

Kurzskript Lineare Algebra I

Immi Halupczok

26. Mai 2023

Inhaltsverzeichnis

Lineare Algebra I	2
1 Mathematische Grundbegriffe	2
1.1 Lineare Gleichungssysteme	2
1.2 Logik und Mengen	5
1.3 Abbildungen	9
1.4 Partitionen und Äquivalenzrelationen	10
2 Algebraische Strukturen	11
2.1 Gruppen, Ringe, Körper	11
2.2 Unter- und Quotientenobjekte	13
2.3 Die komplexen Zahlen	14
2.4 Polynomringe	15
3 Vektorräume	16
3.1 Definition	16
3.2 Untervektorräume	17
3.3 Lineare Unabhängigkeit	18
3.4 Basis und Dimension	18

Lineare Algebra I

1 Mathematische Grundbegriffe

1.1 Lineare Gleichungssysteme

Definitionen, Konventionen, etc., die in **dieser Farbe** geschrieben sind, sind Grundlagen, die thematisch nicht zum Abschnitt gehören (aber eingeführt werden, wenn sie zum ersten Mal benötigt werden).

- Definition 1.1.1 (unpräzise)** (a) Die **natürlichen Zahlen** sind $0, 1, 2, 3, \dots$ ¹. Die Menge aller natürlichen Zahlen wird mit \mathbb{N} bezeichnet, d. h. statt „ x ist eine natürliche Zahl“ schreiben wir auch „ $x \in \mathbb{N}$ “.
- (b) Die **ganzen Zahlen** sind $\dots, -2, -1, 0, 1, 2, \dots$. Die Menge der ganzen Zahlen wird mit \mathbb{Z} bezeichnet.
- (c) Eine **rationale Zahl** ist eine Zahl, die sich als Bruch $\frac{a}{b}$ schreiben lässt, wobei a eine beliebige ganze Zahl ist und b eine ganze Zahl ungleich 0. Die Menge der rationalen Zahlen wird mit \mathbb{Q} bezeichnet.
- (d) (Reelle Zahlen werden in der Analysis-Vorlesung definiert.) Die Menge der reellen Zahlen wird mit \mathbb{R} bezeichnet.

Konvention 1.1.2 Eine **Variable** ist ein Symbol, das für ein mathematisches Objekt (ihr **Wert**) stehen kann. Als Symbol werden meist Buchstaben verwendet, z. T. mit „Dekorationen“ (z. B. a' , \tilde{a} , \hat{a} , \underline{a} , \dots). Kommt das gleiche Symbol mit verschiedenen Dekorationen vor, so sind dies verschiedene Variablen. Ist der Wert einer Variablen festgelegt, so nennt man sie oft auch eine **Konstante**.

Konvention 1.1.3 Symbole können außerdem ein oder mehrere mathematische Objekte als Indizes erhalten (z. B. $a_1, a_2, a_{7,8}$). Das gleiche Symbol mit verschiedenen Indizes sind verschiedene Variablen.

Definition 1.1.4 Sei n eine natürliche Zahl und seien a_1, \dots, a_n und b reelle Zahlen. Einen Ausdruck der Form

$$a_1x_1 + \dots + a_nx_n = b$$

(wobei x_1, \dots, x_n Variablen sind), nennt man eine **lineare Gleichung** (in x_1, \dots, x_n).

Definition 1.1.5 (a) Sind a_1 und a_2 beliebige mathematische Objekte, so schreibt man (a_1, a_2) für das (**geordnete**) **Paar** bestehend aus a_1 und a_2 . Zwei Paare (a_1, a_2) und (b_1, b_2) werden als gleich angesehen (als Formel: „ $(a_1, a_2) = (b_1, b_2)$ “), wenn die entsprechenden Einträge gleich sind, also wenn $a_1 = b_1$ ist und $a_2 = b_2$.

¹Es besteht unter Mathematikern keine Einigkeit darüber, ob 0 als natürliche Zahl bezeichnet wird oder nicht. In dieser Vorlesung ist 0 eine natürliche Zahl.

Lemma 1.1.10 Sei \underline{L} ein homogenes lineares Gleichungssystem in n Variablen. Dann gilt:

- (a) Das n -Tupel $(0, \dots, 0)$ ist eine Lösung von \underline{L} (die **triviale Lösung**).
- (b) Sind $\underline{c} = (c_1, \dots, c_n)$ und $\underline{c}' = (c'_1, \dots, c'_n)$ Lösungen von \underline{L} , so ist auch $\underline{c} + \underline{c}' := (c_1 + c'_1, \dots, c_n + c'_n)$ eine Lösung von \underline{L} .
- (c) Ist $\underline{c} = (c_1, \dots, c_n)$ eine Lösung von \underline{L} und $\lambda \in \mathbb{R}$, so ist auch $\lambda \underline{c} := (\lambda c_1, \dots, \lambda c_n)$ eine Lösung von \underline{L} .

Lemma 1.1.11 Seien $L := „a_1x_1 + \dots + a_nx_n = b“$ und $L' := „a'_1x_1 + \dots + a'_nx_n = b'“$ lineare Gleichungen und sei $\lambda \in \mathbb{R}$. Wir nehmen an, dass $\underline{c} \in \mathbb{R}^n$ sowohl Lösung von L als auch Lösung von L' ist. Dann ist \underline{c} auch eine Lösung von

$$L + L' := „(a_1 + a'_1)x_1 + \dots + (a_n + a'_n)x_n = (b + b')“.$$

und von

$$\lambda \cdot L := „(\lambda a_1)x_1 + \dots + (\lambda a_n)x_n = \lambda b“.$$

Definition 1.1.12 Sei \underline{L} ein Gleichungssystem. Eine **elementare Transformation** von \underline{L} ist ein Gleichungssystem \underline{L}' , das man auf eine der folgenden Arten aus \underline{L} erhält:

- (a) zwei Gleichungen tauschen;
- (b) eine Gleichung durch ihr λ -faches ersetzen, für eine reelle Zahl $\lambda \neq 0$;
- (c) zu einer der Gleichungen von \underline{L} das λ -fache einer anderen Gleichung von \underline{L} addieren, für eine beliebige reelle Zahl λ .

Lemma 1.1.13 Ist \underline{L} ein lineares Gleichungssystem und \underline{L}' eine elementare Transformation von \underline{L} , so ist auch \underline{L} eine elementare Transformation von \underline{L}' .

Satz 1.1.14 Ist \underline{L} ein lineares Gleichungssystem und \underline{L}' eine elementare Transformation von \underline{L} , so haben \underline{L} und \underline{L}' die selben Lösungen.

Definition 1.1.15 Man sagt, ein Gleichungssystem ist in **Zeilenstufenform**, wenn seine Koeffizientenmatrix die folgende Form hat:

$$\left(\begin{array}{cccccccc|cccc|c} 0 & \dots & 0 & \boxed{1} & * & \dots & * & * & \dots & * & * & \dots & * & * & \dots & * & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \boxed{1} & * & \dots & * & * & \dots & * & * & \dots & * & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \boxed{1} & \ddots & \dots & \dots & \dots & \dots & \dots & \dots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & \ddots & \ddots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & \boxed{1} & * & \dots & * & * & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{array} \right);$$

$\underbrace{\hspace{1.5cm}}_{\odot} \quad \underbrace{\hspace{1.5cm}}_{\odot} \quad \underbrace{\hspace{1.5cm}}_{\odot} \quad \underbrace{\hspace{1.5cm}}_{\odot}$

Hierbei steht jedes „*“ für eine beliebige reelle Zahl, und die mit \odot markierten Zeilen und Spalten müssen nicht vorhanden sein. Die eingekästelten 1en (d. h. die ersten nicht-0-Einträge jeder Zeile) nennt man **Pivot-Elemente**.

Satz 1.1.16 (Gauß-Elimination) Jedes Gleichungssystem kann durch endlich viele elementare Transformationen in Zeilenstufenform gebracht werden.

