Kurzskript Lineare Algebra I

Immi Halupczok

12. Juli 2023

Inhaltsverzeichnis

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 $0, 1, 2, 3, \ldots$.*[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 $\ldots, -2, -1, 0, 1, 2, \ldots$. 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', $\tilde{a}$, $\hat{a}$, $\underline{a}$, $\ldots$). 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 $a_1, \ldots, a_n$ und b reelle Zahlen. Einen Ausdruck der Form*

$$a_1x_1 + \cdots + a_nx_n = b$$

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

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

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 $a_2 = b_2$.*

(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 $n \geq 0$.*

(c) *Die Menge der n-Tupel, deren Einträge aus einer gegebenen Menge M stammen, wird mit M^n bezeichnet.*

Bemerkung: Üblicherweise unterscheidet man nicht zwischen einem 1-Tupel (a) und dem Element a selbst.

Definition 1.1.6 *Eine **Lösung** einer linearen Gleichung*

$$a_1x_1 + \cdots + a_nx_n = b$$

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

$$a_1c_1 + \cdots + a_nc_n = b$$

gilt.

Konvention 1.1.7 *Ist $n = 0$, so ist die Notation „$a_1 + \cdots + a_n$“ als 0 zu interpretieren.*

Definition 1.1.8 *Seien m und n natürliche Zahlen. Ein **lineares Gleichungssystem** in einem Variablentupel $\underline{x} = (x_1, \dots, x_n)$ 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 eine Lösung von jeder der Gleichungen $L_1, \dots, L_m$ ist.*

Definition 1.1.9 *Sei*

$$\underline{L} := \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \qquad \vdots \qquad \qquad \vdots \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{pmatrix} \tag{1}$$

ein lineares Gleichungssystem.

(a) *Die **Koeffizientenmatrix** von $\underline{L}$ ist das Tupel*

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right) \in \mathbb{R}^{m\cdot(n+1)}. \tag{2}$$

(b) *Ist $b_1 = \cdots = b_m = 0$, so nennt man $\underline{L}$* ***homogen****. In diesem Fall betrachtet man als Koeffizientenmatrix oft nur das Tupel*

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{R}^{m \cdot n}. \tag{3}$$

(Zur Unterscheidung nennt man (2) manchmal die ***erweiterte Koeffizientenmatrix*** *von $\underline{L}$.)*

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 $L :=$ „$a_1x_1 + \cdots + a_nx_n = b$“ und $L' :=$ „$a'_1x_1 + \cdots + a'_nx_n = b'$“ 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*

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

und von

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

Definition 1.1.12 *Sei $\underline{L}$ ein Gleichungssystem. Eine* ***elementare Transformation*** *von $\underline{L}$ ist ein Gleichungssytem $\underline{L}'$, 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:*

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

Hierbei steht jedes „$*$“ für eine beliege reelle Zahl, und die mit $\circledcirc$ 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) *Enhält die j-te Spalte kein Pivot-Element, so kann x_j beliebig gewählt werden.*
    (ii) *Enhält 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 er-*

gibt, 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 $x_1, \ldots, x_n$ beliebige mathematische Objekte, so schreiben wir*

$$\{x_1, \ldots, x_n\}$$

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

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

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 scheiben 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 veschiedene 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 Vorlesung[2]) $\#M := \infty$.*

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

(a) *Die Notation*
$$\forall x \in M \colon A$$
bedeutet: A gilt für jedes Element x von M. Manchmal schreibt man auch „$A \quad \forall x \in M$“.
Ist M leer, so wird „$\forall x \in M \colon A$“ als wahr angesehen.

(b) *Die Notation*
$$\exists x \in M \colon A$$
bedeutet: Es existiert mindestens ein Element x von M, für das A wahr ist.

(c) *Die Notation*
$$\exists^{=1} x \in M \colon A$$
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.)*

[2]Auch 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.

*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

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

ist eine Kurzschreibweise für „$\forall x \in M\colon \forall y \in M\colon A$“; 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 $A \cup B := \{x \mid x \in A \lor x \in B\}$ (Man sagt auch „A **vereinigt** B“).*

(b) *Der **Schnitt** von A und B ist $A \cap B := \{x \mid x \in A \land x \in B\}$ (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 $A \setminus B := \{x \mid x \in A \land x \notin B\}$ (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 von 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 $\underbrace{M \times \cdots \times M}_{n\ mal}$ 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) $\displaystyle\bigcup_{i=m}^{n} A_i := A_m \cup A_{m+1} \cup \cdots \cup A_n$

