

Kurzskript Lineare Algebra I

Immi Halupczok

4. Dezember 2024

Inhaltsverzeichnis

Lineare Algebra I	2
1 Mathematische Grundbegriffe	2
1.1 Lineare Gleichungssysteme	2
1.2 Notationen, Mengen und Tupel	5
1.3 Abbildungen	9
1.4 Partitionen und Äquivalenzrelationen	11
2 Algebraische Strukturen	12
2.1 Gruppen, Ringe, Körper	12
2.2 Unter- und Quotientenstrukturen	14
2.3 Polynomringe	16
3 Vektorräume	17
3.1 Definition	17
3.2 Untervektorräume	18
3.3 Lineare Unabhängigkeit	19
3.4 Basis und Dimension	20
4 Lineare Abbildungen und Matrizen	21
4.1 Matrizen	21
4.2 Lineare Abbildungen	23

Lineare Algebra I

Mi 9.10.

1 Mathematische Grundbegriffe

1.1 Lineare Gleichungssysteme

In diesem Abschnitt werden wir sehen, wie man sämtliche Lösungen eines linearen Gleichungssystems bestimmen kann. Wir arbeiten dabei etwas informell mit reellen Zahlen, wie Sie sie aus der Schule kennen. Wir werden das später als Motivation verwenden, um präzise zu verstehen, was wir überhaupt „Zahl“ nennen wollen.

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 $n \geq 1$ 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).

Mo 14.10.

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 . Man nennt a_1 und a_2 die **Einträge** (oder **Komponenten**) des Tupels (a_1, 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 sowohl $a_1 = b_1$ als auch $a_2 = b_2$ ist.

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

- (b) Analog definiert man **Tripel** (a_1, a_2, a_3) , **Quadrupel** (a_1, a_2, a_3, a_4) , etc., und allgemeiner **n -Tupel** (a_1, \dots, a_n) für beliebige $n \geq 1$.
- (c) Die Menge der n -Tupel, deren Einträge alle aus einer gegebenen Menge M stammen, wird mit M^n bezeichnet.

Definition 1.1.6 Eine **Lösung** einer linearen Gleichung

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

ist ein n -Tupel $(c_1, \dots, c_n) \in \mathbb{R}^n$, so dass

$$a_1c_1 + \dots + a_nc_n = b$$

gilt.

Lemma 1.1.7 (a) Sei $L := „a_1x_1 + \dots + a_nx_n = b“$ eine lineare Gleichung, sei $r \in \mathbb{R}$, und sei $\underline{c} \in \mathbb{R}^n$ eine Lösung von L . Dann ist \underline{c} auch eine Lösung des r -fachen von der Gleichung L , also der linearen Gleichung

$$(ra_1)x_1 + \dots + (ra_n)x_n = rb$$

- (b) Wir nehmen nun außerdem an, dass $L' := „a'_1x_1 + \dots + a'_nx_n = b'“$ eine weitere lineare Gleichung ist und dass \underline{c} auch eine Lösung von L' ist. Dann ist \underline{c} auch eine Lösung der Summe von L und L' , also der linearen Gleichung

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

Definition 1.1.8 Seien $m \geq 1$ und $n \geq 1$ natürliche Zahlen. Ein **lineares Gleichungssystem** in einem Variablen-tupel $\underline{x} = (x_1, \dots, x_n)$ ist ein Tupel $\underline{L} = (L_1, \dots, L_m)$, wobei jedes L_i eine lineare Gleichung in \underline{x} ist. Eine Lösung von \underline{L} ist ein Tupel $\underline{c} \in \mathbb{R}^n$, das Lösung von jeder der Gleichungen L_1, \dots, L_m ist.

Definition 1.1.9 Seien $m, n \geq 1$ natürliche Zahlen.

- (a) Eine $m \times n$ -**Matrix** (über \mathbb{R}) ist ein $m \cdot n$ -Tupel A von reellen Zahlen, die in einem Rechteck mit m Zeilen und n Spalten geschrieben werden. Die Einträge einer Matrix werden üblicherweise mit Paaren (i, j) für $1 \leq i \leq m, 1 \leq j \leq n$ indiziert, wobei i die Zeile und j die Spalte angibt; also:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix}$$

- (b) Die (**erweiterte**) **Koeffizientenmatrix** eines linearen Gleichungssystems

$$\underline{L} := \begin{pmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n = b_2 \\ \vdots & \vdots & & \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \dots + a_{m,n}x_n = b_m \end{pmatrix} \quad (1)$$

ist die $m \times (n + 1)$ -Matrix

$$\left(\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} & b_m \end{array} \right). \quad (2)$$

(Der senkrechte Strich hat formal keine Bedeutung. Er dient nur dazu, optisch sichtbar zu machen, dass die Zahlen rechts davon die rechten Seiten der Gleichungen sind.)

Definition 1.1.10 Sei

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

eine Matrix. Die folgenden Umformungen von A nennt man **elementare Zeilentransformationen** von A :

- (TAU) Tausche zwei Zeilen.
- (MUL) Wähle eine reelle Zahl $r \neq 0$ und eine Zeile i ; multipliziere alle Einträge der gewählten Zeile mit r . Die i -te Zeile von A wird also ersetzt durch

$$(ra_{i,1} \quad ra_{i,2} \quad \dots \quad ra_{i,n}).$$

- (ADD) Wähle eine reelle Zahl r und zwei verschiedene Zeilen i und j ; addiere zu jedem Eintrag der i -ten Zeile das r -fache des entsprechenden Eintrags der j -ten Zeile. Die i -te Zeile von A wird also ersetzt durch

$$(a_{i,1} + ra_{j,1} \quad a_{i,2} + ra_{j,2} \quad \dots \quad a_{i,n} + ra_{j,n}).$$

Lemma 1.1.11 Sei A eine beliebige Matrix und sei A' eine Matrix, die man aus A durch eine elementare Zeilentransformation erhält. Dann gibt es auch eine elementare Zeilentransformation, die aus A' wieder A macht.

Mi 16.10.

Satz 1.1.12 Seien \underline{L} und \underline{L}' zwei lineare Gleichungssysteme, und seien A und A' ihre Koeffizientenmatrizen. Wir nehmen an, dass man A' aus A durch eine elementare Zeilentransformation erhalten kann. Dann haben \underline{L} und \underline{L}' die selben Lösungen.

Definition 1.1.13 Man sagt, eine (Koeffizienten-)Matrix ist in **Normalform**, wenn sie die folgende Form hat:

$$\left(\begin{array}{cccc|cccc} 0 & \cdots & 0 & \boxed{1} & * & \cdots & * & 0 & * & \cdots & * & 0 & & 0 & * & \cdots & * \\ \vdots & & \vdots & 0 & 0 & \cdots & 0 & \boxed{1} & * & \cdots & * & 0 & \cdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & 0 & 0 & \cdots & 0 & \boxed{1} & & \vdots & \vdots & \vdots & \vdots \\ & & & \vdots & \vdots & \vdots & \vdots & 0 & \ddots & & & & & \vdots & \vdots & \vdots & \vdots \\ & & & \vdots & \vdots & \vdots & \vdots & 0 & & & & & & 0 & \vdots & \vdots & \vdots \\ & & & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & \vdots & \vdots & \vdots & \vdots \\ & & & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & \vdots & \vdots & \vdots & \vdots \\ & & & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & \vdots & \vdots & \vdots & \vdots \\ & & & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & & & & & & 0 & 0 & \cdots & 0 \\ \underbrace{\quad} & & \underbrace{\quad} & \underbrace{\quad} & \underbrace{\quad} & & & & & & & & & \underbrace{\quad} & \underbrace{\quad} & \underbrace{\quad} & \underbrace{\quad} \end{array} \right);$$

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-Einträge** (oder auch **Pivot-Elemente**).