Satz 1.1.17 Sei \underline{L} ein lineares Gleichungssystem in Zeilenstufenform. Dann gilt:

- (a) Existiert in der Koeffizientenmatrix von \underline{L} eine Zeile der Form $(0 \cdots 0 \mid b_i)$ mit $b_i \neq 0$, so besitzt \underline{L} keine Lösung.
- (b) Existiert keine solche Zeile, so besitzt \underline{L} Lösungen. In diesem Fall lassen sich sämtliche Lösungen erhalten, indem man der Reihe nach x_n, x_{n-1}, \dots, x_1 folgendermaßen wählt:
 - (i) Enthält die j -te Spalte kein Pivot-Element, so kann x_j beliebig gewählt werden.
 - (ii) Enthält die j -te Spalte ein Pivot-Element in der i -ten Zeile, so ist x_j durch x_{j+1}, \dots, x_n eindeutig festgelegt, nämlich: Hat die i -te Zeile die Form

$$(0 \cdots 0 \ 1 \ a_{i,j+1} \cdots a_{i,n} \mid b_i),$$

so ist $x_j = b_i - a_{i,j+1}x_{j+1} - a_{i,j+2}x_{j+2} - \cdots - a_{i,n}x_n$.

Korollar 1.1.18 Sei \underline{L} ein lineares Gleichungssystem mit mehr Variablen als Gleichungen.

- (a) Ist \underline{L} homogen, so hat \underline{L} unendlich viele nicht-triviale Lösung.
- (b) Hat \underline{L} mindestens eine Lösung, so hat \underline{L} bereits unendlich viele Lösungen.

1.2 Logik und Mengen

Definition 1.2.1 (unpräzise) (a) Eine (**mathematische**) **Aussage** ist ein Textfragment A (evtl. mit mathematischen Symbolen), für das die Frage Sinn ergibt, ob es wahr oder falsch ist. Man sagt auch, dass A **gilt**, bzw. **nicht gilt**; oder: Der **Wahrheitswert** von A ist wahr bzw. falsch.

Der Wahrheitswert einer Aussage A kann von Variablen abhängen. In diesem Fall sagen wir auch, dass A eine **Aussage über** diese Variablen ist.

- (b) Ein **Term** ist Textfragment T (evtl. mit mathematischen Symbolen), das das ein mathematisches Objekt beschreibt; dieses Objekt nennt man den **Wert** von T . Meistens hängt der Wert von T von Variablen ab; man nennt T dann einen **Term in** diesen Variablen.

Definition 1.2.2 Sind A und B Aussagen, so definiert man daraus die folgenden neuen Aussagen:

- (a) „ $A \wedge B$ “ ist wahr genau dann, wenn sowohl A als auch B wahr ist. Man nennt dies die **Konjunktion** von A und B .
- (b) „ $A \vee B$ “ ist wahr genau dann, wenn mindestens eine der Aussagen A und B wahr sind. Man nennt dies die **Disjunktion** von A und B .
- (c) „ $\neg A$ “ ist wahr genau dann, wenn A falsch ist. Man nennt dies die **Negation** von A .
- (d) „ $A \Rightarrow B$ “ wahr ist genau dann, wenn A falsch ist oder B wahr oder beides. Man schreibt auch „ $B \Leftarrow A$ “ und sagt auch „ A **impliziert** B “ oder „ B **folgt aus** A “.
- (e) „ $A \Leftrightarrow B$ “ wahr ist genau dann, wenn A und B den gleichen Wahrheitswert haben. Man sagt auch, „ A ist **äquivalent** zu B “ oder „ A und B sind äquivalent“ oder „ A gilt genau dann, wenn B gilt“.

- Definition 1.2.3 (ungenau)** (a) Eine **Menge** M ist ein mathematisches Objekt, das dadurch charakterisiert ist, welche mathematischen Objekte ihre **Elemente** sind. Statt „ x ist ein Element von M “ sagt man auch: „ x liegt in M “ oder „ M enthält x “. Notation dafür: „ $x \in M$ “
- (b) Weitere Notationen:
 „ $x \notin M$ “ bedeutet: x ist kein Element von M .
 „ $x, y \in M$ “ bedeutet: sowohl x als auch y sind Elemente von M ; etc.
- (c) Die **leere Menge** ist die Menge, die gar keine Elemente hat. Sie wird mit \emptyset bezeichnet.

Definition 1.2.4 Sind x_1, \dots, x_n beliebige mathematische Objekte, so schreiben wir

$$\{x_1, \dots, x_n\}$$

für die Menge, deren Elemente genau x_1, \dots, x_n sind:

$$y \in \{x_1, \dots, x_n\} \iff (y = x_1 \vee \dots \vee y = x_n).$$

Bemerkung: Eine ein-elementige Menge $\{a\}$ wird *nicht* als das gleiche angesehen wie das Element a selbst. Außerdem: Ist ein Element A von M selbst wieder eine Menge, so werden die Elemente von A *nicht* automatisch auch als Elemente von M angesehen.

- Definition 1.2.5** (a) Ist M eine Menge und A eine Aussage über eine Variable x , so schreiben wir $\{x \in M \mid A\}$ für die Menge derjenigen Elemente $x \in M$, für die die Aussage A wahr ist. (Manche Leute schreiben auch „ $\{x \in M : A\}$ “.) Wenn man M aus dem Kontext erraten kann, schreibt man oft auch nur $\{x \mid A\}$. Ist A' eine weitere Aussage, so schreibt man statt $\{x \mid A \wedge A'\}$ oft auch $\{x \mid A, A'\}$.
- (b) Ist A eine Aussage über eine Variable x und T ein Term in x , so schreibt man $\{T \mid A\}$ für die Menge aller Werte, die der Term T annehmen kann, wenn man für x Objekte einsetzt, für die A wahr ist. Man verwendet auch analoge Notationen, wenn A und T Aussagen in mehreren Variablen sind.

Definition 1.2.6 Ist M eine Menge, so schreiben wir $\#M$ für die Anzahl der Elemente von M ; man nennt dies auch die **Kardinalität** (oder **Mächtigkeit**) von M . (Statt $\#M$ kann man auch $|M|$ schreiben.) Genauer: Lässt sich $M = \{x_1, \dots, x_n\}$ schreiben für paarweise verschiedene x_i , so nennen wir M **endlich** und setzen $\#M := n$. Lässt sich M nicht so schreiben, so nennen wir M **unendlich** und setzen (in dieser Vorlesung²) $\#M := \infty$.

Definition 1.2.7 Sei A eine Aussage über eine Variable x und sei M eine Menge.

- (a) Die Notation

$$\forall x \in M: A$$

²Auch bei unendlichen Mengen M kann man noch „verschieden große“ Mengen unterscheiden: Gibt es eine Bijektion (siehe Definition 1.3.9) von M nach \mathbb{N} , so nennt man M **abzählbar**, sonst **überabzählbar**. Allgemeiner sagt man, zwei Mengen M und M' haben die gleiche Kardinalität, wenn eine Bijektion von M nach M' existiert.

bedeutet: A gilt für jedes Element x von M . Manchmal schreibt man auch „ $A \quad \forall x \in M$ “.

Ist M leer, so wird „ $\forall x \in M: A$ “ als wahr angesehen.

(b) Die Notation

$$\exists x \in M: A$$

bedeutet: Es existiert mindestens ein Element x von M , für das A wahr ist.

(c) Die Notation

$$\exists^1 x \in M: A$$

bedeutet: Es existiert genau ein Element x von M , für das A wahr ist.

(d) Die Aussage „ A gilt für **fast alle** $x \in M$ “ bedeutet: Es gibt nur endlich viele Elemente in M , für die A nicht gilt. (Anders ausgedrückt: Die Menge $\{x \in M \mid \neg A\}$ ist endlich.)

Die Symbole \forall und \exists nennt man **Quantoren**. Wenn man M aus dem Kontext erraten kann, schreibt man in den obigen Notationen oft nur „ x “ statt „ $x \in M$ “.

Die Notation

$$\forall x, y \in M: A$$

ist eine Kurzschreibweise für „ $\forall x \in M: \forall y \in M: A$ “; etc.

Definition 1.2.8 Seien A und B Mengen.