(b) $\displaystyle\bigcap_{i=m}^{n} A_i := A_m \cap A_{m+1} \cap \cdots \cap A_n$

(c) $\displaystyle\prod_{i=m}^{n} A_i := A_m \times A_{m+1} \times \cdots \times A_n$

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) $\displaystyle\bigcup_{i \in I} A_i$ *ist die Menge derjenigen Elemente, die in jeder mindestens einer der Mengen A_i liegen. Im Fall $I = \emptyset$ setzt man $\displaystyle\bigcup_{i \in I} A_i := \emptyset$.*

(b) $\displaystyle\bigcap_{i \in I} A_i$ *ist die Menge derjenigen Elemente, die in jeder der Mengen A_i liegen. Im Fall $I = \emptyset$ ist $\displaystyle\bigcap_{i \in I} A_i$ 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 $\displaystyle\prod_{i \in I} A$ 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, dass 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 $G = \{(a, f(a)) \mid a \in A\}$.

"$\mathrm{Abb}(A, B)$" *bezeichnet die Menge aller Abbildungen von A nach B. Statt „$f \in \mathrm{Abb}(A, B)$" schreibt man auch „$f\colon A \to B$", und statt $f(a) = b$ schreibt man auch „$f\colon a \mapsto b$".*

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

Konvention 1.3.2 *Ist $f\colon A_1 \times A_2 \to B$, 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 $f\colon A_1 \times A_2 \times A_3 \to B$, etc.*

Bemerkung 1.3.3 *Seien A und I Mengen. Jeder Abbildung aus $\mathrm{Abb}(I, A)$ entspricht genau ein Tupel aus A^I und umgekehrt, nämlich: Der Abbildung $f \in \mathrm{Abb}(I, A)$ 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 $\mathrm{id}_A\colon A \to A, a \mapsto a$.*

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

$$g \circ f\colon A \to C, a \mapsto g(f(a)).$$

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

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

Definition 1.3.7 *Seien A und B Mengen, und sei $f\colon A \to B$.*

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

Definition 1.3.9 *Seien A und B Mengen, und sei $f\colon A \to B$.*

(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 „$f\colon A \hookrightarrow B$“.*

(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 „$f\colon A \twoheadrightarrow B$“.*

(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 „$f\colon A \xrightarrow{1:1} B$“.*

(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 $f \in \mathrm{Abb}(A, B)$: Ist f injektiv oder surjektiv, so ist f bereits bijektiv.*

Satz 1.3.11 *Seien A und B Mengen und sei $f\colon A \to B$ eine Abbildung.*

(a) *Ist f bijektiv, so existiert genau eine Abbildung $g\colon B \to A$, so dass gilt: $f \circ g = \mathrm{id}_B$ und $g \circ f = \mathrm{id}_A$.*

(b) *Es gilt auch umgekehrt: Existiert eine Abbildung g wie in (a), so ist f bijektiv.*

Definition 1.3.12 *Ist $f\colon A \to B$ 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 $f\colon A \to B$ 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) $\forall a \in A\colon a \sim a$ ***(Reflexivität)***

(ii) $\forall a, b \in A\colon (a \sim b \Rightarrow b \sim a)$ ***(Symmetrie)***

(iii) $\forall a, b, c \in A\colon (a \sim b \wedge b \sim c \Rightarrow a \sim c)$ ***(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 „$a \equiv b \mod m$“; 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 nichtleeren 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 $\circ\colon G \times G \to G$ und einem Element $e \in G$ mit folgenden Eigentschaften:*

(i) $\forall a, b, c \in G\colon (a \circ b) \circ c = a \circ (b \circ c)$ ***(Assoziativität)***

(ii) $\forall a \in G\colon a \circ e = e \circ a = a$ *(Man sagt, „e ist ein* ***neutrales Element*** *für $\circ$“.)*

(iii) $\forall a \in G \colon \exists b \in G \colon a \circ b = b \circ a = e$. *(Ein solches b heißt **Inverses** von a.)*
*Die Bedingungen (i)–(iii) nennt man die **Gruppenaxiome**.*

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

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 Verküpfung $\circ \colon G \times G \to G$ und einem Element $e \in G \dots$“.*

Beispiel 2.1.4 *Ist A eine beliebige Menge, so bildet die Menge aller Bijektion von von A nach A eine Gruppe, mit der Verkettung von Abbildungen als Verknüpfung und id_A als neutralem Element. Diese Gruppe wird auch mit $\mathrm{Sym}(A)$ 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 $a^0 := e$, $a^n := \underbrace{a \circ \cdots \circ a}_{n \text{ mal}}$, $a^{-n} := (a^{-1})^n$*

