Glossar zur Linearen Algebra I

Dustin Hartmann
Benno Kuckuck
Matteo Vannacci

3. April 2018

Symbole

Mengensymbole

$\emptyset$	die leere Menge
$\mathbb{N}$	die Menge der natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$
$\mathbb{N}_0$	die Menge der natürlichen Zahlen mit Null $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$	der Ring der ganzen Zahlen $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Q}$	der Körper der rationalen Zahlen $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\, b \neq 0\}$
$\mathbb{R}$	der Körper der reellen Zahlen
$\mathbb{P}$	die Menge der Primzahlen
$\mathbb{H}$	der Ring der Hamiltonschen Quaternionen

Grundlegendes

$\exists x \in A : S$	Es existiert ein Element x der Menge A, das die Bedingung S erfüllt
$\forall x \in A : S$	Für alle Elemente der Menge A gilt die Bedingung S
$x \in A$, $A \ni x$	x ist Element der Menge A
$x \notin A$	x ist nicht Element der Menge A
$A \subseteq B$, $B \supseteq A$	A ist Teilmenge von B
$A \subsetneq B$	A ist echte Teilmenge von B
$A \not\subseteq B$	A ist nicht Teilmenge von B
$A = B$	für A, B Mengen, siehe Mengengleichheit
$A \setminus B$	die Differenz der Mengen A und B
$A \cup B$	die Vereinigung von A und B
$\bigcup_{i \in I} A_i$	die Vereinigung aller Mengen A_i
$\bigcup \mathcal{A}$	die Vereinigung aller Elemente von $\mathcal{A}$
$A \cap B$	der Schnitt von A und B
$\bigcap_{i \in I} A_i$	der Schnitt aller Mengen A_i
$\bigcap \mathcal{A}$	der Schnitt aller Elemente von $\mathcal{A}$
$\mathcal{P}(A)$	die Potenzmenge von A

$A \times B$	das Cartesische Produkt von A und B
A^n	für eine Menge A: das Cartesische Produkt von n Kopien von A
$\alpha : A \to B$	α ist eine Abbildung von A nach B
$\mathrm{Abb}(A, B)$	die Menge aller Abbildungen von A nach B
$\alpha\beta$ oder $\beta \circ \alpha$	für Abbildungen α und β: Das Kompositum von α und β
id_A	die identische Abbildung auf der Menge A
$A \approx B$	für Mengen A und B: A und B sind gleichmächtig
$\lvert A\rvert$ oder $\#A$	für eine Menge A: Die Mächtigkeit von A

Vektorräume und lineare Abbildungen

$U + W$	für Unterräume U und W eines Vektorraums V: Summe der Unterräume U und W
$V = U \oplus W$	für Unterräume U und W eines Vektorraums V: V ist die direkte Summe der Unterräume U und W
$\dim V$	die Dimension von V
$\langle M \rangle$	die lineare Hülle von M
$\langle v_1, \ldots, v_n \rangle$	die lineare Hülle von $v_1, \ldots, v_n$
$v \perp w$	v und w sind $\to$*senkrecht*
A^{tr}	die Transponierte der Matrix A
$\mathrm{Eig}(\alpha, \lambda)$	der $\to$*Eigenraum* von α zu λ
$\mathrm{Hom}_K(V, W)$	die Menge aller linearen Abbildungen von V nach W
$\mathrm{End}_K(V)$	die Menge aller Endomorphismen von V
$\mathrm{GL}(V)$	die Menge aller Automorphismen von V
$\mathrm{GL}_n(K)$	die allgemeine lineare Gruppe vom Rang n
$V \cong W$	V und W sind isomorph
$A \approx B$	für A und B Matrizen: A und B sind ähnlich
$A \sim B$	für A und B Matrizen: A und B sind äquivalent

Anderes

$a \mid b$ oder $a \mid_R b$	a teilt b in R
$a \sim_R b$	a ist assoziiert zu b im Ring R
R^*	für einen Ring R: die Einheitengruppe von R
$\mathrm{Sym}(X)$	die symmetrische Gruppe von X
$\mathrm{Sym}(n)$	die symmetrische Gruppe vom Grad n
$K[X]$	der Polynomring über dem Körper K
$\mathrm{grad}\, f$	der Grad des Polynoms f

Glossar

Primzahl $\to$ *Beispiel 1.3d)*

Eine natürliche Zahl $p \in \mathbb{N}$ heißt Primzahl falls $p \neq 1$ und es gilt

$$p = ab \text{ mit } a, b \in \mathbb{N} \implies a \in \{1, p\}.$$

In anderen Worten: Die einzige Möglichkeit p als Produkt von natürlichen Zahlen zu schreiben ist $p = 1 \cdot p$ oder $p = p \cdot 1$.

Es gibt unendlich viele Primzahlen (→*Satz 1.6*).

Die Menge der Primzahlen wird oft mit $\mathbb{P}$ bezeichnet.

Für Verallgemeinerungen des Konzepts der Primzahlen auf andere Ringe, siehe Primelemente und unzerlegbare Elemente.

Teilmenge → *Definition 1.7*

Sind A und B Mengen, so heißt A Teilmenge von B, wenn alle Element von A auch Elemente von B sind, also

$$\forall x \in A : x \in B.$$

Man schreibt dann $A \subseteq B$ oder $B \supseteq A$ und sagt auch „A ist enthalten in B“.

Um auszudrücken, dass A *nicht* Teilmenge von B ist, also dass

$$\exists x \in A : x \notin B$$

schreibt man $A \nsubseteq B$ oder $B \nsupseteq A$.

Man nennt A eine *echte Teilmenge* von B (oder „A echt enthalten in B“), wenn $A \subseteq B$ aber *nicht* $A = B$. Das heißt

$$\forall x \in A : x \in B \quad \text{und} \quad \exists b \in B : b \notin A.$$

Man schreibt dann $A \subsetneq B$ oder $B \supsetneq A$.

Viele Autoren schreiben auch einfach $A \subset B$ bzw. $B \supset A$, für $A \subseteq B$ bzw. $B \supseteq A$, aber Vorsicht: Bei anderen Autoren bedeutet $A \subset B$ bzw. $B \supset A$, dass A eine echte Teilmenge von B ist, also $A \subsetneq B$ bzw. $B \supsetneq A$.

Untermenge → *Definition 1.7*

siehe Teilmenge.

Mengengleichheit → *Definition 1.7*

Zwei Mengen A und B sind gleich, wenn sie dieselben Elemente enthalten, d.h.

$$x \in A \iff x \in B.$$

Äquivalent dazu ist

$$A \subseteq B \quad \text{und} \quad B \subseteq A.$$

Siehe Teilmenge.

Differenz (von Mengen) → *Definition 1.7b)*

Die Differenz der Mengen A und B ist

$$A \setminus B = \{a \in A \mid a \notin B\}.$$

Vereinigung → *Definition 1.7d)*

Die Vereinigung der Mengen A und B ist

$$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}.$$

Hat man eine Familie von Mengen A_i, die durch ein i aus einer beliebigen Indexmenge I indiziert sind (oft ist etwa $I = \mathbb{N}$, d.h. man hat Mengen $A_1, A_2, A_3, \dots$), so definiert man ihre Vereinigung als

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ für mindestens ein } i \in I\}.$$

Ist $\mathcal{A}$ eine Menge deren Elemente selber Mengen sind so schreibt man für die Vereinigung

$$\bigcup \mathcal{A} = \{x \mid x \in A \text{ für mindestens ein } A \in \mathcal{A}\}.$$

Schnitt → *Definition 1.7d)*

Der Schnitt der Mengen A und B ist

$$A \cap B = \{x \mid x \in A \text{ und } x \in B\}.$$

Hat man eine Familie von Mengen A_i, die durch ein i aus einer beliebigen Indexmenge I indiziert sind (oft ist etwa $I = \mathbb{N}$, d.h. man hat Mengen $A_1, A_2, A_3, \dots$), so definiert man ihren Schnitt als

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ für alle } i \in I\}.$$

Ist $\mathcal{A} \neq \emptyset$ eine Menge deren Elemente selber Mengen sind so schreibt man für den Schnitt

$$\bigcap \mathcal{A} = \{x \mid x \in A \text{ für alle } A \in \mathcal{A}\}.$$

Potenzmenge → *Definition 1.7c)*

Die Potenzmenge einer Menge A ist die Menge aller Teilmengen von A, also $\mathcal{P}(A) = \{X \mid X \subseteq A\}$.

Mengengesetze → *Lemma 1.9*

Für Vereinigung, Schnitt und Differenz von Mengen gelten gewisse „Rechenregeln“. Ist M eine Menge und $A, B, C \subset M$ Teilmengen, so gilt

- Kommutativgesetze:

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

- Assoziativgesetze:

$$A \cup (B \cup C) = (A \cup B) \cup C$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$

- Distributivgesetze:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

- de Morgansche Regeln:

$$M \setminus (A \cup B) = (M \setminus A) \cap (M \setminus B)$$
$$M \setminus (A \cap B) = (M \setminus A) \cup (M \setminus B)$$

de Morgansche Regeln → *Lemma 1.9*

siehe Mengengesetze

Cartesisches Produkt → *Definition 1.10*

Seien A, B Mengen. Das *cartesische Produkt* von A und B ist die Menge

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

Hierbei ist (a, b) das *geordnete Paar* von a und b. Es gilt

$$(a, b) = (a', b') \iff a = a' \text{ und } b = b'.$$

Allgemeiner kann man für endlich viele Mengen $A_1, \ldots, A_n$ sogenannte n-Tupel $(a_1, \ldots, a_n)$ mit $a_i \in A_i$ für $i \in \{1, \ldots, n\}$ betrachten, für die entsprechend gilt

$$(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n) \iff a_i = a'_i \text{ für alle } i \in \{1, \ldots, n\}.$$

Die Menge aller solcher n-Tupel bezeichnet man dann als

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } i \in \{1, \ldots, n\}\}.$$

In dem Spezialfall $A_1 = \cdots = A_n = A$ schreibt man auch

$$A^n = \underbrace{A \times \cdots \times A}_{n \text{ Stück}} = \{(a_1, \ldots, a_n) \mid a_i \in A \text{ für } i \in \{1, \ldots, n\}\}.$$

geordnetes Paar → *Definition 1.10*

siehe Cartesisches Produkt.

Tupel → *Definition 1.10*

siehe Cartesisches Produkt.

Relation → *Definition 1.10 c)*

Eine (binäre) *Relation* R auf einer Menge A ist eine Teilmenge $R \subseteq A \times A$.

Man schreibt dann für $(a, b) \in R$ oft aRb. So ist zum Beispiel

$$\{(a, a) \mid a \in A\}$$

eine Relation auf A, die man mit „=“ bezeichnet. Man schreibt für gewöhnlich aber $a = b$ statt $(a, b) \in =$.

Abbildung → *Definition 2.2*

Anschaulich gesprochen ist eine Abbildung von einer Menge A in eine Menge B eine Vorschrift die jedem $a \in A$ eindeutig ein $b \in B$ zuordnet. Formal definiert man eine Abbildung von A nach B als eine Teilmenge $\alpha \subseteq A \times B$ mit folgender Eigenschaft:

$$\text{Zu jedem } a \in A \text{ gibt es genau ein } b \in B \text{ mit } (a, b) \in \alpha.$$

Für ein gegebenes $a \in A$ bezeichnet man dieses eindeutige $b \in B$ für das $(a, b) \in \alpha$, dann als $a\alpha$, oder a^α oder $\alpha(a)$, d.h.

$$a\alpha = b \iff a^\alpha = b \iff \alpha(a) = b \iff (a, b) \in \alpha.$$

Man schreibt für „α ist eine Abbildung von A nach B“ in der Regel $\alpha : A \to B$. Man nennt dann A den Definitionsbereich von α. Oft

gibt man eine Abbildung in Form einer Abbildungsvorschrift an, so schreibt man etwa

$$\alpha : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$$

für die Abbildung

$$\alpha = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a = x,\ b = x^2 \text{ für ein } x \in \mathbb{R}\},$$

sodass also

$$x\alpha = \alpha(x) = x^2 \quad \text{für } x \in \mathbb{R}.$$

Die Menge aller Abbildungen von A nach B bezeichnet man mit

$$\mathrm{Abb}(A, B) = \{\alpha \mid \alpha : A \to B \text{ ist eine Abbildung}\}.$$

Funktion → *Definition 2.2*

siehe Abbildung.

Definitionsbereich → *Definition 2.2*

Ist $\alpha : A \to B$ eine Abbildung, so heißt A Definitionsbereich von α. Es gilt immer

$$A = \{a \mid \exists (x, y) \in \alpha : x = a\}.$$

Bild → *Definition 2.2*

Ist $\alpha : A \to B$ eine Abbildung so heißt die Menge

$$\mathrm{Bild}\,\alpha = \{b \in B \mid \exists a \in A : a\alpha = b\} = \{a\alpha \mid a \in A\}$$

das Bild von α.

Ist $\alpha : V \to W$ eine lineare Abbildung, so ist $\mathrm{Bild}\,\alpha \subseteq W$ ein Unterraum von W.

injektiv → *Definition 2.3 b)*

Seien A, B Mengen. Eine Abbildung $\alpha : A \to B$ heißt *injektiv*, falls für $a, a' \in A$ aus $a\alpha = a'\alpha$ stets $a = a'$ folgt.

Oft verwendet man auch die äquivalente Definition: α ist injektiv, wenn für $a, a' \in A$ mit $a \neq a'$ auch $a\alpha \neq a'\alpha$ ist.

surjektiv → *Definition 2.3 b)*

Seien A, B Mengen. Eine Abbildung $\alpha : A \to B$ heißt *surjektiv* (auf B), falls $\mathrm{Bild}(\alpha) = B$ (siehe Bild). Mit anderen Worten: $\alpha : A \to B$ ist surjektiv, falls es zu jedem $b \in B$ ein $a \in A$ gibt mit $a\alpha = b$.

Kompositum → *Definition 2.5*

Das *Kompositum* (auch: Hintereinanderausführung oder Verkettung) von Abbildungen $\alpha : A \to B$ und $\beta : B \to C$ ist die Abbildung

$$\alpha\beta : A \to C,\ a \mapsto (a\alpha)\beta.$$

Sind $\alpha : A \to B$, $\beta : B \to C$ und $\gamma : C \to D$ drei Abbildungen, so gilt das Assoziativgesetz

$$(\alpha\beta)\gamma = \alpha(\beta\gamma).$$

Schreibt man Abbildungen von links (also $\alpha(a)$ statt $a\alpha$), so schreibt man auch

$$\beta \circ \alpha : A \to C,\ a \mapsto \beta(\alpha(a)).$$

Man liest $\beta \circ \alpha$ als „β nach α“.

Hintereinanderausführung → *Definition 2.5*

siehe Kompositum.

identische Abbildung → *Definition 2.5*

Die identische Abbildung auf einer Menge A ist die Abbildung

$$\mathrm{id}_A : A \to A,\ a \mapsto a.$$

Umkehrabbildung → *Definition 2.5 b)*

Sei $\alpha : A \to B$ injektiv. Dann hat α eine sogenannte Umkehrabbildung $\alpha^{-1} : \mathrm{Bild}(\alpha) \to A$, definiert als

$$\alpha^{-1} = \{(b, a) \mid (a, b) \in \alpha\}.$$

Es gilt

$$\alpha\alpha^{-1} = \mathrm{id}_A \quad \text{und} \quad \alpha^{-1}\alpha = \mathrm{id}_{\mathrm{Bild}\,\alpha}.$$

Man beachte: Im allgemeinen ist der Definitionsbereich der Umkehrabbildung $\mathrm{Bild}(\alpha)$. Ist α surjektiv (also bijektiv), so ist $\mathrm{Bild}\,\alpha = B$, also ist dann $\alpha^{-1} : B \to A$ auf ganz B definiert.

Ist $\alpha : V \to W$ eine injektive lineare Abbildung, so ist die Umkehrabbildung automatisch ebenfalls linear.

inverse Abbildung → *Definition 2.5 b)*

siehe Umkehrabbildung.

bijektiv → *Definition 2.3b)*

Seien A, B Mengen. Eine Abbildung $\alpha : A \to B$ heißt bijektiv oder Bijektion, falls α injektiv und surjektiv ist.

Eine Abbildung $\alpha : A \to B$ ist genau dann bijektiv, wenn es eine Umkehrabbildung $\beta : B \to A$ gibt. Das bedeutet, dass $\alpha\beta = \mathrm{id}_A$ und $\beta\alpha = \mathrm{id}_B$, also

$$a\alpha\beta = a \quad \text{für alle } a \in A$$
$$b\beta\alpha = b \quad \text{für alle } b \in B.$$

Bijektion → *Defintion 2.3b)*

siehe bijektiv.

gleichmächtig → *Definition 3.1 a)*

Zwei Mengen A, B heißen *gleichmächtig*, falls es eine Bijektion $f : A \to B$ gibt. Wir schreiben dann $A \approx B$.

Endlichkeit von Mengen → *Definition 3.1 b)*

Sei A eine Menge. Dann heißt A endlich, falls

$$A = \emptyset \quad \text{oder} \quad A \approx \{1, 2, 3, \ldots, n\} \text{ für ein } n \in \mathbb{N}$$

gilt (siehe gleichmächtig). Ist in diesem Fall

$$f : \{1, 2, 3, \ldots, n\} \to A$$

eine Bijektion, so gilt

$$A = \{a_1, a_2, a_3, \ldots, a_n\},$$

wobei $a_i = f(i)$ für $i \in \{1, \ldots, n\}$ paarweise verschieden sind.

Kardinaliät → *Definition 3.1 a)*

Siehe Mächtigkeit.

Mächtigkeit → *Definition 3.1a)*

Sei A eine Menge. Dann nennt man

$$|A| = \begin{cases} 0 & \text{falls } A = \emptyset \\ n & \text{falls } A \text{ endlich und } A \approx \{1, 2, \ldots, n\} \\ \infty & \text{falls } A \text{ unendlich} \end{cases}$$

die Mächtigkeit oder Kardinalität von A. Anschaulich ist dies die Anzahl der Elemente von A.

abzählbar unendlich → *Beispiel 3.2*

Eine Menge A heißt abzählbar unendlich wenn sie gleichmächtig zu $\mathbb{N}$ ist.

