektor v_0 des inhomogenen Gleichungssystems verschobene Unterraum der Lösungen des zugehörigen homogenen Gleichungssystems, $L_{\text{inhom}} = v_0 + L_{\text{hom}}$, wobei $v_0 \neq 0$.

5.3 Norm

Der Begriff der Norm lässt sich nicht nur im $\mathbb{R}^n$, wobei n stets eine natürliche Zahl darstellt, sondern auch allgemeiner in reellen oder komplexen Vektorräumen (d. h. Vektorräumen über $\mathbb{C}$) betrachten.

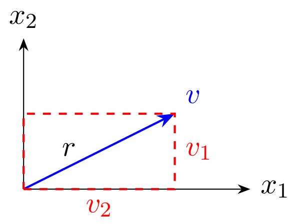
DEFINITION 5.3.1 (Norm, Betrag, Länge)

Für einen Vektor $v = (v_i) \in \mathbb{R}^n$ nennt man

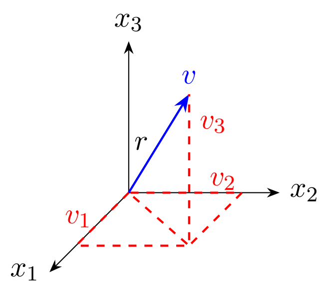
$$\|v\| := \sqrt{\sum_{i=1}^{n} v_i^2}$$

die ***Norm***, den ***Betrag*** oder die ***Länge*** des Vektors.

Vektoren mit Länge 1 nennt man ***normiert*** oder ***Einheitsvektoren***.



Norm $r = \|v\|$ im $\mathbb{R}^2$



Norm $r = \|v\|$ im $\mathbb{R}^3$

BEMERKUNG 5.3.2 (Kanonische Einheitsvektoren)

Die normierten Vektoren

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \; e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \; \ldots, \; e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in \mathbb{R}^n,$$

wobei e_i genau an der i-ten Stelle den Eintrag 1 und ansonsten den Eintrag 0 besitzt, stellen die ***kanonischen Einheitsvektoren*** dar und bilden die sog. ***kanonische Basis*** des $\mathbb{R}^n$.

SATZ 5.3.3 (Rechengesetze der Norm)

Die Norm von Vektoren aus $\mathbb{R}^n$ liefert eine Abbildung

$$\|\cdot\| : \mathbb{R}^n \longrightarrow \mathbb{R} \qquad\qquad v \longmapsto \|v\|$$

mit folgenden Eigenschaften:

Positiv definit $\forall v \in \mathbb{R}^n$: $\|v\| \geq 0$, wobei $\|v\| = 0$ genau für $v = 0$.

Homogen $\forall \lambda \in \mathbb{R}, v \in \mathbb{R}^n$: $\|\lambda v\| = |\lambda| \, \|v\|$.

Dreiecksungleichung $\forall v, w \in \mathbb{R}^n$: $\|v + w\| \leq \|v\| + \|w\|$.

Bemerkung 5.3.4 (Abstand, Metrik)

Jede Norm $\|\cdot\|$ auf dem $\mathbb{R}^n$ induziert durch

$$d\colon \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R} \qquad\qquad (v, w) \longmapsto d(v, w) := \|v - w\|$$

einen ***Abstand*** oder eine ***Metrik*** mit folgenden Eigenschaften:

Positiv definit $\forall v, w \in \mathbb{R}^n\colon d(v, w) \geq 0$, wobei $d(v, w) = 0$ genau für $v = w$.

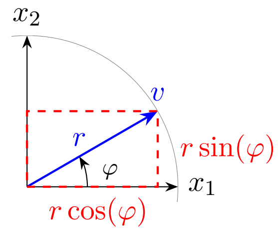
Symmetrisch $\forall v, w \in \mathbb{R}^n\colon d(v, w) = d(w, v)$.

Dreiecksungleichung $\forall u, v, w \in \mathbb{R}^n\colon d(u, w) \leq d(u, v) + d(v, w)$.

Satz und Definition 5.3.5 (Polardarstellung)

Jeder Vektor v im $\mathbb{R}^2$ besitzt neben der ***kartesischen Darstellung*** $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ auch eine ***Polardarstellung*** (r, φ), die repräsentativ für

$$v = \begin{pmatrix} r\cos(\varphi) \\ r\sin(\varphi) \end{pmatrix}$$



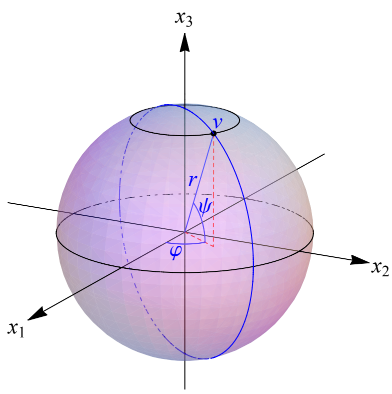
steht. Hierbei ist $r = \|v\| \geq 0$ die Länge des Vektors und $\varphi \in \mathbb{R}$ der Winkel zwischen v und der x_1-Achse.

Wählt man den Winkel φ für $v \neq 0$ beispielsweise nur aus dem Bereich $0 \leq \varphi < 2\pi$ oder nur aus $-\pi < \varphi \leq \pi$ und für $v = 0$ nur $\varphi = 0$, dann ist die Polardarstellung eindeutig.

Bemerkung 5.3.6

Analog zur Polardarstellung im $\mathbb{R}^2$ lässt sich jeder Vektor $v \in \mathbb{R}^3$ der Länge $r = \|v\| \geq 0$ in der Form

$$v = \begin{pmatrix} r\cos(\varphi)\cos(\psi) \\ r\sin(\varphi)\cos(\psi) \\ r\sin(\psi) \end{pmatrix}$$



mit den Winkeln $\psi \in \mathbb{R}$ zwischen v und der x_1-x_2-Ebene und $\varphi \in \mathbb{R}$ zwischen v und der Projektion von v auf die x_1-x_2-Ebene darstellen.