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

(c) ***Additive Notation**: Verknüpfung: $a + b$; neutrales Element: 0; Inverses von a: $-a$. Wir definieren auch $a - b := a + (-b)$, $0 \cdot a := 0$, $n \cdot a := \underbrace{a + \cdots + a}_{n \text{ mal}}$, $(-n) \cdot a := n \cdot (-a)$*

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 $(G_1, \circ, e_1), \ldots, (G_n, \circ, e_n)$ Gruppen, so ist auch $G_1 \times \cdots \times G_n$ eine Gruppe, mit der **komponentenweisen Verknüpfung***

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

und mit neutralem Element $(e_1, \ldots, e_n)$.

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

Definition 2.1.10 (a) *Ein **Ring** ist eine Menge R mit zwei Verknüpfungen $+\colon R \times R \to R$ und $\cdot\colon R \times R \to R$ 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) *$\forall a, b, c \in R\colon \big((a + b) \cdot c = a \cdot c + b \cdot c \;\wedge\; a \cdot (b + c) = a \cdot b + a \cdot c\big)$ **(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 $a_1, \ldots, a_n, b \in K$, so nennt man „$a_1 x_1 + \cdots + a_n x_n = b$“ eine **lineare Gleichung über** K (Definition 1.1.4). Analog definiert man ein **lineares Gleichungssystem über** K (Definition 1.1.8).*
(b) *Koeffizientenmatrix, elementare Tranformation 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 definert 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 $G/H := G/\sim$ (Ausssprache: „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 $G \to G/H, a \mapsto \bar{a}$ 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 $a_m, a_{m+1}, \ldots, a_n \in G$, 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:*

$$\sum_{i \in \mathbb{N}} a_i x^i + \sum_{i \in \mathbb{N}} b_i x^i := \sum_{i \in \mathbb{N}} (a_i + b_i) x^i$$

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

Satz 2.4.3 *Ist R ein kommutativer Ring, so ist auch $R[x]$ ist 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 $M = \{a_1, \ldots, a_n\}$ 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 $\cdot : K \times V \to V$, 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*

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

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

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

Beispiel 3.1.4 *Ist A eine beliebige Menge, so ist $\mathrm{Abb}(A, K)$ ein K-Vektorraum, mit* ***punktweiser Vektorraddition*** *und* ***punktweiser Skalarmultiplikation****: $(f + g)(a) = f(a) + g(a)$ und $(r \cdot f)(a) = r \cdot (f(a))$ für alle $f, g \in \mathrm{Abb}(A, K)$, 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) $r \cdot v = 0 \iff (r = 0 \lor v = 0)$
(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 $\langle A \rangle_K \subseteq V$.*

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. („Nicht-triviale Linearkombination“ bedeutet: $r_i \in K$, und mindestens eins der r_i ist ungleich 0.) 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 abhängig“ (und meint damit das Tupel als Ganzes).*

(b) *Auch für unendlich viele Vektoren $v_i \in V$ (für i aus einer Index-Menge I) definiert man: Das Tupel $(v_i)_{i \in I}$ ist **linear abhängig**, wenn eine nicht-triviale Linearkombination*

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

existiert, die gleich 0 ist.

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

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

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

*eine Basis, die **Standardbasis**.*

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

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

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

Lemma 3.4.6 *Ist $v_1, \ldots, v_n \in V$ ein Erzeugendensystem von V und sind $w_1, \ldots, w_m \in V$ beliebig mit $m > n$, so sind $w_1, \ldots, w_m$ 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 *Es gilt sogar allgemeiner: Sind $(v_i)_{i \in I}$ und $(w_j)_{j \in J}$ zwei Basen eines Vektorraums V, so gilt $\#I = \#J$.*[3]

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 $U = V$.*

3.5 Summen, Komplemente und Quotienten

Sei weiterhin K ein Körper und sei V jetzt ein endlich-dimensionaler K-Vektorraum.[4]

Definition 3.5.1 *Sind $U, U' \subseteq V$ Untervektorräume, so setzen wir $U + U' := \{u + u' \mid u \in U, u' \in U'\}$. (Man nennt $U + U'$ die **Summe** von U und U').*

Bemerkung 3.5.2 *Sind $U, U' \subseteq V$ Untervektorräume, so ist $U + U' = \langle U \cup U' \rangle_K$; insbesondere ist $U + U'$ ein Untervektorraum von V.*