Körper → *Definition 4.1*

Ein *Körper* $K = (K, +, \cdot)$ ist eine Menge K, für welche eine „Addition“

$$+ : K \times K \to K,\ (a, b) \mapsto a + b$$

und eine „Multiplikation“

$$\cdot : K \times K \to K,\ (a, b) \mapsto a \cdot b = ab$$

gegeben sind, sodass die folgenden „Rechenregeln“ erfüllt sind:

(A1) Assoziativität von $+$.

$$(a + b) + c = a + (b + c) \quad \text{für alle } a, b, c \in K$$

(A2) Kommutativität von $+$.

$$a + b = b + a \quad \text{für alle } a, b \in K$$

(A3) Existenz eines Nullelements. Es existiert ein eindeutiges Element, genannt $0 \in K$ (Nullelement), sodass gilt

$$a + 0 = a = 0 + a \quad \text{für alle } a \in K.$$

(A4) Existenz von Inversen bezüglich $+$. Es gibt zu jedem $a \in K$ ein eindeutiges Element, genannt $-a \in K$ sodass

$$a + (-a) = 0 = (-a) + a.$$

(M1) Assoziativität von $\cdot$.

$$(ab)c = a(bc) \quad \text{für alle } a, b, c \in K.$$

(M2) Kommutativität von $\cdot$.

$$ab = ba \quad \text{für alle } a, b \in K.$$

(M3) Existenz eines Einselements. Es existiert genau ein von 0 verschiedenes Element in K, genannt $1 \in K$ (Einselement), für das gilt:

$$a \cdot 1 = 1 \cdot a = a \quad \text{für alle } a \in K.$$

(M4) Existenz von Inversen bezüglich $\cdot$. Zu jedem $a \in K \setminus \{0\}$ gibt es genau ein Element in K, genannt $\frac{1}{a}$ oder a^{-1} (das zu a inverse Element bezüglich $\cdot$), für das gilt:

$$a\frac{1}{a} = \frac{1}{a}a = 1.$$

(D) Distributivgesetze.

$$\begin{aligned} a(b+c) &= ab + ac \\ (a+b)c &= ac + bc \end{aligned} \quad \text{für alle } a, b, c \in K$$

Beispiele für Körper sind die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die Restklassenringe $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{P}$.

nullteilerfrei → *Folgerungen 4.2*

Ein kommutativer Ring R heißt nullteilerfrei, wenn aus $ab = 0$ für $a, b \in R$ stets $a = 0$ oder $b = 0$ folgt. Mit anderen Worten: R ist nullteilerfrei, wenn es in R keinen Nullteiler außer 0 selbst gibt.

Ein Körper ist immer nullteilerfrei. Aber auch der Ring der ganzen Zahlen $\mathbb{Z}$ ist nullteilerfrei. Ein Beispiel für einen Ring der nicht nullteilerfrei ist, ist der Restklassenring $\mathbb{Z}/6\mathbb{Z}$ oder das Produkt $\mathbb{Z} \times \mathbb{Z}$.

Vektorraum → *Definition 4.7*

Sei K ein Körper (beispielsweise $K = \mathbb{R}$). Ein *Vektorraum* $V = (V, +, \cdot)$ über K ist eine Menge V, für welche eine „Addition“

$$+ : V \times V \to V,\ (x, y) \mapsto x + y$$

und eine „Skalarmultiplikation“

$$\cdot : K \times V \to V,\ (a, x) \mapsto ax$$

gegeben sind, sodass die folgenden „Rechenregeln“ erfüllt sind:

(A1) Assoziativität von $+$.

$$x + (y + z) = (x + y) + z \quad \text{für } x, y, z \in V.$$

(A2) Kommutativität von $+$.

$$x + y = y + x \quad \text{für } x, y \in V.$$

(A3) Existenz eines Nullelements. Es existiert genau ein Element in V, welches wir mit $0 = 0_V$ bezeichnen (der *Nullvektor*), für das gilt:

$$x + 0 = 0 + x = x \quad \text{für } x \in V.$$

(A4) Existenz von Inversen bezüglich $+$. Zu jedem $x \in V$ existiert genau ein Element in V, welches wir mit $-x$ bezeichnen, für das gilt:

$$x + (-x) = (-x) + x = 0 \quad \text{für alle} x \in V.$$

(SM1) $(ab)x = a(bx)$ für alle $a, b \in K$ und $x \in V$.

(SM2) $1x = x$ für alle $x \in V$ (wobei $1 = 1_K \in K$ das Einselement von K ist).

(SM3) $a(x + y) = ax + ay$ für alle $a \in K$ und $x, y \in V$.

(SM4) $(a + b)x = ax + bx$ für alle $a, b \in K$ und $x \in V$.

Die kanonischen Beispiele für K-Vektorräume sind die *Standardvektorräume*

$$K^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in K\}$$

mit der Addition

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

und Skalarmultiplikation

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$$

für $a \in K$ und $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$.

Nullvektorraum → *Beispiele 4.9*

Der Vektorraum, der nur aus dem Nullvektor besteht.

Untervektorraum → *Definition 5.1*

Eine Teilmenge eines Vektorraums V, die bezüglich der in V definierten Verknüpfungen $+$ und $\cdot$ selber ein Vektorraum ist heißt Untervektorraum (auch: Unterraum oder (linearer) Teilraum) von V.

Um zu prüfen ob eine Teilmenge $U \subseteq V$ ein Untervektorraum ist, verwendet man in der Regel das Unterraumkriterium (→ *Hilfssatz 5.2*): U bildet einen Unterraum von V genau dann, wenn die folgenden Bedinungen erfüllt sind:

(U1) U ist nicht leer. D.h. $U \neq \emptyset$.

(U2) U ist abgeschlossen bezüglich der Addition. D.h. $x + y \in U$ für alle $x, y, \in U$.

(U3) U ist abgeschlossen bezüglich der Skalarmultiplikation. D.h. $ax \in U$ für alle $a \in K, x \in U$.

Beispiel: Im Standardvektorraum $\mathbb{R}^3$ sind die Unterräume genau der Nullvektorraum, die Geraden und Ebenen die 0 enthalten und der gesamte Raum.

Die Dimension eines Unterraums $U \leq V$ ist höchstens die Dimension von V. Es gilt $\dim U = \dim V$ genau dann, wenn $U = V$ (→ *Satz 10.5*).

Unterraum → *Definition 5.1*

siehe Untervektorraum.

linearer Teilraum → *Definition 5.1*

siehe Untervektorraum.

Unterraumkriterium → *Definition 5.2*

siehe Untervektorraum.

Summe von Unterräumen → *Definition 5.4*

Ist V ein Vektorraum und $U_1, \ldots, U_n$ Unterräume, so definiert man ihre Summe als

$$U_1 + \cdots + U_n = \{x_1 + \cdots + x_n \mid x_i \in U_i \text{ für } 1 \leq i \leq n\}.$$

Allgemeiner kann man auch für eine (eventuell unendliche) Menge $\mathcal{U} \neq \emptyset$ von Unteräumen von V die Summe definieren als

$$\sum \mathcal{U} = \sum_{U \in \mathcal{U}} U = \{x_1 + \cdots + x_r \mid r \in \mathbb{N}_0, x_j \in \bigcup \mathcal{U} \text{ für } 1 \leqslant j \leqslant r\}.$$

Die Summe von Unterräumen ist stets wieder ein Unterraum von V.

Der wichtigste Spezialfall ist die Summe zweier Unterräume $U, W \leq V$:

$$U + W = \{u + w \mid u \in U, w \in W\}.$$

Zur Dimension der Summe siehe Dimensionsformel für Unterräume.

Linearkombination → *Definition 6.1*

Sei V ein Vektorraum. Man sagt, dass $w \in V$ eine Linearkombination von $v_1, \ldots, v_n \in V$ sei, wenn

$$w = a_1 v_1 + \cdots + a_n v_n \quad \text{für gewisse } a_1, \ldots, a_n \in K.$$

Die Menge aller Linearkombinationen von $v_1, \ldots, v_n \in V$ nennt man die lineare Hülle von $v_1, \ldots, v_n$.

Allgemeiner kann man für eine beliebige (eventuell unendliche) Teilmenge $M \subseteq V$ definieren: $w \in V$ ist eine Linearkombination von Vektoren aus M, falls es $a_1, \ldots, a_m \in K$ und $v_1, \ldots, v_m \in M$ (für ein $m \in \mathbb{N}_0$) gibt mit

$$w = a_1 v_1 + \cdots + a_m v_m.$$

lineare Hülle → *Definition 6.2*

Sei V ein Vektorraum und $v_1, \ldots, v_n \in V$. Die lineare Hülle von $v_1, \ldots, v_n$ ist die Menge aller Linearkombinationen dieser Vektoren

$$\langle v_1, \ldots, v_n \rangle = \{a_1 v_1 + \cdots + a_n v_n \mid a_1, \ldots, a_n \in K\}.$$

Diese Menge ist stets ein Untervektorraum von V, und zwar der „kleinste“ Untervektorraum der $v_1, \ldots, v_n$ enthält, (d.h. ist $U \subseteq V$ ein Unterraum der $v_1, \ldots, v_n$ enthält, so ist auch $\langle v_1, \ldots, v_n \rangle \subseteq U$, →*Satz 6.5*).

Allgemeiner kann man für eine (eventuell unendliche) Menge $M \subseteq V$ die lineare Hülle von M definieren als

$$\langle M \rangle = \{a_1 v_1 + \cdots + a_m v_m \mid m \in \mathbb{N}_0,\ a_1, \ldots, a_m \in K,\ v_1, \ldots, v_m \in M\}.$$

Dies ist der „kleinste“ Untervektorraum von V, der M enthält. Weitere Eigenschaften der linearen Hülle (→*Lemma 6.6*) sind

- $M \subseteq \langle M \rangle$
- Sind $M_1 \subseteq M_2 \subseteq V$, so ist $\langle M_1 \rangle \subseteq \langle M_2 \rangle$
- $\langle \langle M \rangle \rangle = \langle M \rangle$
- $M = \langle M \rangle$ genau dann, wenn M ein Unterraum von V ist
- $\langle M \rangle = \bigcap \{W \mid W \text{ Unterraum von V mit } M \subseteq W\}$
- Sind U_1, U_2 Unterräume von V, so ist $\langle U_1 \cup U_2 \rangle = U_1 + U_2$.

lineares Gleichungssystem $\to$ *?*

Ein lineares Gleichungssystem (oder LGS) über einem Körper K ist ein System von Gleichungen der Form

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_m &= b_m \end{aligned} \qquad (*)$$

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

Ein Tupel $(x_1, \ldots, x_n) \in K^n$ heißt Lösung für das LGS wenn die Gleichungen für diese $x_1, \ldots, x_m$ erfüllt sind.

Definiert man

$$a_i = (a_{1i}, a_{2i}, \ldots, a_{mi}) \quad \text{für } i \in \{1, \ldots, n\}$$

und

$$b = (b_1, \ldots, b_m),$$

so kann man das LGS $(*)$ auch schreiben als

$$x_1 a_1 + \cdots + x_n a_n = b.$$

Man sieht so ($\to$*Beispiele 6.7b)*), dass $(*)$ genau dann eine Lösung hat, wenn b eine Linearkombination von $a_1, \ldots, a_n$ ist, also

$$b \in \langle a_1, \ldots, a_n \rangle.$$

Man kann ein LGS auch durch eine Matrixgleichung darstellen. Schreibt man die Koeffizienten in eine Matrix $A = (a_{ij})$, so ist das LGS $(*)$ äquivalent zu

$$(x_1, \ldots, x_n)A^{\mathrm{tr}} = (b_1, \ldots, b_m)$$

Sind $b_1 = \cdots = b_m = 0$, so ist die Menge aller Lösungen ein Untervektorraum von K^n ($\to$ *Beispiel 5.3*), nämlich genau der Kern der linearen Abbildung $K^n \to K^n$, $x \mapsto xA^{\mathrm{tr}}$.

Um ein lineares Gleichungssystem zu lösen, bringt man zunächst die Matrix

$$(A \mid b) = \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$$

durch Zeilenumformungen auf reduzierte Zeilenstufenform.

$$(A' \mid b') = \left(\begin{array}{ccccccc|c} \boxed{1} & * & 0 & * & 0 & * & & \\ & & \boxed{1} & * & 0 & * & & \\ & & & \ddots & & & & * \\ & & 0 & & \boxed{1} & * & & \\ & & & & & & & \end{array}\right)$$

Zeilenumformungen an der Matrix entsprechen Äquivalenzumformungen an dem LGS, somit ändern sie die Lösungsmenge nicht, d.h. es ist

$$\{x \in K^n \mid xA^{\mathrm{tr}} = b\} = \{x \in K^n \mid xA'^{\mathrm{tr}} = b'\}.$$

Die Lösungsmenge des LGS $xA'^{\mathrm{tr}} = b'$ lässt sich dann ablesen. Wir demonstrieren dies an einem Beispiel:

Beispiel zur Bestimmung der Lösungsmenge eines homogenen LGS Zuerst betrachten wir den Spezialfall eines *homogenen* LGS, in dem also alle $b_i = 0$ sind (dies ist etwa der Fall der bei der Berechnung des Kerns einer Matrix eintritt). Nehmen wir an die Matrix hat, nachdem sie auf Zeilenstufenform gebracht wurde, die folgende Form:

$$\left(\begin{array}{ccccccccc|c} 0 & 1 & 5 & 0 & 0 & 2 & -17 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Sie beschreibt das folgende Gleichungssystem:

$$\begin{aligned} x_2 + 5x_3 + 2x_6 - 17x_7 + 3x_8 &= 0 \\ x_4 + 2x_6 + x_7 - x_8 &= 0 \\ x_5 + 3x_7 - 4x_8 &= 0 \\ x_9 &= 0 \end{aligned} \tag{1}$$

Hier nennt man x_1, x_3, x_6, x_7, x_8 (also diejenigen Variablen, die nicht am Anfang einer Gleichung stehen) die „freien Variablen“. Man bringt diese nun auf die andere Seite:

$$\begin{aligned} x_2 &= -5x_3 - 2x_6 + 17x_7 - 3x_8 \\ x_4 &= -2x_6 - x_7 + x_8 \\ x_5 &= -3x_7 + 4x_8 \\ x_9 &= 0 \end{aligned}$$

Nun erhält man die „Fundamentallösungen“, bei denen man eine der freien Variablen 1 setzt und die anderen 0:

$$x_1 = 1, x_3 = 0, x_6 = 0, x_7 = 0, x_8 = 0$$
$$\text{somit } x_2 = 0, x_4 = 0, x_5 = 0, x_9 = 0$$
$$\text{Lösungsvektor: } b_1 = (1, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$x_1 = 0, x_3 = 1, x_6 = 0, x_7 = 0, x_8 = 0$$
$$\text{somit } x_2 = -5, x_4 = 0, x_5 = 0, x_9 = 0$$
$$\text{Lösungsvektor: } b_2 = (0, -5, 1, 0, 0, 0, 0, 0, 0)$$

$$x_1 = 0, x_3 = 0, x_6 = 1, x_7 = 0, x_8 = 0$$
$$\text{somit } x_2 = -2, x_4 = -2, x_5 = 0, x_9 = 0$$
$$\text{Lösungsvektor: } b_3 = (0, -2, 0, -2, 0, 1, 0, 0, 0)$$

$$x_1 = 0, x_3 = 0, x_6 = 0, x_7 = 1, x_8 = 0$$
$$\text{somit } x_2 = 17, x_4 = -1, x_5 = -3, x_9 = 0$$
$$\text{Lösungsvektor: } b_4 = (0, 17, 0, -1, -3, 0, 1, 0, 0)$$

$$x_1 = 0, x_3 = 0, x_6 = 0, x_7 = 0, x_8 = 1$$
$$\text{somit } x_2 = -3, x_4 = 1, x_5 = 4, x_9 = 0$$
$$\text{Lösungsvektor: } b_5 = (0, -3, 0, 1, 4, 0, 0, 1, 0)$$

Die Fundamentallösungen sind nun eine Basis der Lösungsmenge des LGS (1) (in einem homogenen Gleichungssystem ist die Lösungsmenge stets ein Unterraum). Die Menge aller Lösungen von (1) ist also:

$$\langle b_1, b_2, b_3, b_4, b_5 \rangle$$
$$= \{a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4 + a_5 b_5 \mid a_1, a_2, a_3, a_4, a_5 \in K\}$$

Beispiel zur Bestimmung eines inhomogenen LGS Betrachten wir nun ein inhomogenes Gleichungssystem. Angenommen die Matrix des LGS hat, nachdem sie auf Zeilenstufenform gebracht wurde, die folgende Gestalt:

$$\left(\begin{array}{ccccccccc|c} 0 & 1 & 5 & 0 & 0 & 2 & -17 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & -4 & 0 & -7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Diese Matrix beschreibt das folgende Gleichungssystem:

$$\begin{aligned} x_2 + 5x_3 + 2x_6 - 17x_7 + 3x_8 &= 1 \\ x_4 + 2x_6 + x_7 - x_8 &= 0 \\ x_5 + 3x_7 - 4x_8 &= -7 \\ x_9 &= 8 \end{aligned} \tag{2}$$

Wie zuvor bringen wir die freien Variablen auf die rechte Seite:

$$\begin{aligned} x_2 &= 1 - 5x_3 - 2x_6 + 17x_7 - 3x_8 \\ x_4 &= 0 - 2x_6 - x_7 + x_8 \\ x_5 &= -7 - 3x_7 + 4x_8 \\ x_9 &= 8 \end{aligned}$$

Nun erhält man zunächst eine „spezielle Lösung“, in der man alle freien Variablen 0 setzt:

$$x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = -7, x_6 = 0, x_7 = 0, x_8 = 0, x_9 = 9$$
$$x = (0, 1, 0, 0, -7, 0, 0, 0, 9)$$

Um alle Lösungen des Gleichungssystems zu bekommen, löst man nun (wie oben beschrieben) das homogene LGS in dem man den Vektor b durch den Nullvektor ersetzt:

$$\left(\begin{array}{ccccccccc|c} 0 & 1 & 5 & 0 & 0 & 2 & -17 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Man erhält dann wieder einen Satz von Fundamentallösungen, in diesem Fall die Lösungen b_1, b_2, b_3, b_4, b_5 von oben. Die Lösungsmenge des Gleichungssystems (2) ist dann:

$$\begin{aligned} &x + \langle b_1, b_2, b_3, b_4, b_5 \rangle \\ &\quad = \{x + a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4 + a_5 b_5 \mid a_1, a_2, a_3, a_4, a_5 \in K\} \end{aligned}$$

Basis → *Definition 6.8*

Eine Teilmenge M eines Vektorraums V ist eine Basis von V, wenn sich jedes Element von V eindeutig als Linearkombination von paarweise verschiedenen Elementen aus M darstellen lässt.