Wählt man $0 \leq \varphi < 2\pi$ und $-\frac{\pi}{2} \leq \psi \leq \frac{\pi}{2}$, so ist die Darstellung eindeutig, wenn man im Fall $\psi = \pm\frac{\pi}{2}$ (Nord- und Südpol) nur den Winkel $\varphi = 0$ zulässt.

5.4 Skalarprodukt

Der Begriff des Skalarprodukts lässt sich nicht nur im $\mathbb{R}^n$, wobei n stets eine natürliche Zahl darstellt, sondern auch allgemeiner in reellen oder komplexen Vektorräumen betrachten, wobei im Komplexen wesentliche Modifikationen nötig sind.

Definition 5.4.1 (Skalarprodukt)

Für zwei Vektoren $v = (v_i), w = (w_i) \in \mathbb{R}^n$ nennt man

$$\langle v\,, w\rangle := \sum_{i=1}^{n} v_i w_i$$

das ***Skalarprodukt*** der beiden Vektoren.

Bemerkung 5.4.2

(a) Für Vektoren $v \in \mathbb{R}^n$ gilt folgender Zusammenhang zwischen Skalarprodukt und Norm:

$$\langle v\,, v\rangle = \|v\|^2 \qquad \text{bzw.} \qquad \|v\| = \sqrt{\langle v\,, v\rangle}.$$

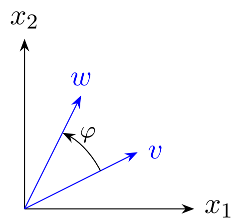
(b) Betrachtet man den zu $v \in \mathbb{R}^n$ ***transponierten Zeilenvektor*** $v^\top := \begin{pmatrix} v_1 & \dots & v_n \end{pmatrix}$, der durch Überführen von der Spaltendarstellung in die Zeilendarstellung entsteht, so ergibt sich das Skalarprodukt mit einem Spaltenvektor $w \in \mathbb{R}^n$ aus der Matrixmultiplikation:

$$\langle v\,, w\rangle = v^\top \cdot w = \begin{pmatrix} v_1 & \dots & v_n \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}.$$

Satz 5.4.3 (Zwischenwinkel)

Im $\mathbb{R}^2$ bzw. $\mathbb{R}^3$ gilt für den Zwischenwinkel φ zweier Vektoren v und w die Beziehung

$$\langle v\,, w\rangle = \|v\|\,\|w\|\cos(\varphi).$$



Satz 5.4.4 (Rechengesetze des Skalarprodukts)

Das Skalarprodukt von Vektoren aus $\mathbb{R}^n$ liefert eine Abbildung

$$\langle\cdot\,,\cdot\rangle\colon \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R} \qquad (v, w) \longmapsto \langle v\,, w\rangle$$

mit folgenden Eigenschaften:

Positiv definit $\forall v \in \mathbb{R}^n : \langle v\,, v\rangle \geq 0$, wobei $\langle v\,, v\rangle = 0$ genau für $v = 0$.

Symmetrisch $\forall v, w \in \mathbb{R}^n : \langle w\,, v\rangle = \langle v\,, w\rangle$.

Linear im 1. Argument $\forall v, v', w \in \mathbb{R}^n : \langle v + v' , w\rangle = \langle v , w\rangle + \langle v' , w\rangle$ und $\forall \lambda \in \mathbb{R}$, $v, w \in \mathbb{R}^n : \langle \lambda v , w\rangle = \lambda\langle v , w\rangle$.

Korollar 5.4.5

Das Skalarprodukt von Vektoren aus $\mathbb{R}^n$ genügt weiteren Rechenregeln:

Linearität im 2. Argument $\forall v, v', w \in \mathbb{R}^n : \langle v , w + w'\rangle = \langle v , w\rangle + \langle v , w'\rangle$ und $\forall \lambda \in \mathbb{R}, v, w \in \mathbb{R}^n : \langle v , \lambda w\rangle = \lambda\langle v , w\rangle$.

Bilinear $\forall \lambda, \lambda', \mu, \mu' \in \mathbb{R},\ v, v', w, w' \in \mathbb{R}^n : \langle \lambda v + \lambda' v' , \mu w + \mu' w'\rangle = \lambda\mu\langle v , w\rangle + \lambda\mu'\langle v , w'\rangle + \lambda'\mu\langle v' , w\rangle + \lambda'\mu'\langle v' , w'\rangle$.

Summenformel $\forall \lambda_i, \mu_j \in \mathbb{R}$ und $v_i, w_j \in \mathbb{R}^n$ für $i = 1, \ldots, k,\ j = 1, \ldots, m$: $\langle \sum\limits_{i=1}^{k} \lambda_i v_i , \sum\limits_{j=1}^{m} \mu_j w_j\rangle = \sum\limits_{i=1}^{k} \sum\limits_{j=1}^{m} \lambda_i \mu_j \langle v_i , w_j\rangle$.

Definition 5.4.6 (Orthogonal)

Zwei Vektoren v, w im $\mathbb{R}^n$ heißen ***orthogonal***, wenn

$$\langle v , w\rangle = 0.$$

Im $\mathbb{R}^2$ und $\mathbb{R}^3$ sagt man im Fall $v \neq 0 \neq w$ auch, v und w ***stehen aufeinander senkrecht***.

Definition 5.4.7 (Orthogonal-, Orthonormalsystem und -basis)

Vektoren $v_1, \ldots, v_k \in U$ mit $k \in \mathbb{N}_0$ eines Unterraums $U \subseteq \mathbb{R}^n$ nennt man:

Orthogonalsystem, wenn die Vektoren alle von 0 verschieden und paarweise orthogonal sind, d. h.

$$\forall i : v_i \neq 0 \qquad \text{und} \qquad \forall i \neq j : \langle v_i , v_j\rangle = 0.$$

Orthonormalsystem, wenn die Vektoren alle normiert und paarweise orthogonal sind, d. h.

$$\forall i : \|v_i\| = 1 \qquad \text{und} \qquad \forall i \neq j : \langle v_i , v_j\rangle = 0.$$

Orthogonalbasis von U, wenn die Vektoren ein Orthogonalsystem bilden, welches darüber hinaus eine Basis von U darstellt.