- (a) A heißt **Teilmenge** von B wenn jedes Element von A auch Element von B ist. Man sagt auch: „ A ist eine **Untermenge** von B “; oder: „ B ist eine **Obermenge** von A “. Notationen: $A \subseteq B$; $B \supseteq A$.
- (b) Die Notation $A \subsetneq B$ bedeutet: $A \subseteq B$ aber $A \neq B$; man sagt: „ A ist eine **echte Teilmenge** von B .“

Definition 1.2.9 Seien A und B Mengen.

- (a) Die **Vereinigung** von A und B ist $A \cup B := \{x \mid x \in A \vee x \in B\}$ (Man sagt auch „ A **vereinigt** B “).
- (b) Der **Schnitt** von A und B ist $A \cap B := \{x \mid x \in A \wedge x \in B\}$ (Man sagt auch „ A **geschnitten** B “). Ist $A \cap B = \emptyset$, so sagt man, die Mengen A und B sind **disjunkt**.
- (c) Die **Differenz** von A und B ist $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$ (Man sagt auch „ A **ohne** B “).

Definition 1.2.10 Ist A eine Menge, so bezeichnet

$$\mathcal{P}(A) := \{B \mid B \subseteq A\}$$

die Menge aller Teilmengen von A ; $\mathcal{P}(A)$ wird **Potenzmenge** von A genannt.

Definition 1.2.11 (a) Sind M_1 und M_2 Mengen, so schreibt man $M_1 \times M_2$ für die Menge der Paare (x_1, x_2) bestehend aus einem Element x_1 von M_1 und einem Element x_2 von M_2 . Man nennt $M_1 \times M_2$ das **kartesische Produkt** von M_1 und M_2 . Analog schreibt man $M_1 \times M_2 \times M_3$ für die Menge der Tripel, etc.

(b) Ist M eine Menge, so schreibt man statt $\underbrace{M \times \cdots \times M}_{n \text{ mal}}$ auch M^n (vgl.

Definition 1.1.5). Hierbei ist $M^1 = M$, und M^0 ist die Menge, deren einziges Element das leere Tupel ist.

Bemerkung: Meistens identifiziert man verschiedene Klammerungen von kartesischen Produkten, also z. B.: $(M_1 \times M_2) \times M_3 = M_1 \times M_2 \times M_3 = M_1 \times (M_2 \times M_3)$.

Notation 1.2.12 Sind $m \leq n$ zwei ganze Zahlen und sind A_m, A_{m+1}, \dots, A_n Mengen, so verwendet man folgende Notationen:

- (a) $\bigcup_{i=m}^n A_i := A_m \cup A_{m+1} \cup \cdots \cup A_n$
- (b) $\bigcap_{i=m}^n A_i := A_m \cap A_{m+1} \cap \cdots \cap A_n$
- (c) $\prod_{i=m}^n A_i := A_m \times A_{m+1} \times \cdots \times A_n$

Die Beschriftung „ $i = m$ “ und „ n “ am großen Symbol ist also zu interpretieren als: i soll alle ganzen Zahlen von m bis n durchlaufen.

Konvention 1.2.13 Sei I eine (möglicherweise unendliche) Indexmenge und sei A_i eine Menge für jedes $i \in I$.

- (a) $\bigcup_{i \in I} A_i$ ist die Menge derjenigen Elemente, die in jeder mindestens einer der Mengen A_i liegen. Im Fall $I = \emptyset$ setzt man $\bigcup_{i \in I} A_i := \emptyset$.
- (b) $\bigcap_{i \in I} A_i$ ist die Menge derjenigen Elemente, die in jeder der Mengen A_i liegen. Im Fall $I = \emptyset$ ist $\bigcap_{i \in I} A_i$ nicht definiert.

Definition 1.2.14 Sei I eine (möglicherweise unendliche) Indexmenge.

- (a) Ein **mit I indiziertes Tupel** ist ein mathematisches Objekt \underline{a} , das jedem Index $i \in I$ ein mathematisches Objekt a_i zuordnet. Sind diese a_i gegeben, so schreibt man auch $(a_i)_{i \in I}$ für das Tupel \underline{a} .
- (b) Ist A_i eine Menge für jedes $i \in I$, so bezeichnet

$$\prod_{i \in I} A_i$$

die Menge derjenigen mit I indizierten Tupel $(a_i)_{i \in I}$, bei denen $a_i \in A_i$ ist für alle $i \in I$. Man nennt diese Menge das **kartesische Produkt** der Mengen A_i . Ist $I = \emptyset$, so ist $\prod_{i \in I} A_i$ die Menge, die das leere Tupel als einziges Element hat.

- (c) Ist A eine Menge, so schreibt man statt $\prod_{i \in I} A$ auch A^I .

1.3 Abbildungen

Definition 1.3.1 Seien A und B Mengen. Eine **Abbildung** f (oder **Funktion**) von A nach B ist ein mathematisches Objekt f , das jedem Element $a \in A$ ein Element $f(a) \in B$ zuordnet. Ist $f(a) = b$, so sagt man, f **bildet** a auf b **ab**.

Formal ist eine Abbildung gegeben durch eine Menge $G \subseteq A \times B$, mit der Eigenschaft, dass für jedes $a \in A$ genau ein $b \in B$ existiert mit $(a, b) \in G$; die einer Abbildung f entsprechende Menge ist $G = \{(a, f(a)) \mid a \in A\}$.

„ $\text{Abb}(A, B)$ “ bezeichnet die Menge aller Abbildungen von A nach B . Statt „ $f \in \text{Abb}(A, B)$ “ schreibt man auch „ $f: A \rightarrow B$ “, und statt $f(a) = b$ schreibt man auch „ $f: a \mapsto b$ “.

Man nennt A den **Definitionsbereich** von f , B den **Wertebereich** von f und G den **Graph** von f .

Konvention 1.3.2 Ist $f: A_1 \times A_2 \rightarrow B$, so schreibt man statt $f((a_1, a_2))$ auch $f(a_1, a_2)$ (für $a_1 \in A_1, a_2 \in A_2$). Und analog für $f: A_1 \times A_2 \times A_3 \rightarrow B$, etc.

Bemerkung 1.3.3 Seien A und I Mengen. Jeder Abbildung aus $\text{Abb}(I, A)$ entspricht genau ein Tupel aus A^I und umgekehrt, nämlich: Der Abbildung $f \in \text{Abb}(I, A)$ entspricht das Tupel $(a_i)_{i \in I} \in A^I$ mit $a_i = f(i)$ für alle $i \in I$.

Definition 1.3.4 Die **Identität** auf einer Menge A ist $\text{id}_A: A \rightarrow A, a \mapsto a$.

Definition 1.3.5 Seien A, B, C Mengen und seien $f: A \rightarrow B$ und $g: B \rightarrow C$ Abbildungen. Dann ist die **Verkettung** (man sagt auch „**Verknüpfung**“) von f und g die Abbildung

$$g \circ f: A \rightarrow C, a \mapsto g(f(a)).$$

„ $g \circ f$ “ spricht man oft „ g **nach** f “ aus.

Definition 1.3.6 Ist $f: A \rightarrow A$ eine Abbildung von A in sich selbst und ist $k \in \mathbb{N}$, so setzen wir $f^k := \underbrace{f \circ \dots \circ f}_{k \text{ mal}}$ falls $k \geq 1$, und $f^0 := \text{id}_A$.

Definition 1.3.7 Seien A und B Mengen, und sei $f: A \rightarrow B$.

- Ist $A' \subseteq A$, so ist $f(A') := \{f(a) \mid a \in A'\}$ das **Bild von A' unter f** .
- Das Bild unter f des gesamten Definitionsbereichs A wird auch einfach nur **Bild** von f genannt. Notation dafür: $\text{im } f := f(A)$.
- Ist $B' \subseteq B$, so ist $f^{-1}(B') := \{a \in A \mid f(a) \in B'\}$ das **Urbild von B' unter f** .
- Ist $b \in B$, so schreibt man oft auch $f^{-1}(b)$ statt $f^{-1}(\{b\})$. Besteht die Menge $f^{-1}(b)$ aus genau einem Element a , so meint man mit $f^{-1}(b)$ oft auch nur dieses Element a (und nicht die Menge $\{a\}$).