Häufig verwendet man das folgende Kriterium: Eine Teilmenge $M \subseteq V$ ist eine Basis genau dann wenn M ein linear unabhängiges Erzeugendensystem von V ist (→ *Satz 8.3*).

Sind $v_1, \ldots, v_n \in V$, so nennt man das Vektorsystem $(v_1, \ldots, v_n)$ eine geordnete Basis von V, wenn jeder Vektor $v \in V$ eine eindeutige Darstellung als Linearkombination

$$v = a_1 v_1 + \cdots + a_n v_n \quad \text{mit } a_1, \ldots, a_n \in K$$

besitzt. Dies ist wiederum genau dann der Fall, wenn das Vektorsystem $(v_1, \ldots, v_n)$ linear unabhängig ist und V von $\{v_1, \ldots, v_n\}$ erzeugt wird.

Andere äquivalente Charakterisierungen sind: $M \subseteq V$ ist genau dann eine Basis wenn es ein minimales Erzeugendensystem oder eine maximale linear unabhängige Teilmenge ist (→ *Satz 8.3*).

Jeder Vektorraum hat eine Basis, jede linear unabhängige Menge ist Teilmenge einer Basis (Basisergänzungssatz) und jedes Erzeugendensystem enthält eine Basis (Basisauswahlsatz), siehe → *Satz 8.6*.

Eine Basis kann man als Koordinatensystem auf einem Vektorraum betrachten. Sei V ein Vektorraum mit Basis $b_1, \ldots, b_n$. Dann gibt es nach Definition eindeutige $a_1, \ldots, a_n \in K$ mit

$$v = a_1 b_1 + \cdots + a_n b_n,$$

und man bezeichnet $(a_1, \ldots, a_n) \in K^n$ als den Koordinatenvektor von v bezüglich der Basis $b_1, \ldots, b_n$. Die Abbildung $V \to K^n$, die jedem Vektor ihren Koordinatenvektor zuordnet, heißt Koordinatenabbildung. Sie ist stets ein Isomorphismus (insbesondere ist also jeder endlich erzeugte Vektorraum isomorph zu einem K^n).

Alle Basen desselben endlich erzeugten Vektorraums haben immer die gleiche Anzahl an Elementen (→ *Satz 10.2*), siehe Dimension.

geordnete Basis → *Definition 6.8*

siehe Basis.

Standardbasis → *Beispiele 6.9*

Die Standardeinheitsvektoren

$$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, 0, \ldots, 0),\ \ldots,\ e_n = (0, \ldots, 0, 1) \in K^n$$

bilden eine Basis des K^n, die Standardbasis genannt wird.

Erzeugendensystem → *Definition 7.1*

Sei V ein Vektorraum. Eine Menge M heißt Erzeugendensystem von V, wenn $\langle M \rangle = V$ (siehe lineare Hülle). Allgemeiner sagt man, dass

ein Unterraum $U \subseteq V$ von einer Menge M erzeugt wird (oder dass M ein Erzeugendensystem von U ist), wenn $\langle M \rangle = U$.

Gelegentlich nennt man auch ein Vektorsystem $(v_1, \ldots, v_n)$ ein Erzeugendensystem von U, wenn $\langle v_1, \ldots, v_n \rangle = U$.

Ein Erzeugendensystem eines Unterraums U enthält stets eine Basis von U (Basisauswahlsatz, → *Satz 8.6*), daher hat ein Erzeugendensystem immer mindestens $\dim(U)$ Elemente (siehe Dimension). Umgekehrt ist ein Erzeugendensystem mit $\dim(U)$ Elementen immer eine Basis von U.

endlich erzeugt → *Definition 7.1*

Ein Vektorraum V heißt endlich erzeugt, wenn er ein endliches Erzeugendensystem hat.

linear unabhängig → *Definition 7.3*

Eine Teilmenge $M \subset V$ eines Vektorraums V heißt linear unabhängig, wenn

$$\langle M \setminus \{x\} \rangle \neq \langle M \rangle \quad \text{für alle } x \in M.$$

Ist M nicht linear unabhängig so heißt M linear abhängig. Also ist M linear abhängig, falls es ein $x \in M$ gibt mit

$$\langle M \setminus \{x\} \rangle = \langle M \rangle.$$

(Anschaulich gesprochen ist M also linear abhängig, wenn nicht alle $x \in M$ wirklich nötig sind, um $\langle M \rangle$ zu erzeugen).

Um zu prüfen ob eine Menge linear unabhängig ist, verwendet man in der Regel die folgende Charakterisierung (→ *Satz 7.7*): M ist linear abhängig, wenn es $v_1, \ldots, v_m \in M$ und $a_1, \ldots, a_m \in K$ gibt mit

$$a_1 v_1 + \cdots + a_m v_m = 0 \quad \text{und} \quad a_i \neq 0 \text{ für ein } i \in \{1, \ldots, m\}.$$

Umgekehrt bedeutet dies, dass eine Menge M linear unabhängig ist, wenn aus

$$a_1 v_1 + \cdots + a_m v_m = 0 \quad \text{für } a_1, \ldots, a_m \in K,\ v_1, \ldots, v_m \in M$$

stets $a_1 = \cdots = a_m = 0$ folgt.

Ein Vektorsystem $(x_1, \ldots, x_n)$ heißt linear unabhängig, falls aus

$$a_1 x_1 + \cdots + a_n x_n = 0 \quad \text{für } a_1, \ldots, a_n \in K \qquad (*)$$

stets $a_1 = \cdots = a_n = 0$ folgt. Um also zu überprüfen, ob ein Vektorsystem $(x_1, \ldots, x_n)$ linear unabhängig ist, löst man das lineare Gleichungssystem $(*)$ (mit den Unbekannten $a_1, \ldots, a_n$) und überprüft ob $a_1 = \cdots = a_n = 0$ die einzige Lösung ist.

Dies ist genau dann der Fall, wenn $\text{Rang}(x_1, \ldots, x_n) = n$ ist (siehe Rang, → *Definition 9.1*).

Ein linear unabhängiges Erzeugendensystem von V heißt Basis von V. Jede linear unabhängige Menge, lässt sich zu einer Basis erweitern (Basisergänzungssatz, → *Satz 8.6*), daher kann eine linear unabhängige Menge höchstens $\dim(V)$ Elemente haben. Umgekehrt ist jede linear unabhängige Menge mit $\dim(V)$ Elementen eine Basis.

linear abhängig → *Definition 7.3*

siehe linear unabhängig.

Ordnung → *Definition 8.4*

Sei M eine Menge. Eine *Halbordnung* auf M ist eine Relation $\preceq$ auf M mit den folgenden Eigenschaften:

- Reflexivität. Für alle $x \in M$ ist $x \preceq x$.
- Transitivität. Sind $x, y, z \in M$ mit $x \preceq y$ und $y \preceq z$, so ist $x \preceq z$.
- Anti-Symmetrie. Sind $x, y \in M$ mit $x \preceq y$ und $y \preceq x$, so ist $x = y$.

Wir sagen $(M, \preceq)$ ist eine *geordnete Menge*, falls $\preceq$ eine Halbordnung auf M darstellt.

$(M, \preceq)$ heißt *total* (oder vollständig oder linear) geordnete Menge, falls zusätzlich je zwei Elemente stets *vergleichbar* sind:

$$\text{Für alle } x, y \in M \text{ ist } x \preceq y \text{ oder } y \preceq x.$$

Wir nennen $(M, \preceq)$ eine *wohlgeordnete Menge*, falls $\preceq$ eine Halbordnung auf M ist, für die zusätzlich gilt:

$$\text{Ist } X \subseteq M \text{ mit } X \neq \emptyset, \text{ so existiert } x \in X \text{ mit } x \preceq y \text{ für alle } y \in X.$$

Mit anderen Worten: In einer wohlgeordneten Menge, hat jede nichtleere Teilmenge ein kleinstes Element.

Halbordnung → *Definition 8.4*

siehe Ordnung.

total geordnet → *Definition 8.4*

siehe Ordnung.

vollständig geordnet → *Definition 8.4*

siehe Ordnung.

wohlgeordnet → *Definition 8.4*

siehe Ordnung.

Wohlordnung → *Definition 8.4*

siehe Ordnung.

Wohlordnungssatz → *Satz 8.5*

Der Zermelosche Wohlordnungssatz besagt, dass jede Menge eine Wohlordnung hat.

Der Wohlordnungssatz ist äquivalent zum Auswahlaxiom (siehe → *Lemma 2.6*).

Vektorsystem → *Definition 9.1*

Einen Tupel $(v_1, \ldots, v_n)$ von Vektoren $v_1, \ldots, v_n \in V$ in einem Vektorraum V nennt man ein Vektorsystem.

Rang eines Vektorsystems → *Definition 9.1*

Sei V ein Vektorraum und $v_1, \ldots, v_m \in V$. Der *Rang* des Vektorsystems $(v_1, \ldots, v_m)$ ist diejenige Zahl,

$$\text{Rang}(v_1, \ldots, v_m) = r \in \mathbb{N}_0,$$

für die gilt:

1. Es existiert eine linear unabhängige Teilmenge von $\{v_1, \ldots, v_m\}$, welche aus genau r Elementen besteht.
2. Jede Teilmenge von $\{v_1, \ldots, v_m\}$, welche aus mehr als r Elementen besteht, ist linear abhängig.

Mit anderen Worten, r ist die Mächtigkeit der größten linear unabhängigen Teilmenge von $\{v_1, \ldots, v_m\}$. Somit ist stets ($\rightarrow$ *Hilfssatz 10.1*)

$$0 \leq \text{Rang}(v_1, \ldots, v_m) \leq \dim(V).$$

Es ist $\text{Rang}(v_1, \ldots, v_m) = m$ genau dann, wenn das Vektorsystem $(v_1, \ldots, v_m)$ linear unabhängig ist.

Der Rang eines Vektorsystems ändert sich nicht unter elementaren Umformungen ($\rightarrow$ *Satz 9.4*). Diese Tatsache kann man verwenden, um den Rang eines Vektorsystems $(v_1, \ldots, v_m)$ konkret zu bestimmen, siehe Rangbestimmung

Rangbestimmung $\rightarrow$ *Abschnitt 9.5*

Sei V ein Vektorraum und $v_1, \ldots, v_m \in V$.

Um den Rang des Vektorsystems $(v_1, \ldots, v_m)$ zu bestimmen, übersetzt man das Vektorsystem zunächst in ein System von Koordinatenvektoren, d.h. man wählt eine feste Basis $(b_1, \ldots, b_n)$ und schreibt

$$\begin{aligned} v_1 &= a_{11}b_1 + \cdots + a_{1n}b_n \\ v_2 &= a_{21}b_1 + \cdots + a_{2n}b_n \\ &\vdots \\ v_m &= a_{m1}b_1 + \cdots + a_{mn}b_m \end{aligned}$$

Das System $(a_1, \ldots, a_m)$ der Koordinatenvektoren $a_i = (a_{i1}, \ldots, a_{in})$ hat dann denselben Rang wie $(v_1, \ldots, v_m)$. Auf $(a_1, \ldots, a_m)$ kann man nun elementare Umformungen anwenden (welches den Rang nicht ändert), bis man eine besonders einfache Form erreicht. Dazu schreibt man die Vektoren als Zeilenvektoren in eine Matrix $A = (a_{ij})$. Elementare Umformungen der Zeilenvektoren sind nun einfach Zeilenumformungen an der Matrix und der Rang des Vektorsystems $(v_1, \ldots, v_m)$ entspricht dem Zeilenrang der Matrix A.

Durch Anwenden von Zeilenumformungen und eventuell Spaltenvertauschungen (die ebenfalls den Rang der Matrix nicht ändern) kann man die Matrix A stets in die folgende Form bringen ($\rightarrow$ *Satz 9.7*):

$$\left(\begin{array}{ccc|ccc} 1 & & 0 & * & \ldots & * \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & * & \ldots & * \\ \hline 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{array}\right)$$

Der Rang dieser Matrix (und damit der Rang von A und der Rang von $(v_1, \ldots, v_m)$) ist genau die Größe des Einheitsmatrixblocks oben links.

Erlaubt man keine Spaltenvertauschungen, so kann man A durch Zeilenumformungen immer noch auf reduzierte Zeilenstufenform bringen. Der Rang der Matrix ist dann die Anzahl der Zeilen, die nicht nur Nullen enthalten.

elementare Zeilenumformungen → *Definition 9.5*

Sei $A = (a_{ij}) \in \mathrm{Mat}_{m,n}(K)$ eine $m \times n$-Matrix. Als elementare Zeilenumformungen bezeichnet man die folgenden Operationen:

(ZU1) Ersetze die i-te Zeile von A durch die Summe der i-ten Zeile und eines skalaren Vielfachen der j-ten Zeile für $i \neq j$.

(ZU2) Vertausche die i-te und die j-te Zeile von A.

(ZU3) Ersetze die i-te Zeile von A durch ein skalares Vielfaches $\neq 0$ ihrer selbst.

Ist A die Koordinatenmatrix eines Vektorsystems $(v_1, \ldots, v_m)$, so entsprechen elementare Zeilenumformungen von A elementaren Umformungen des Vektorsystems $(v_1, \ldots, v_m)$.

Elementare Zeilenumformungen ändern nicht den Rang der Matrix.

Zeilenumformung → *Definition 9.5*

siehe elementare Zeilenumformungen.

elementare Spaltenumformungen → *?*

Sei $A = (a_{ij}) \in \mathrm{Mat}_{m,n}(K)$ eine $m \times n$-Matrix. Als elementare Spaltenumformungen bezeichnet man die folgenden Operationen:

(SU1) Ersetze die i-te Spalte von A durch die Summe der i-ten Spalte und eines skalaren Vielfachen der j-ten Spalte für $i \neq j$.

(SU2) Vertausche die i-te und die j-Spalte von A.

(SU3) Ersetze die i-te Spalte von A durch ein skalares Vielfaches $\neq 0$ ihrer selbst.

Ist A die Koordinatenmatrix eines Vektorsystems $(v_1, \ldots, v_m)$ bezüglich einer Basis $(b_1, \ldots, b_n)$, so entsprechen elementare Spaltenumformungen von A elementaren Umformungen der Basis $(b_1, \ldots, b_n)$ (genauer: Geht A' aus A durch eine elementare Spaltenumformung

(SU1), (SU2) oder (SU3) hervor, so ist A' die Koordinatenmatrix von $(v_1, \ldots, v_m)$ bezüglich der Basis die aus $\mathcal{B} = (b_1, \ldots, b_n)$ hervorgeht indem man die entsprechende elementare Umformung (EU1), (EU2) oder (EU3) an $\mathcal{B}$ vornimmt).

Elementare Spaltenumformungen ändern nicht den Rang der Matrix.

Spaltenumformung → *?*

siehe elementare Spaltenumformungen.

Elementare Umformungen eines Vektorsystems → *Definition 9.3*

Eine *elementare Umformung* eines Vektorsystems $(v_1, \ldots, v_m)$ ist eine der folgenden Operationen, welche $(v_1, \ldots, v_m)$ in ein System $(v'_1, \ldots, v'_m)$ überführt:

(EU1) Ersetze ein v_i in $(v_1, \ldots, v_m)$ durch $v_i + av_j$, wobei $a \in K$ und $j \neq i$.

(EU2) Platzvertauschung von v_i und v_j in $(v_1, \ldots, v_m)$.

(EU3) Ersetze ein v_i in $(v_1, \ldots, v_m)$ durch av_i, wobei $a \in K \setminus \{0\}$.

Elementare Umformungen ändern nicht den Rang des Vektorsystems.

Genauer: Geht $(v'_1, \ldots, v'_n)$ aus $(v_1, \ldots, v_n)$ durch eine Folge von elementare Umformungen hervor, so ist $\langle v'_1, \ldots, v'_n \rangle = \langle v_1, \ldots, v_n \rangle$).

Koordinatenmatrix (eines Vektorsystems) → *Definition 9.5*

Sei V ein Vektorraum und $\mathcal{B} = (b_1, \ldots, b_n)$ eine geordnete Basis. Die Koordinatenmatrix eines Vektorsystems $(v_1, \ldots, v_m)$ bezüglich der Basis $\mathcal{B}$ ist die Matrix, die als Zeilenvektoren die Koordinatenvektoren der v_i enthält. Genauer: Jedes v_i lässt sich eindeutig als Linearkombination der $b_1, \ldots, b_n$ schreiben

$$\begin{aligned} v_1 &= a_{11}b_1 + \cdots + a_{1n}b_n \\ &\vdots \\ v_m &= a_{m1}b_1 + \cdots + a_{mn}b_n \end{aligned}$$

Die Matrix $A = (a_{ij})$ der Koeffizienten heißt dann Koordinatenmatrix des Vektorsystems $(v_1, \ldots, v_m)$ bezüglich der Basis $(b_1, \ldots, b_n)$.

Zeilenstufenform → *Übungsblatt 12*

Eine $m \times n$-Matrix $A = (a_{ij}) \in \mathrm{Mat}_{m,n}(K)$ ist in Zeilenstufenform, wenn sie von der folgenden Gestalt ist:

$$\begin{pmatrix} \boxed{1} & & & & \\ & \boxed{1} & & * & \\ & & \ddots & & \\ & 0 & & \boxed{1} & \\ & & & & \end{pmatrix}$$

mit Nullen unterhalb der Linie, und beliebigen Einträgen oberhalb (mit Ausnahme der Einsen). Formal definiert man: Eine Matrix $A = (a_{ij})$ ist in Zeilenstufenform wenn sie die folgenden beiden Bedingungen erfüllt:

(ZSF1) Ist eine Zeile von A von Null verschieden, so ist der erste von 0 verschiedene Eintrag in dieser Zeile gleich 1. Die Position dieses Eintrags heißt dann *Angelpunkt* der Zeile.

(ZSF2) Von Null verschiedene Zeilen liegen allesamt oberhalb von Nullzeilen. Sind die $i$te und $j$te Zeile von Null verschieden und $i < j$, dann erscheint der Angelpunkt der $j$ten Zeile in einer Spalte rechts von der des Angelpunktes der $i$ten Zeile.

Man sagt, dass eine Matrix in reduzierter Zeilenstufenform ist, wenn sie außerdem noch die folgende Bedingung erfüllt

(ZSF3) Alle Einträge einer Spalte, in der ein Angelpunkt liegt, sind bis auf den Eintrag 1 im Angelpunkt selbst gleich 0.