Orthonormalbasis von U, wenn die Vektoren ein Orthonormalsystem bilden, welches darüber hinaus eine Basis von U darstellt.

Satz 5.4.8 (Lineare Unabhängigkeit eines Orthogonalsystems)

Die Vektoren eines Orthogonalsystems bzw. eines Orthonormalsystems im $\mathbb{R}^n$ sind stets linear unabhängig.

Satz 5.4.9 (Linearkombination aus Orthogonal- oder Orthonormalbasis)

Ein Vektor u eines Unterraums $U \subseteq \mathbb{R}^n$ der Dimension $d \in \{0, \ldots, n\}$ lässt sich aus den Vektoren $b_1, \ldots, b_d$ einer Basis von U durch

$$u = \sum_{i=1}^{d} \lambda_i b_i$$

eindeutig linear kombinieren, wobei sich die Koeffizienten λ_i für $i = 1, \ldots, d$ wie folgt ergeben:

- im allgemeinen Fall einer beliebigen Basis durch Lösen eines inhomogenen linearen Gleichungssystems mit d Unbekannten und n Gleichungen (vom Rang d),
- im Fall einer Orthogonalbasis aus $\lambda_i = \dfrac{\langle u\, , b_i\rangle}{\langle b_i\, , b_i\rangle} = \dfrac{\langle u\, , b_i\rangle}{\|b_i\|^2}$,
- im Fall einer Orthonormalbasis aus $\lambda_i = \langle u\, , b_i\rangle$.

Satz 5.4.10 (Orthogonale Projektion)

Bilden Vektoren $b_1, \ldots, b_d$ mit $d \in \{0, \ldots, n\}$ eine Orthogonal- bzw. Orthonormalbasis eines Unterraums $U \subseteq \mathbb{R}^n$, so stellt für einen beliebigen Vektor $v \in \mathbb{R}^n$ der Vektor

$$u := \sum_{i=1}^{d} \lambda_i b_i \qquad \text{mit} \qquad \lambda_i = \frac{\langle v\, , b_i\rangle}{\langle b_i\, , b_i\rangle} = \frac{\langle v\, , b_i\rangle}{\|b_i\|^2} \quad \text{bzw.} \quad \lambda_i = \langle v\, , b_i\rangle$$

die ***orthogonale Projektion*** von v auf den Unterraum U dar, woraus sich durch die Differenz $w := v - u$ eine Zerlegung in zwei zueinander orthogonale Komponenten ergibt:

$$v = u + w \qquad \text{mit} \qquad u \in U \quad \text{und} \quad \langle u\, , w\rangle = 0.$$

Satz 5.4.11 (Schmidtsches Orthogonalisierungsverfahren)

Liegt eine Basis $u_1, \ldots, u_d$ eines Unterraums $U \subseteq \mathbb{R}^n$ der Dimension $d \in \{0, \ldots, n\}$ vor, dann lässt sich hieraus eine Orthogonalbasis von U konstruieren:

(1) Setze $i := 0$.

(2) Falls $i = d$, beende Algorithmus.

(3) Ansonsten setze $b_{i+1} := u_{i+1} - \displaystyle\sum_{j=1}^{i} \frac{\langle u_{i+1}\, , b_j\rangle}{\|b_j\|^2} b_j$.

(4) Erhöhe i um 1 und gehe zu (2).

Das Verfahren endet nach genau d Durchläufen mit einer Orthogonalbasis aus den d Vektoren $b_1, \ldots, b_d$.

Eine Orthonormalbasis ergibt sich durch Normieren der Orthogonalbasis:

(5) Setze $b_i^{(0)} := \dfrac{1}{\|b_i\|} b_i$ für $i = 1, \ldots, d$.

Dann bildet $b_1^{(0)}, \ldots, b_d^{(0)}$ eine Orthonormalbasis von U.

6 Lineare Abbildungen

Alle Definitionen und Aussagen in diesem Kapitel lassen sich statt über den reellen Zahlen $\mathbb{R}$ analog über beliebige Körper (wie $\mathbb{F}_q$ oder $\mathbb{C}$) formulieren.

Ferner seien alle auftretenden Größen m, n und k natürliche Zahlen.

6.1 Lineare Abbildung und Abbildungsmatrix

Definition 6.1.1 (Lineare Abbildung)

Eine Abbildung

$$f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m, \qquad x \longmapsto f(x),$$

heißt ***linear***, wenn gilt

- $\forall x, x' \in \mathbb{R}^n : f(x + x') = f(x) + f(x')$,
- $\forall \lambda \in \mathbb{R}, x \in \mathbb{R}^n : f(\lambda x) = \lambda f(x)$.

Satz und Definition 6.1.2 (Lineare Abbildung)

Lineare Abbildungen und Matrixmultiplikation entsprechen sich:

- Eine Matrix $A \in \mathrm{M}_{m,n}(\mathbb{R})$ induziert stets eine lineare Abbildung

$$f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m, \qquad x \longmapsto f(x) := Ax.$$

- Umgekehrt existiert für jede lineare Abbildung

$$f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m, \qquad x \longmapsto f(x),$$

  eine zugehörige und durch f eindeutig bestimmte ***Abbildungsmatrix*** $A \in \mathrm{M}_{m,n}(\mathbb{R})$, so dass $f(x) = Ax$ für alle $x \in \mathbb{R}^n$ gilt.

Insbesondere stehen in den Spalten $a_1, \ldots, a_n$ der Abbildungsmatrix $A \in \mathrm{M}_{m,n}(\mathbb{R})$ die Bildvektoren $f(e_1), \ldots, f(e_n) \in \mathbb{R}^m$ der kanonischen Basisvektoren $e_1, \ldots, e_n \in \mathbb{R}^n$.