Definition 3.5.3 *Sind $U, U' \subseteq V$ Untervektorräume mit $U + U' = V$ und $U \cap U' = \{0\}$, so nennt man U' ein **Komplement** von U (in V).*

Satz 3.5.4 *Ist $U \subseteq V$ ein Untervektorraum und $U' \subseteq V$ ein Komplement von U, so gilt $\dim U + \dim U' = \dim V$.*

Satz 3.5.5 *Zu jedem Untervektorraum $U \subseteq V$ existiert ein Komplement U'.*

Korollar 3.5.6 *Für beliebige Untervektorräume $U_1, U_2 \subseteq V$ gilt:*

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

Satz 3.5.7 *Sei $U \subseteq V$ ein Untervektorraum. Dann wird die Quotientengruppe V/U (im Sinne von Satz 2.2.5) mit der folgenden Skalarmultiplikation zu einem K-Vektorraum:*

$$r \cdot \bar{v} := \overline{rv}.$$

[3] Dies gilt auch im Sinne der unendlichen Kardinalitäten aus der Fußnote zu Definition 1.2.6, das heißt also hier: Es existiert eine Bijektion zwischen I und J.

[4] Die Bedingung, dass V endlich-dimensional sein soll, ist nur dazu da, die Vorlesung etwas einfacher zu machen; alle Definitionen und Sätze in diesem Abschnitt funktionieren auch für unendlich-dimensionale Vektorräume. (Die Beweise sind aber z. T. komplizierter.)

Definition 3.5.8 *Man nennt V/U einen **Quotientenvektorraum**. Die Äquivalenzklassen $\bar{v} = v + U \subseteq V$ nennt man auch **Nebenklassen** von U.*

Satz 3.5.9 *Ist $U \subseteq V$ ein Untervektorraum und W ein Komplement von U, so enthält W genau ein Element aus jeder Nebenklasse von U, so dass man V/U mit W identifizieren kann. (Diese Identifikation ist mit der Vektoraddition und der Skalarmultiplikation kompatibel.)*

Korollar 3.5.10 *Ist $U \subseteq V$ ein Untervektorraum, so gilt $\dim V = \dim U + \dim(V/U)$.*

4 Lineare Abbildungen und Matritzen

4.1 Matrizen

Sei weiterhin K ein Körper.

Definition 4.1.1 *Seien $m, n \in \mathbb{N}$ natürliche Zahlen.*

(a) *Eine $m \times n$-**Matrix** über K ist ein $m \cdot n$-Tupel A von Elementen aus K, dessen Einträge mit Paaren (i, j) für $1 \leq i \leq m, 1 \leq j \leq n$ indiziert sind. Notation:*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}.$$

*(Hierbei ist der Index „ij" eine Kurzschreibweise für „i, j".) Ist $m = n$, so nennt man die Matrix **quadratisch**.*

(b) *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 oft 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 $(AB)v = A(Bv)$.*

Bemerkung 4.1.4 *Die Spalten einer Matrix $A \in K^{m\times n}$ sind genau die Bilder der Standardbasisvektoren $e_1, \ldots, e_n \in K^n$ (siehe Beispiel 3.4.2).*

Beispiel 4.1.5 *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*

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

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

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

Lemma 4.1.7 *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* $AI_\ell = A$.
(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 2.1.5 gilt *nicht* für Matrixmultiplikation, d. h. aus $AB = A'B$ folgt i. A. *nicht* $A = A'$ (für Matrizen A, A', B).

Bemerkung 4.1.8 *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 4.1.9 *$K^{n\times n}$ 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.*

(a) *Eine Abbildung $f\colon V \to W$ heißt **linear** oder **(Vektorraum-) Homomorphismus**, wenn für alle $v, v' \in V$ und alle $r \in K$ gilt:*

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

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

(b) *Eine bijektive lineare Abbildung $f \in \mathrm{Hom}(V,W)$ nennt man einen **(Vektorraum-) Isomorphismus**. Um auszudrücken, dass eine Abbildung $f\colon V \to W$ ein Isomorphismus ist, schreiben wir auch $f\colon V \xrightarrow{\sim} W$.*

(c) *Man sagt, ein K-Vektorraum ist V ist **isomorph** zu einem K-Vektorraum W, wenn ein Isomorphismus $f\colon V \to W$ existiert. Statt „V ist isomorph zu W“ sagt man auch „V und W sind isomorph (zueinander)“. Notation dafür: $V \cong W$.*

Bemerkung 4.2.2 (a) *Eine Abbildung $f\colon V \to W$ 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.*

Beispiel 4.2.4 (a) *Ist V ein K-Vektorraum und $U \subseteq V$ ein Untervektorraum, so ist die kanonische Abbildung $V \to V/U, v \mapsto \bar{v} = v + U$ linear.*

(b) *Ist außerdem W ein Komplement von U in V, so ist die Abbildung $W \to V/U, w \mapsto \bar{w}$ ein Isomorphismus (siehe Satz 3.5.9).*

Beispiel 4.2.5 *Ist V ein K-Vektorraum und $v_1, \ldots, v_n$ eine Basis von V, so ist*

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

ein Isomorphismus von Vektorräumen.