Satz 1.1.14 (Gauß-Elimination) Jede Matrix kann durch endlich viele elementare Transformationen in Normalform gebracht werden.

Bemerkung 1.1.15 Die Lösungen eines beliebigen linearen Gleichungssystems \underline{L} lassen sich wie folgt bestimmen: Bringe zunächst die Koeffizientenmatrix von \underline{L} in Normalform. (Dadurch ändern sich nach Satz 1.1.12 die Lösungen nicht.) Danach lassen sich folgendermaßen alle Lösungen von \underline{L} ablesen:

- (a) Existiert in der Koeffizientenmatrix 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 folgendermaßen erhalten:
 - (i) Für jedes $j \leq n$: Enthält die j -te Spalte keinen Pivot-Eintrag, so kann x_j beliebig gewählt werden.
 - (ii) Danach sind die restlichen Variablen eindeutig festgelegt: Enthält die j -te Spalte ein Pivot-Element in der i -ten Zeile, so hat die i -te Gleichung die Form

$$x_j + a_{i,j+1}x_{j+1} + \cdots + a_{i,n}x_n = b_i,$$

wobei nur diejenigen Koeffizienten $a_{i,k}$ ungleich null sein können, deren Spalte kein Pivot-Eintrag enthält. Insbesondere haben wir die entsprechenden x_k bereits in Schritt (i) gewählt. Diese Gleichung legt also x_j eindeutig fest, nämlich: $x_j = b_i - a_{i,j+1}x_{j+1} - a_{i,j+2}x_{j+2} - \cdots - a_{i,n}x_n$.

Mo 21.10.

Korollar 1.1.16 Ist \underline{L} ein lineares Gleichungssystem mit mehr Variablen als Gleichungen, so hat \underline{L} entweder gar keine Lösung oder unendlich viele Lösungen.²

1.2 Notationen, Mengen und Tupel

In diesem Abschnitt führen wir viele grundlegende Notationen und Konventionen aus der Mathematik ein, die im gesamten Studium verwendet werden. Insbesondere werden wir einige (weitere) Notationen zu Mengen und Tupeln sehen.

Manchmal möchte man mathematische Aussagen kompakt mit Symbolen aufschreiben, statt als ausgeschriebene (deutsche) Sätze. Dafür gibt es einige Notationen.³

Notation 1.2.1 Im folgenden sind A und B zwei mathematische Aussagen.

²Achtung: Wir werden später lineare Gleichungen auch in einem allgemeineren Kontext sehen. In der Verallgemeinerung muss dieses Korollar etwas abgewandelt werden; siehe Bemerkung 2.1.12.

³Das ist insbesondere nützlich für Tafelanschriften und eigene Notizen. In ausformulierten Beweisen, die jemand anderes lesen und verstehen können soll, ist es jedoch oft besser, Dinge als Text auszuformulieren.

- (a) „ $A \wedge B$ “ bedeutet: Sowohl Aussage A als auch Aussage B ist wahr.
- (b) „ $A \vee B$ “ bedeutet: Mindestens eine der Aussagen A und B ist wahr.
- (c) „ $\neg A$ “ bedeutet: Die Aussage A ist nicht wahr.
- (d) „ $A \Rightarrow B$ “ bedeutet: Wenn A wahr ist, dann ist auch B wahr.
Man schreibt auch „ $B \Leftarrow A$ “ und sagt auch „ A **impliziert** B “ oder „ B **folgt aus** A “.
- (e) „ $A \Leftrightarrow B$ “ bedeutet: Wenn A wahr ist, dann auch B , und wenn B wahr ist, dann auch A .
Man sagt auch „ A ist **äquivalent** zu B “ oder „ A und B sind äquivalent“ oder „ A gilt genau dann, wenn B gilt“.

Notation 1.2.2 Im folgenden ist A eine mathematische Aussage, in der eine Variable x vorkommt.

- (a) „ $\forall x \in M: A$ “ bedeutet: Man kann in der Aussage A für x jedes beliebige Element von M einsetzen und erhält immer eine wahre Aussage.
Man sagt auch: „ A gilt für alle x aus M “. Manchmal schreibt man auch „ $A \quad \forall x \in M$ “.
- (b) „ $\exists x \in M: A$ “ bedeutet: Es gibt (mindestens) ein Element aus M , das man für x einsetzen kann, so dass A wahr wird.
Man sagt auch: „Es existiert ein x aus M , so dass A wahr ist.“ (Mit „existiert ein“ ist immer „existiert mindestens ein“ gemeint.)
- (c) „ $\exists^1 x \in M: A$ “ bedeutet: Es existiert genau ein Element x von M , für das A wahr ist. (Für alle anderen x aus M ist A falsch.)
Manche Leute schreiben auch „ $\exists! x \in M: A$ “

Statt „ $\forall x \in M: A$ “ schreibt man auch „ $\forall x: A$ “, wenn, man M aus dem Kontext erraten kann; und analog bei (b), (c).

Statt „ $\forall x \in M: \forall y \in M: A$ “ schreibt man auch „ $\forall x, y \in M: A$ “, etc.; und analog bei (b).

Bemerkung 1.2.3 Die Symbole \forall und \exists nennt man **Quantoren**. („ \forall “ ist der **All-Quantor**, „ \exists “ ist der **Existenz-Quantor**.)

- Definition 1.2.4 (unpräzise)** (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 „ x ist aus M “ oder „ M enthält x “. Notation dafür: „ $x \in M$ “
Zwei Mengen M_1 und M_2 sind also gleich (als Formel: „ $M_1 = M_2$ “) genau dann, wenn für jedes mathematische Objekt x gilt: $x \in M_1 \Leftrightarrow x \in M_2$.
- (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.

Konvention 1.2.5 Ist A eine Aussage und $M = \emptyset$, so wird „ $\forall x \in M: A$ “ als wahr angesehen.

Definition 1.2.6 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, also:

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

Konvention 1.2.7 (a) Eine ein-elementige Menge $\{a\}$ wird nicht als das gleiche angesehen wie das Element a selbst.

(b) Ist ein Element A von M selbst wieder eine Menge, so werden die Elemente von A nicht automatisch auch als Elemente von M angesehen.

Mi 23.10.

Definition 1.2.8 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**.

Notation 1.2.9 Ist M eine Menge und A eine Aussage, die eine Variable x enthält, so schreiben wir $\{x \in M \mid A\}$ für die Menge derjenigen Elemente x von M , für die die Aussage A wahr ist. (Manche Leute schreiben auch „ $\{x \in M : A\}$ “ oder „ $\{x \in M ; A\}$ “.) 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 $\{x \mid A, A'\}$.

Definition 1.2.10 Seien M_1 und M_2 Mengen.

- (a) M_1 heißt **Teilmenge** von M_2 , wenn jedes Element von M_1 auch ein Element von M_2 ist. Man sagt auch: „ M_1 ist eine **Untermenge** von M_2 “; oder: „ M_2 ist eine **Obermenge** von M_1 “. Notationen: $M_1 \subseteq M_2$; $M_2 \supseteq M_1$.
- (b) Die Notation $M_1 \subsetneq M_2$ bedeutet: $M_1 \subseteq M_2$ aber $M_1 \neq M_2$; man sagt: „ M_1 ist eine **echte Teilmenge** von M_2 “.

Bemerkung: In Analogie zu „ $<$ “ und „ \leq “ wäre es naheliegend, dass man statt „ \subsetneq “ auch „ \subset “ schreiben kann. Allerdings wird \subseteq deutlich häufiger benötigt als \subsetneq ; deshalb ist es üblicher, dass „ \subset “ für „ \subseteq “ steht.