Satz 6.1.3 (Drehung, Spiegelung, Projektion)

(a) Die ***Drehung*** $d_\varphi \colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ um den Nullpunkt mit Drehwinkel $\varphi \in \mathbb{R}$ stellt eine lineare Abbildung dar. Die zugehörige Abbildungsmatrix ist die ***Drehmatrix***

$$D_\varphi = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \in \mathrm{M}_2(\mathbb{R}).$$

(b) Die ***Spiegelung*** $s_\psi \colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ an der Geraden, die mit der x_1-Achse den Winkel $\frac{\psi}{2} \in \mathbb{R}$ einschließt, stellt eine lineare Abbildung dar. Die zugehörige Abbildungsmatrix ist die ***Spiegelungsmatrix***

$$S_\varphi = \begin{pmatrix} \cos(\psi) & \sin(\psi) \\ \sin(\psi) & -\cos(\psi) \end{pmatrix} \in \mathrm{M}_2(\mathbb{R}).$$

(c) Die ***Projektion*** $p_b \colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ auf die durch den Vektor $b \neq 0$ des $\mathbb{R}^2$ aufgespannte Gerade stellt eine lineare Abbildung dar. Die zugehörige Abbildungsmatrix ist die ***Projektionsmatrix***

$$P_b = \frac{1}{b_1^2 + b_2^2} \begin{pmatrix} b_1 b_1 & b_1 b_2 \\ b_2 b_1 & b_2 b_2 \end{pmatrix} \in \mathrm{M}_2(\mathbb{R}) \qquad \text{für } b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}.$$

6.2 Bild und Kern

Satz und Definition 6.2.1 (Bild, Urbild, Kern, Faser)

Für eine lineare Abbildung $f \colon \mathbb{R}^n \longrightarrow \mathbb{R}^m$ mit zugehöriger Abbildungsmatrix $A \in \mathrm{M}_{m,n}(\mathbb{R})$ gilt:

- Es ist stets $f(0) = 0$.
- Das ***Bild***

  $$\mathrm{Bild}(f) := f(\mathbb{R}^n) := \{y \in \mathbb{R}^m \mid \exists x \in \mathbb{R}^n : y = f(x)\} = \{f(x) \mid x \in \mathbb{R}^n\}$$

  ist ein Unterraum des $\mathbb{R}^m$, der von den Spalten der Abbildungsmatrix A aufgespannt wird.
- Das ***Urbild*** des Nullvektors, der sog. ***Kern***

  $$\mathrm{Kern}(f) := f^{-1}(\{0\}) := \{x \in \mathbb{R}^n \mid f(x) = 0\},$$

  ist ein Unterraum des $\mathbb{R}^n$, nämlich der Lösungsraum des homogenen linearen Gleichungssystems $Ax = 0$.
- Das ***Urbild*** eines beliebigen Vektors $b \in \mathbb{R}^m$ ist leer oder, falls mindestens ein Urbild $x_0 \in \mathbb{R}^n$ existiert, die sog. ***Faser***

  $$f^{-1}(\{b\}) := \{x \in \mathbb{R}^n \mid f(x) = b\} = x_0 + \mathrm{Kern}(f),$$

  ein verschobener (sog. affiner) Unterraum des $\mathbb{R}^n$, nämlich die Lösungsmenge des inhomogenen linearen Gleichungssystems $Ax = b$.

Korollar 6.2.2 (Injektiv, surjektiv, bijektiv)

Eine lineare Abbildung $f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m$ mit Abbildungsmatrix $A \in \mathrm{M}_{m,n}(\mathbb{R})$ ist

injektiv, wenn $\mathrm{Kern}(f) = \{0\}$ bzw. die Spalten von A linear unabhängig sind. Insbesondere muss dann $n \leq m$ sein.

surjektiv, wenn $\mathrm{Bild}(f) = \mathbb{R}^m$ bzw. die Spalten von A den $\mathbb{R}^m$ aufspannen. Insbesondere muss dann $n \geq m$ sein.

bijektiv, wenn die Spalten von A eine Basis des $\mathbb{R}^m$ darstellen. Insbesondere muss dann $n = m$, also A eine quadratische Matrix sein.

6.3 Komposition von linearen Abbildungen

Definition und Satz 6.3.1 (Komposition)

Sind

$$g\colon \mathbb{R}^n \longrightarrow \mathbb{R}^k \qquad \text{und} \qquad f\colon \mathbb{R}^k \longrightarrow \mathbb{R}^m$$

zwei Abbildungen, so stellt die ***Komposition*** (oder ***Verknüpfung*** oder ***Hintereinanderschaltung***) eine Abbildung

$$f \circ g\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m, \qquad (f \circ g)(x) := f(g(x)),$$

dar.

- Sind f und g linear, dann ist auch $f \circ g$ linear.
- Sind $A \in \mathrm{M}_{m,k}(\mathbb{R})$ und $B \in \mathrm{M}_{k,n}(\mathbb{R})$ die zu f bzw. g gehörigen Abbildungsmatrizen, dann gehört zu $f \circ g$ die Abbildungsmatrix $A \cdot B \in \mathrm{M}_{m,n}(\mathbb{R})$.

Definition und Satz 6.3.2 (Umkehrabbildung)

Eine Abbildung $f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m$ heißt ***umkehrbar***, wenn eine Abbildung $f^{-1}\colon \mathbb{R}^m \longrightarrow \mathbb{R}^n$, die sog. ***Umkehrabbildung***, mit $f \circ f^{-1} = \mathrm{id}$ und $f^{-1} \circ f = \mathrm{id}$ existiert, wobei id die ***Identität*** $x \mapsto x$ bezeichnet.

- Die Abbildung f ist genau dann umkehrbar, wenn sie bijektiv ist. In diesem Fall ist auch f^{-1} umkehrbar mit $(f^{-1})^{-1} = f$.
- Ist eine umkehrbare Abbildung f linear, dann ist auch f^{-1} linear. Ferner muss $n = m$ gelten.
- Ist $A \in \mathrm{M}_n(\mathbb{R})$ die Abbildungsmatrix einer umkehrbaren linearen Abbildung f, dann besitzt die Umkehrabbildung f^{-1} die Abbildungsmatrix A^{-1}. Hierbei ist A^{-1} die ***inverse Matrix*** zu A, d. h. die Matrix mit $AA^{-1} = E$ und $A^{-1}A = E$, wobei $E \in \mathrm{M}_n(\mathbb{R})$ die Einheitsmatrix bezeichnet.