Eine Matrix in reduzierter Zeilenstufenform ist also von der Gestalt

$$\begin{pmatrix} \boxed{1} & * & 0 & * & 0 & * \\ & & \boxed{1} & * & 0 & * \\ & & & \ddots & & \\ & & 0 & & \boxed{1} & * \\ & & & & & \end{pmatrix}$$

mit Nullen oberhalb der Einsen an den Angelpunkten und ansonsten beliebigen Einträgen oberhalb der Linie.

Jede Matrix kann durch Anwenden von Zeilenumformungen auf reduzierte Zeilenstufenform gebracht werden (→ *Aufgabe 12.2*).

Dimension → *Definition 10.3*

Sei V ein endlich erzeugter K-Vektorraum über K. Dann haben alle Basen von V dieselbe Anzahl von Elementen (→ *Satz 10.2*). Diese Anzahl von Elementen einer beliebigen Basis nennt man die Dimension von V. Sie wird mit $\dim_K(V)$ oder $\dim(V)$ bezeichnet.

Die Dimension klassifiziert endlich erzeugte Vektorräume vollständig bis auf Isomorphie. Das heißt: Zwei endlich erzeugte K-Vektorräume V und W sind isomorph genau dann, wenn $\dim V = \dim W$.

Komplementärraum → *Definition 10.6*

Sei V ein Vektorraum und U ein Unterraum von V. Ein *Komplementärraum* zu U in V ist ein Unterraum W von V mit

- $U \cap W = \{0\}$
- $U + W = V$

Man schreibt dann $V = U \oplus W$ und sagt, V sei eine *direkte Summe* von U und W.

Zu jedem Unterraum U von V gibt es (wenigstens) einen Komplementärraum W in V (→ *Satz 10.8*).

direkte Summe → *Definition 10.6*

Sei V ein Vektorraum und $U, W \leq V$ Unterräume. Dann heißt V direkte Summe von U und W, geschrieben $V = U \oplus W$, wenn

$$U + W = V \quad \text{und} \quad U \cap W = \{0\},$$

d.h. wenn W ein Komplementärraum zu U ist (und umgekehrt).

Gilt bereits $V = U + W$, so folgt (→ *Korollar 10.10*) aus der Dimensionsformel für Unterräume, dass

$$V = U \oplus W \iff \dim V = \dim(U) + \dim(W).$$

Dimensionsformel für Unterräume → *Satz 10.9*

Seien U, W Unterräume eines endlich dimensionalen Vektorraums V. Dann gilt:

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W).$$

Als Folgerung hat man:

$$\dim(U \cap W) = \{0\} \iff \dim(U + W) = \dim U + \dim W.$$

Ring → *Definition 11.1*

Ein Ring $R = (R, +, \cdot)$ ist eine Menge R mit einer „Addition“

$$+ : R \times R \to R, (a, b) \mapsto a + b$$

und einer „Multiplikation“

$$\cdot : R \times R \to R, (a, b) \mapsto ab,$$

welche die folgenden Regeln erfüllen:

(A1) $+$ ist assoziativ.

$$(a + b) + c = a + (b + c) \quad \text{für alle } a, b, c \in R$$

(A2) $+$ ist kommutativ.

$$a + b = b + a \quad \text{für alle } a, b \in R$$

(A3) Es gibt ein Nullelement. D.h. es existiert ein eindeutiges Element, genannt $0 \in R$, sodass gilt

$$a + 0 = a = 0 + a \quad \text{für alle } a \in R.$$

(A4) Es gibt inverse Elemente bezüglich der Addition. D.h. es gibt zu jedem $a \in R$ ein eindeutiges Element, genannt $-a \in R$ sodass

$$a + (-a) = 0 = (-a) + a.$$

(M1) $\cdot$ ist assoziativ.

$$(ab)c = a(bc) \quad \text{für alle } a, b, c \in R$$

(D) $+$ und $\cdot$ erfüllen die Distributivgesetze.

$$\begin{matrix} a(b + c) = ab + ac \\ (a + b)c = ac + bc \end{matrix} \quad \text{für alle } a, b, c \in R$$

Im Gegensatz zu einem Körper muss ein Ring also kein neutrales Element bezüglich der Multiplikation besitzen, die Multiplikation muss nicht kommutativ sein und es müssen keine inversen Elemente bezüglich der Multiplikation existieren. Viele Ringe erfüllen jedoch trotzdem manche dieser zusätzlichen Bedingungen (siehe Ring mit 1, kommutativer Ring, Divisionsring).

kommutativer Ring → *Definition 11.1*

Ein kommutativer Ring ist ein Ring $R = (R, +, \cdot)$ in dem zusätzlich zu den anderen Ringaxiomen gilt:

(M2) $\cdot$ ist kommutativ.

$$ab = ba \quad \text{für alle } a, b \in R.$$

Ring mit 1 → *Definition 11.1*

Ein Ring mit 1 ist ein Ring $R = (R, +, \cdot)$ in dem zusätzlich zu den anderen Ringaxiomen gilt:

(M3) Es gibt ein neutrales Element der Multiplikation. D.h. es existiert ein eindeutiges Element, genannt $1 \in R$, sodass

$$a \cdot 1 = a = 1 \cdot a \quad \text{für alle } a \in R.$$

Schiefkörper → *Definition 11.1*

siehe Divisionsring.

Divisionsring → *Definition 11.1*

Ein Divisionsring ist ein Ring $R = (R, +, \cdot)$ in dem zusätzlich zu den anderen Ringaxiomen gelten:

(M3) Es gibt ein neutrales Element der Multiplikation. D.h. es existiert ein eindeutiges Element, genannt $1 \in R$, sodass

$$a \cdot 1 = a = 1 \cdot a \quad \text{für alle } a \in R.$$

(M4) Es gibt inverse Elemente der Multiplikation. D.h. zu jedem $a \in R \setminus \{0\}$ existiert ein eindeutiges Element, genannt a^{-1} oder $\frac{1}{a}$ mit

$$a\frac{1}{a} = 1 = \frac{1}{a}a.$$

Beispiele für Divisionsringe sind Körper (diese sind zusätzlich kommutativ) und der Ring der Quaternionen (der nicht kommutativ ist).

Integritätsbereich → *Definition 11.1*

Ein Integritätsbereich ist ein nullteilerfreier kommutativer Ring mit 1, der nicht nur aus der 0 besteht.

In Integritätsbereichen gilt die nützliche Kürzungsregel:

$$\text{Ist } ac = bc \text{ und } c \neq 0, \text{ so ist } a = b \ (a, b, c \in R).$$

Jeder Körper ist ein Integritätsbereich, aber auch viele andere Ringe, wie $\mathbb{Z}$ und der Polynomring $K[X]$ über einem Körper K sind Integritätsbereiche.

Quaternionen → *Beispiele 11.1*

Die HAMILTONschen Quaternionen

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

ein 4-dimensionaler $\mathbb{R}$-Vektorraum mit Basis 1, i, j, k, bilden einen Ring mit 1 unter den Verknüpfungen

$$\begin{aligned}(a + bi + cj + dk) + (a' + b'i + c'j + d'k)& \\ = (a + a') + (b + b')i + (c + c')j + (d + d')k&\end{aligned}$$

$$\begin{aligned}(a + bi + cj + dk) \cdot (a' + b'i + c'j + d'k)& \\ = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i& \\ + (ac' - bd' + ca' + db')j + (ad' + bc' - cb' + da')k.&\end{aligned}$$

In diesem Ring hat jedes Element $z \in \mathbb{H} \setminus \{0\}$ ein multiplikatives Inverses (→ *Aufgabe 9.2*), sodass $\mathbb{H}$ sogar ein Divisionsring ist. Allerdings ist $\mathbb{H}$ nicht kommutativ.

vollständige Induktion → *Definition 11.2*

Die vollständige Induktion ist eine Beweismethode um Aussagen zu beweisen, die von einer natürlichen Zahl n (oder allgemeiner: einer ganzen Zahl $n \geq n_0$ für ein $n_0 \in \mathbb{Z}$) abhängen.

Sei $n_0 \in \mathbb{Z}$, und für $n \in \mathbb{Z}$ mit $n \geq 0$ seien $\mathcal{A}_n$ mathematische Aussagen. Ferner gelte:

1. *Induktionsanfang.* Die Aussage $\mathcal{A}_{n_0}$ ist wahr.
2. *Induktionsschritt.* Für jedes $n \in \mathbb{Z}$ mit $n > n_0$ gilt: Sind sie Aussagen $\mathcal{A}_{n_0}, \mathcal{A}_{n_0+1}, \ldots, \mathcal{A}_{n-1}$ allesamt wahr (*Induktionsvoraussetzung*), so ist auch $\mathcal{A}_n$ wahr (*Induktionsschluss*).

Dann ist $\mathcal{A}_n$ für jedes $n \in \mathbb{Z}$ mit $n \geq n_0$ wahr.

Induktion → *Definition 11.2*

siehe vollständige Induktion.

Teiler → *Definition 11.3*

Sei R ein kommutativer Ring mit 1. Dann heißt a ein Teiler von b (für $a, b \in R$), wenn es ein $c \in R$ gibt mit $ac = b$. Man schreibt dann $a \mid_R b$ (oder nur $a \mid b$) und sagt „a teilt b in R“.

assoziierte Elemente → *Definition 11.3*

Sei R ein kommutativer Ring mit 1. Zwei Elemente $a, b \in R$ heißen assoziiert in R, falls $a \mid_R b$ und $b \mid_R a$ (siehe Teiler). Man schreibt dann $a \sim_R b$.

Ist R nullteilerfrei, so sind a und b genau dann assoziiert, wenn es eine Einheit $u \in R$ gibt mit $au = b$. Zwei ganze Zahlen $a, b \in \mathbb{Z}$ sind genau dann assoziiert, wenn $a = b$ oder $a = -b$. Zwei Polynome $p, q \in K[X]$ sind assoziiert genau dann, wenn es ein $a \in K \setminus \{0\}$ gibt mit $p = aq$.

Nullteiler → *Definition 11.3*

Sei R ein kommutativer Ring mit 1. Dann heißt $a \in R$ ein Nullteiler, wenn es ein $c \in R$ mit $c \neq 0$ gibt, sodass $ac = 0$.

Beispiele für nicht-triviale Nullteiler sind etwa $2, 3 \in \mathbb{Z}/6\mathbb{Z}$, da in diesem Ring gilt: $2 \cdot 3 = 6 = 0$.

Einheit → *Definition 11.3*

Sei R ein Ring mit 1. Ein $a \in R$ heißt Einheit von R (oder invertierbar), wenn es ein $b \in R$ gibt mit $ab = 1 = ba$. Man nennt dann b das Inverse von a und schreibt $b = a^{-1}$.

Die Menge aller Einheiten in R heißt Einheitengruppe und wird mit R^* bezeichnet. Sie ist eine Gruppe bezüglich der Multiplikation (siehe → *Definition 12.6*)

Einheitengruppe → *Definition 12.6*

siehe Einheit.

invertierbar → *Definition 11.3*

Allgemein heißt ein Element eines kommutativen Ringes R mit 1 invertierbar, wenn es ein $b \in R$ gibt mit $ab = 1$, siehe Einheit.

In der Linearen Algebra sind zwei Fälle besonders wichtig:

1. Ein Endomorphismus $\alpha : V \to V$ eines Vektorraums V ist invertierbar, wenn es einen Endomorphismus $\beta : V \to V$ gibt mit $\alpha\beta = \mathrm{id}_V$. Man schreibt dann $\beta = \alpha^{-1}$. Es gilt: α ist genau dann invertierbar, wenn α bijektiv (also ein Isomorphismus) ist. Aufgrund der Dimensionsformel gilt:

$$\begin{array}{ccccc} \alpha \text{ ist invertierbar} & \iff & \alpha \text{ ist injektiv} & \iff & \alpha \text{ ist surjektiv} \\ & & \Updownarrow & & \Updownarrow \\ & & \operatorname{Kern}\alpha = \{0\} & & \operatorname{Bild}\alpha = V \\ & & & & \Updownarrow \\ & & & & \operatorname{Rang}\alpha = \dim V \\ & & & & \Updownarrow \\ & & & & \det\alpha \neq 0 \end{array}$$

   Allgemeiner heißt eine beliebige lineare Abbildung $\alpha : V \to W$ zwsichen zwei Vektorräumen V und W invertierbar, wenn es ein $\beta : W \to V$ gibt mit $\alpha\beta = \mathrm{id}_V$ und $\beta\alpha = \mathrm{id}_W$. Dies ist genau dann der Fall, wenn α bijektiv also ein Isomorphismus ist (die anderen Äquivalenzen gelten in diesem Fall jedoch nicht!).

2. Eine Matrix $A \in \mathrm{Mat}_n(K)$ heißt invertierbar, wenn es eine Matrix $B \in \mathrm{Mat}_n(K)$ gibt mit $AB = \mathrm{Id}$ (wobei $\mathrm{Id} \in \mathrm{Mat}_n(K)$ die Einheitsmatrix bezeichnet). Man nennt dann $B = A^{-1}$ das Inverse von A.

Inverse (einer Matrix) → *Definition 11.3*

Ist $A \in \mathrm{Mat}_n(K)$ eine Matrix, und $B \in \mathrm{Mat}_n(K)$ sodass

$$AB = \mathrm{Id},$$

(wobei Id die Einheitsmatrix bezeichnet), so nennt man B das Inverse von A und schreibt $B = A^{-1}$.

größter gemeinsamer Teiler → *Definition 11.3*

Sei R ein kommutativer Ring mit 1. und seien $a, b \in R$. Dann heißt $d \in R$ ein größter gemeinsamer Teiler von a und b, falls

(GGT1) $d \mid a$ und $d \mid b$ (siehe Teiler).

(GGT2) Ist $t \in R$ mit $t \mid a$ und $t \mid b$ so gilt $t \mid d$.

Man schreibt dann $d = \mathrm{ggT}(a, b)$.

Im Ring der ganzen Zahlen $\mathbb{Z}$ und dem Polynomring $K[X]$ haben zwei Elemente stets einen größten gemeinsamen Teiler (→ *Satz 11.9*), den man mithilfe des euklidischen Algorithmus konkret bestimmen kann.

unzerlegbar → *Definition 11.3*

Sei R ein Integritätsbereich. Ein $a \in R$ heißt unzerlegbar, falls

- $a \neq 0$ und $a \notin R^*$ (siehe Einheit), sowie
- Sind $b, c \in R$ mit $a = bc$, so ist $b \in R^*$ oder $c \in R^*$.

Im Ring der ganzen Zahlen $\mathbb{Z}$ und dem Polynomring $K[X]$ über einem Körper K, ist ein Element genau dann unzerlegbar, wenn es prim ist.

In $\mathbb{Z}$ sind diese Elemente genau die Primzahlen (Lemma von Euklid, → *Lemma 11.13*).

irreduzibel → *Definition 11.3*

siehe unzerlegbar

prim → *Definition 11.3*

Sei R ein Integritätsbereich. Ein $a \in R$ heißt prim oder Primelement, falls

- $a \neq 0$ und $a \notin R^*$ (siehe Einheit), sowie
- Sind $b, c \in R$ mit $a \mid bc$, so gilt $a \mid b$ oder $a \mid c$ (siehe Teiler).

In $\mathbb{Z}$ ist ein $a \in \mathbb{Z}$ genau dann prim, wenn a eine Primzahl ist.

In einem Integritätsbereich ist jedes Primelement unzerlegbar.

Im Ring der ganzen Zahlen $\mathbb{Z}$ und dem Polynomring $K[X]$ über einem Körper K ist ein Element sogar *genau dann* prim, wenn es unzerlegbar ist.

Äquivalenzrelation → *Definition 11.4*

Sei $\rho \subseteq A \times A$ eine Relation auf einer Menge A. Dann heißt ρ eine *Äquivalenzrelation* auf A, falls folgende Bedingungen erfüllt sind:

(Ä1) ρ *ist reflexiv.* Für alle $a \in A$ gilt $a \rho a$.

(Ä2) ρ *ist symmetrisch.* Sind $a, b \in R$ mit $a \rho b$, so gilt auch $b \rho a$.

(Ä3) ρ *ist transitiv.* Sind $a, b, c \in R$ mit $a \rho b$ und $b \rho c$, so gilt auch $a \rho c$.

Ist ρ eine Äquivalenzrelation auf A, so heißt $\{b \in A \mid a \rho b\}$ die zu $a \in A$ gehörige *Äquivalenzklasse* bezüglich ρ. Man schreibt für die Äquivalenzklasse von a oft $[a]_\rho$ oder nur $[a]$ oder $\bar{a}$.

Zwei Äquivalenzklassen sind entweder disjunkt oder gleich (→ *Hilfssatz 11.6*), und zwar gilt $[a]_\rho = [b]_\rho$ genau dann, wenn $a \rho b$. Damit ist A die disjunkte Vereinigung der Äquivalenzklassen bezüglich ρ.

Man bezeichnet mit A/ρ die Menge aller Äquivalenzklassen bezüglich ρ:

$$A/\rho = \{[a]_\rho \mid a \in A\} = \{\{b \in A \mid a\rho b\} \mid a \in A\}.$$

Restklassenring → *Beispiel 11.5*

Sei $m \in \mathbb{N}$. Man kann auf $\mathbb{Z}$ eine Äquivalenzrelation $\equiv_m$ definieren durch

$$a \equiv_m b \iff m \mid (a - b).$$

Gilt $a \equiv_m b$, so sagt man, a und b seien „kongruent modulo m“.

Die Äquivalenzklassen sind von der Form

$$k + m\mathbb{Z} = \{k + mt \mid t \in \mathbb{Z}\} = \{\ldots, k-2m, k-m, k, k+m, k+2m \ldots\},$$

und es gilt $k + m\mathbb{Z} = k' + m\mathbb{Z}$ genau dann, wenn $k \equiv_m k'$. Man nennt diese Äquivalenzklassen „Restklassen modulo m“.

Division mit Rest zeigt, dass es für jedes $k \in \mathbb{Z}$ ein $r \in \{0, \ldots, m-1\}$ gibt mit $k \equiv_m r$. Es gibt also genau m Äquivalenzklassen, nämlich

$$0 + m\mathbb{Z},\ 1 + m\mathbb{Z},\ \ldots,\ (m-1) + m\mathbb{Z}.$$

Die Menge dieser Äquivalenzklassen bezeichnet man mit $\mathbb{Z}/m\mathbb{Z}$.