Definition 1.2.11 Seien M_1 und M_2 Mengen.

- (a) Die **Vereinigung** von M_1 und M_2 ist $M_1 \cup M_2 := \{x \mid x \in M_1 \vee x \in M_2\}$ (Man sagt auch „ M_1 **vereinigt** M_2 “).
- (b) Der **Schnitt** von M_1 und M_2 ist $M_1 \cap M_2 := \{x \mid x \in M_1 \wedge x \in M_2\}$ (Man sagt auch „ M_1 **geschnitten** M_2 “). Ist $M_1 \cap M_2 = \emptyset$, so sagt man, die Mengen M_1 und M_2 sind **disjunkt**.
- (c) Die **Differenz** von M_1 und M_2 ist $M_1 \setminus M_2 := \{x \mid x \in M_1 \wedge x \notin M_2\}$ (Man sagt auch „ M_1 **ohne** M_2 “).

Notation 1.2.12 Sei I eine Indexmenge und sei M_i eine Menge für jedes $i \in I$. (Mit **Indexmenge** ist eine normale Menge gemeint, deren Elemente als Indizes verwendet werden.)

- (a) $\bigcup_{i \in I} M_i$ ist die Menge derjenigen Elemente, die in mindestens einer der Mengen M_i liegen, also formal:

$$x \in \bigcup_{i \in I} M_i \iff \exists i \in I: x \in M_i$$

Im Fall $I = \emptyset$ setzt man $\bigcup_{i \in I} M_i := \emptyset$.

- (b) $\bigcap_{i \in I} M_i$ ist die Menge derjenigen Elemente, die in jeder der Mengen M_i liegen, also formal:

$$x \in \bigcap_{i \in I} M_i \iff \forall i \in I: x \in M_i$$

Im Fall $I = \emptyset$ ist $\bigcap_{i \in I} M_i$ nicht definiert.

Notation 1.2.13 Ist $I = \{m, m+1, \dots, n\}$ für ganze Zahlen $m \leq n$, so schreibt man statt

$$\bigcup_{i \in I} M_i \quad \text{und} \quad \bigcap_{i \in I} M_i$$

auch

$$\bigcup_{i=m}^n M_i \quad \text{und} \quad \bigcap_{i=m}^n M_i.$$

Definition 1.2.14 Ist M eine Menge, so bezeichnet

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

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

Definition 1.2.15 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.

Bemerkung 1.2.16 Laut Definition 1.1.5 ist also M^n eine Kurzschreibweise für $\underbrace{M \times \dots \times M}_{n \text{ mal}}$.

Notation 1.2.17 Für ein Tupel (a_1, \dots, a_n) verwendet man als Kurzschreibweise auch $(a_i)_{1 \leq i \leq n}$. Ist aus dem Kontext klar, dass i von 1 bis n laufen soll, so schreibt man auch noch kürzer $(a_i)_i$.

Konvention 1.2.18 (a) Man unterscheidet nicht zwischen einem 1-Tupel (a) und dem Element a selbst. Anders ausgedrückt: $M^1 = M$.

- (b) Wenn manche Einträge eines Tupels selbst wieder Tupel sind, fasst man das oft als ein langes Tupel auf, also z. B. $(a, (b, c)) = (a, b, c)$. Anders ausgedrückt: Man indentifiziert oft verschiedene Klammerungen von kartesischen Produkten, also z. B.: $A \times (B \times C) = A \times B \times C$.
- (c) Manchmal ist es praktisch, auch 0-Tupel zu betrachten. Es gibt nur ein einziges 0-Tupel; es ist das einzige Element von M^0 (egal, was M ist).

1.3 Abbildungen

Ein weiteres grundlegendes Objekt in der Mathematik sind Abbildungen. Wir führen in diesem Abschnitt diesbezügliche Definitionen, Notationen und Konventionen ein.

Definition 1.3.1 Seien A und B Mengen. Eine **Abbildung** (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 f gegeben durch drei Mengen A , B und $G \subseteq A \times B$, mit der Eigenschaft, dass für jedes $a \in A$ genau ein $b \in B$ existiert mit $(a, b) \in G$. Für jedes $a \in A$ bezeichnet $f(a)$ dann das (eindeutige) Element von B , so dass $(a, f(a)) \in G$ ist.

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

Mo 28.10.

Bemerkung 1.3.2 Ist f eine Abbildung von A nach B und ist $B' \subseteq B$ eine Teilmenge, so dass $f(a) \in B'$ gilt für jedes $a \in A$, so fassen wir f manchmal auch als Abbildung von A nach B' auf, auch wenn es sich formal gesehen um eine andere Abbildung handelt.⁴

Definition 1.3.3 Sind A und B Mengen, so bezeichnet $\text{Abb}(A, B)$ die Menge aller Abbildungen von A nach B .

Notation 1.3.4 Statt „ $f \in \text{Abb}(A, B)$ “ schreibt man auch „ $f: A \rightarrow B$ “ oder „ $A \xrightarrow{f} B$ “. Statt „ $f(a) = b$ “ schreibt man auch „ $f: a \mapsto b$ “. Ist T ein mathematischer Ausdruck, in dem a als Variable vorkommt, so bedeutet

$$f: A \rightarrow B, a \mapsto T,$$

dass $f \in \text{Abb}(A, B)$ die Abbildung ist, die jedes $a \in A$ auf den entsprechenden Wert von T abbildet.

Konvention 1.3.5 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.

Definition 1.3.6 Die **Identität** auf einer Menge A ist die Abbildung $\text{id}_A: A \rightarrow A, a \mapsto a$.

⁴Manchmal wird gar nicht zwischen diesen $f: A \rightarrow B$ und $f: A \rightarrow B'$ unterschieden; das würde in dieser Vorlesung allerdings manchmal zu Verwirrung führen.

Definition 1.3.7 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 „**nach f** “ aus.

Definition 1.3.8 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 $f^0 := \text{id}_A$.

Notation 1.3.9 Ist A eine Aussage, in der eine Variable x vorkommt und $f: B \rightarrow C$ eine Abbildung, so schreibt man $\{f(x) \mid A\}$ für die Menge all der Elemente von C , die man erhält, wenn man f auf alle Elemente $x \in B$ anwendet, für die die Aussage A wahr ist; also formal:

$$\{f(x) \mid A\} = \{c \in C \mid \exists x \in B: A\}.$$

Definition 1.3.10 Seien A und B Mengen, und sei $f: A \rightarrow B$.

- (a) Ist $A' \subseteq A$, so ist $f(A') := \{f(a) \mid a \in A'\}$ das **Bild von A' unter f** .
- (b) Das Bild unter f des gesamten Definitionsbereichs A wird auch einfach nur **Bild** von f genannt. Notation dafür: $\text{im } f := f(A)$.
- (c) Ist $B' \subseteq B$, so ist $f^{-1}(B') := \{a \in A \mid f(a) \in B'\}$ das **Urbild von B' unter f** .
- (d) 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 1.3.11 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 „ $f: A \xrightarrow{1:1} B$ “.

Satz 1.3.12 Seien A und B Mengen und sei $f: A \rightarrow B$ eine Abbildung.

- (a) Die Abbildung f ist bijektiv genau dann, wenn eine Abbildung $g: B \rightarrow A$ existiert, so dass $f \circ g = \text{id}_B$ und $g \circ f = \text{id}_A$ gilt.
- (b) Ist dies der Fall, so ist die Abbildung g aus (a) eindeutig durch f festgelegt.

Mi 30.10.