Definition 1.3.8 Ist $f: A \rightarrow B$ eine Abbildung und $A' \subseteq A$ eine Teilmenge, so schreiben wir $f|_{A'}$ für die **Einschränkung** von f auf A' , d. h. $f|_{A'}: A' \rightarrow B, a \mapsto f(a)$.

Definition 1.3.9 Seien A und B Mengen, und sei $f: A \rightarrow B$.

- (a) f heißt **injektiv**, wenn für alle $b \in B$ gilt: $\#(f^{-1}(b)) \leq 1$.
Man sagt auch „ f ist eine **Injektion** von A nach B “ und schreibt dafür „ $f: A \hookrightarrow B$ “.
- (b) f heißt **surjektiv**, wenn für alle $b \in B$ gilt: $\#(f^{-1}(b)) \geq 1$.
Man sagt auch „ f ist eine **Surjektion** von A nach B “ und schreibt dafür „ $f: A \twoheadrightarrow B$ “.
- (c) f heißt **bijektiv**, wenn für alle $b \in B$ gilt: $\#(f^{-1}(b)) = 1$.
Man sagt auch „ f ist eine **Bijektion** zwischen A und B “ und schreibt dafür „ $f: A \xrightarrow{1:1} B$ “.

(Ob eine Abbildung surjektiv bzw. bijektiv ist, hängt davon ab, welche Menge man als den Wertebereich betrachtet.)

Satz 1.3.10 Seien A und B endliche Mengen gleicher Kardinalität. Dann gilt für Abbildungen $f \in \text{Abb}(A, B)$: Ist f injektiv oder surjektiv, so ist f bereits bijektiv.

Satz 1.3.11 Seien A und B Mengen und sei $f: A \rightarrow B$ eine Abbildung.

- (a) Ist f bijektiv, so existiert genau eine Abbildung $g: B \rightarrow A$, so dass gilt: $f \circ g = \text{id}_B$ und $g \circ f = \text{id}_A$.
- (b) Es gilt auch umgekehrt: Existiert eine Abbildung g wie in (a), so ist f bijektiv.

Definition 1.3.12 Ist $f: A \rightarrow B$ bijektiv, so nennt man die Abbildung g aus Satz 1.3.11 das **Inverse** von f (oder auch auch „**Umkehrabbildung** von f “). Die Notation für diese Abbildung ist f^{-1} . Im Fall $B = A$ setzt man auch $f^{-k} := (f^{-1})^k$ für $k \in \mathbb{N}$.

Bemerkung 1.3.13 Bei bijektiven Abbildungen $f: A \rightarrow B$ passt die Notation f^{-1} für die Umkehrabbildung mit der Notation für Urbilder (Definition 1.3.7) zusammen: Für $B' \subseteq B$ ist das Urbild von B' unter f das selbe wie das Bild von B' unter der Umkehrabbildung f^{-1} , und für $b \in B$ ist das Urbild von b unter f genau das Bild von b unter f^{-1} .

1.4 Partitionen und Äquivalenzrelationen

Definition 1.4.1 Sei A eine Menge.

- (a) Eine **Relation** auf A ist gegeben durch eine Teilmenge $R \subseteq A \times A$. Meistens werden Relationen mit einem Symbol bezeichnet (z. B. „ \sim “), das man zwischen zwei Elemente $a, b \in A$ schreibt (also z. B. „ $a \sim b$ “), um auszudrücken, dass $(a, b) \in R$ ist.
- (b) Eine **Äquivalenzrelation** \sim auf A ist eine Relation \sim auf A mit folgenden Eigenschaften:
 - (i) $\forall a \in A: a \sim a$ (**Reflexivität**)
 - (ii) $\forall a, b \in A: (a \sim b \Rightarrow b \sim a)$ (**Symmetrie**)
 - (iii) $\forall a, b, c \in A: (a \sim b \wedge b \sim c \Rightarrow a \sim c)$ (**Transitivität**)
Ist dies der Fall, so wird „ $a \sim b$ “ oft ausgesprochen als „ a ist äquivalent zu b “ oder „ a und b sind äquivalent“.

- (c) Ist \sim eine Äquivalenzrelation auf A und ist $a \in A$, so nennt man $\{b \in A \mid b \sim a\}$ die **Äquivalenzklasse** von a . Die Menge all dieser Äquivalenzklassen wird mit A/\sim bezeichnet; dies wird „ A modulo \sim “ ausgesprochen. (A/\sim ist also eine Menge von Mengen.)

Beispiel 1.4.2 Sind $a, m \in \mathbb{Z}$ und $m \neq 0$, so schreiben wir „ $m \mid a$ “ für: „ a ist durch m **teilbar**.“ (D. h.: $\frac{a}{m}$ ist eine ganze Zahl.) Man sagt auch: m **teilt** a .

Sei nun $m \in \mathbb{N} \setminus \{0\}$. Dann wird durch

$$a \sim b : \iff m \mid a - b$$

eine Äquivalenzrelation auf \mathbb{Z} definiert. Die übliche Notation für diese Relation ist „ $a \equiv b \pmod{m}$ “; man sagt: „ a ist **kongruent** zu b modulo m “ oder „ a und b sind **kongruent** modulo m “.

Lemma 1.4.3 Sei A eine Menge und \sim eine Äquivalenzrelation auf A . Dann gilt, für $a, b \in A$:

- (a) $a \in a/\sim$
- (b) $a \sim b \iff a/\sim = b/\sim$

Definition 1.4.4 Eine **Partition** einer Menge A ist eine Menge P von nicht-leeren Teilmengen von A , so dass es für jedes $a \in A$ genau ein $B \in P$ gibt mit $a \in B$.

Satz 1.4.5 Ist \sim eine Äquivalenzrelation auf einer Menge A , so ist A/\sim eine Partition von A .

2 Algebraische Strukturen

2.1 Gruppen, Ringe, Körper

Definition 2.1.1 (a) Eine **Gruppe** ist ein Tripel (G, \circ, e) bestehend aus einer Menge G , einer Abbildung $\circ: G \times G \rightarrow G$ und einem Element $e \in G$ mit folgenden Eigenschaften:

- (i) $\forall a, b, c \in G: (a \circ b) \circ c = a \circ (b \circ c)$ (**Assoziativität**)
- (ii) $\forall a \in G: a \circ e = e \circ a = a$ (Man sagt, „ e ist ein **neutrales Element** für \circ “.)
- (iii) $\forall a \in G: \exists b \in G: a \circ b = b \circ a = e$. (Ein solches b heißt **Inverses** von a .)

Die Bedingungen (i)–(iii) nennt man die **Gruppenaxiome**.

- (b) Gilt außerdem $\forall a, b \in G: a \circ b = b \circ a$, so nennt man G **kommutativ** oder **abelsch**. (Gilt $a \circ b = b \circ a$, so sagt man auch: „ a und b **kommutieren**“.)

Konvention 2.1.2 Eine Abbildung, die man, wie das obige „ \circ “, zwischen zwei Elemente schreibt, nennt man oft auch **Verknüpfung**.

Konvention 2.1.3 Oft nennt man auch (G, \circ) oder G eine Gruppe, wenn klar ist, was e (und \circ) sein soll. Man nennt (\circ, e) auch eine **Gruppenstruktur**

auf der Menge G . Man sagt auch: „Eine Gruppe ist eine Menge G mit einer Verknüpfung $\circ: G \times G \rightarrow G$ und einem Element $e \in G \dots$ “.

Beispiel 2.1.4 Ist A eine beliebige Menge, so bildet die Menge aller Bijektionen von A nach A eine Gruppe, mit der Verkettung von Abbildungen als Verknüpfung und id_A als neutralem Element. Diese Gruppe wird auch mit $\text{Sym}(A)$ bezeichnet und die **symmetrische Gruppe** (auf A) genannt.