Satz 6.3.3 (Basiswechsel)

Wird ein Vektor $v = v_1e_1 + \cdots + v_ne_n$ des $\mathbb{R}^n$ bezüglich der kanonischen Basis $e_1, \ldots, e_n$ durch den Spaltenvektor $v_{\text{kan}} = (v_i)$ beschrieben, so ergeben sich die Koordinaten $v_{\text{neu}} = (v'_i)$ bezüglich einer neuen Basis $b_1, \ldots, b_n$, d. h. die Koeffizienten von $v = v'_1b_1 + \cdots + v'_nb_n$, unter Verwendung der invertierbaren Matrix $B \in \mathrm{M}_n(\mathbb{R})$, in deren Spalten die neuen Basisvektoren bezüglich der kanonischen Basis stehen und die den ***Basiswechsel*** beschreibt:

$$v_{\text{kan}} = B \cdot v_{\text{neu}} \qquad \text{bzw.} \qquad v_{\text{neu}} = B^{-1} \cdot v_{\text{kan}} \qquad \text{mit} \qquad B = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix}.$$

Korollar 6.3.4 (Basiswechsel bei einer linearen Abbildung)

Eine lineare Abbildung $f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m$ werde bezüglich der kanonischen Basen durch die Abbildungsmatrix $A \in \mathrm{M}_{m,n}(\mathbb{R})$ beschrieben.

Geht man im $\mathbb{R}^n$ durch eine Matrix $B = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix} \in \mathrm{M}_n(\mathbb{R})$ und im $\mathbb{R}^m$ durch eine Matrix $C = \begin{pmatrix} c_1 & \cdots & c_m \end{pmatrix} \in \mathrm{M}_m(\mathbb{R})$ auf neue Basen über, so wird f bezüglich dieser Basen durch eine Abbildungsmatrix $A' \in \mathrm{M}_{m,n}(\mathbb{R})$ beschrieben, die sich aus dem ***Basiswechsel für lineare Abbildungen*** ergibt:

$$A' = C^{-1} \cdot A \cdot B.$$

$$\begin{tikzcd}
\text{Basis } e_1, \ldots, e_n & \mathbb{R}^n \arrow[r, "A"] & \mathbb{R}^m \arrow[d, "C^{-1}"] & \text{Basis } e_1, \ldots, e_m \\
\text{Basis } b_1, \ldots, b_n & \mathbb{R}^n \arrow[u, "B"] \arrow[r, "A'"] & \mathbb{R}^m & \text{Basis } c_1, \ldots, c_m
\end{tikzcd}$$

7 Quadratische Matrizen

7.1 Inverse Matrix

Alle Definitionen und Aussagen in diesem Abschnitt lassen sich statt über den reellen Zahlen $\mathbb{R}$ analog über beliebige Körper (wie $\mathbb{F}_q$ oder $\mathbb{C}$) formulieren.

Ferner sei die auftretende Größe n eine natürliche Zahl.

Satz 7.1.1 (Inverse Matrix)

Für eine Matrix $A \in \mathrm{M}_n(\mathbb{R})$ sind äquivalent:

(i) Die Matrix A ist invertierbar.

(ii) Die Spalten von A bilden eine Basis des $\mathbb{R}^n$.

(iii) Die Spalten von A sind linear unabhängig.

(iv) Die Spalten von A spannen den $\mathbb{R}^n$ auf.

(v) Der Rang der Matrix A ist n.

(vi) Die reduzierte Zeilenstufenform der Matrix A ist die Einheitsmatrix $E \in \mathrm{M}_n(\mathbb{R})$.

Im Fall der Invertierbarkeit ergibt sich die Inverse $A^{-1} \in \mathrm{M}_n(\mathbb{R})$ durch Überführen der ***erweiterten Koeffizientenmatrix*** $A \mid E$ in reduzierte Zeilenstufenform $E \mid X$ gemäß dem Gaußschen Eliminationsverfahren. Es gilt dann $X = A^{-1}$.

Ergibt die Umformung $A \mid E$ in reduzierte Zeilenstufenform auf der linken Seite keine Einheitsmatrix $E \mid X$, dann ist A auch nicht invertierbar.

Korollar 7.1.2

Eine quadratische Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$ ist genau dann invertierbar, wenn für die reelle Zahl $\Delta := ad - bc \neq 0$ gilt. In diesem Fall gilt für die inverse Matrix

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

7.2 Determinanten

Alle Definitionen und Aussagen in diesem Abschnitt lassen sich statt über den reellen Zahlen $\mathbb{R}$ analog über beliebige Körper (wie $\mathbb{F}_q$ oder $\mathbb{C}$) formulieren.

Ferner sei die auftretende Größe n eine natürliche Zahl.

Definition und Satz 7.2.1 (Permutationen)

Eine bijektive Abbildung $\pi\colon \{1,2,\dots,n\} \longrightarrow \{1,2,\dots,n\}$ für ein gegebenes $n \in \mathbb{N}$ heißt ***Permutation*** der Elemente $1,2,\dots,n$. Man notiert sie in der Form

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

Eine Permutation, die genau zwei Elemente vertauscht und die übrigen fest lässt, nennt man ***Transposition***.

Die Menge S_n aller Permutationen der Elemente $1,2,\dots,n$ versehen mit der Komposition

$$\circ\colon S_n \times S_n \longrightarrow S_n, \qquad (\pi,\sigma) \longmapsto \pi\circ\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(\sigma(1)) & \pi(\sigma(2)) & \dots & \pi(\sigma(n)) \end{pmatrix},$$

stellt eine Gruppe, die sog. ***symmetrische Gruppe***, mit $n!$ Elementen dar:

Assoziativität $\forall \pi,\sigma,\tau \in S_n : (\pi\circ\sigma)\circ\tau = \pi\circ(\sigma\circ\tau)$.