Definition 1.3.13 Ist $f: A \rightarrow B$ bijektiv, so nennt man die Abbildung g aus Satz 1.3.12 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 1.3.14 Bei bijektiven Abbildungen $f: A \rightarrow B$ passt die Notation f^{-1} für die Umkehrabbildung mit der Notation für Urbilder (Definition 1.3.10) 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} .

Definition 1.3.15 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. $f|_{A'}: A' \rightarrow B, a \mapsto f(a)$.

Satz 1.3.16 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.

1.4 Partitionen und Äquivalenzrelationen

Manchmal möchte man eine Menge M in Teile zerlegen. Dies nennt man eine Partition von M . Anstatt direkt anzugeben, was die Teile sind, ist es manchmal praktischer zu beschreiben, wann Elemente im gleichen Teil liegen sollen (und wann nicht). Dies führt zum Begriff einer Äquivalenzrelation auf M . Wir werden auch ein wichtiges Beispiel einer Äquivalenzrelation auf \mathbb{Z} sehen.

Definition 1.4.1 Eine **Partition** einer Menge M ist eine Menge P von nicht-leeren Teilmengen von M (die man die **Teile** von P nennt), so dass jedes $a \in M$ in genau einem Teil $T \in P$ liegt.

Definition 1.4.2 Sei M eine Menge. Eine **Relation** auf M ist gegeben durch eine Teilmenge $R \subseteq M \times M$. Meistens werden Relationen mit einem Symbol bezeichnet (z. B. „ $<$ “), das man zwischen zwei Elemente $a, b \in M$ schreibt (also z. B. „ $a < b$ “), um auszudrücken, dass $(a, b) \in R$ ist.

Beispiel 1.4.3 Ist P eine Partition einer Menge M , so können wir eine Relation \sim wie folgt definieren: $a \sim b$ genau dann, wenn a und b im gleichen Teil von P liegen. Dies ist eine Äquivalenzrelation im Sinne der folgenden Definition.

Definition 1.4.4 Sei M eine Menge.

(a) Eine **Äquivalenzrelation** auf M ist eine Relation \sim auf M mit folgenden Eigenschaften:

- (i) $\forall a \in M: a \sim a$ (**Reflexivität**)
- (ii) $\forall a, b \in M: (a \sim b \Rightarrow b \sim a)$ (**Symmetrie**)
- (iii) $\forall a, b, c \in M: (a \sim b \wedge b \sim c \Rightarrow a \sim c)$ (**Transitivität**)

Ist dies der Fall, so wird „ $a \sim b$ “ oft ausgesprochen als „ a ist **äquivalent** zu b “ oder „ a und b sind **äquivalent**“.

(b) Ist \sim eine Äquivalenzrelation auf M und ist $a \in M$, so nennt man

$$a/\sim := \{b \in M \mid b \sim a\}$$

die **Äquivalenzklasse** von a . Man schreibt

$$M/\sim := \{a/\sim \mid a \in M\}$$

für die Menge all dieser Äquivalenzklassen. (Den Schrägstrich „/“ spricht man in diesem Zusammenhang „modulo“ aus.)

Beispiel 1.4.5 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 “.

Satz 1.4.6 Ist \sim eine Äquivalenzrelation auf einer Menge M , so ist M/\sim eine Partition von M .

Definition 1.4.7 Sei \sim eine Äquivalenzrelation auf einer Menge M .

- (a) Die Abbildung $M \rightarrow M/\sim, a \mapsto a/\sim$ nennt man die **kanonische Abbildung** von M nach M/\sim .
- (b) Ist $T \in M/\sim$ und $a \in T$, so nennt man a auch einen **Repräsentanten** von T .

2 Algebraische Strukturen

2.1 Gruppen, Ringe, Körper

In Abschnitt 1.1 haben wir mit reellen Zahlen gearbeitet, aber welche Eigenschaften von Zahlen haben wir wirklich benötigt? In diesem Abschnitt werden wir dies präzise machen, indem wir entsprechende algebraische Strukturen einführen.

Definition 2.1.1 (a) Eine **Gruppe** ist gegeben durch eine Menge G , eine Abbildung $\circ : G \times G \rightarrow G$ und ein 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**. Man sagt „ G ist eine Gruppe“ oder „ (G, \circ) ist eine Gruppe“ oder „ (G, \circ, e) ist eine Gruppe“, je nachdem, was aus dem Kontext klar ist.

- (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 **Verknüpfung**.

Beispiel 2.1.3 Ist M eine beliebige Menge, so bildet die Menge aller Bijektion von M nach M eine Gruppe, mit der Verkettung von Abbildungen als Verknüpfung und id_M als neutralem Element. Diese Gruppe wird auch mit $\text{Sym}(M)$ bezeichnet und die **symmetrische Gruppe** (auf M) genannt.

Bemerkung 2.1.4 Ist G eine Gruppe und sind $a, a', b, b' \in G$, so gilt:

- (a) $a \circ b = a' \circ b \Rightarrow a = a'$ und
 $a \circ b = a \circ b' \Rightarrow b = b'$
- (b) $a \circ b = b \Rightarrow a = e$ und
 $a \circ b = a \Rightarrow b = e$

Bemerkung 2.1.5 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, und um zu prüfen, ob b das Inverse von a ist, reicht es, zu prüfen, ob $a \circ b = e$ ist.

Mi 6.11.

Notation 2.1.6 Es gibt mehrere übliche 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 2.1.7 Ist G eine Gruppe, so gilt für beliebige $a, b \in G$ und $m, n \in \mathbb{Z}$:

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

Definition 2.1.8 (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**.

Beispiel 2.1.9 \mathbb{Z} ist ein Ring. \mathbb{Q} , \mathbb{R} und \mathbb{C} sind Körper.

Konvention 2.1.10 (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 2.1.11 Sei R ein Ring und seien $a, b \in R$. Dann gilt:

- (a) $a \cdot (-b) = -(a \cdot b)$
 (b) $a = 0 \vee b = 0 \Rightarrow a \cdot b = 0$
 (c) Ist R ein Körper, so gilt bei (b) auch die Umkehrung.

Bemerkung 2.1.12 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) (Koeffizienten)matrizen, elementare Transformationen und die Normalform werden auch entsprechend definiert (Definitionen 1.1.9, 1.1.10, 1.1.13), 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 1.1.7, Lemma 1.1.11, Satz 1.1.12, Satz 1.1.14 (Gauß-Elimination), Bemerkung 1.1.15.
 (d) Die Ausnahme ist Korollar 1.1.16: Dieses muss wie folgt umformuliert werden: Ist \underline{L} ein lineares Gleichungssystem mit mehr Variablen als Gleichungen, so hat \underline{L} entweder gar keine Lösung oder mindestens $\#K$ viele Lösungen.

Mo 11.11.

2.2 Unter- und Quotientenstrukturen

In diesem Abschnitt betrachten wir zwei Möglichkeiten, aus einer algebraischen Struktur eine neue („kleinere“) algebraische Struktur zu konstruieren: indem man eine Teilmenge nimmt, oder indem man Elemente, die ursprünglich verschieden waren, miteinander identifiziert. Auf diese Art können wir insbesondere einen Körper mit endlich vielen Elementen konstruieren.

Beispiel 2.2.1 (a) Ist K ein Körper, so ist K^n eine abelsche Gruppe, mit der Verknüpfung

$$(b_1, \dots, b_n) + (b'_1, \dots, b'_n) := (b_1 + b'_1, \dots, b_n + b'_n).$$

Wenn wir in Zukunft K^n als Gruppe auffassen, ist diese Verknüpfung gemeint.