Bemerkung 2.1.5 Beim Rechnen in einer Gruppe G kann man „kürzen“: Aus $a \circ b = a' \circ b$ folgt $a = a'$ (für $a, a', b \in G$); und aus $b \circ a = b \circ a'$ folgt auch $a = a'$.

Lemma 2.1.6 Ist G eine Gruppe und $a \in G$, so existiert genau ein $b \in G$ mit $a \circ b = e$. Insbesondere hat a genau ein Inverses.

Notation 2.1.7 Es gibt mehrere verschiedene typische Notationen für Gruppen; im Folgenden sind a, b Gruppenelemente und $n \in \mathbb{N} \setminus \{0\}$:

- (a) **Verknüpfung:** $a \circ b$; **neutrales Element:** e ; **Inverses von a :** a^{-1} . Wir definieren auch $a^0 := e$, $a^n := \underbrace{a \circ \dots \circ a}_{n \text{ mal}}$, $a^{-n} := (a^{-1})^n$
- (b) **Multiplikative Notation:** **Verknüpfung:** $a \cdot b$ (oder ab); **neutrales Element:** 1 ; **Inverses von a :** a^{-1} . Wir definieren auch $\frac{a}{b} := a \cdot b^{-1}$, $a^0 := e$, $a^n := \underbrace{a \cdot \dots \cdot a}_{n \text{ mal}}$, $a^{-n} := (a^{-1})^n$
- (c) **Additive Notation:** **Verknüpfung:** $a + b$; **neutrales Element:** 0 ; **Inverses von a :** $-a$. Wir definieren auch $a - b := a + (-b)$, $0 \cdot a := 0$, $n \cdot a := \underbrace{a + \dots + a}_{n \text{ mal}}$, $(-n) \cdot a := n \cdot (-a)$

Wenn nicht anders angegeben, verwenden wir Notation (a).

Bemerkung 2.1.8 Ist G eine Gruppe, so gilt für beliebige $a, b \in G$ und $m, n \in \mathbb{Z}$:

- (a) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$
- (b) $a^{m+n} = a^m \circ a^n$

Satz 2.1.9 Sind $(G_1, \circ, e_1), \dots, (G_n, \circ, e_n)$ Gruppen, so ist auch $G_1 \times \dots \times G_n$ eine Gruppe, mit der **komponentenweisen Verknüpfung**

$$(a_1, \dots, a_n) \circ (b_1, \dots, b_n) := (a_1 \circ b_1, \dots, a_n \circ b_n)$$

und mit neutralem Element (e_1, \dots, e_n) .

Bemerkung: Wenn wir ein kartesisches Produkt $G_1 \times \dots \times G_n$ als Gruppe bezeichnen, ist als Verknüpfung die komponentenweise Verknüpfung gemeint (wenn nicht anders angegeben). Diese Verknüpfung wird mit gleichem Symbol wie die Verknüpfungen der G_i geschrieben.

Definition 2.1.10 (a) Ein **Ring** ist eine Menge R mit zwei Verknüpfungen $+$: $R \times R \rightarrow R$ und \cdot : $R \times R \rightarrow R$ und mit Elementen $0 \in R$ und $1 \in R$, so dass die folgenden **Ringaxiome** gelten:

- (i) $(R, +, 0)$ ist eine abelsche Gruppe.
- (ii) \cdot ist assoziativ und 1 ist ein neutrales Element für \cdot .
- (iii) $\forall a, b, c \in R: ((a + b) \cdot c = a \cdot c + b \cdot c \wedge a \cdot (b + c) = a \cdot b + a \cdot c)$
(**Distributivität**)
- (b) Der Ring R heißt **kommutativ**, wenn die Verknüpfung \cdot kommutativ ist.
- (c) Ein **Körper** ist ein Ring K , bei dem $(K \setminus \{0\}, \cdot, 1)$ eine abelsche Gruppe ist.
- (d) Man nennt 0 auch das **Null-Element** von R und 1 das **Eins-Element**.

Konvention 2.1.11 (a) Wenn wir einen Ring R als Gruppe auffassen, ist $(R, +)$ gemeint.
 (b) Ist K ein Körper, so setzen wir $K^\times := K \setminus \{0\}$ und fassen dies als Gruppe mit \cdot als Verknüpfung auf.

Bemerkung 2.1.12 Ist K ein Körper, so gilt für alle $a, b \in K$:

- (a) $ab = 0 \iff (a = 0 \vee b = 0)$
- (b) $a \cdot (-b) = -(a \cdot b)$

Bemerkung 2.1.13 Sei K ein Körper. Fast im gesamten Abschnitt 1.1 kann man „reelle Zahl“ durch „Element von K “ ersetzen:

- (a) Sind $a_1, \dots, a_n, b \in K$, so nennt man „ $a_1x_1 + \dots + a_nx_n = b$ “ eine **lineare Gleichung über K** (Definition 1.1.4). Analog definiert man ein **lineares Gleichungssystem über K** (Definition 1.1.8).
- (b) Koeffizientenmatrix, elementare Transformation und Zeilenstufenform werden auch entsprechend definiert (Definitionen 1.1.9, 1.1.12, 1.1.15), wobei mit 0 und 1 jeweils das entsprechende Element von K gemeint ist.
- (c) Mit einer Ausnahme gelten alle Aussagen aus Abschnitt 1.1 für beliebige Körper K : Lemma 1.1.10, Lemma 1.1.11, Lemma 1.1.13, Satz 1.1.14, Satz 1.1.16 (Gauß-Elimination), Satz 1.1.17.
- (d) Die Ausnahme ist Korollar 1.1.18: Dieses muss wie folgt umformuliert werden: Sei \underline{L} ein lineares Gleichungssystem über K mit mehr Variablen als Gleichungen. Hat \underline{L} mindestens eine Lösung (dies gilt insbesondere, wenn \underline{L} homogen ist), so hat \underline{L} sogar mindestens $\#K$ viele Lösungen.

2.2 Unter- und Quotientenobjekte

Definition 2.2.1 (a) Sei (G, \circ, e) eine Gruppe. Ist $H \subseteq G$ eine Teilmenge, so dass $(H, \circ|_{H \times H}, e)$ auch eine Gruppe ist, so nennt man H eine **Untergruppe** von G und G eine **Obergruppe** von H .
 (b) Analog definiert man **Unter- und Oberringe** und **Unter- und Oberkörper**.

Beispiel 2.2.2 Ist $(G, +)$ eine abelsche Gruppe und $n \in \mathbb{N}$, so ist

$$nG := \{na \mid a \in G\}$$

eine Untergruppe von G .

Bemerkung 2.2.3 (a) Möchte man prüfen, dass eine Teilmenge H einer Gruppe G eine Untergruppe ist, so reicht es, folgendes zu prüfen:

- (i) $e \in H$
 - (ii) H ist **abgeschlossen unter** der Verknüpfung, d. h. sind $a, b \in H$, so ist auch $a \circ b \in H$.
 - (iii) H ist **abgeschlossen unter** Inversen, d. h. ist $a \in H$, so ist auch $a^{-1} \in H$.
- (b) Analoges gilt für Unterringe und Unterkörper.

Definition 2.2.4 Sei $(G, +)$ eine abelsche Gruppe und $H \subseteq G$ eine Untergruppe. Dann setzen wir $G/H := G/\sim$ (Aussprache: „ G modulo H “), wobei \sim die Äquivalenzrelation ist, die definiert ist durch

$$a \sim b \iff a - b \in H.$$

Für die Äquivalenzklasse $a/\sim \in H$ eines Elements $a \in G$ schreibt oft $a + H$ oder \bar{a} . Man nennt a auch einen **Repräsentanten** von \bar{a} , und die Abbildung $G \rightarrow G/H, a \mapsto \bar{a}$ nennt man die „**kanonische Abbildung** von G nach G/H “.

Satz 2.2.5 Ist $(G, +, 0)$ eine abelsche Gruppe und H eine Untergruppe, so ist auch G/H eine Gruppe mit der Verknüpfung

$$\bar{a} + \bar{b} := \overline{a + b}$$

und mit neutralem Element $\bar{0}$. (Man nennt G/H eine **Quotientengruppe**.)