Man kann auf $\mathbb{Z}/m\mathbb{Z}$ eine Addition und Multiplikation definieren durch

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}$$
$$(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = a \cdot b + m\mathbb{Z}$$

Dies macht $\mathbb{Z}/m\mathbb{Z}$ zu einem kommutativen Ring mit 1, den man „Restklassenring modulo m“ nennt.

Für $k + m\mathbb{Z}$ schreibt man manchmal $\bar{k}$ oder (etwas ungenau) auch einfach k, wenn klar ist, über welchem Ring (also $\mathbb{Z}$ oder $\mathbb{Z}/m\mathbb{Z}$) gearbeitet werden soll. Dann kann man mit den Restklassen rechnen wie mit ganzen Zahlen, wobei man jedoch beachten muss, dass $m = 0$, und somit $k = k + m = k - m = k + 2m = \cdots$.

Die Einheiten von $\mathbb{Z}/m\mathbb{Z}$ sind genau die Restklassen $a + m\mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Alle anderen Elemente von $\mathbb{Z}/m\mathbb{Z}$, also die Restklassen $a + m\mathbb{Z}$ mit $\mathrm{ggT}(a, m) \neq 1$ sind Nullteiler in $\mathbb{Z}/m\mathbb{Z}$ (→ *Hilfssatz 11.17*).

Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper genau dann, wenn m eine Primzahl ist (→ *Satz 11.18*).

teilerfremd → *Hilfssatz 11.17*

Zwei Elemente a und b eines kommutativen Rings mit 1 heißen teilerfremd, wenn $\mathrm{ggT}(a, b) = 1$ (siehe größter gemeinsamer Teiler).

kongruent → *Beispiel 11.5*

siehe Restklassenring.

Division mit Rest → *Lemma 11.8, Lemma 13.8*

- In $\mathbb{Z}$: Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$.
- Im Polynomring $K[X]$ über einem Körper K: Seien $f, g \in K[X]$ und $f \neq 0$. Dann existieren eindeutig bestimmte Polynome $q, r \in K[X]$ mit
$$g = qf + r \text{ und } \operatorname{grad}(r) < \operatorname{grad}(f).$$

euklidischer Algorithmus → *Bemerkung 11.10*

Der euklidische Algorithmus beschreibt ein Verfahren zur Bestimmung eines größten gemeinsamen Teilers, durch sukzessive Division mit Rest.

Sind $a, b \in \mathbb{Z}$ zwei ganze Zahlen mit $b \neq 0$ (bzw. $a, b \in K[X]$ zwei Polynome über einem Körper K), so kann man eine Division mit Rest ausführen, d.h. man findet $q, r \in \mathbb{Z}$ (bzw. $q, r \in K[X]$) mit

$$a = qb + r$$

und $|r| < |b|$ (bzw. $\operatorname{grad} r < \operatorname{grad} b$). Dann ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$. Nun wiederholt man diesen Prozess (bestimme den Rest bei Division von b durch r) bis bei einer Division kein Rest bleibt. Der Rest bei der vorherigen Division ist dann der größte gemeinsame Teiler von a und b.

Formal kann man das Verfahren so beschreiben: Setze $r_{-1} = a$, $r_0 = b$. Ist $r_n \neq 0$, so definiere rekursiv r_{n+1} als den Rest bei Division von r_{n-1} durch r_n:
$$r_{n-1} = q_{n+1} r_n + r_{n+1}.$$
Ist $r_m = 0$ für ein m, so ist $\mathrm{ggT}(a, b) = r_{m-1}$.

$$r_{-1} = a \qquad r_0 = b$$

$$
\begin{aligned}
r_{-1} &= q_1 r_0 + r_1 && r_1 \neq 0 \\
r_0 &= q_2 r_1 + r_2 && r_2 \neq 0 \\
&\vdots \\
r_{m-3} &= q_m r_{m-2} + r_{m-1} && r_{m-1} \neq 0 \\
r_{m-2} &= q_{m+1} r_{m-1} + 0
\end{aligned}
$$

$$\mathrm{ggT}(a, b) = r_{m-1}$$

Bézout-Koeffizienten → *Hilfssatz 11.11*

Das Lemma von Bézout besagt: Sind $a, b \in \mathbb{Z}$ ganze Zahlen und $d = \mathrm{ggT}(a, b)$, so existieren $s, t \in \mathbb{Z}$ mit $sa + tb = d$.

Genauso gilt: Sind $a, b \in K[X]$ Polynome über einem Körper K und $d = \mathrm{ggT}(a, b)$, so existieren $s, t \in K[X]$ mit $sa + tb = d$.

Man nennt in beiden Fällen s und t Bézout-Koeffizienten. Man kann diese konkret mithilfe des euklidischen Algorithmus ermitteln.

Fundamentalsatz der Arithmetik → *Satz 11.16*

Sei $a \in \mathbb{Z} \setminus \{0\}$. Dann besitzt a eine Faktorisierung

$$a = u \cdot p_1 \cdots p_r,$$

wobei $u \subset \{1, -1\}$, $r \in \mathbb{N}_0$ und $p_1, \ldots, p_r \in \mathbb{P}$. Man nennt dann diese Faktorisierung eine Primfaktorzerlegung von a. Sie ist — bis auf die Reihenfolge der Primfaktoren — eindeutig.

Primfaktorzerlegung →

siehe Fundamentalsatz der Arithmetik.

Ringhomomorphismus → *Definition 12.1*

Ein *Homomorphismus* zwischen Ringen R und S ist eine Abbildung $\varphi : R \to S$ mit

$$(a + b)\varphi = a\varphi + b\varphi \quad \text{und} \quad (ab)\varphi = (a\varphi)(b\varphi) \quad \text{für alle } a, b \in R.$$

Sind R und S Ringe mit $1 \neq 0$, so verlangt man gewöhnlich zusätzlich $1\varphi = 1$.

Ringisomorphismus → *Definition 12.2*

Ein *Isomorphismus* zwischen Ringen R und S ist ein bijektiver Ringhomomorphismus $\varphi : R \to S$.

Besteht ein Isomorphismus $R \to S$, so heißen R und S *isomorph*, in Zeichen $R \cong S$.

Gruppe → *Definition 12.4*

Eine Gruppe $G = (G, \circ)$ ist eine Menge G mit einer Verknüpfung $\circ : G \times G \to G, (g, h) \mapsto g \circ h$, sodass gilt:

(G1) $\circ$ *ist assoziativ.* Für alle $g_1, g_2, g_3 \in G$ ist

$$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3).$$

(G2) *Es gibt ein neutrales Element.* Es existiert ein Element $e \in G$, für das gilt:

$$e \circ g = g = g \circ e \quad \text{für alle } g \in G.$$

(G3) *Es gibt Inverse bezülich* $\circ$. Zu jedem $g \in G$ existiert genau ein Element h in G, für das gilt:

$$g \circ h = e = h \circ g$$

Ist die Verknüpfung $\circ$ zusätzlich kommutativ, d.h.

$$g \circ h = h \circ g \quad \text{für alle } g, h \in G,$$

so heißt die Gruppe G *abelsch* (oder kommutativ).

Beispiele für Gruppen sind:

- $(\mathbb{Z}, +)$, die ganzen Zahlen mit Addition $+$ als Verknüpfung.
- $(\mathbb{Q}\backslash\{0\}, \cdot)$, die rationalen Zahlen ungleich Null mit Multiplikation als Verknüpfung.
- $(\mathrm{GL}_n(K), \cdot)$, die allgemeine lineare Gruppe aller invertierbaren $n \times n$-Matrizen mit Matrizenmultiplikation als Verknüpfung.
- $(\mathrm{GL}(V), \circ)$, die Menge aller invertierbaren Endomorphismen eines Vektorraums V mit Hintereinanderausführung als Verknüpfung.

Je nachdem, was die Verknüpfung in einer Gruppe ist, benutzt man meist spezielle Bezeichnungen für das neutrale Element und die inversen Elemente. Ist G eine Gruppe mit Multiplikation (oder Hintereinanderausführung von Abbildungen) als Verknüpfung, so nennt man

das neutrale Element e in (G2) in der Regel 1 und das inverse Element zu g aus (G3) g^{-1}. Ist dagegen G eine Gruppe mit Addition als Verknüpfung, so bezeichnet man das neutrale Element als 0 und das inverse Element zu g als $-g$.

In der Regel benutzt man in nicht-abelschen Gruppen als Verknüpfungssymbol die Multiplikation (und nennt somit das neutrale Element 1 und die Inversen g^{-1}), während man in abelschen Gruppen als Verknüpfungssybol oft $+$ verwendet (und dann das neutrale Element 0 und die Inversen $-g$ nennt).

Gruppenhomomorphismus → *?*

Ein Gruppenhomomorphismus ist eine Abbildung $\varphi : G \to H$ zwischen Gruppen G und H mit

$$(gh)\varphi = (g\varphi)(h\varphi).$$

abelsch → *Definition 12.4*

siehe Gruppe

Permutation → *Definition 12.7d)*

Eine Permutation einer Menge X ist eine bijektive Abbildung $X \to X$.

Die Menge aller Permutationen von X (mit der Hintereinanderausführung als Verknüpfung) bildet die symmetrische Gruppe von X.

Symmetrische Gruppe → *Definition 12.7d)*

Sei X eine Menge.

Die *symmetrische Gruppe* $\mathrm{Sym}(X)$ ist die Menge aller Permutationen von X, mit der Hintereinanderausführung als Verknüpfung

$$\mathrm{Sym}(X) = \{\pi : X \to X \mid \pi \text{ bijketiv}\}.$$

Ist $X = \{1, 2, \ldots, n\}$, so schreibt man für $\mathrm{Sym}(X)$ auch $\mathrm{Sym}(n)$ und nennt dies die *symmetrische Gruppe vom Grad n*.

Jedes Element $\pi \in \mathrm{Sym}(n)$ lässt sich eindeutig durch eine *Abbildungstafel*

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ 1\pi & 2\pi & \ldots & n\pi \end{pmatrix}$$

beschreiben. Die Identität

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

ist das neutrale Element. Das Inverse zu $\pi : X \to X$ ist die Umkehrabbildung $\pi^{-1} : X \to X$.

Transposition → *Definition 12.7d)*

Eine Permutation $\tau \in \mathrm{Sym}(n)$, die zwei Zahlen $i, j \in \{1, \ldots, n\}$, $i \neq j$, vertauscht und alle anderen festhält, heißt eine *Transposition*:

$$\tau = \begin{pmatrix} 1 & \cdots & i-1 & \boxed{i} & i+1 & \cdots & j-1 & \boxed{j} & j+1 & \cdots & n \\ 1 & \cdots & i-1 & \boxed{j} & i+1 & \cdots & j-1 & \boxed{i} & j+1 & \cdots & n \end{pmatrix}.$$

Untergruppe → *Übungslatt 9*

Sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt Untergruppe von G, wenn sie bezüglich der auf G definierten Verknüpfung selber wieder eine Gruppe ist.

Um zu überprüfen ob H eine Untergruppe ist, verwendet man in der Regel das Untergruppenkriterium: H ist eine Untergruppe genau dann, wenn

(UG1) Nicht-leer. $H \neq \emptyset$.

(UG2) Abgeschlossenheit bezüglich der Verknüpfung. Sind $x, y \in H$, so ist auch $xy \in H$.

(UG3) Abgeschlossenheit bezüglich Inversen. Ist $x \in H$, so ist auch $x^{-1} \in H$.

Man kann die letzten beiden Forderungen auch zusammenfassen als

(UG2+UG3) Sind $x, y \in H$, so ist auch $x^{-1}y$ in H.

Algebra → *Definition 13.1*

Sei K ein Körper. Eine *K-Algebra* ist ein Ring R mit 1, der gleichzeitig ein Vektorraum über K ist und für den gilt:

$$a(rs) = (ar)s = r(as) \quad \text{für alle } a \in K \text{ und } r, s \in R.$$

Ein *K-Algebrenhomomorphismus* ist eine Abbildung $\varphi : R \to S$ zwischen K-Algebren R und S, die zugleich ein Ringhomomorphismus und eine K-lineare Abbildung ist.

Polynomring → *Definition 13.1, Definition 13.5*

Sei K ein Körper. Ist R eine K-Algebra und $X \in R$ ein Element, sodass sich jedes $f \in R$ eindeutig schreiben lässt als

$$f = f_0 \cdot X^0 + f_1 \cdot X^1 + f_2 \cdot X^2 + \cdots + f_n \cdot X^n \qquad (*)$$

mit $n \in \{-\infty\} \cup \mathbb{N}_0$ und $f_0, f_1, \ldots, f_n \in K, f_n \neq 0$ so nennt man R einen Polynomring. Die Zahl n in $(*)$ heißt dann der Grad von f.

Es gibt (bis auf Isomorphie) genau einen Polynomring (→ *Folgerung 13.3*, → *Satz 13.4*), den man mit $K[X]$ bezeichnet.

Ist

$$f = f_0 \cdot X^0 + f_1 \cdot X^1 + f_2 \cdot X^2 + \cdots + f_n \cdot X^n$$

ein Polynom und $a \in K$ so setzt man

$$f(a) = f_0 + f_1 \cdot a^1 + f_2 \cdot X^2 + \cdots + f_n \cdot a^n.$$

Die Abbildung

$$\varphi_a : K[X] \to K,\ f \mapsto f(a),$$

heißt Einsetzungshomomorphismus.

Der Polynomring $K[X]$ über einem Körper K ist stets ein Integritätsbereich (→ *Lemma 13.7*) Seine Einheitengruppe besteht aus den konstanten Polynomen (also den Polynomen von Grad 0):

$$K[X]^* = \{f \in K[X] \mid \operatorname{grad} f = 0\} \cong K^*.$$

Grad (eines Polynoms) → *Definition 13.1*

Ist $f \in K[X]$ ein Polynom über K mit

$$f(X) = f_0 + f_1 X + \cdots + f_n X^n, \quad f_0, \ldots, f_n \in K, f_n \neq 0,$$

so nennt man n den Grad von f, geschrieben $\operatorname{grad} f$.

Für das Nullpolynom $f(X) = 0$, setzt man $\operatorname{grad} f = -\infty$.

Sind $f, g \in K[X]$ Polynome so gilt

$$\operatorname{grad}(f + g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\}$$

und

$$\operatorname{grad}(f + g) = \max\{\operatorname{grad} f, \operatorname{grad} g\} \quad \text{falls } \operatorname{grad} f \neq \operatorname{grad} g.$$

Außerdem gilt

$$\operatorname{grad}(fg) = \operatorname{grad} f + \operatorname{grad} g.$$

Leitterm → *Definition 13.5*

Ist $f \in K[X]$ ein Polynom (ungleich 0) über K mit

$$f(X) = f_0 + f_1 X + \cdots + f_n X^n, \quad f_0, \ldots, f_n \in K, f_n \neq 0,$$

so nennt man $f_n X^n$ den Leitterm und f_n den Leitkoeffizienten von f.

Leitkoeffizient → *Definition 13.5*

siehe Leitterm

normiert (Polynom) → *Definition 13.5*

Ist $f \in K[X]$ ein Polynom (ungleich 0) über K mit

$$f(X) = f_0 + f_1 X + \cdots + f_n X^n, \quad f_0, \ldots, f_n \in K, f_n \neq 0,$$

so nennt man f normiert, falls der Leitkoeffizient $f_n = 1$ ist.

Jedes Polynom ist assoziiert zu genau einem normierten Polynom.

Nullstelle (eines Polynoms) → *Korollar 13.9*

Ist $f \in K[X]$ ein Polynom über K

$$f(X) = f_0 + f_1 X + \cdots + f_n X^n, \quad f_0, \ldots, f_n \in K, f_n \neq 0,$$

so heißt $a \in K$ eine Nullstelle von f, falls

$$f(a) = f_0 + f_1 \cdot a^1 + f_2 \cdot X^2 + \cdots + f_n \cdot a^n = 0.$$

Ist a eine Nullstelle von f, so ist f durch $X - a$ teilbar, d.h. es ist

$$f(X) = (X - a)g(X) \quad \text{für ein } g(X) \in K[X].$$

Man nennt das größte n mit $(X-a)^n \mid f$, die Vielfachheit der Nullstelle a.

Ein Polynom von Grad n hat höchstens n Nullstellen. Genauer gilt: die Summe der Vielfachheiten aller Nullstellen ist höchstens n (→ *Korollar 13.11*).

Linearfaktor → *Definition 13.12*

Sei $f \in K[X]$ ein Polynom über K. Ein Linearfaktor von f ist ein Polynom der Form $X - a$ mit $a \in K$ welches f teilt, d.h.

$$f(X) = (X - a)g(X) \quad \text{für ein } g(X) \in K[X].$$

Es gilt: $X - a$ ist ein Linearfaktor von f genau dann, wenn a eine Nullstelle von f ist.

Man kann also die Linearfaktoren von f bestimmen indem man die Nullstellen findet. Indem man alle Nullstellen bestimmt, erhält man, dass sich f in der Form

$$f(X) = (X - a_1)^{e_1} \cdots (X - a_n)^{e_n} g(X), \quad \begin{array}{l} a_1, \ldots, a_n \in K, \\ e_1, \ldots, e_n \in \mathbb{N}, \\ g \in K[X] \end{array}$$

schreiben lässt, wobei $a_1, \ldots, a_n$ die Nullstellen von f sind und $g(X) \in K[X]$ keine weiteren Nullstellen in K hat. Diese Faktorisierung ist sogar eindeutig (→ *Korollar 13.10*).

Man sagt f zerfalle vollständig in Linearfaktoren, wenn man f schreiben kann als

$$f(X) = c(X - a_1)^{e_1} \cdots (X - a_n)^{e_n}$$

mit $c, a_1, \ldots, a_n \in K$ und $e_1, \ldots, e_n \in \mathbb{N}$.

lineare Abbildung → *Definition 14.1*

Seien V und W K-Vektorräume. Eine Abbildung $\vartheta : V \to W$ heißt K-lineare Abbildung (oder nur „lineare Abbildung“, wenn klar ist, welcher Körper gemeint ist), falls gilt

(LA1) $(u + v)\vartheta = u\vartheta + v\vartheta$ für alle $u, v \in V$-

(LA2) $(av)\vartheta = a(v\vartheta)$ für alle $a \in K$ und $v \in V$.