(b) Wir betrachten nun eine lineare Gleichung der Form

$$a_1x_1 + \dots + a_nx_n = 0$$

(für $a_1, \dots, a_n \in K$). Ihre Lösungsmenge $\{(c_1, \dots, c_n) \in K^n \mid a_1c_1 + \dots + a_nc_n = 0\}$ auch eine Gruppe (mit der gleichen Verknüpfung). Sie ist eine Untergruppe von K^n im Sinne der folgenden Definition.

Definition 2.2.2 (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**.

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.

Lemma 2.2.4 Eine Teilmenge H einer Gruppe G ist eine Untergruppe genau dann, wenn H nicht leer ist, und wenn für alle $a, b \in H$ gilt: $a \circ b^{-1} \in H$.

Definition 2.2.5 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

$$a/\sim = \{a + h \mid h \in H\}$$

schreibt man oft $a + H$ oder \bar{a} , und solche Äquivalenzklassen nennt man auch **Nebenklassen** von H .

Beispiel 2.2.6 Seien $a_1, \dots, a_n, b \in K$. Wir nehmen an, dass die lineare Gleichung

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

mindestens eine Lösung besitzt. Dann ist ihre Lösungsmenge eine Nebenklasse der Lösungsmenge von

$$a_1x_1 + \dots + a_nx_n = 0.$$

Satz 2.2.7 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** oder **Faktorgruppe**.)

Satz 2.2.8 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 2.2.9 Ist p eine Primzahl, so ist der Ring $\mathbb{Z}/p\mathbb{Z}$ sogar ein Körper.

Definition 2.2.10 Der Körper $\mathbb{Z}/p\mathbb{Z}$ (für p prim) wird mit \mathbb{F}_p bezeichnet. Die Elemente von \mathbb{F}_p werden mit $0, 1, \dots, p-1$ bezeichnet (statt mit $\bar{0}, \bar{1}, \dots, \overline{p-1}$).

Mi 13.11.

2.3 Polynomringe

In diesem Abschnitt werden die Grundlagen zu Polynomen eingeführt. Sie werden gegen Ende des Semesters nützlich sein, um gewisse Probleme aus der linearen Algebra zu lösen (nämlich um die Eigenwerte einer Matrix zu bestimmen). Der Polynomring dient auch als (wichtiges) Beispiel für einen Ring.

Definition 2.3.1 Eine **Folge** von Elementen einer Menge M ist eine Funktion $a: \mathbb{N} \rightarrow M$, wobei man a_i statt $a(i)$ schreibt und $(a_i)_{i \in \mathbb{N}}$ statt a . Wir schreiben $M^{\mathbb{N}}$ für die Menge aller Folgen von Elementen von M .

Konvention 2.3.2 Ist A eine mathematische Aussage, in der eine Variable x vorkommt, so bedeutet „ A gilt für **fast alle** $x \in M$ “: 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.)

Definition 2.3.3 Sei R ein kommutativer Ring und x eine Variable.

(a) Ein **Polynom** in x über R ist ein Ausdruck der Form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

für $n \in \mathbb{N}$ und $a_0, \dots, a_n \in R$. Wir setzen $a_i = 0$ für $i > n$, so dass ein Polynom formal gegeben ist durch eine Folge $(a_i)_{i \in \mathbb{N}} \in R^{\mathbb{N}}$, wobei fast alle a_i gleich 0 sind.

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

Notation 2.3.4 Ist $a_i = 0$ für $i > n$, so schreiben wir statt $\sum_{i=0}^n a_i x^i$ auch $\sum_{i \in \mathbb{N}} a_i x^i$.

Definition 2.3.5 Sind $f = \sum_{i \in \mathbb{N}} a_i x^i$ und $g = \sum_{i \in \mathbb{N}} b_i x^i$ zwei Polynome in $R[x]$, so definieren wir die Summe $f + g \in R[x]$ und das Produkt $f \cdot g \in R[x]$ so, wie man es von Termen erwartet:

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

Satz 2.3.6 Ist R ein kommutativer Ring, so ist auch $R[x]$ ein kommutativer Ring.

Mo 18.11.

Konvention 2.3.7 Wir fassen einen kommutativen Ring R als Unterring von $R[x]$ auf, indem wir jedes Element $a \in R$ mit dem Polynom $ax^0 \in R[x]$ identifizieren.

Definition 2.3.8 Sei R ein kommutativer Ring und $f = \sum_{n \in \mathbb{N}} a_n x^n \in R[x]$ ein Polynom über R . Der **Grad** $\deg f \in \mathbb{N} \cup \{-\infty\}$ von f ist wie folgt definiert: Ist f nicht das Nullpolynom, so ist $\deg f := \max\{i \in \mathbb{N} \mid a_i \neq 0\}$. Den Grad des Nullpolynoms definieren wir als $-\infty$.

Satz 2.3.9 Sei R ein kommutativer Ring und seien $f, g \in R[x]$. Dann ist $\deg(f \cdot g) \leq \deg f + \deg g$. Ist R ein Körper, so gilt sogar $\deg(f \cdot g) = \deg f + \deg g$. Hierbei verwenden wir die Konvention $-\infty + a = -\infty$, für $a \in \mathbb{N} \cup \{-\infty\}$.

Definition 2.3.10 Sei R ein kommutativer 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 2.3.11 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 2.3.12 Ist R ein kommutativer Ring, $f \in R[x]$ und ist $b \in R$ eine Nullstelle von f , so gibt es ein $g \in R[x]$ mit $f = (x - b) \cdot g$.

Korollar 2.3.13 Ist K ein Körper und $f \in K[x] \setminus \{0\}$, so lässt sich f schreiben in der Form

$$f = \left(\prod_{i=1}^n (x - b_i) \right) \cdot g$$

schreiben, für $b_1, \dots, b_n \in K$ und wobei $g \in K[x]$ ein Polynom ohne Nullstellen ist. Außerdem hat f maximal $\deg f$ verschiedene Nullstellen.

Bemerkung 2.3.14 Der **Fundamentalsatz der Algebra** besagt, dass jedes nicht-konstante Polynom $f \in \mathbb{C}[x]$ mindestens eine Nullstelle besitzt, d. h. im Fall $K = \mathbb{C}$ ist das g aus Korollar 2.3.13 in \mathbb{C}^\times . Körper mit dieser Eigenschaft nennt man **algebraisch abgeschlossen**. In der Algebra-Vorlesung werden wir auch sehen: Jeder Körper hat einen algebraisch abgeschlossenen Oberkörper.

Mi 20.11.

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 neutrale Element $0 \in V$ der Vektoraddition nennt man **Nullvektor**.

In Abschnitt 3.1 habe ich die Vektoraddition, die Skalarmultiplikation und den Nullvektor in rot geschrieben, damit man sie von $+$, \cdot und 0 in K unterscheiden kann.

Beispiel 3.1.2 K^n ist ein Vektorraum mit der Skalarmultiplikation

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

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 M eine beliebige Menge, so ist $\text{Abb}(M, K)$ 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 $a \in M$.

Beispiel 3.1.5 Sei K ein Körper und seien x_1, \dots, x_n Variablen. Die Menge aller linearen Gleichungen über K in x_1, \dots, x_n bildet einen K -Vektorraum, mit der Vektoraddition und der Skalarmultiplikation aus Lemma 1.1.7.

Satz 3.1.6 Ist V ein K -Vektorraum, so gilt für alle $r \in K$ und alle $v \in V$:

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

3.2 Untervektorräume

Sei weiterhin K ein Körper.

Definition 3.2.1 Sei $(V, +, \cdot)$ ein K -Vektorraum. Ist $U \subseteq V$ eine Teilmenge, so dass $(U, +|_{U \times U}, \cdot|_{K \times U})$ auch ein K -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: $ru + u' \in U$.