Neutrales Element (Identität) $\exists\, \mathrm{id} \in S_n : \forall \pi \in S_n : \pi \circ \mathrm{id} = \pi = \mathrm{id}\circ\pi$.

Inverse Elemente (Inverse) $\forall \pi \in S_n : \exists \pi^{-1} \in S_n : \pi\circ\pi^{-1} = \mathrm{id} = \pi^{-1}\circ\pi$.

Die Kommutativität $\pi\circ\sigma = \sigma\circ\pi$ gilt für $n \le 2$ stets, aber für $n \ge 3$ i. a. nicht.

Definition 7.2.2 (Vorzeichen)

Eine Permutation heißt ***gerade***, wenn sie sich als Komposition einer geraden Anzahl von Transpositionen darstellen lässt, ansonsten heißt sie ***ungerade***.

Das ***Vorzeichen*** (***Signum***) einer Permutation ist definiert durch

$$\mathrm{sgn}\colon S_n \longrightarrow \{-1,+1\}, \qquad \pi \longmapsto \mathrm{sgn}(\pi) := \begin{cases} +1, & \text{falls } \pi \text{ gerade}, \\ -1, & \text{falls } \pi \text{ ungerade}. \end{cases}$$

Satz und Definition 7.2.3 (Normierte alternierende Multilinearform)

Die ***Determinante***

$$\det\colon \mathrm{M}_n(\mathbb{R}) \longrightarrow \mathbb{R}, \qquad A \longmapsto \det(A),$$

ist die eindeutig bestimmte ***normierte alternierende Multilinearform***:

multilinear det ist linear in jeder Zeile, d. h.

$$\det\left(\begin{pmatrix} a^1 \\ \vdots \\ \lambda a^i + \mu b^i \\ \vdots \\ a^n \end{pmatrix}\right) = \lambda \det\left(\begin{pmatrix} a^1 \\ \vdots \\ a^i \\ \vdots \\ a^n \end{pmatrix}\right) + \mu \det\left(\begin{pmatrix} a^1 \\ \vdots \\ b^i \\ \vdots \\ a^n \end{pmatrix}\right).$$

alternierend det verschwindet, falls zwei gleiche Zeilen vorkommen, d. h.

$$\det(\begin{pmatrix} \vdots \\ a^i \\ \vdots \\ a^i \\ \vdots \end{pmatrix}) = 0.$$

normiert det liefert für die Einheitsmatrix

$$\det(E) = 1.$$

Korollar 7.2.4 (Leibnizsche Darstellung)

Die eindeutig definierte Determinante

$$\det\colon \mathrm{M}_n(\mathbb{R}) \longrightarrow \mathbb{R}, \qquad A \longmapsto \det(A),$$

besitzt die ***Leibnizsche Darstellung***

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{k=1}^{n} a_{k,\pi(k)}.$$

Insbesondere gilt

$$\det(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bc, \qquad \begin{array}{cc} a & b \\ c & d \end{array}$$

$$\det(\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}) = aei + bfg + cdh - ceg - afh - bdi. \qquad \begin{array}{ccccc} a & b & c & a & b \\ d & e & f & d & e \\ g & h & i & g & h \end{array}$$

Regel von Sarrus

Satz 7.2.5 (Laplacescher Entwicklungssatz)

Für eine Matrix $A \in \mathrm{M}_n(\mathbb{R})$ bezeichne $A_{i,j}$ die Matrix, die nach Streichen der i-ten Zeile und j-ten Spalte entsteht. Dann gilt die ***Laplacesche Entwicklung*** nach der

ersten Zeile $\det(A) = a_{1,1}\det(A_{1,1}) - a_{1,2}\det(A_{1,2}) + \cdots + (-1)^{n+1} a_{1,n}\det(A_{1,n}),$

ersten Spalte $\det(A) = a_{1,1}\det(A_{1,1}) - a_{2,1}\det(A_{2,1}) + \cdots + (-1)^{n+1} a_{n,1}\det(A_{n,1}),$

i-ten Zeile $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j}\det(A_{i,j}),$

j-ten Spalte $\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j}\det(A_{i.j}).$

Als Merkregel für die Vorzeichen dient das Schema $\begin{pmatrix} + & - & + & \dots \\ - & + & - & \dots \\ + & - & + & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$

Satz 7.2.6 (Gaußsches Eliminationsverfahren für Determinanten)

Die Determinante einer Matrix $A \in \mathrm{M}_n(\mathbb{R})$ ändert sich bei elementaren Zeilenumformungen in eine Matrix A' wie folgt:

Typ A Addition des λ-fachen einer Zeile zu einer anderen Zeile, wobei $\lambda \in \mathbb{R}$ beliebig: Determinante bleibt gleich,

$$\det(A') = \det(A).$$

Typ B Vertauschen zweier Zeilen: Determinante ändert ihr Vorzeichen,

$$\det(A') = -\det(A).$$

Typ C Multiplikation einer Zeile mit $\lambda \in \mathbb{R}$, wobei $\lambda \neq 0$: Determinante ändert sich um den Faktor λ,

$$\det(A') = \lambda \det(A).$$

Führt man A durch beliebige Umformungen vom Typ A, durch s Umformungen vom Typ B und t Umformungen vom Typ C mit Faktoren $\lambda_1, \ldots, \lambda_t \neq 0$ in Zeilenstufenform $B = (b_{i,j})$ über, dann gilt

$$\det(A) = (-1)^s \cdot \prod_{k=1}^{t} \frac{1}{\lambda_k} \cdot \det(B) = (-1)^s \cdot \prod_{k=1}^{t} \frac{1}{\lambda_k} \cdot \prod_{i=1}^{n} b_{i,i}.$$

Hat man A sogar in reduzierte Zeilenstufenform übergeführt, dann gilt

$$\det(A) = \begin{cases} (-1)^s \prod_{k=1}^{t} \frac{1}{\lambda_k}, & \text{falls die reduzierte Zeilenstufenform } E \text{ ist,} \\ 0, & \text{ansonsten.} \end{cases}$$

Korollar 7.2.7

Eine Matrix $A \in \mathrm{M}_n(\mathbb{R})$ ist genau dann invertierbar, wenn $\det(A) \neq 0$ gilt.