Äquivalent zu diesen beiden Bedingungen ist die einzelne Bedingung

$$(au + v)\vartheta = a(u\vartheta) + v\vartheta \quad \text{für alle } a \in K \text{ und } u, v \in V.$$

Die Menge aller K-linearen Abbildungen von V nach W bezeichnet man mit

$$\mathrm{Hom}_K(V, W) = \{\vartheta \mid \vartheta : V \to W \text{ linear}\}.$$

Sind $\varphi : U \to V$ und $\psi : V \to W$ lineare Abbildungen zwischen K-Vektorräumen U, V und W, so ist auch die Hintereinanderausführung $\varphi\psi : U \to W, u \mapsto (u\varphi)\psi$ linear (→*Lemma 14.9*).

Vektorraumhomomorphismus → *lineare Abbildung*

Monomorphismus → *Definition 14.1*

Eine →*lineare Abbildung* $\vartheta : V \to W$ heißt Monomorphismus, wenn sie injektiv ist. Das ist genau dann der Fall, wenn $\mathrm{Kern}(\vartheta) = \{0\}$ (siehe Kern, →*Hilfssatz 14.7*).

Epimorphismus → *Definition 14.1*

Eine lineare Abbildung $\vartheta : V \to W$ heißt Epimorphismus, wenn sie surjektiv ist. Das ist genau dann der Fall, wenn $\mathrm{Rang}\,\vartheta = \dim W$ (Rang, →*Hilfssatz 16.7*).

Endomorphismus → *Definition 14.1*

Eine K-lineare Abbildung $\alpha : V \to V$ von einem Vektorraum V in sich heißt Endomorphismus. Die Menge aller Endomorphismen von V bezeichnet man mit

$$\mathrm{End}_K(V) = \mathrm{Hom}_K(V, V) = \{\vartheta \mid \vartheta : V \to V \text{ linear}\}.$$

Man kann auf $\mathrm{End}_K(V)$ eine Addition und Skalarmultiplikation definieren, indem man für $\varphi, \psi \in \mathrm{End}_K(V)$ und $a \in K$ setzt:

$$v(\varphi + \psi) = v\varphi + v\psi$$
$$v(a\varphi) = a(v\varphi)$$

Mit diesen Operationen wird $\mathrm{End}_K(V)$ selber zu einem K-Vektorraum (→*Definition/Satz 14.14*).

Mit der obigen Addition und der Hintereinanderausführung als „Multiplikation“ erhält $\mathrm{End}_K(V)$ zudem die Struktur eines Rings mit Nullelement $V \to V, v \mapsto 0$ und Einselement $\mathrm{id}_V : V \to V, v \mapsto v$. Ist $V \neq \{0\}$, so wird $\mathrm{End}_K(V)$ auf dieses Weise zu einer K-Algebra.

Isomorphismus (von Vektorräumen) → *Definition 14.1*

Eine lineare Abbildung $\vartheta : V \to W$, die bijektiv ist, heißt Isomorphismus. In diesem Fall ist die Umkehrabbildung $\vartheta^{-1} : W \to V$ ebenfalls linear.

Einen Isomorphismus $\vartheta : V \to V$ eines Vektorraums in sich bezeichnet man als Automorphismus.

isomorph → *Defintion 14.1*

- Zwei Vektorräume V und W heißen isomorph, falls es einen Isomorphismus $\vartheta : V \to W$ gibt. Äquivalent dazu ist: V und W sind isomorph, falls es lineare Abbildungen $\vartheta : V \to W$ und $\vartheta' : W \to V$ gibt mit $\vartheta\vartheta' = \mathrm{id}_V$ und $\vartheta'\vartheta = \mathrm{id}_W$. Man schreibt dann $V \cong W$.
- Zwei Ringe R und S heißen isomorph falls es einen Ringisomorphismus $R \to S$ gibt. Äquivalent dazu ist: R und S sind isomorph falls es Ringhomomorphismen $\varphi : R \to S$ und $\psi : S \to R$ gibt mit $\varphi\psi = \mathrm{id}_R$ und $\psi\varphi = \mathrm{id}_S$.

Homothetie → *Beispiel 14.2*

Ist V ein K-Vektorraum und $a \in K$ so nennt man die Abbildung

$$\mu_a : V \to V,\ v \mapsto av$$

eine Homothetie. Diese sind stets lineare Abbildungen.

Kern → *Definition/Satz 14.3*

Der Kern einer linearen Abbildung $\vartheta : V \to W$ ist die Menge

$$\mathrm{Kern}(\vartheta) = \{v \in V \mid v\vartheta = 0\}.$$

Der Kern von ϑ ist stets ein Unterraum von V.

Um den Kern einer linearen Abbildung ϑ konkret zu bestimmen, wählt man zunächst Basen $\mathcal{B} = (v_1, \ldots, v_m)$ von V und $\mathcal{C} = (w_1, \ldots, w_m)$ von W und ermittelt die Koordinatenmatrix $A = [\vartheta]_{\mathcal{B},\mathcal{C}} = (a_{ij})$ von ϑ. Nun löst man

das lineare Gleichungssystem

$$xA = 0 \iff \begin{array}{c} a_{11}x_1 + \cdots + a_{m1}x_m = 0 \\ \vdots \\ a_{1n}x_1 + \cdots + a_{mn}x_m = 0 \end{array} \qquad (*)$$

Aus den Lösungen des LGS erhält man nun den Kern von ϑ: Es gilt

$$x = (x_1, \ldots, x_m) \text{ ist eine Lösung von } (*) \iff x_1b_1 + \cdots + x_mb_m \in \mathrm{Kern}\,\vartheta.$$

Rang (einer linearen Abbildung) → *Definition 14.4*

Der Rang einer linearen Abbildung $\vartheta : V \to W$ ist die Dimension des Bildes von ϑ (man beachte, dass das Bild einer linearen Abbildung stets ein Unterraum ist):

$$\mathrm{Rang}(\vartheta) = \dim \mathrm{Bild}(\vartheta).$$

Ist $(v_1, \ldots, v_m)$ ein beliebiges Erzeugendensystem von V, so ist der Rang von ϑ der Rang des Vektorsystems $(v_1\vartheta, \ldots, v_m\vartheta)$.

Ist $T = [\vartheta]_{\mathcal{B},\mathcal{C}}$ die Koordinatenmatrix von ϑ bezüglich Basen $\mathcal{B}$ von V und $\mathcal{C}$ von W, so ist $\mathrm{Rang}\,\vartheta = \mathrm{Rang}\,T$ (Rang einer Matrix, →*Beobachtung 15.6*).

Dimensionsformel für lineare Abbildungen → *Satz 14.6*

Ist $\vartheta : V \to W$ eine lineare Abbildung, so gilt

$$\dim \mathrm{Kern}(\vartheta) + \dim \mathrm{Bild}(\vartheta) = \dim V.$$

Automorphismus → *Korollar 14.8*

Eine lineare Abbildung $\vartheta : V \to V$ von einem Vektorraum V in sich, die bijektiv ist, heißt Automorphismus.

Die Menge aller Automorphismen eines Vektorraums V bezeichnet man mit

$$\mathrm{GL}(V) = \{\vartheta \in \mathrm{End}_K(V) \mid \vartheta \text{ Isomorphismus}\}.$$

Diese Menge bildet eine Gruppe mit der Komposition von Abbildungen als Verknüpfung.

Basisabbildung → *Definition 14.10*

Ist V ein K-Vektorraum mit einer endlichen Basis $\mathcal{B} = (v_1, \ldots, v_n)$, so heißt die Abbildung

$$\iota_{\mathcal{B}} : K^n \to V,\ (x_1, \ldots, x_n) \mapsto x_1 v_1 + \cdots + x_n v_n$$

die zu $\mathcal{B}$ gehörige Basisabbildung. Diese Abbildung ist stets ein Isomorphismus. Das Inverse ist die entsprechende Koordinatenabbildung.

Koordinatenabbildung → *Definition 14.10*

Ist V ein K-Vektorraum mit einer endlichen Basis $\mathcal{B} = (v_1, \ldots, v_n)$, so lässt sich jeder Vektor $x \in V$ auf eindeutige Weise in der Form

$$x = x_1 v_1 + \cdots + x_n v_n, \quad \text{mit } x_1, \ldots, x_n \in K$$

schreiben. Man nennt dann $(x_1, \ldots, x_n) \in K^n$ den Koordinatenvektor von x (bezüglich $\mathcal{B}$). Die Abbildung

$$\gamma_{\mathcal{B}} : V \to K^n,\ x \mapsto (x_1, \ldots, x_n),$$

die jedem Vektor in V ihren Koordinatenvektor in K^n zuordnet, heißt die zu $\mathcal{B}$ gehörige Koordinatenabbildung.

Sie ist stets ein Isomorphismus, das Inverse ist die zu $\mathcal{B}$ gehörige Basisabbildung.

Matrix → *Definition 15.1*

Eine $m \times n$-Matrix $T = (t_{ij})$ über einem Körper K ist eine Sammlung von Einträgen t_{ij} mit $1 \leq i \leq m$ und $1 \leq j \leq n$. Man schreibt diese dann oft in der Form

$$T = \begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ t_{m1} & \cdots & \cdots & t_{mn} \end{pmatrix}.$$

und sagt T habe m Zeilen und n Spalten. Man bezeichnet

$$(t_{11}, \ldots, t_{1n}), \quad \ldots, \quad (t_{m1}, \ldots, t_{mn})$$

als die Zeilenvektoren und

$$\begin{pmatrix} t_{11} \\ \vdots \\ t_{m1} \end{pmatrix}, \ldots, \begin{pmatrix} t_{1n} \\ \vdots \\ t_{mn} \end{pmatrix}$$

als die Spaltenvektoren von T.

Formal kann man eine $m \times n$-Matrix über K als Abbildung

$$T : \{1, \ldots, m\} \times \{1, \ldots, n\} \to K$$

betrachten, wobei dann $T(i, j)$ dem Eintrag t_{ij} entspricht.

Die Menge aller $m \times n$-Matrizen über K bezeichnet man mit $\mathrm{Mat}_{m,n}(K)$. Im Fall $m = n$ schreibt man auch einfach $\mathrm{Mat}_n(K) = \mathrm{Mat}_{n,n}(K)$.

Man kann Matrizen addieren und mit Skalaren multiplizieren: Für $S = (s_{ij}), T = (t_{ij}) \in \mathrm{Mat}_{m,n}(K)$ definiert man

$$S + T = (s_{ij} + t_{ij})$$

und für $T = (t_{ij}) \in \mathrm{Mat}_{m,n}(K)$ und $a \in K$ definiert man

$$aT = (at_{ij}).$$

Mit diesen beiden Verknüpfungen wird $\mathrm{Mat}_{m,n}(K)$ zu einem K-Vektorraum mit der Nullmatrix als Nullelement.

Matrizen sind in der Linearen Algebra vor allem deshalb enorm wichtig, da sie verwendet werden können um lineare Abbildungen zu repräsentieren und mit ihnen zu rechnen: Ist $A \in \mathrm{Mat}_{m,n}(K)$, so ist die Abbildung $K^m \to K^n, v \mapsto vA$ eine lineare Abbildung. Ist umgekehrt $\vartheta : V \to W$ eine lineare Abbildung zwischen endlich dimensionalen K-Vektorräumen so kann man ϑ (nach Wahl von Basen in V und W) durch eine Matrix über K repräsentieren (siehe Koordinatenmatrix).

Nullmatrix → *Definition 15.1*

Die Matrix $T = (t_{ij}) \in \mathrm{Mat}_{m,n}(K)$ mit $t_{ij} = 0$ für alle i und j heißt Nullmatrix.

Transponierte → *Definition 15.1*

Ist $A = (a_{i,j}) \in \mathrm{Mat}_{m,n}(K)$ eine $m \times n$-Matrix, so heißt die $m \times n$-Matrix $A^{\mathrm{tr}} = (a'_{i,j}) \in \mathrm{Mat}_{m,n}(K)$ mit $a'_{i,j} = a_{j,i}$ die Transponierte von A.

Matrizenmultiplikation → *Definition 15.3*

Ist $S = (s_{ij}) \in \mathrm{Mat}_{l,m}(K)$ eine $l \times m$-Matrix und $T = (t_{ij}) \in \mathrm{Mat}_{m,n}(K)$ eine $m \times n$-Matrix, so können wir das Produkt von S und T definieren (→*Definition 15.3*) durch

$$ST = (a_{ij}) \in \mathrm{Mat}_{l,m}(K), \quad \text{mit } a_{ij} = \sum_{k=1}^{m} s_{ik} t_{kj}.$$

Mit dieser Multiplikation und der zuvor definierten Addition wird $\mathrm{Mat}_n(K)$ zu einem Ring mit der Einheitsmatrix als Einselement. In Verbindung mit der Vektorraumstruktur ist $\mathrm{Mat}_n(K)$ sogar eine K-Algebra.

Koordinatenmatrix (einer linearen Abbildung) → *Definition 15.2*

Sei $\vartheta : V \to W$ eine lineare Abbildung zwsichen K-Vektorräumen V und W und $\mathcal{B} = (v_1, \ldots, v_m)$ bzw. $\mathcal{C} = (w_1, \ldots, w_n)$ Basen von V bzw. W. Für gewisse eindeutig festgelegte $t_{ij} \in K$ ist dann

$$\begin{aligned} v_1\vartheta &= t_{11}w_1 + \cdots + t_{1n}w_n \\ &\vdots \\ v_m\vartheta &= t_{m1}w_1 + \cdots + t_{mn}w_n \end{aligned} \qquad (*)$$

Die Matrix

$$T = (t_{ij}) \in \mathrm{Mat}_{m,n}(K)$$

heißt dann Koordinatenmatrix von ϑ bezüglich der Basen $\mathcal{B}$, $\mathcal{C}$ (sie ist die Koordinatenmatrix des Vektorsystems $(v_1\vartheta, \ldots, v_m\vartheta)$ bezüglich der Basis $\mathcal{C}$). Man schreibt

$$T = [\vartheta]_{\mathcal{B},\mathcal{C}}.$$

Umgekehrt ist die Abbildung durch die Koeffizienten t_{ij} eindeutig bestimmt, d.h. für gegebene $t_{ij} \in K$ gibt es genau eine lineare Abbildung

$\vartheta : V \to W$ die $(*)$ erfüllt. Somit ist die Abbildung die jeder linearen Abbildung $\vartheta : V \to W$ ihre Koordinatenmatrix zuordnet

$$\Phi : \mathrm{Hom}_K(V, W) \to \mathrm{Mat}_{m,n}(K),\ \vartheta \mapsto [\vartheta]_{\mathcal{B},\mathcal{C}}$$

eine bijektive Abbildung.

Die Koordinatenmatrix $[\vartheta]_{\mathcal{B},\mathcal{C}}$ hängt von der Wahl der Basen ab. Andere Wahlen von Basen führen zu äquivalenten Matrizen. Man kann die Koordinatenmatrix $[\vartheta]_{\mathcal{B}',\mathcal{C}'}$ bezüglich anderer Basen $\mathcal{B}'$ und $\mathcal{C}'$ aus $[\vartheta]_{\mathcal{B},\mathcal{C}}$ mithilfe der Tranformationsformel ermitteln.

Für lineare Abbildungen $\vartheta, \vartheta' : V \to W$ und $a \in K$ gilt:

$$\begin{aligned}[\vartheta + \vartheta']_{\mathcal{B},\mathcal{C}} &= [\vartheta]_{\mathcal{B},\mathcal{C}} + [\vartheta']_{\mathcal{B},\mathcal{C}} \\ [a\vartheta]_{\mathcal{B},\mathcal{C}} &= a[\vartheta]_{\mathcal{B},\mathcal{C}},\end{aligned}$$

d.h. Addition und Skalarmultiplikation von linearen Abbildungen entspricht der Addition und Skalarmultiplikation der Koordinatenmatrizen. Somit ist Φ sogar eine lineare Abbildung zwischen K-Vektorräumen, also ein Isomorphismus.

Ist $\vartheta : V \to W$ eine lineare Abbildung, $\mathcal{B} = (v_1, \ldots, v_m)$ eine Basis von V und $\mathcal{C} = (w_1, \ldots, w_m)$ eine Basis von W und $T := [\vartheta]_{\mathcal{B},\mathcal{C}}$ die Koordinatenmatrix, so gilt

$$\gamma_{\mathcal{B}} \mu_T \iota_{\mathcal{C}} = \vartheta,$$

wobei $\gamma_{\mathcal{B}}$ die zu $\mathcal{B}$ gehörige Koordinatenabbildung und $\iota_{\mathcal{C}}$ die zu $\mathcal{C}$ gehörige Basisabbildung ist (→*Hilfssatz 15.11*). Mit anderen Worten: Man kann $x\vartheta$ zu einem $x \in V$ mithilfe der Matrix T bestimmen. Dazu ermittelt man zunächst eine Koordinatendarstellung von x als

$$x = x_1 v_1 + \cdots + x_n v_n,$$

und multipliziert dann den Zeilenvektor $\gamma_{\mathcal{B}}(v) = (x_1, \ldots, x_n)$ mit der Matrix T:

$$(x_1, \ldots, x_n)T = (y_1, \ldots, y_n).$$

Schließlich ist

$$x\vartheta = \iota_{\mathcal{C}}(y_1, \ldots, y_n) = y_1 w_1 + \cdots + y_n w_n.$$

Sind U, V und W drei K-Vektorräume mit endlichen geordneten Basen $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, und $\vartheta : U \to V$ sowie $\vartheta' : V \to W$ zwei lineare Abbildungen, so ist

$$[\vartheta\vartheta']_{\mathcal{A},\mathcal{C}} = [\vartheta]_{\mathcal{A},\mathcal{B}} \cdot [\vartheta']_{\mathcal{B},\mathcal{C}}.$$

Die Komposition von Abbildungen entspricht also der Multiplikation der Koordinatenmatrizen.

Zeilenrang → *Definition 15.4*

Ist $T = (t_{ij}) \in \mathrm{Mat}_{m,n}(K)$ eine Matrix mit Zeilenvektoren

$$z_1 = (t_{11}, \ldots, t_{1n}), \quad \ldots, \quad z_m = (t_{m1}, \ldots, t_{mn}) \in K^n,$$

so nennt man

$$\mathrm{Rang}(z_1, \ldots, z_m) = \dim(\langle z_1, \ldots, z_m \rangle)$$

den Zeilenrang von T.

Der Zeilenrang ist stets gleich dem Spaltenrang (→*Satz/Definition 15.9*), und wird daher oft auch einfach als Rang der Matrix bezeichnet.