Mo 25.11.

Definition 3.2.3 Wir nennen ein lineares Gleichungssystem \underline{L} **homogen**, wenn die rechte Seite jeder Gleichung 0 ist, also wenn die Koeffizientenmatrix die Form

$$\left(\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & 0 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} & 0 \end{array} \right)$$

hat.

Beispiel 3.2.4 Ist \underline{L} ein homogenes lineares Gleichungssystem über K in n Variablen, so ist die Lösungsmenge von \underline{L} ein Untervektorraum von K^n .

Definition 3.2.5 Sei V ein K -Vektorraum.

- (a) Eine **Linearkombination** von Vektoren $v_1, \dots, v_n \in V$ ist ein Vektor der Form

$$\sum_{i=1}^n r_i \cdot v_i$$

für $r_1, \dots, r_n \in K$. Man nennt eine solche Linearkombination **nicht-trivial**, wenn mindestens eins der r_i nicht 0 ist. Man schreibt

$$\langle v_1, \dots, v_n \rangle_K := \left\{ \sum_{i=1}^n r_i \cdot v_i \mid r_1, \dots, r_n \in K \right\}$$

für die Menge aller Linearkombinationen von v_1, \dots, v_n .

Ist allgemeiner $A \subseteq V$ eine beliebige Teilmenge von V , so schreibt man

$$\langle A \rangle_K := \left\{ \sum_{i=1}^n r_i \cdot v_i \mid n \in \mathbb{N}, r_i \in K, v_i \in A \right\}.$$

für die Menge aller Linearkombinationen von (jeweils endlich vielen) Vektoren aus A .

Man nennt $\langle v_1, \dots, v_n \rangle_K$ bzw. $\langle A \rangle_K$ die **lineare Hülle** (oder den **Span** oder das **Erzeugnis**) von v_1, \dots, v_n bzw. von A .

Das Erzeugnis der leeren Mengen definiert man als $\langle \emptyset \rangle_K := \{0\}$.

- (b) Gilt $\langle A \rangle_K = V$, so nennt man A ein **Erzeugendensystem** von V ; man sagt auch: A **erzeugt** V .

Satz 3.2.6 Sei 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 (a) Eine **lineare Abhängigkeit** zwischen Vektoren $v_1, \dots, v_n \in V$ ist eine nicht-triviale Linearkombination

$$\sum_{i=1}^n r_i \cdot v_i,$$

die gleich 0 ist. Existiert eine lineare Abhängigkeit zwischen den Vektoren v_1, \dots, v_n , so nennt man das Tupel (v_1, \dots, v_n) **linear abhängig**; sonst nennt man es **linear unabhängig**. Man sagt auch: „Die Vektoren v_1, \dots, v_n sind linear (un)abhängig“ (und meint damit, dass das Tupel linear (un)abhängig ist).

- (b) Eine Teilmenge $A \subseteq V$ heißt **linear abhängig**, wenn endlich viele, paarweise verschiedene Vektoren $v_1, \dots, v_n \in A$ existieren, die linear abhängig sind.

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 $\langle v_1, \dots, v_n \rangle_K = \langle v_1, \dots, v_{n-1} \rangle_K$.

Mi 27.11.

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 Sei B entweder eine Teilmenge von V oder ein Tupel von Vektoren aus V . Man nennt B eine **Basis** von V , wenn B 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 von K^n , die **Standardbasis**.

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

- (v_1, \dots, v_n) ist eine Basis von V .
- (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: $\langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n \rangle_K \neq V$.
- (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.
- 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.

Satz 3.4.4 (Basisergänzungssatz) Entweder V besitzt eine Basis v_1, \dots, v_n , oder es existiert eine unendliche linear unabhängige Menge $\{v_i \mid i \in \mathbb{N}_{\geq 1}\} \subseteq V$. Sind linear unabhängige Vektoren $w_1, \dots, w_k \in V$ gegeben, so kann (in beiden Fällen) außerdem $v_1 = w_1, \dots, v_k = w_k$ gewählt werden.

Mo 2.12.

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_1, \dots, v_n und w_1, \dots, w_m zwei Basen eines Vektorraums V , so gilt $n = m$.

Bemerkung 3.4.8 Man kann definieren, was die **Kardinalität** einer unendlichen Menge ist. Die präzise Definition ist kompliziert, aber die wichtigste Eigenschaft dieser Definition ist: Zwei (beliebige) Mengen M und M' haben die gleiche Kardinalität genau dann, wenn eine Bijektion $M \rightarrow M'$ existiert. (Man nennt eine unendliche Menge **abzählbar (unendlich)**, wenn Sie die gleiche Kardinalität wie \mathbb{N} hat und **überabzählbar** sonst.)

Mit dieser Definition gilt die folgende Verallgemeinerung von Satz 3.4.7: Sind $B, B' \subseteq V$ zwei Basen eines Vektorraums V , so haben B und B' die gleiche Kardinalität. (Ohne Beweis.)

Definition 3.4.9 Die **Dimension** eines Vektorraums V ist die Kardinalität einer beliebigen Basis von V ; Notation dafür: $\dim V$. Man nennt V **endlich dimensional**, wenn $\dim V \in \mathbb{N}$ ist und **unendlich dimensional** sonst.

Satz 3.4.10 Sei V endlich-dimensional und sei $U \subseteq V$ ein Untervektorraum. Dann ist $\dim U \leq \dim V$, und aus $\dim U = \dim V$ folgt $U = V$.

Bemerkung 3.4.11 Sind $U, U' \subseteq V$ Untervektorräume, so sind auch $U \cap U'$ und

$$U + U' := \{u + u' \mid u \in U, u' \in U'\}$$

Untervektorräume von V . (Man nennt $U + U'$ die **Summe** von U und U').

Satz 3.4.12 Für beliebige Untervektorräume $U, U' \subseteq V$ eines endlich-dimensionalen Vektorraums V gilt:

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

Mi 4.12.

4 Lineare Abbildungen und Matrizen

4.1 Matrizen

Sei weiterhin K ein Körper.

Hier sind einige Ergänzungen zur Definition von Matrizen (1.1.9):

Definition 4.1.1 Seien $m, n \in \mathbb{N}$ und $a_{i,j} \in K$ für $1 \leq i \leq m$ und $1 \leq j \leq n$.

- (a) Betrachtet man die $m \times n$ -Matrix mit Einträgen $a_{i,j}$, so lässt man in der Notation oft das Komma im Index weg:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Außerdem schreibt man für diese Matrix auch $(a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$ oder $(a_{ij})_{ij}$.

- (b) Man nennt eine Matrix **quadratisch**, wenn sie gleich viele Zeilen wie Spalten hat, also wenn $m = n$ ist.
- (c) Die Menge aller $m \times n$ -Matrizen über K wird mit $K^{m \times n}$ bezeichnet und auf übliche Weise als K -Vektorraum aufgefasst (d. h. mit komponentenweiser Vektoraddition und Skalarmultiplikation). Die Matrix, deren Einträge alle 0 sind, heißt **Nullmatrix** (und wird wie üblich selbst mit 0 bezeichnet).

Definition 4.1.2 Seien $\ell, m, n \in \mathbb{N}$.

- (a) Ist $A = (a_{ij})_{ij} \in K^{\ell \times m}$ und $B = (b_{jk})_{jk} \in K^{m \times n}$, so definieren wir das **(Matrix-)Produkt** $A \cdot B$ als diejenige Matrix $(c_{ik})_{ik} \in K^{\ell \times n}$, die gegeben ist durch

$$c_{ik} = \sum_{j=1}^m a_{ij} b_{jk}.$$

(Statt $A \cdot B$ schreibt man auch AB .)