Satz 7.2.8 (Transponierte Matrix)

Für eine Matrix $A = (a_{i,j})_{i,j} \in \mathrm{M}_n(\mathbb{R})$ stimmt die Determinante mit der Determinante ihrer ***transponierten Matrix*** $A^\top := (a_{j,i})_{i,j}$, die durch Vertauschung von Zeilen mit Spalten aus A entsteht, überein:

$$\det(A^\top) = \det(A).$$

Satz 7.2.9 (Multiplikationsformel)

Für zwei Matrizen $A, B \in \mathrm{M}_n(\mathbb{R})$ gilt

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

Insbesondere gilt ferner für invertierbare Matrizen $A \in \mathrm{M}_n(\mathbb{R})$

$$\det(A^{-1}) = \det(A)^{-1} = \frac{1}{\det(A)}.$$

Satz 7.2.10 (Volumenänderung)

Bei einer linearen Abbildung $f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^n$, $x \longmapsto Ax$, ändert sich das n-dimensionale ***Volumen*** (im Fall $n = 2$ also die ***Fläche***) einer messbaren Teilmenge $M \subseteq \mathbb{R}^n$ um den Absolutbetrag der Determinante der zugehörigen Abbildungsmatrix $A \in \mathrm{M}_n(\mathbb{R})$:

$$\mathrm{Vol}(f(M)) = |\det(A)| \cdot \mathrm{Vol}(M).$$

7.3 Hauptachsentransformation

Die Begriffe in diesem Abschnitt sind nur für den Vektorraum $\mathbb{R}^2$ formuliert, können aber auch für andere Dimensionen und andere Körper (wie $\mathbb{C}$) untersucht werden.

Definition 7.3.1 (Charakteristisches Polynom, Eigenwerte)

- Für eine Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$ nennt man das Polynom

  $$\chi_A(t) := \det(A - tE) = t^2 - (a+d)t + (ad - bc) = t^2 - \mathrm{sp}(A)t + \det(A)$$

  in der Unbestimmten t das ***charakteristische Polynom*** der Matrix A mit ***Spur*** $\mathrm{sp}(A) := a+d$ (Summe der Hauptdiagonaleinträge) und Determinante $\det(A) = ad-bc$
- Die Nullstellen des charakteristischen Polynoms werden als ***Eigenwerte*** der Matrix A bezeichnet.

Satz 7.3.2

Wird für eine Matrix $A \in \mathrm{M}_2(\mathbb{R})$ eine Basistransformation mittels einer Matrix $B \in \mathrm{M}_2(\mathbb{R})$ durchgeführt,

$$A' = B^{-1} \cdot A \cdot B,$$

so ändern sich das charakteristische Polynom und damit auch die Menge der Eigenwerte nicht:

$$\chi_{A'}(t) = \chi_A(t).$$

Definition 7.3.3 (Eigenvektoren)

Für eine Matrix $A \in \mathrm{M}_2(\mathbb{R})$ und einen Eigenwert $\lambda \in \mathbb{R}$ nennt man einen Vektor $v \neq 0$ aus $\mathbb{R}^2$ mit

$$(A - \lambda E)v = 0 \qquad \text{bzw.} \qquad Av = \lambda v$$

einen ***Eigenvektor*** von A zum Eigenwert λ.

Satz 7.3.4 (Hauptachsentransformation)

Für eine symmetrische Matrix $A = \begin{pmatrix} a & c \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$ gilt:

(a) Das quadratische Polynom χ_A besitzt stets zwei reelle Nullstellen

$$\lambda_{\frac{1}{2}} = \frac{a+d}{2} \pm \frac{\sqrt{(a-d)^2 + 4c^2}}{2}.$$

Für diese gilt insbesondere $\lambda_1 + \lambda_2 = \mathrm{sp}(A) = a + d$ und $\lambda_1 \cdot \lambda_2 = \det(A) = ad - c^2$.

(b) Es lässt sich eine Orthonormalbasis b_1, b_2 des $\mathbb{R}^2$ wählen, so dass die Matrixdarstellung bezüglich dieser Basis Diagonalgestalt besitzt,

$$A' = B^{-1} \cdot A \cdot B = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \qquad \text{mit } B = \begin{pmatrix} b_1 & b_2 \end{pmatrix},$$

wobei die Einträge der Hauptdiagonalen von A' genau die Eigenwerte λ_1, λ_2 von A sind und b_1 bzw. b_2 einen Eigenvektor der Matrix A zum Eigenwert λ_1 bzw. λ_2 darstellt.

Alphabete

Griechisches Alphabet

In der nachfolgenden Tabelle sind die griechischen Buchstaben aufgelistet. Hinter den Symbolen ist jeweils der zugehörige Befehl angegeben, der in dem für mathematische Texte hervorragend geeigneten (kostenlosen) Textsatzsystem LaTeX innerhalb einer mathematischen Umgebung verwendet werden kann.

Name	Großbuchstabe		Kleinbuchstabe		Variante	
Alpha	A	`A`	α	`\alpha`		
Beta	B	`B`	β	`\beta`		
Gamma	$\varGamma$	`\varGamma`*	γ	`\gamma`		
Delta	$\varDelta$	`\varDelta`*	δ	`\delta`		
Epsilon	E	`E`	ϵ	`\epsilon`	ε	`\varepsilon`
Zeta	Z	`Z`	ζ	`\zeta`		
Eta	H	`H`	η	`\eta`		
Theta	$\varTheta$	`\varTheta`*	θ	`\theta`	ϑ	`\vartheta`
Iota	I	`I`	ι	`\iota`		
Kappa	K	`K`	κ	`\kappa`		
Lambda	$\varLambda$	`\varLambda`*	λ	`\lambda`		
My	M	`M`	μ	`\mu`		
Ny	N	`N`	ν	`\nu`		
Xi	$\varXi$	`\varXi`*	ξ	`\xi`		
Omikron	O	`O`	o	`o`		
Pi	$\varPi$	`\varPi`*	π	`\pi`	ϖ	`\varpi`
Rho	P	`P`	ρ	`\rho`	ϱ	`\varrho`
Sigma	$\varSigma$	`\varSigma`*	σ	`\sigma`	ς	`\varsigma`
Tau	T	`T`	τ	`\tau`		
Ypsilon	$\varUpsilon$	`\varUpsilon`*	υ	`\upsilon`		
Phi	$\varPhi$	`\varPhi`*	ϕ	`\phi`	φ	`\varphi`
Chi	X	`X`	χ	`\chi`		
Psi	$\varPsi$	`\varPsi`*	ψ	`\psi`		
Omega	$\varOmega$	`\varOmega`*	ω	`\omega`		