Spaltenrang → *Definition 15.4*

Ist $T = (t_{ij}) \in \mathrm{Mat}_{m,n}(K)$ eine Matrix mit Spaltenvektoren (betrachtet als Vektoren im K^m)

$$s_1 = (t_{11}, \ldots, t_{m1}), \quad \ldots, \quad s_m = (t_{1n}, \ldots, t_{mn}) \in K^m,$$

so nennt man

$$\mathrm{Rang}(s_1, \ldots, s_m) = \dim(\langle s_1, \ldots, s_m \rangle)$$

den Spaltenrang von T.

Der Spaltenrang ist stets gleich dem Zeilenrang (→*Satz/Definition 15.9*), und wird daher oft auch einfach als Rang der Matrix bezeichnet.

Rang (einer Matrix) → *Satz/Definition 15.9*

siehe Zeilenrang, Spaltenrang.

Standardbilinearform → *Definition 15.5*

Sei $V = K^m$ der Standardvektorraum. Die Abbildung $K^m \times K^m \to K$,

$$((x_1, \ldots, x_m), (y_1, \ldots, y_m)) \mapsto (x_1, \ldots, x_m) \cdot (y_1, \ldots, y_m) := \sum_{i=1}^{m} x_i y_i$$

heißt Standardbilinearform auf $V = K^m$. Sind $v, w \in V$ mit $v \cdot w = 0$, so sagen wir, v steht senkrecht auf w, i.z. $v \perp w$. Für $M \subseteq V$ setzen wir

$$M^\perp = \{w \in V \mid \forall v \in M,\ v \perp w\}.$$

$\mathrm{M}_m(K)$ als K-algebra → *Korollar/Def. 15.12*

Betrachten wir den Spezialfall von Endomorphismen eines Vektorraums V, so hat $\mathrm{End}_K(V)$ genauso wie $\mathrm{Mat}_m(K)$ die Struktur einer K-Algebra (siehe Endomorphismus und Matrix). Für eine fest gewählte Basis $\mathcal{B}$ von V ist die zuvor definierte Abbildung

$$\Phi : \mathrm{End}_K(V) \to \mathrm{Mat}_m(K),\ \vartheta \mapsto [\vartheta]_{\mathcal{B}}$$

ein K-Algebra-Isomorphismus (→*Korollar/Definition 15.8*), also eine bijektive Abbildung, die alle drei Verknüpfungen (Addition, Skalarmultiplikation, Komposition/Multiplikation) erhält:

$$\begin{aligned}[\vartheta + \vartheta']_{\mathcal{B}} &= [\vartheta]_{\mathcal{B}} + [\vartheta']_{\mathcal{B}} \\ [a\vartheta]_{\mathcal{B}} &= a[\vartheta]_{\mathcal{B}} \\ [\vartheta \circ \vartheta']_{\mathcal{B}} &= [\vartheta]_{\mathcal{B}} \cdot [\vartheta']_{\mathcal{B}}\end{aligned}$$

Unter diesem Isomorphismus korrespondiert die Automorphismengruppe $\mathrm{GL}(V)$ zu der allgemeinen linearen Gruppe $\mathrm{GL}_m(K)$.

allgemeine lineare Gruppe → *Korollar/Definition 15.12*

Die allgemeine lineare Gruppe vom Rang n ist die Menge der invertierbaren $n \times n$-Matrizen

$$\begin{aligned}\mathrm{GL}_n(K) &= \{A \in \mathrm{Mat}_n(K) \mid A \text{ invertierbar}\} \\ &= \{A \in \mathrm{Mat}_n(K) \mid \mathrm{Rang}\, A = n\} \\ &= \{[\alpha]_{\mathcal{B},\mathcal{B}} \mid \alpha \in \mathrm{GL}(V)\}\end{aligned}$$

wobei in der letzten Zeile V ein beliebiger Vektorraum von Dimension n mit einer Basis $\mathcal{B}$ ist.

Mit der Matrixmultiplikation bildet $\mathrm{GL}_n(K)$ eine Gruppe (mit die Einheitsmatrix als neutrales Element)

Einheitsmatrix → *Korollar/Definition 15.12*

Die Einheitsmatrix $\mathrm{Id} = (a_{ij}) \in \mathrm{Mat}_n(K)$ ist die Matrix mit $a_{ij} = 0$ für $i \neq j$ und $a_{ij} = 1$ für $i = j$. Sie hat also die Gestalt

$$\mathrm{Id} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Die Einheitsmatrix hat die Eigenschaft, dass für alle $A \in \mathrm{Mat}_{n,k}(K)$ und $B \in \mathrm{Mat}_{m,n}(K)$ gilt

$$\begin{aligned} \mathrm{Id} \cdot A &= A && \text{für alle } A \in \mathrm{Mat}_{n,k}(K) \\ B \cdot \mathrm{Id} &= B && \text{für alle } B \in \mathrm{Mat}_{m,n}(K) \end{aligned}$$

Assoziierte lineare Abbildung einer Matrix → *Def. 15.13*

Für $A \in \mathrm{Mat}_{m,n}(K)$ bezeichne

$$\begin{aligned} \mu_A : K^m \to K^m,\ (x_1, \ldots, x_m) \mapsto (x_1, \ldots, x_m)A \\ = \left(\sum_{j=1}^{m} x_j a_{j1}, \ldots, \sum_{j=1}^{m} x_j a_{jn} \right) \end{aligned}$$

die lineare Abbildung zwischen Standardvektorräumen, die durch Multiplikation mit A gegeben ist. Es gilt dann $[\mu_A]_{\mathcal{E}} = A$.

Transformationsformel für lineare Abbildungen → *Satz 15.15*

Seien V und W endlich-dimensionale K-Vektorräume und $\alpha : V \to W$ eine lineare Abbildung. Die Transformationsformel beschreibt, wie die Koordinatenmatrizen von α bezüglich verschiedener Wahlen von Basen in V und W miteinander in Beziehung stehen und wie man, gegeben eine Koordinatenmatrix bezüglich einer Wahl von Basen, die Koordinatenmatrix bezüglich einer anderen Wahl von Basen gewinnen kann.

Seien $\mathcal{B} = (v_1, \ldots, v_m)$ und $\mathcal{B}' = (v'_1, \ldots, v'_m)$ zwei Wahlen von Basen von V sowie $\mathcal{C} = (w_1, \ldots, w_n)$ und $\mathcal{C}' = (w'_1, \ldots, w'_n)$ zwei Wahlen von Basen von W. Wir können dann zu beiden Wahlen jeweils die Koordinatenmatrizen betrachten:

$$\begin{aligned} A &= [\vartheta]_{\mathcal{B},\mathcal{C}} \in \mathrm{Mat}_{m,n}(K) \\ A' &= [\vartheta]_{\mathcal{B}',\mathcal{C}'} \in \mathrm{Mat}_{m,n}(K) \end{aligned}$$

Die Transformationsformel besagt, dass

$$A' = SAT \quad \text{wobei} \quad \begin{aligned} S &= [\iota_{\mathcal{B}'} \gamma_{\mathcal{B}}]_{\mathcal{E},\mathcal{E}} \in \mathrm{Mat}_m(K) \\ T &= [\iota_{\mathcal{C}} \gamma_{\mathcal{C}'}]_{\mathcal{F},\mathcal{F}} \in \mathrm{Mat}_n(K) \end{aligned}.$$

Hier sind $\mathcal{E}$ und $\mathcal{F}$ die Standardbasen in K^m bzw. K^n. Konkret kann man S und T bestimmen indem man jeweils die Vektoren der Basis $\mathcal{B}'$

als Linearkombinationen in der Basis $\mathcal{B}$ ausdrückt

$$\begin{aligned} v_1' &= s_{11}v_1 + \cdots + s_{1m}v_m \\ &\vdots \\ v_m' &= s_{m1}v_1 + \cdots + s_{mm}v_m \end{aligned}$$

und die Vektoren der Basis $\mathcal{C}$ in der Basis $\mathcal{C}'$:

$$\begin{aligned} w_1 &= t_{11}w_1' + \cdots + t_{1n}w_n \\ &\vdots \\ w_n &= t_{n1}w_1' + \cdots + t_{nn}w_n' \end{aligned}$$

Dann ist $S = (s_{ij})$ und $T = (t_{ij})$.

Die Matrizen S und T heißen Übergangsmatrizen (von $\mathcal{B}'$ auf $\mathcal{B}$ bzw. von $\mathcal{C}$ auf $\mathcal{C}'$) und sind stets invertierbar. Somit sind A und A' äquivalente Matrizen.

In dem Fall, dass $\alpha : V \to V$ ein Endomorphismus ist, betrachtet man in der Regel Koordinatenmatrizen $[\alpha]_{\mathcal{B},\mathcal{B}}$ bezüglich einer Basis $\mathcal{B}$ (anstelle von $[\alpha]_{\mathcal{B},\mathcal{C}}$ für zwei verschiedene Basen $\mathcal{B}$ und $\mathcal{C}$ von V). Für diesen Fall beschreibt die Transformationsformel für Endomorphismen wie diese Koordinatenmatrizen zueinander in Beziehung stehen.

äquivalente Matrizen → *Definition/Satz 15.16*

Zwei Matrizen $A, B \in \mathrm{Mat}_{m,n}(K)$ heißen äquivalent falls

$$B = SAT \quad \text{für gewisse } S \in \mathrm{GL}_m(K) \text{ und } T \in \mathrm{GL}_n(K).$$

Man schreibt dann $A \sim B$. Dies definiert eine Äquivalenzrelation auf $\mathrm{Mat}_{m,n}(K)$.

Zwei Matrizen sind genau dann äquivalent, wenn sie dieselbe lineare Abbildung $\alpha : V \to W$ bezüglich verschiedener Wahlen von Basen in V und W repräsentieren (siehe Koordinatenmatrix, Transformationsformel).

Jede Matrix ist äquivalent zu genau einer Matrix der Form

$$\left(\begin{array}{cccc|ccc} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{array}\right),$$

wobei die Anzahl der Einsen dem Rang der Matrix entspricht (→*Satz 15.17*).

Transformationsformel für Endomorphismen → *Satz 15.18*

Sei V ein endlich-dimensionaler K-Vektorraum und $\alpha : V \to V$ ein Endomorphismus. Die Transformationsformel für Endomorphismen beschreibt, wie die Koordinatenmatrizen $[\alpha]_{\mathcal{B},\mathcal{B}}$ von α bezüglich verschiedener Wahlen von Basen $\mathcal{B}$ in V zueinander in Beziehung stehen und wie man, gegeben eine Koordinatenmatrix bezüglich einer Basis, die Koordinatenmatrix bezüglich einer anderen Basis gewinnen kann.

Seien $\mathcal{B} = (v_1, \ldots, v_m)$ und $\mathcal{B}' = (v'_1, \ldots, v'_m)$ zwei Basen von V und

$$A = [\alpha]_{\mathcal{B},\mathcal{B}} \in \mathrm{Mat}_m(K)$$
$$A' = [\alpha]_{\mathcal{B}',\mathcal{B}'} \in \mathrm{Mat}_m(K)$$

die Koordinatenmatrizen von α bezüglich $\mathcal{B}$ bzw. $\mathcal{B}'$.

Die Transformationsformel besagt dann, dass

$$A' = T^{-1}AT \quad \text{mit } T = [\iota_{\mathcal{B}}\gamma_{\mathcal{B}'}]_{\mathcal{E},\mathcal{E}}$$

ist, wobei $\mathcal{E}$ die Standardbasis von K^m bezeichnet. Konkret erhält man T indem man die Vektoren der Basis $\mathcal{B}$ als Linearkombinationen in der Basis $\mathcal{B}'$ ausdrückt:

$$\begin{aligned} v_1 &= t_{11}v'_1 + \cdots + t_{1m}v'_m \\ &\vdots \\ v_m &= t_{m1}v'_1 + \cdots + t_{mm}v'_m \end{aligned}$$

Dann ist $T = (t_{ij})$.

Die Matrix T heißt Übergangsmatrix von $\mathcal{B}$ auf $\mathcal{B}'$ und ist stets invertierbar. Somit sind A und A' ähnliche Matrizen.

ähnliche Matrizen → *Definition/Satz 15.19*

Zwei Matrizen $A, B \in \mathrm{Mat}_m(K)$ heißen ähnlich, falls

$$B = T^{-1}AT \quad \text{für ein } T \in \mathrm{GL}_m(K).$$

Man schreibt dann $A \approx B$. Dies definiert eine Äquivalenzrelation auf $\mathrm{Mat}_m(K)$.

Ähnliche Matrizen sind stets äquivalent, aber die Umkehrung gilt im allgemeinen nicht.

Determinantenabbildung → *Definition 16.1*

Eine Determinantenabbildung auf $\mathrm{Mat}_n(K)$ ist eine Abbildung $\delta : \mathrm{Mat}_n(K) \to K$ mit den folgenden Eigenschaften:

(DET1) Linear in jeder Zeile: Für jedes i ist

$$\delta \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ ba_{i1} + a'_{i1} & \cdots & ba_{in} + a'_{in} \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$
$$= b\delta \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} + \delta \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a'_{i1} & \cdots & a'_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

(DET2) Alternierend: Besitzt $A \in \mathrm{Mat}_n(K)$ zwei gleiche Zeilen, so ist $\delta(A) = 0$.

(DET3) Normiert: Bezeichnet $\mathrm{Id} \in \mathrm{Mat}_n(K)$ die Einheitsmatrix, so ist $\delta(\mathrm{Id}) = 1$.

Obwohl aus der Definition nicht sofort ersichtlich ist, dass es Determinantenabbildungen überhaupt gibt, stellt sich dann heraus, dass (für gegebenes n und K) *genau eine* Determinantenabbildung existiert (→*Satz 16.9*). Diese wird dann meistens mit $\det : \mathrm{Mat}_n(K) \to K$ bezeichnet. Konkret kann diese etwa mittels der Leibniz-Formel oder der Laplace-Entwicklung definiert werden.

Mithilfe der Determinante kann man feststellen ob eine Matrix $A \in \mathrm{Mat}_n(K)$ invertierbar ist. Dies ist genau dann der Fall, wenn $\delta(A) \neq 0$.

Der Determinantenmultiplikationssatz (→*Satz 16.11*) besagt, dass

$$\det(AB) = \det(A)\det(B), \quad \text{für } A, B \in \mathrm{Mat}_n(K).$$

Insbesondere ist die Determinante ein Gruppenhomomorphismus

$$\det|_{\mathrm{GL}_n(K)} : \mathrm{GL}_n(K) \to K^*$$

von der multiplikativen Gruppe der $n \times n$-Matrizen in die multiplikative Gruppe $K^* = K \setminus \{0\}$ der Einheiten des Körpers K.

Fehlstand → *Definition 16.4*

Ist $\pi \in \mathrm{Sym}(n)$ eine Permutation von $\{1, \ldots, n\}$, so heißt ein Paar (i, j) mit $i, j \in \{1, \ldots, n\}$ ein Fehlstand falls $i < j$ aber $i\pi > j\pi$.

Signum → *Definition 16.4*

Ist $\pi \in \mathrm{Sym}(n)$ eine Permutation von $\{1, \ldots, n\}$ und

$$\mathrm{Fehl}(\pi) = \{(i, j) \mid (i, j) \text{ ein Fehlstand von } \pi\}$$

die Menge der Fehlstände von π, so ist das Signum von π definiert als

$$\mathrm{sgn}(\pi) = (-1)^{\#\,\mathrm{Fehl}(\pi)}.$$

Also ist $\mathrm{sgn}(\pi) = +1$ wenn die Anzahl der Fehlstände gerade und $\mathrm{sgn}(\pi) = -1$ wenn die Anzahl der Fehlstände ungerade ist.

Die Abbildung $\mathrm{sgn} : \mathrm{Sym}(n) \to \{+1, -1\}$ ist ein Gruppenhomomorphismus (wobei $\mathrm{Sym}(n)$ eine Gruppe bezüglich Hintereinanderausführung und $\{+1, -1\}$ eine Gruppe bezüglich Multiplikation ist).

alternierende Gruppe → *Definition 16.8*

Die alternierende Gruppe vom Grad n ist die Menge

$$\mathrm{Alt}(n) = \{\alpha \in \mathrm{Sym}(n) \mid \mathrm{sgn}(\alpha) = +1\}.$$

Sie bildet eine Untergruppe der symmetrischen Gruppe $\mathrm{Sym}(n)$ (siehe auch Signum).

Leibniz-Formel → *Satz/Definition 16.9*

Die Leibniz-Formel definiert eine Abbildung auf $\mathrm{Mat}_n(K)$ durch

$$A = (a_{ij}) \mapsto \sum_{\sigma \in \mathrm{Sym}(n)} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i,i\sigma}.$$

Diese Abbildung ist eine Determinantenabbildung, und zwar die eindeutige Determinantenabbildung auf $\mathrm{Mat}_n(K)$. Sie wird daher in der Regel mit det bezeichnet.

Die Leibniz-Formel führt sofort zu den bekannten Formeln für Determinanten von 2×2- und 3×3-Matrizen:

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc,$$

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

komplementäre Matrix → *Definition 16.2*

Sei $A \in \mathrm{Mat}_n(K)$ eine $n \times n$-Matrix. Für $i, j \in \{1, \ldots, n\}$ sei $A_{ij}^{[\mathrm{ZS}]}$ die Matrix die aus A entsteht, indem man den (i, j)-ten Eintrag durch 1 und alle weiteren Einträge in der i-ten Zeile und der j-ten Spalte durch 0 ersetzt. Dann heißt die Matrix

$$\tilde{A} = (\tilde{a}_{ij}) \in \mathrm{Mat}_n(K) \quad \text{mit } \tilde{a}_{ij} = \det A_{ij}^{[\mathrm{ZS}]}$$

die komplementäre Matrix zu A.