- (b) Wir identifizieren n -Tupel in K^n oft mit der entsprechenden Matrix in $K^{n \times 1}$, die nur aus einer Spalte besteht. Dadurch können wir eine Matrix $A \in K^{m \times n}$ als Abbildung von K^n nach K^m auffassen, die $v \in K^n$ abbildet auf das Matrixprodukt $Av \in K^m$.

Satz 4.1.3 Das Matrixprodukt entspricht der Verknüpfung der entsprechenden Abbildungen: Ist $A \in K^{\ell \times m}$, $B \in K^{m \times n}$ und $v \in K^n$, so gilt $(AB)v = A(Bv)$.

Notation 4.1.4 Sind $v_1, \dots, v_n \in K^m$, so schreiben wir $(v_1 \mid \dots \mid v_n)$ für die Matrix, die man erhält, indem man die Vektoren v_1, \dots, v_n als Spalten nebeneinander schreibt.

Bemerkung 4.1.5 Für eine Matrix $A = (v_1 \mid \dots \mid v_n) \in K^{m \times n}$ mit Spalten $v_i \in K^m$ gilt:

$$A \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \sum_{i=1}^n r_i v_i.$$

Insbesondere gilt für Standard-Basisvektoren $e_i \in K^n$ (siehe Beispiel 3.4.2) $Ae_i = v_i$, und das Bild im A (im Sinne von Definition 1.3.10) ist genau das Erzeugnis $\langle v_1, \dots, v_n \rangle_K$.

Beispiel 4.1.6 Ist $A = (a_{ij})_{ij} \in K^{m \times n}$ und $\underline{b} = (b_i)_i \in K^m$, so lässt sich das Gleichungssystem mit Koeffizientenmatrix

$$(A \mid \underline{b}) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right)$$

jetzt als eine einzige Gleichung in K^m schreiben, nämlich $A\underline{x} = \underline{b}$, wobei \underline{x} als eine Variable in K^n aufgefasst wird.

Definition 4.1.7 Sei $n \in \mathbb{N}$. Die **Einheitsmatrix** $I_n \in K^{n \times n}$ ist die Matrix, die der Identitätsabbildung $K^n \rightarrow K^n$ entspricht:

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Mo 9.12.

Lemma 4.1.8 Für Matrizen $A, A' \in K^{k \times \ell}$, $B, B' \in K^{\ell \times m}$ und $C \in K^{m \times n}$ gilt:

- (a) $(AB)C = A(BC)$
- (b) $I_k A = A$ und $A I_\ell = A$.
- (c) $(rA)B = r(AB)$ und $A(rB) = r(AB)$.
- (d) $(A + A')B = AB + A'B$ und $A(B + B') = AB + AB'$

Achtung: Das Analogon von Bemerkung 2.1.4 gilt *nicht* für Matrixmultiplikation, d. h. aus $AB = A'B$ folgt i. A. *nicht* $A = A'$ (für Matrizen A, A', B).

Bemerkung 4.1.9 Insbesondere gilt, für $A \in K^{m \times n}$, $v, v' \in K^n$ und $r \in K$: $A(v + v') = Av + Av'$ und $A(rv) = r(Av)$.

Korollar 4.1.10 $K^{n \times n}$ ist mit der Matrixmultiplikation ein Ring; I_n ist das neutrale Element der Multiplikation.

4.2 Lineare Abbildungen

Sei weiterhin K ein Körper.

Definition 4.2.1 Seien V und W K -Vektorräume. Eine Abbildung $f: V \rightarrow W$ heißt **linear** oder (**Vektorraum-**) **Homomorphismus**, wenn für alle $v, v' \in V$ und alle $r \in K$ gilt:

$$f(v + v') = f(v) + f(v') \quad \text{und} \quad f(rv) = rf(v).$$

Die Menge aller Vektorraum-Homomorphismen von V nach W wird mit $\text{Hom}(V, W)$ bezeichnet. (Manchmal schreibt man auch $\text{Hom}_K(V, W)$.)

Bemerkung 4.2.2 (a) Eine Abbildung $f: V \rightarrow W$ ist linear genau dann, wenn für alle $v, v' \in V$ und alle $r \in K$ gilt: $f(rv + v') = rf(v) + f(v')$.
 (b) Ist f linear, so gilt automatisch auch $f(0) = 0$.

Beispiel 4.2.3 Jede durch eine Matrix $A \in K^{m \times n}$ gegebene Abbildung von K^n nach K^m ist linear.

Bemerkung 4.2.4 Sind U, V und W K -Vektorräume und $f: U \rightarrow V$ und $g: V \rightarrow W$ lineare Abbildungen, so ist auch die Verknüpfung $g \circ f: U \rightarrow W$ ist eine lineare Abbildung.

Satz 4.2.5 Sind V und W K -Vektorräume, ist v_1, \dots, v_n eine Basis von V und sind w_1, \dots, w_n beliebige Vektoren in W , so gibt es genau eine lineare Abbildung $f: V \rightarrow W$, die v_i auf w_i abbildet für $1 \leq i \leq n$.

Korollar 4.2.6 Die linearen Abbildungen von K^n nach K^m sind genau diejenigen Abbildungen, die durch Matrizen $A \in K^{m \times n}$ gegeben sind. Wir haben also eine Bijektion von $K^{m \times n}$ nach $\text{Hom}(K^n, K^m)$ (die einer Matrix die zugehörige Abbildung zuordnet).

Korollar 4.2.7 Sind V und W K -Vektorräume und $U \subseteq V$ ein Untervektorraum, so lässt sich jede lineare Abbildung $U \rightarrow W$ zu einer linearen Abbildung $V \rightarrow W$ fortsetzen.

Definition 4.2.8 Der **Kern** einer linearen Abbildung $f \in \text{Hom}(V, W)$ ist

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

Satz 4.2.9 Seien V und W K -Vektorräume und $f: V \rightarrow W$ eine lineare Abbildung. Dann gilt:

- (a) Der Kern $\ker f$ ist ein Untervektorraum von V .
- (b) Das Bild $\text{im } f$ ist ein Untervektorraum von W (vgl. Definition 1.3.10).
- (c) Für $v, v' \in V$ gilt: $f(v) = f(v') \iff v - v' \in \ker f$. Insbesondere ist f injektiv genau dann, wenn $\ker f = \{0\}$ ist.

Definition 4.2.10 Seien V und W K -Vektorräume.

- (a) Eine bijektive lineare Abbildung $f \in \text{Hom}(V, W)$ nennt man einen (**Vektorraum-**) **Isomorphismus**. Um auszudrücken, dass eine Abbildung $f: V \rightarrow W$ ein Isomorphismus ist, schreiben wir auch $f: V \xrightarrow{\sim} W$.
- (b) Man sagt, ein K -Vektorraum V ist **isomorph** zu einem K -Vektorraum W , wenn ein Isomorphismus $f: V \rightarrow W$ existiert. Statt „ V ist isomorph zu W “ sagt man auch „ V und W sind isomorph (zueinander)“. Notation dafür: $V \cong W$.

Beispiel 4.2.11 Ist V ein K -Vektorraum und v_1, \dots, v_n eine Basis von V , so ist

$$K^n \rightarrow V, \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_{i=1}^n a_i v_i$$

ein Isomorphismus von Vektorräumen.

Satz 4.2.12 Seien V und W K -Vektorräume und sei $f: V \rightarrow W$ ein Isomorphismus. Dann ist die inverse Abbildung $f^{-1}: W \rightarrow V$ auch ein Isomorphismus.

Bemerkung: Ist $f \in \text{Hom}(V, W)$ ein Isomorphismus von Vektorräumen, so lassen sich mit f „Eigenschaften zwischen V und W übertragen“.