Satz 2.2.6 Sei $n \in \mathbb{N} \setminus \{0\}$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring, mit der Multiplikation

$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$$

und mit Eins-Element $\bar{1}$. ($\mathbb{Z}/n\mathbb{Z}$ ist ein **Quotientenring**.)

Satz 2.2.7 Ist p eine Primzahl, so ist der Ring $\mathbb{Z}/p\mathbb{Z}$ sogar ein Körper.

Definition 2.2.8 Der Körper $\mathbb{Z}/p\mathbb{Z}$ (für p prim) wird mit \mathbb{F}_p bezeichnet. Die Elemente von \mathbb{F}_p werden mit $0, 1, \dots, n-1$ bezeichnet (statt mit $\bar{0}, \bar{1}, \dots, \overline{n-1}$).

2.3 Die komplexen Zahlen

Definition 2.3.1 (a) Die **komplexen Zahlen** \mathbb{C} sind wie folgt definiert: Als Gruppe setzen wir $(\mathbb{C}, +) := (\mathbb{R}^2, +)$. Das Produkt von zwei komplexen Zahlen $(a, b), (c, d) \in \mathbb{C}$ ist definiert durch $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$.
 (b) Der **Betrag** einer komplexen Zahl $z = (a, b) \in \mathbb{C}$ ist $|z| := \sqrt{a^2 + b^2} \in \mathbb{R}$.

Satz 2.3.2 (a) Die komplexen Zahlen bilden einen Körper mit Eins-Element $(1, 0)$.
 (b) Für $z, z' \in \mathbb{C}$ gilt: $|z \cdot z'| = |z| \cdot |z'|$.

Konvention 2.3.3 Wir fassen \mathbb{R} als Unterkörper von \mathbb{C} auf, indem wir $a \in \mathbb{R}$ mit $(a, 0) \in \mathbb{C}$ identifizieren. (Diese Identifikation ist mit Addition und Multiplikation kompatibel.) Die komplexe Zahl $(0, 1) \in \mathbb{C}$ wird mit i bezeichnet. So lässt sich jede komplexe Zahl $(a, b) \in \mathbb{C}$ schreiben als $a + bi$ (für $a, b \in \mathbb{R}$).

Definition 2.3.4 Sei $z = a + ib \in \mathbb{C}$.

- (a) Der **Realteil** von z ist $\operatorname{Re}(z) := a$, der **Imaginärteil** ist $\operatorname{Im}(z) := b$.
- (b) Das **(komplex) Konjugierte** von z ist $\bar{z} := a - ib$.

Satz 2.3.5 Für $z, z' \in \mathbb{C}$ gilt:

- (a) $\bar{\bar{z}} = z$
- (b) $z \in \mathbb{R} \iff z = \bar{z}$.
- (c) $\overline{z + z'} = \bar{z} + \bar{z}'$
- (d) $\overline{z \cdot z'} = \bar{z} \cdot \bar{z}'$
- (e) $z \cdot \bar{z} = |z|^2$
- (f) $z + \bar{z} = 2\operatorname{Re}(z)$

2.4 Polynomringe

Notation 2.4.1 Sei $(G, +, 0)$ eine abelsche Gruppe.

- (a) Sind $m \leq n$ zwei ganze Zahlen und sind $a_m, a_{m+1}, \dots, a_n \in G$, so setzen wir

$$\sum_{i=m}^n a_i := a_m + a_{m+1} \cdots + a_n.$$

- (b) Sei I eine Index-Menge und seien $a_i \in G$ (für $i \in I$) so, dass $a_i = 0$ ist für fast alle $i \in I$. Dann schreiben wir

$$\sum_{i \in I} a_i$$

für die Summe all derjenigen a_i , die nicht 0 sind.

Definition 2.4.2 Sei R ein kommutativer Ring und x eine Variable.

- (a) Ein **Polynom** in x über R ist gegeben durch ein Tupel $(a_i)_{i \in \mathbb{N}} \in R^{\mathbb{N}}$, wobei fast alle a_i gleich 0 sind. Wir schreiben ein solches Polynom als Term der Form

$$\sum_{i \in \mathbb{N}} a_i x^i$$

Die Menge aller Polynome in x über R wird mit $R[x]$ bezeichnet.

- (b) Die Summe und das Produkt von zwei Polynomen $\sum_{i \in \mathbb{N}} a_i x^i, \sum_{i \in \mathbb{N}} b_i x^i \in R[x]$ sind so definiert, wie es die Term-Notation suggeriert:

$$\begin{aligned} \sum_{i \in \mathbb{N}} a_i x^i + \sum_{i \in \mathbb{N}} b_i x^i &:= \sum_{i \in \mathbb{N}} (a_i + b_i) x^i \\ \left(\sum_{i \in \mathbb{N}} a_i x^i \right) \cdot \left(\sum_{i \in \mathbb{N}} b_i x^i \right) &:= \sum_{i \in \mathbb{N}} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i \end{aligned}$$

Satz 2.4.3 Ist R ein kommutativer Ring, so ist auch $R[x]$ ein kommutativer Ring.

Konvention 2.4.4 Wir fassen einen kommutativen Ring R als Unterring von $R[x]$ auf, indem wir ein Element $a \in R$ mit dem Polynom $ax^0 \in R[x]$ identifizieren.

Notation 2.4.5 Ist $M = \{a_1, \dots, a_n\}$ eine endliche Menge von reellen Zahlen, so bezeichnet $\min M$ das kleinste Element von M und $\max M$ das größte Element von M (also $\min M, \max M \in M$, und für alle $1 \leq i \leq n$ gilt: $\min M \leq a_i \leq \max M$).

Definition 2.4.6 Sei R ein Ring und $f = \sum_{n \in \mathbb{N}} a_n x^n \in R[x] \setminus \{0\}$ ein Polynom über R .

- (a) Der **Grad** von f ist definiert als $\deg f := \max\{i \in \mathbb{N} \mid a_i \neq 0\}$.
- (b) Ist $a_{\deg f} = 1$, so nennt man f **normiert**.

Satz 2.4.7 Sei R ein kommutativer Ring und seien $f, g \in R[x] \setminus \{0\}$. Dann ist $\deg(f \cdot g) \leq \deg f + \deg g$. Ist R ein Körper, so gilt sogar $\deg(f \cdot g) = \deg f + \deg g$.

Definition 2.4.8 Sei R ein Ring und $f = \sum_{n \in \mathbb{N}} a_n x^n \in R[x]$ ein Polynom über R .

- (a) Das Polynom f definiert eine Funktion von R nach R , die auch mit f bezeichnet wird: $f(b) := \sum_{n \in \mathbb{N}} a_n b^n$. Hierbei verwenden wir die Konvention $0^0 := 1$.
- (b) Eine **Nullstelle** von f ist ein Element $b \in R$ mit $f(b) = 0$.

Bemerkung 2.4.9 Ist R ein kommutativer Ring, sind $f, g \in R[x]$ und ist $a \in R$, so gilt: $(f + g)(a) = f(a) + g(a)$ und $(f \cdot g)(a) = f(a) \cdot g(a)$.

Satz 2.4.10 Ist R ein kommutativer Ring, $f \in R[x] \setminus \{0\}$ und ist $b \in R$ eine Nullstelle von f , so gibt es ein $g \in R[x]$ mit $f = (x - b) \cdot g$.

Korollar 2.4.11 Ist K ein Körper und $f \in K[x] \setminus \{0\}$, so hat f maximal $\deg f$ verschiedene Nullstellen.

Satz 2.4.12 (Fundamentalsatz der Algebra) Ist $f \in \mathbb{C}[x]$ und $\deg f \geq 1$, so besitzt f mindestens eine Nullstelle.

Korollar 2.4.13 Ist $f \in \mathbb{C}[x]$ ein normiertes Polynom vom Grad $n \in \mathbb{N}$, so existieren $a_1, \dots, a_n \in \mathbb{C}$ so dass $f = \prod_{i=1}^n (x - a_i)$ gilt. Die Menge $\{a_1, \dots, a_n\}$ ist genau die Menge der Nullstellen von f . (Allerdings kann die selbe Nullstelle mehrfach auftauchen.)