Eine andere Möglichkeit $\tilde{A}$ zu definieren ist die folgenden: Für $i, j \in \{1, \ldots, n\}$ sei $A_{ij}^{\#} \in \mathrm{Mat}_{n-1}(K)$ die Matrix die aus A durch Streichen der i-ten Zeile und j-ten Spalte entsteht. Dann ist

$$\tilde{A} = (\tilde{a}_{ij}) \in \mathrm{Mat}_n(K) \quad \text{mit } \tilde{a}_{ij} = (-1)^{i+j} \det A_{ji}^{\#}.$$

Die komplementäre Matrix kann verwendet werden um das Inverse von A zu bestimmen (→*Hilfssatz 16.14*, →*Satz 16.15*), denn es ist

$$\tilde{A}A = A\tilde{A} = \det A \cdot \mathrm{Id}.$$

Ist also A invertierbar, so ist

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

Laplace-Entwicklung → *Satz 16.16*

Die Laplace-Entwicklung ist eine Methode um rekursiv die Determinante einer Matrix zu bestimmen. Ist $A = (a_{ij}) \in \mathrm{Mat}_n(K)$, so gilt

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}^{\#} \quad \text{für } i \in \{1, \ldots, n\}$$

(Entwicklung nach der i-ten Zeile)

und

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}^{\#} \quad \text{für } j \in \{1, \ldots, n\}$$

(Entwicklung nach der j-ten Spalte)

wobei $A_{ij}^{\#}$ jeweils die Matrix ist die aus A durch Streichen der i-ten Zeile und j-ten Spalte hervorgeht.

Cramersche Regel → *Satz 16.17*

Die Cramersche Regel gibt ein Verfahren zur Berechnung der Lösung eines eindeutig lösbaren linearen Gleichungssystems. Ein lineares Gleichungssystem kann man schreiben als

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \quad A \in \mathrm{Mat}_n(K) \text{ und } b \in K^n.$$

Dieses LGS hat genau dann eine eindeutige Lösung wenn $\mathrm{Rang}(A) = n$ d.h. $A \in \mathrm{GL}_n(K)$ ist. Die Lösung ist dann

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

Die Cramersche Regel besagt, dass

$$x_i = \frac{\det A_i^b}{\det A},$$

wobei $\det A_i^b$ die Marix bezeichne, die aus A hervorgeht indem man die i-te Spalte durch b ersetzt.

Eigenwert → *Definition 17.1*

Ist $\alpha : V \to V$ ein Endomorphismus eines K-Vektorraums V, so heißt $\lambda \in K$ Eigenwert von α, falls es ein $v \in V \setminus \{0\}$ gibt mit $v\alpha = \lambda v$. Ein solches v heißt dann Eigenvektor von α (zum Eigenwert λ).

Eigenvektor → *Definition 17.1*

Ist $\alpha : V \to V$ ein Endomorphismus eines K-Vektorraums V, so heißt $v \in V \setminus \{0\}$ Eigenvektor von α (zum Eigenwert λ) falls $v\alpha = \lambda v$ für ein $\lambda \in K$.

Die Menge aller Eigenvektoren zu einem festen Eigenwert, zusammen mit dem Nullvektor, bildet einen Unterraum, den Eigenraum zum Eigenwert λ.

Eigenraum → *Definition 17.1*

Ist $\alpha : V \to V$ ein Endomorphismus eines K-Vektorraums V und $\lambda \in K$, so heißt

$$\mathrm{Eig}(\alpha, \lambda) = \{v \in V \mid v\alpha = \lambda v\}$$

der Eigenraum von α zu λ. Er ist stets ein Unterraum (→*Hilfssatz 17.3*).

$\mathrm{Eig}(\alpha, \lambda)$ ist genau dann nicht-trivial (d.h. enthält nicht nur den Nullvektor), wenn λ ein Eigenwert von α ist. In diesem Fall besteht $\mathrm{Eig}(\alpha, \lambda)$ genau aus den Eigenvektoren von α zum Eigenwert λ und dem Nullvektor.

charakteristisches Polynom → *Definition/Satz 17.4*

Ist $A = (a_{ij}) \in \mathrm{Mat}_n(K)$ eine Matrix, so heißt

$$\begin{aligned}\mathrm{Charpol}(A) &= \det(X\mathrm{Id} - A) \\ &= \det \begin{pmatrix} X - a_{11} & -a_{12} & \cdots & -a_{1n} \\ a_{21} & X - a_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ -a_{n1} & \cdots & \cdots & X - a_{nn} \end{pmatrix} \in K[X]\end{aligned}$$

das charakteristische Polynom von A. Hierbei ist $X\mathrm{Id} - A$ eine Matrix deren Einträge Polynome aus $K[X]$ sind. Solche Polynome kann man multiplizieren und addieren und so kann man die Determinante mit den bekannten Methoden (Leibniz-Formel, Laplace-Entwicklung) ausrechnen.

Ist $\alpha : V \to V$, ein Endomorphismus eines endlich-dimensionalen K-Vektorraums V, so definiert man das charakteristische Polynom von α indem man die Matrix $A = [\alpha]_{\mathcal{BB}}$ bezüglich einer beliebigen Basis $\mathcal{B}$ von V aufstellt und setzt

$$\mathrm{Charpol}(\alpha) = \mathrm{Charpol}(A).$$

Diese Definition liefert für jede Basis dasselbe Ergebnis, hängt also nicht von der konkreten Wahl der Basis ab (siehe →*Definition/Satz 17.4*).

Das charakteristische Polynom ist stets ein normiertes Polynom vom Grad $n = \dim V$.

Das charakteristische Polynom liefert Informationen über die Eigenwerte und Eigenräume von α: Die Eigenwerte von α sind genau die Nullstellen des charakteristischen Polynoms $\mathrm{Charpol}(\alpha)$ (→*Hilfssatz 17.5*). Ist λ ein Eigenwert von α (also eine Nullstelle von $\mathrm{Charpol}(\alpha)$), so ist die Dimension von $\mathrm{Eig}(\alpha, \lambda)$ (die geometrische Vielfachheit) höchstens die Vielfachheit der Nullstelle λ in $\mathrm{Charpol}(A)$ (die algebraische Vielfachheit), →*Satz 17.8*.

algebraische Vielfachheit → *Satz 17.8*

Ist $\alpha : V \to V$ ein Endomorphismus des endl.-dim. K-Vektorraums V und λ ein Eigenwert von α, so ist λ eine Nullstelle von $\chi(X) := \text{Charpol}(\alpha)$. Dann gilt $(X - \alpha) \mid \chi(X)$. Die Vielfachheit der Nullstelle α in $\chi(X)$ (d.h. die größte natürliche Zahl $n \in \mathbb{N}$ mit $(X-\alpha)^n \mid \chi(X)$) heißt dann algebraische Vielfachheit des Eigenwerts λ von α.

Die algebraische Vielfachheit von λ ist eine obere Schranke für die geometrische Vielfachheit von λ.

geometrische Vielfachheit → *Satz 17.8*

Ist $\alpha : V \to V$ ein Endomorphismus des K-Vektorraums V und $\lambda \in K$ ein Eigenwert, so nennt man die Dimension des Eigenraums $\text{Eig}(\alpha, \lambda)$ die geometrische Vielfachheit des Eigenwerts λ.

diagonalisierbarer Endomorphismus → *Definition 17.11*

Ein Endomorphismus $\alpha : V \to V$ eines endl.-dim. K-Vektorraums V heißt diagonalisierbar, falls es eine Basis $\mathcal{B}$ von V gibt, sodass $[\alpha]_{\mathcal{B}\mathcal{B}}$ eine Diagonalmatrix ist.

Ist $A = [\alpha]_{\mathcal{C},\mathcal{C}}$ eine Koordinatenmatrix von α bezüglich einer beliebigen Basis $\mathcal{C}$ von V, so ist α genau dann diagonalisierbar, wenn A eine diagonalisierbare Matrix ist.

Der Endomorphismus α ist genau dann diagonalisierbar, wenn V eine Basis aus Eigenvektoren von α besitzt (→*Satz 17.12*).

Insbesondere ist der Endomorphismus α diagonalisierbar wenn er $\dim V$ paarweise verschiedene Eigenwerte besitzt, wenn also das charakteristische Polynom $\chi(X) = \text{Charpol}(\alpha)$ genau $\dim V$ verschiedene Nullstellen besitzt. Ist dies nicht der Fall, so muss man für die Diagonalisierbarkeit überprüfen ob $\chi(X)$ in Linearfaktoren zerfällt. Zerfällt χ nicht in Linearfaktoren, so ist α nicht diagonalisierbar. Zerfällt $\chi(X)$ in Linearfaktoren als

$$\chi(X) = (X - \lambda_1)^{e_1} \cdots (X - \lambda_k)^{e_k}$$

so ist α diagonalisierbar genau dann, wenn die Dimension des Eigenraums $\text{Eig}(\alpha, \lambda_i)$ zu jedem Eigenwert λ_i gleich der Vielfachheit e_i der Nullstelle λ_i in $\chi(X)$ ist (→*Satz 17.12*).

diagonalisierbare Matrix → *Definition 17.11*

Eine Matrix $A \in \text{Mat}_n(K)$ heißt diagonalisierbar, falls es eine Matrix $T \in \text{GL}_n(K)$ gibt, sodass $T^{-1}AT$ eine Diagonalmatrix ist.

Die Matrix A ist genau dann diagonalisierbar, wenn die Abbildung $K^n \to K^n, x \mapsto xA$ ein diagonalisierbarer Endomorphismus ist.

Skalarprodukt → *Definition 18.1*

Ein Skalarprodukt auf einem $\mathbb{R}$-Vektorraum V ist eine Abbildung

$$\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R},\ (v, w) \mapsto \langle v, w \rangle$$

mit den folgenden Eigenschaften:

(SP1) Bilinearität. Für alle $a \in \mathbb{R}$ und $u, v, w \in V$ gilt

$$\langle au+v, w \rangle = a\langle u, w \rangle + \langle v, w \rangle \quad \text{und} \quad \langle u, av+w \rangle = a\langle u, v \rangle + \langle u, w \rangle.$$

(SP2) Symmetrie. Für alle $v, w \in V$ gilt

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

(SP3) Positiv-Definitheit. Für alle $v \in V \setminus \{0\}$ gilt

$$\langle v, v \rangle > 0.$$

Siehe auch euklidischer Vektorraum. Mithilfe des Skalarprodukts definiert man die euklidische Norm.

euklidischer Vektorraum → *Definition 18.1*

Ein euklidischer Vektorraum ist ein $\mathbb{R}$-Vektorraum mit einem Skalarprodukt (welches dann meist $\langle \cdot, \cdot \rangle_V$ geschrieben wird, oder einfach $\langle \cdot, \cdot \rangle$, wenn keine Verwechslungsgefahr besteht).

Norm → *Definition 18.1*

Eine Norm auf einem $\mathbb{R}$-Vektorraum V ist eine Abbildung

$$\|\cdot\| : V \to \mathbb{R}_{\geq 0}$$

mit den Eigenschaften

- Für alle $v \in V \setminus \{0\}$ ist $\|v\| > 0$.
- Für alle $a \in \mathbb{R}$ und $v \in V$ ist $\|av\| = |a|\,\|v\|$.
- Für alle $v, w \in V$ ist $\|v + w\| \leq \|v\| + \|w\|$ (Dreiecksungleichung).

Man fasst $\|v\|$ oft als die „Länge“ von v auf, und kann so die Norm verwenden um einen Abstandsbegriff zu definieren: Der Abstand von v und w ist $d(v, w) = \|v - w\|$.

Verwendet man das Standardskalarprodukt auf $\mathbb{R}^n$ mit der euklidischen Norm, so entspricht dieser Abstandsbegriff dem vertrauten euklidischen Abstand.

euklidische Norm → *Definition 18.1*

Auf einem euklidischen Vektorraum V mit Skalarprodukt $\langle \cdot, \cdot \rangle$ definiert man die euklidische Norm durch

$$\|\cdot\| : V \to \mathbb{R}_{\geq 0}, v \mapsto \|v\| = \sqrt{\langle v, v \rangle}.$$

Die euklidische Norm ist eine Norm.

Standardskalarprodukt → *Beispiel 18.2*

Auf $\mathbb{R}^n$ definiert man das Standardskalarprodukt $\langle \cdot, \cdot \rangle : \mathbb{R}^n \to \mathbb{R}$ durch

$$\langle (v_1, \ldots, v_n), (w_1, \ldots, w_n) \rangle = v_1 w_1 + \cdots + v_n w_n.$$

Dies ist ein Skalarprodukt und macht $\mathbb{R}^n$ zu einem euklidischen Vektorraum.

Cauchy-Schwarzsche Ungleichung → *Satz 18.3*

In einem euklidischen Vektorraum mit Skalarprodukt $\langle \cdot, \cdot \rangle$ und Norm $\|\cdot\|$ (definiert als $\|v\| = \sqrt{\langle v, v \rangle}$) gilt

$$|\langle v, w \rangle| \leq \|v\| \cdot \|w\|.$$

Gleichheit gilt genau dann, wenn v und w linear abhängig sind, also $\langle v \rangle \subseteq \langle w \rangle$ oder $\langle w \rangle \subseteq \langle v \rangle$.

orthogonal → *Definition 18.4*

siehe senkrecht

senkrecht → *Definition 18.4*

Gilt in einem euklidischen Vektorraum V für zwei Vektoren $v, w \in V$, dass $\langle v, w \rangle = 0$, so sagt man v und w seien senkrecht oder orthogonal und schreibt $v \perp w$.

orthogonales Komplement → *Definition 18.4*

Sei V ein euklidischer Vektorraum und $U \subseteq V$. Dann heißt

$$U^\perp = \{v \in V \mid v \perp u \text{ für alle } u \in U\}$$

das orthogonale Komplement von U (siehe senkrecht). Dieses ist stets ein Unterraum. Ist U selber ein Unterraum mit $\dim U < \infty$, so gilt $V = U \oplus U^\perp$ (→*Satz 18.6*).

Orthonormalsystem → *Definition 18.4*

Ein Orthonormalsystem in einem euklidischen Vektorraum V ist ein Vektorsystem $(v_1, \ldots, v_n)$ mit $v_i \perp v_j$ für $i \neq j$ und $\|v_i\| = 1$ für alle i.

Orthonormalbasis → *Definition 18.4*

Eine Orthonormalbasis eines euklidischen Vektorraumes V ist eine Basis von V deren Elemente senkrecht zueinander stehen und jeweils Norm 1 haben.

Eine geordnete Orthonormalbasis ist also ein Vektorsystem $(v_1, \ldots, v_n)$ welches sowohl eine geordnete Basis als auch ein Orthonormalsystem ist.

Um eine Orthonormalbasis eines Vektorraums oder eines Unterraums zu bestimmen, verwendet man oft das Gram-Schmidt-Vefahren.

Gram-Schmidt-Verfahren → *Abschnitt 18.8*

Das Gram-Schmidt-Verfahren wird verwendet um Orthonormalbasen (für einen Vektorraum oder Unterraum) zu finden. Genauer: Ist V ein euklidischer Vektorraum und U ein Unterraum mit einer gegebenen Basis $(v_1, \ldots, v_m)$, so definiert man induktiv ein Vektorsystem $(u_1, \ldots, u_m)$ durch

$$u_i = \frac{1}{\|w_i\|} w_i, \quad \text{wobei} \quad w_i = v_i - \sum_{j=1}^{i-1} \langle v_i, u_j \rangle u_j.$$

Dann ist $(u_1, \ldots, u_m)$ eine Orthonormalbasis von U.

orthogonale Abbildung → *Definition 18.9*

Sei V ein euklidischer Vektorraum. Eine lineare Abbildung $\alpha : V \to V$ heißt orthogonal, falls

$$\langle v\alpha, w\alpha \rangle = \langle v, w \rangle \quad \text{für alle } v, w \in V.$$

Solch ein α ist dann auch abstandserhaltend:

$$\|v\alpha - w\alpha\| = \|v - w\| \quad \text{für alle } v, w \in V.$$

Insbesondere ist $\operatorname{Kern} \alpha = 0$ (siehe Kern), d.h. für $\dim V < \infty$ ist α (invertierbar), $\alpha \in \mathrm{GL}(V)$.

Ist $A = [\alpha]_{\mathcal{B},\mathcal{B}}$ die Koordinatenmatrix von α bezüglich einer Orthonormalbasis $\mathcal{B}$ von V so ist α orthogonal genau dann, wenn A eine orthogonale Matrix ist (→*Satz 18.10*).

orthogonale Matrix → *Definition 18.9*

Eine Matrix $A \in \mathrm{Mat}_n \mathbb{R}$ heißt orthogonal, falls A invertierbar ist und $A^{-1} = A^{\mathrm{tr}}$. Die Menge aller orthogonalen Matrizen in $\mathrm{Mat}_n \mathbb{R}$ heißt orthogonale Gruppe vom Grad n.

Die lineare Abbildung $\mathbb{R}^n \to \mathbb{R}^n, v \mapsto vA$ ist eine orthogonale Abbildung genau dann, wenn A eine orthogonale Matrix ist (→*Satz 18.10*).

orthogonale Gruppe → *Definition 18.9*

Die Menge

$$O(n, \mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^{-1} = A^{\mathrm{tr}}\}$$

aller orthogonalen Matrizen in $\mathrm{Mat}_n(\mathbb{R})$ ist eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$ und heißt orthogonale Gruppe vom Grad n.

selbst-adjungierter Endomorphismus → *Definition 18.12*

Ein Endomorphismus $\alpha : V \to V$ eines euklidischen Vektorraums V heißt selbst-adjungiert, falls

$$\langle v\alpha, w\rangle = \langle v, w\alpha\rangle \quad \text{für alle } v, w \in V.$$

Bezüglich einer Orthonormalbasis wird eine selbst-adjungierte Abbildung stets durch eine symmetrische Matrix repräsentiert (→*Satz 18.13*).

symmetrische Matrix → *Definition 18.12*

Eine Matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ heißt symmetrisch falls $A = A^{\mathrm{tr}}$ (Transponierte), d.h. $a_{ij} = a_{ji}$ für alle $i, j \in \{1, \ldots, n\}$.

Die Abbildung $\mathbb{R}^n \to \mathbb{R}^n, v \mapsto vA$ ist selbst-adjungiert genau dann, wenn A symmetrisch ist.

Spektralsatz → *Satz 18.14*

Der Spektralsatz für endlich-dimensionale euklidische Vektorräume besagt, dass zu einem selbst-adjungierter Endomorphismus $\alpha : V \to V$ eines endl.-dim. eukl. Vektorraumes stets eine Orthonormalbasis von V aus Eigenvektoren von α existiert. Insbesondere ist α also diagonalisierbar.

Ist $A \in \mathrm{Mat}_n(\mathbb{R})$ eine symmetrische Matrix, so ist die Abbildung $\mathbb{R}^n \to \mathbb{R}^n, v \mapsto vA$ selbst-adjungiert. Der Spektralsatz besagt dann, dass es eine orthogonale Matrix $S \in O(n, \mathbb{R})$ gibt, sodass $S^{-1}AS = S^{\mathrm{tr}}AS$ eine Diagonalmatrix ist.