Index

- /, 15
- #, 7
- \Leftarrow , 6
- \Leftrightarrow , 6
- \Rightarrow , 6
- $\xrightarrow{1:1}$, 10
- \hookrightarrow , 10
- \mapsto , 9
- \neg , 6
- \setminus , 7
- \sim , 11
- \rightarrow , 10
- \twoheadrightarrow , 9
- Sym, 12
- |, 12
- \forall , 6
- \wedge , 6
- Abb, 9
- \subseteq , 7
- \supseteq , 7
- deg, 16
- dim, 21
- \exists , 6
- \in , 6
- e_i (Standardbasis), 20
- $\exists^{=1}$, 6
- \mathbb{F}_p , 15
- Hom, 23
- I_n , 23
- id, 9
- im, 10
- ker, 24
- \mathbb{N} , 2
- \cap , 7
- n -Tupel, 3
- \circ , 10, 12
- \mathcal{P} , 8
- \mathbb{Q} , 2
- \mathbb{R} , 2
- \cup , 7
- \vee , 6
- \times , 8
- \mathbb{Z} , 2

- abbilden, 9
- Abbildung, 9
 - Identitätsabbildung, 9
 - inverse, 10
 - lineare, 23
 - Umkehrabbildung, 10
- abelsch, 12
- abgeschlossen
 - algebraisch, 17
- abgeschlossen unter einer Verknüpfung, 15
- abgeschlossen unter Inversen, 15
- abhängig
 - linear, 19
- abzählbar (unendlich), 21
- Additive Notation, 13
- algebraisch abgeschlossen, 17
- All-Quantor, 6
- äquivalent, 11
 - e Aussagen, 6
- Äquivalenz
 - von Aussagen, 6
- Äquivalenzrelation, 11
- Assoziativität, 12
- Axiom
 - Gruppenaxiome, 12
 - Ringaxiome, 13
- Basis, 20
 - Standardbasis, 20
- Basisergänzungssatz, 20
- Bijektion, 10
- bijektiv, 10
- Bild, 10

- Definitionsbereich, 9
- Differenz
 - von Mengen, 7
- Dimension, 21
- disjunkt, 7
- distributiv, 13
- Distributivität, 13

- echte Teilmenge, 7
- Einheitsmatrix, 23
- Eins-Element, 13
- Einschränkung, 11
- Eintrag, 2
- Element, 6
 - neutrales, 12

elementare Zeilentransformation, 4
 endlich dimensional, 21
 endliche Menge, 7
 (erweiterte) Koeffizientenmatrix, 3
 erzeugen, 19
 Erzeugendensystem, 19
 Erzeugnis, 19
 Existenz-Quantor, 6

 Faktorgruppe, 15
 fast alle, 16
 Folge, 16
 folgen aus, 6
 Fundamentalsatz der Algebra, 17
 Funktion, 9

 ganze Zahl, 2
 Gauß-Elimination, 5
 geordnetes Paar, 2
 geschnitten, 7
 Gleichungssystem
 lineares, 3
 Grad, 16
 Graph, 9
 Gruppe, 12
 Obergruppe, 14
 symmetrische, 12
 Untergruppe, 14
 Gruppenaxiome, 12

 homogenes lineares Gleichungssystem,
 18
 Homomorphismus
 Vektorraum-Homomorphismus, 23

 Identität, 9
 Identitätsabbildung, 9
 implizieren, 6
 Indexmenge, 8
 Injektion, 10
 injektiv, 10
 Inverse, 10
 Inverse Abbildung, 10
 Inverses, 12
 isomorph, 24
 Isomorphismus
 von Vektorräumen, 24

 kanonische Abbildung, 12
 Kardinalität
 einer Menge, 7

 von unendlichen Mengen, 21
 kartesisches Produkt, 8
 Kern, 24
 Koeffizientenmatrix
 erweiterte, 3
 kommutieren, 12
 kommutativ, 13
 -e Gruppe, 12
 Komponente, 2
 kongruent, 12
 Konstante, 2
 Körper, 13
 oberkörper, 15
 Unterkörper, 15

 leere Menge, 6
 linear abhängig, 19, 20
 linear unabhängig, 19
 lineare Abbildung, 23
 lineare Abhängigkeit, 19
 lineare Gleichung, 2
 über K , 14
 lineare Hülle, 19
 lineares Gleichungssystem, 3
 über K , 14
 Linearkombination, 19
 nicht-triviale, 19
 triviale, 19
 Lösung
 einer linearen Gleichung, 3

 Matrix, 3
 Einheitsmatrix, 23
 Nullmatrix, 22
 Matrixmultiplikation, 22
 Matrixprodukt, 22
 Menge, 6
 Obermenge, 7
 Potenzmenge, 8
 Teilmenge, 7
 Untermenge, 7
 modulo, 15
 Multiplikative Notation, 13
 Mächtigkeit, 7

 nach, 10
 natürliche Zahl, 2
 Nebenklasse, 15
 neutrales Element, 12
 nicht-triviale Linearkombination, 19

Normalform, 4
 Null-Element, 13
 Nullmatrix, 22
 Nullstelle, 17
 Nullvektor, 17

 Obergruppe, 14
 Oberkörper, 15
 Obermenge, 7
 Oberring, 15
 ohne
 Mengendifferenz, 7

 Paar
 geordnetes, 2
 Partition, 11
 Pivot-Eintrag, 5
 Pivot-Element, 5
 Polynom, 16
 Potenzmenge, 8
 Produkt
 von Matrizen, 22
 punktweise Skalarmultiplikation, 18
 punktweise Vektoraddition, 18

 quadratische Matrix, 22
 Quadrupel, 3
 Quantor, 6
 Quotientengruppe, 15
 Quotientenring, 15

 Reflexivität, 11
 Relation, 11
 Äquivalenz-, 11
 reflexive, 11
 symmetrische, 11
 transitive, 11
 Ring, 13
 kommutativer, 13
 oberring, 15
 Unterring, 15
 Ringaxiome, 13
 Representant
 einer Aquivalenzklasse, 12

 Satz
 Basiserganzungssatz, 20
 Fundamentalsatz der Algebra, 17
 Gau-Elimination, 5
 Schnitt, 7
 Skalar, 17

 Skalarmultiplikation, 17
 Span, 19
 Standardbasis, 20
 Standardbasisvektor, 20
 Summe
 von Untervektorraumen, 21
 Surjektion, 10
 surjektiv, 10
 symmetrische Gruppe, 12

 teilbar, 12
 Teile
 einer Partition, 11
 teilen, 12
 Teilmenge, 7
 Transformation
 elementare Zeilen-, 4
 Transitivitat, 11
 Tripel, 3
 triviale Linearkombination, 19
 Tupel, 3

 Umkehrabbildung, 10
 unabhangig
 linear, 19
 unendlich dimensional, 21
 unendliche Menge, 7
 Untergruppe, 14
 Unterkorper, 15
 Untermenge, 7
 Unterring, 15
 Untervektorraum, 18
 Urbild, 10

 Variable, 2
 Vektor, 17
 Nullvektor, 17
 Vektoraddition, 17
 Vektorraum, 17
 Untervektorraum, 18
 Vektorraum-Homomorphismus, 23
 Vektorraum-Isomorphismus, 24
 vereinigt, 7
 Vereinigung, 7
 Verkettung, 10
 Verknufung
 assoziative, 12
 Verknufung, 12
 von Abbildungen, 10
 von Relationen, 11

Wert, 2

Wertebereich, 9

Zahl

ganze, 2

natürliche, 2

Zeilentransformation

elementare, 4

Äquivalenzklasse, 11

überabzählbar, 21