3 Vektorräume

3.1 Definition

Im Folgenden sei K ein Körper.

Definition 3.1.1 Ein **Vektorraum** über K (auch: ein **K -Vektorraum**) ist eine abelsche Gruppe $(V, +)$, zusammen mit einer Verknüpfung $\cdot: K \times V \rightarrow V$, so dass für alle $r, s \in K$ und alle $u, v \in V$ gilt:

- (a) $r \cdot (u + v) = r \cdot u + r \cdot v$
- (b) $(r + s) \cdot v = r \cdot v + s \cdot v$
- (c) $(r \cdot s) \cdot v = r \cdot (s \cdot v)$
- (d) $1 \cdot v = v$

Die Elemente von V nennt man **Vektoren**, die Elemente von K nennt man **Skalare**; $+$ heißt **Vektoraddition**, \cdot heißt **Skalarmultiplikation**. Das Element $0 \in V$ nennt man **Nullvektor**.

Beispiel 3.1.2 K^n ist ein Vektorraum mit der Skalarmultiplikation

$$r \cdot (a_1, \dots, a_n) := (ra_1, \dots, ra_n).$$

Elemente von K^n werden oft $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ geschrieben (statt (a_1, \dots, a_n)).

Beispiel 3.1.3 $K[x]$ ist ein Vektorraum über K .

Beispiel 3.1.4 Ist A eine beliebige Menge, so ist $\text{Abb}(A, K)$ ein K -Vektorraum, mit **punktweiser Vektoraddition** und **punktweiser Skalarmultiplikation**: $(f + g)(a) = f(a) + g(a)$ und $(r \cdot f)(a) = r \cdot (f(a))$ für alle $f, g \in \text{Abb}(A, K)$, alle $r \in K$ und alle $a \in A$.

Satz 3.1.5 Ist V ein K -Vektorraum, so gilt für alle $r \in K$ und alle $v \in V$:

- (a) $r \cdot v = 0 \iff (r = 0 \vee v = 0)$
- (b) $(-1) \cdot v = -v$.

3.2 Untervektorräume

Sei weiterhin K ein Körper.

Definition 3.2.1 Sei $(V, +, 0, \cdot)$ ein K -Vektorraum. Ist $U \subseteq V$ eine Teilmenge, so dass $(U, +|_{U \times U}, 0, \cdot|_{K \times U})$ auch ein Vektorraum ist, so nennt man U einen **Untervektorraum** von V .

Lemma 3.2.2 Eine Teilmenge U eines K -Vektorraums V ist ein Untervektorraum genau dann, wenn sie nicht leer ist und für alle $u, u' \in U$ und alle $r \in K$ gilt: $ru + u' \in U$.

Beispiel 3.2.3 Ist \underline{L} ein homogenes lineares Gleichungssystem über K in n Variablen, so ist die Lösungsmenge von \underline{L} ein Untervektorraum von K^n .

Bemerkung 3.2.4 Wir werden später sehen: Jeder Untervektorraum von K^n lässt sich als Lösungsmenge eines homogenen linearen Gleichungssystems über K schreiben.

Definition 3.2.5 Sei V ein K -Vektorraum, sei I eine Index-Menge und sei $v_i \in V$ für alle $i \in I$.

- (a) Eine „**Linearkombination**“ der Vektoren v_i für $i \in I$ “ ist ein Vektor, der sich in der Form

$$\sum_{i \in I} r_i \cdot v_i,$$

schreiben lässt, wobei die $r_i \in K$ Skalare sind, die fast alle 0 sind. Sind nicht alle $r_i = 0$, so nennt man die Linearkombination **nicht-trivial**.

- (b) Die Menge aller Linearkombinationen der Vektoren v_i wird mit $\langle v_i \mid i \in I \rangle_K$ bezeichnet; man nennt dies die **lineare Hülle** (oder den **Span** oder das **Erzeugnis**) der Vektoren v_i . Andere Notationen dafür: Ist $A = \{v_i \mid i \in I\}$, so schreibt man auch $\langle A \rangle_K$ statt $\langle v_i \mid i \in I \rangle_K$; ist $I = \{1, \dots, n\}$, so schreibt man auch $\langle v_1, \dots, v_n \rangle_K$.
- (c) Gilt $\langle v_i \mid i \in I \rangle_K = V$, so nennt man die Vektoren v_i ein **Erzeugendensystem** von V .

Satz 3.2.6 Ist V ein K -Vektorraum und $A \subseteq V$ eine beliebige Teilmenge. Dann ist $\langle A \rangle_K$ der kleinste Untervektorraum von V , der A enthält. Mit „kleinste“ ist gemeint: Ist $U \subseteq V$ ein beliebiger Untervektorraum, der A enthält, so ist $\langle A \rangle_K \subseteq U$.

Korollar 3.2.7 Ist V ein K -Vektorraum, $A \subseteq V$ und $B \subseteq \langle A \rangle_K$, so ist $\langle A \cup B \rangle_K = \langle A \rangle_K$.

3.3 Lineare Unabhängigkeit

Sei weiterhin K ein Körper, und sei außerdem V ein K -Vektorraum.

Definition 3.3.1 Sei I eine Indexmenge und sei $(v_i)_i \in V^I$ ein Tupel von Vektoren.

- (a) Eine nicht-triviale Linearkombination der Vektoren v_i , die gleich 0 ist, nennt man auch eine **lineare Abhängigkeit** zwischen den Vektoren v_i .
- (b) Existiert eine lineare Abhängigkeit zwischen den Vektoren v_i , so nennt man sie **linear abhängig**, sonst **linear unabhängig**.

Lemma 3.3.2 Seien $v_1, \dots, v_n \in V$. Ist $\sum_{i=1}^n r_i v_i = 0$ eine lineare Abhängigkeit mit $r_n \neq 0$, so ist $\langle v_1, \dots, v_n \rangle_K = \langle v_1, \dots, v_{n-1} \rangle_K$.

Satz 3.3.3 Seien $v_1, \dots, v_{n-1} \in V$ linear unabhängig und sei $v_n \in V \setminus \langle v_1, \dots, v_{n-1} \rangle_K$. Dann sind auch v_1, \dots, v_n linear unabhängig.

3.4 Basis und Dimension

Sei weiterhin K ein Körper und V ein K -Vektorraum.

Definition 3.4.1 Ein Tupel $(v_i)_{i \in I}$ von Vektoren $v_i \in V$ nennt man **Basis** von V , wenn es linear unabhängig ist und V erzeugt.

Beispiel 3.4.2 In K^n bilden die Vektoren

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

eine Basis, die **Standardbasis**.

Satz 3.4.3 Seien $v_1, \dots, v_n \in V$. Dann sind äquivalent:

- (a) v_1, \dots, v_n ist eine Basis von V .
- (b) v_1, \dots, v_n ist ein minimales Erzeugendensystem von V , d. h. $\langle v_1, \dots, v_n \rangle_K = V$, aber für jedes $i \leq n$ gilt: $\langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n \rangle_K \neq V$.
- (c) (v_1, \dots, v_n) ist ein maximales linear unabhängiges Tupel, d. h. (v_1, \dots, v_n) ist linear unabhängig, aber für jeden weiteren Vektor $v_{n+1} \in V$ ist das Tupel (v_1, \dots, v_{n+1}) linear abhängig.
- (d) Jeder Vektor $v \in V$ lässt sich auf eindeutige Weise als Linearkombination der Vektoren v_i schreiben, d. h. für jedes $v \in V$ existiert genau ein Tupel $(r_1, \dots, r_n) \in K^n$, so dass $\sum_{i=1}^n r_i v_i = v$ gilt.

Korollar 3.4.4 Ist V ein Vektorraum mit einem endlichen Erzeugendensystem, so existiert eine Basis von V . Sind bereits linear unabhängige Vektoren $v_1, \dots, v_n \in V$ gegeben, so existiert sogar eine Basis von V , die v_1, \dots, v_n enthält.