* Die Befehle ohne `var`, wie `\Gamma` etc., erzeugen die zugehörigen aufrechten Symbole, also Γ, Δ, Θ, Λ, Ξ, Π, Σ, Υ, Φ, Ψ, Ω.

Kalligraphisches Alphabet

In der nachfolgenden Tabelle sind die kalligraphischen Großbuchstaben aufgelistet. Sie stehen (nur im Mathematikmodus) mittels des Aufrufs {`\cal` TEXT} zur Erzeugung von $\mathcal{TEXT}$ bzw. `\mathcal T` zur Erzeugung des kalligraphischen Buchstabens $\mathcal{T}$ zur Verfügung.

Buchstabe	
$\mathcal{A}$	A
$\mathcal{B}$	B
$\mathcal{C}$	C
$\mathcal{D}$	D
$\mathcal{E}$	E
$\mathcal{F}$	F
$\mathcal{G}$	G
$\mathcal{H}$	H
$\mathcal{I}$	I

Buchstabe	
$\mathcal{J}$	J
$\mathcal{K}$	K
$\mathcal{L}$	L
$\mathcal{M}$	M
$\mathcal{N}$	N
$\mathcal{O}$	O
$\mathcal{P}$	P
$\mathcal{Q}$	Q
$\mathcal{R}$	R

Buchstabe	
$\mathcal{S}$	S
$\mathcal{T}$	T
$\mathcal{U}$	U
$\mathcal{V}$	V
$\mathcal{W}$	W
$\mathcal{X}$	X
$\mathcal{Y}$	Y
$\mathcal{Z}$	Z

Die kalligraphischen Buchstaben stehen nur für Großbuchstaben zur Verfügung.

Altdeutsches Alphabet (Sütterlin)

In der nachfolgenden Tabelle sind die Buchstaben des altdeutschen Alphabets (Sütterlin) aufgelistet. Für die Verwendung im Textsatzsystem LaTeX muss man zunächst das Paket `suetterl` mittels `\usepackage{suetterl}` in der Präambel des Dokuments einbinden. Dann stehen die Sütterlin-Buchstaben (nur im Textmodus) mittels des Aufrufs {`\suetterlin Text`} zur Erzeugung von Text bzw. `\textsuetterlin T` zur Erzeugung von T zur Verfügung.

Großbuchstabe		Kleinbuchstabe	
A	A	a	a
B	B	b	b
C	C	c	c
D	D	d	d
E	E	e	e
F	F	f	f
G	G	g	g
H	H	h	h
I	I	i	i
J	J	j	j
K	K	k	k
L	L	l	l
M	M	m	m

Großbuchstabe		Kleinbuchstabe	
N	N	n	n
O	O	o	o
P	P	p	p
Q	Q	q	q
R	R	r	r
S	S	s	s
T	T	t	t
U	U	u	u
V	V	v	v
W	W	w	w
X	X	x	x
Y	Y	y	y
Z	Z	z	z

Die hier abgebildeten Buchstaben besitzen die Schriftgröße `\LARGE`, ansonsten hätten sie statt A, B, C, a, b, c die Größe A, B, C, a, b, c.

Literaturverzeichnis

M. Aigner Diskrete Mathematik Vieweg Verlag, Braunschweig Wiesbaden, 1993

H. Anton Lineare Algebra Spektrum Akademischer Verlag, Heidelberg Berlin

M. Brill **Mathematik für Informatiker** Hanser Verlag, München, 2005[2]

H. J. Dirschmid Höhere Mathematik – Matrizen und Lineare Gleichungen Fortis Verlag FH

G. Fischer **Lineare Algebra** Vieweg Verlag

K.-H. Gärtner, R. Schnieder Lineare Algebra und Analytische Geometrie in Fragen und Übungsaufgaben Teubner Verlag Stuttgart Leipzig

D. Hachenberger Mathematik für Informatiker Pearson Studium Addison-Wesley, München, 2005

R. Haggarty Diskrete Mathematik für Informatiker Pearson Studium Addison-Wesley, München, 2004

D. Labuch Aufgaben zur Linearen Algebra Teubner Verlag Stuttgart

W. Nehrlich **Diskrete Mathematik, Basiswissen für Informatiker (Mathematica-gestützt)** Fachbuchverlag Leipzig, 2003

B. Pareigis Lineare Algebra für Informatiker Springer Verlag

E.-A. Pforr et al. Übungsaufgaben zur linearen Algebra und linearen Optimierung Teubner Verlag Leipzig

W. Preuss, G. Wenisch **Mathematik 3 (Lineare Algebra – Stochastik)** Fachbuchverlag Leipzig im Carl Hanser Verlag

W. Preuss, G. Wenisch **Mathematik für Informatiker – Lineare Algebra und Anwendungen** Fachbuchverlag Leipzig im Carl Hanser Verlag

G. Teschl, S. Teschl **Mathematik für Informatiker, Band 1** Springer Verlag, Berlin, 2008[3]

GRIPS-Kurs https://elearning.uni-regensburg.de/course/view.php?id=21383
Homepage https://www.oth-regensburg.de/rainer.loeschel
E-Mail rainer.loeschel@oth-regensburg.de

Symbolverzeichnis

Stichwortverzeichnis

E

F

G

H

I