Bemerkung 3.4.5 Es gilt sogar allgemeiner: Jeder Vektorraum besitzt eine Basis. (Ohne Beweis.)

Lemma 3.4.6 Ist $v_1, \dots, v_n \in V$ ein Erzeugendensystem von V und sind $w_1, \dots, w_m \in V$ beliebig mit $m > n$, so sind w_1, \dots, w_m linear abhängig.

Satz 3.4.7 Sind $(v_i)_{i \in I}$ und $(w_j)_{j \in J}$ zwei Basen eines Vektorraums V , so gilt $\#I = \#J$.

Definition 3.4.8 Die **Dimension** „ $\dim V$ “ von V ist die Kardinalität einer (beliebigen) Basis von V . Ist $\dim V = n$, so sagt man auch „ V ist n -dimensional“. V heißt **endlich dimensional** falls $\dim V \in \mathbb{N}$ und **unendlich dimensional** sonst.

Satz 3.4.9 Ist $U \subseteq V$ ein Untervektorraum, so ist $\dim U \leq \dim V$.

Index

- #, 6
- \Leftarrow , 5
- \Leftrightarrow , 5
- \Rightarrow , 5
- $\xrightarrow{1:1}$, 10
- ∞ , 6
- \hookrightarrow , 10
- \mapsto , 9
- \neg , 5
- \setminus , 7
- \rightarrow , 10
- \rightarrow , 9
- Sym, 12
- |, 11
- \forall , 7
- \wedge , 5
- Abb, 9
- \mathbb{C} , 14
- \subseteq , 7
- \supseteq , 7
- deg, 16
- \exists , 7
- \in , 6
- e_i , 19
- \mathbb{F}_p , 14
- i , 14
- id, 9
- Im, 15
- im, 9
- max, 16
- min, 16
- \mathbb{N} , 2
- \cap , 7
- n -Tupel, 3
- \circ , 9, 11
- \mathcal{P} , 7
- \mathbb{Q} , 2
- \mathbb{R} , 2
- Re, 15
- \cup , 7
- \vee , 5
- \times , 7
- \mathbb{Z} , 2

- abbilden, 9
- Abbildung, 9
 - Identitätsabbildung, 9
 - inverse, 10
 - kanonische, 14
 - Umkehrabbildung, 10
- abelsch, 11
- abgeschlossen unter, 14
- abzählbar, 6
- Additive Notation, 12
- äquivalent, 10
 - e Aussagen, 5
- Äquivalenz
 - von Aussagen, 5
- Äquivalenzrelation, 10
- Assoziativität, 11
- Aussage, 5
- Axiom
 - Gruppenaxiome, 11
 - Ringaxiome, 12

- Basis, 18
 - Standardbasis, 19
- Betrag, 14
- Bijektion, 10
- bijektiv, 10
- Bild, 9

- Definitionsbereich, 9
- Differenz
 - von Mengen, 7
- Dimension, 19
- disjunkt, 7
- Disjunktion, 5
- distributiv, 13
- Distributivität, 13

- echte Teilmenge, 7
- Eins-Element, 13
- Einschränkung, 9
- Element, 6
 - neutrales, 11
- elementare Transformation, 4
- endlich dimensional, 19
- endliche Menge, 6
- erweiterte Koeffizientenmatrix, 3
- Erzeugendensystem, 18
- Erzeugnis, 18

- fast alle, 7
- folgen aus, 5

Fundamentalsatz der Algebra, 16
 Funktion, 9

 ganze Zahl, 2
 Gauß-Elimination, 4
 gelten
 (Aussage), 5
 geordnetes Paar, 2
 geschnitten, 7
 Gleichungssystem
 lineares, 3
 Grad, 16
 Graph, 9
 Gruppe, 11
 Obergruppe, 13
 symmetrische, 12
 Untergruppe, 13
 Gruppenaxiome, 11
 Gruppenstruktur, 11

 homogenes lineares Gleichungssystem,
 3

 Identität, 9
 Identitätsabbildung, 9
 Imaginärteil, 15
 implizieren, 5
 Injektion, 10
 injektiv, 10
 Inverse, 10
 Inverse Abbildung, 10
 Inverses, 11

 kanonische Abbildung, 14
 Kardinalität
 einer Menge, 6
 kartesisches Produkt, 7, 8
 Koeffizientenmatrix, 3
 erweiterte, 3
 kommutieren, 11
 kommutativ, 13
 -e Gruppe, 11
 komplexe Konjugation, 15
 komplexe Zahl, 14
 komponentenweise Verknüpfung, 12
 kongruent, 11
 Konjugation, 15
 Konjunktion, 5
 Konstante, 2
 Körper, 13

 oberkörper, 13
 Unterkörper, 13

 leere Menge, 6
 linear abhängig, 18
 linear unabhängig, 18
 lineare Abhängigkeit, 18
 lineare Gleichung, 2
 über K , 13
 lineare Hülle, 18
 lineares Gleichungssystem, 3
 homogenes, 3
 über K , 13
 Linearkombination, 18
 nicht-triviale, 18
 triviale, 18
 Lösung
 einer linearen Gleichung, 3

 mathematische Aussage, 5
 Matrix
 Koeffizienten-, 3
 Menge, 6
 Obermenge, 7
 Potenzmenge, 7
 Teilmenge, 7
 Untermenge, 7
 mit einer Menge indizierte Tupel, 8
 modulo, 11, 14
 Multiplikative Notation, 12
 Mächtigkeit, 6

 nach, 9
 natürliche Zahl, 2
 Negation, 5
 neutrales Element, 11
 nicht-triviale Linearkombination, 18
 normiert, 16
 Null-Element, 13
 Nullstelle, 16
 Nullvektor, 17

 Obergruppe, 13
 Oberkörper, 13
 Obermenge, 7
 Oberring, 13
 ohne
 Mengendifferenz, 7

 Paar
 geordnetes, 2

Partition, 11
 Pivot-Element, 4
 Polynom, 15
 normiertes, 16
 Potenzmenge, 7
 punktweise Skalarmultiplikation, 17
 punktweise Vektoraddition, 17

 Quadrupel, 3
 Quantor, 7
 Quotientengruppe, 14
 Quotientenring, 14

 Realteil, 15
 Reflexivität, 10
 Relation, 10
 Äquivalenz-, 10
 reflexive, 10
 symmetrische, 10
 transitive, 10
 Repräsentant, 14
 Ring, 12
 kommutativer, 13
 oberring, 13
 Unterring, 13
 Ringaxiome, 12

 Satz
 Fundamentalsatz der Algebra, 16
 Gauß-Elimination, 4
 Schnitt, 7
 Skalar, 17
 Skalarmultiplikation, 17
 Span, 18
 Standardbasis, 19
 Standardbasisvektor, 19
 Surjektion, 10
 surjektiv, 10
 symmetrische Gruppe, 12

 teilbar, 11
 teilen, 11
 Teilmenge, 7
 Term, 5
 Transformation
 elementare, 4
 Transitivität, 10
 Tripel, 3
 triviale Linearkombination, 18
 triviale Lösung, 4

 Tupel, 3
 mit einer Menge indizierte, 8
 unendliche, 8

 Umkehrabbildung, 10
 unendlich dimensional, 19
 unendliche Menge, 6
 Untergruppe, 13
 Unterkörper, 13
 Untermenge, 7
 Unterring, 13
 Untervektorraum, 17
 Urbild, 9

 Variable, 2
 Vektor, 17
 Nullvektor, 17
 Vektoraddition, 17
 Vektorraum, 16
 Untervektorraum, 17
 vereinigt, 7
 Vereinigung, 7
 Verkettung, 9
 Verknüpfung
 assoziative, 11
 Verknüpfung, 11
 von Abbildungen, 9
 von Relationen, 10

 Wahrheitswert, 5
 Wert, 2, 5
 Wertebereich, 9

 Zahl
 ganze, 2
 komplexe, 14
 natürliche, 2
 Zeilenstufenform, 4

 Äquivalenzklasse, 11
 überabzählbar, 6