Satz 4.2.6 *Seien U, V und W K-Vektorräume und seien $f\colon U \to V$ und $g\colon V \to W$ lineare Abbildungen. Dann gilt:*

(a) *Die Verknüpfung $g \circ f\colon U \to W$ ist auch eine lineare Abbildung.*

(b) *Ist f ein Isomorphismus, so ist auch die inverse Abbildung f^{-1} eine lineare Abbildung (und damit ein Isomorphismus).*

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

Satz 4.2.7 *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 $f \colon V \to W$, die v_i auf w_i abbildet für $1 \leq i \leq n$.*

Korollar 4.2.8 *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 $\mathrm{Hom}(K^n, K^m)$ (die einer Matrix die zugehörige Abbildung zuordnet).*

Korollar 4.2.9 *Sind V und W K-Vektorräume und $U \subseteq V$ ein Untervektorraum, so lässt sich jede lineare Abbildung $U \to W$ zu einer linearen Abbildung $V \to W$ fortsetzen.*

Definition 4.2.10 *Der* ***Kern*** *einer linearen Abbildung $f \in \mathrm{Hom}(V, W)$ ist*

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

Satz 4.2.11 *Seien V und W K-Vektorräume und $f \colon V \to W$ eine lineare Abbildung. Dann gilt:*

(a) *Der Kern $\ker f$ ist ein Untervektorraum von V.*
(b) *Das Bild $\mathrm{im}\, f$ ist ein Untervektorraum von W (vgl. Definition 1.3.7).*
(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.*

4.3 Homomorphiesatz und Rang

Satz 4.3.1 (Homomorphiesatz) *Sind V und W K-Vektorräume und ist $f \in \mathrm{Hom}(V, W)$, so erhält man einen Isomorphismus*

$$\tilde{f} \colon V/(\ker f) \to \mathrm{im}\, f, \bar{v} \mapsto f(v).$$

Definition 4.3.2 (a) *Seien V und W endlich-dimensionale Vektorräume. Der* ***Rang*** *einer linearen Abbildung $f \in \mathrm{Hom}(V, W)$ ist*

$$\mathrm{rk}\, f := \dim(\mathrm{im}(f)) = \dim(V/\ker(f)) = \dim V - \dim\ker(f).$$

(b) *Der* ***Rang*** *$\mathrm{rk}\, A$ einer Matrix $A \in K^{m \times n}$ ist der Rang der zugehörigen Abbildung $K^m \to K^n$.*

Bemerkung 4.3.3 *Sind V und W zwei endich-dimensionale K-Vektorräume und ist $f \in \operatorname{Hom}(V, W)$, so gilt:*

(a) *Die Abbildung f ist injektiv genau dann, wenn $\operatorname{rk} f = \dim V$; im Allgemeinen gilt $\operatorname{rk} f \leq \dim V$.*
(b) *Die Abbildung f ist surjektiv genau dann, wenn $\operatorname{rk} f = \dim W$; im Allgemeinen gilt $\operatorname{rk} f \leq \dim W$.*

Satz 4.3.4 *Sind U, V und W endlich-dimensionale K-Vektorräume und $U \xrightarrow{f} V \xrightarrow{g} W$ lineare Abbildungen, so gilt*

$$\operatorname{rk}(f) + \operatorname{rk}(g) - \dim V \leq \operatorname{rk}(g \circ f) \leq \min\{\operatorname{rk} g, \operatorname{rk} f\}.$$

*(Die erste Ungleichung nennt man **Sylvesters Rang-Ungleichung**.)*

Satz 4.3.5 *Für quadratische Matritzen $A \in K^{n\times n}$ sind die folgenden Bedingungen äquivalent:*

(a) $\operatorname{rk} A = n$
(b) *Es existiert eine Matrix $B \in K^{n\times n}$ mit $AB = I_n$.*
(c) *Es existiert eine Matrix $B \in K^{n\times n}$ mit $BA = I_n$.*
(d) *Die Abbildung $A\colon K^n \to K^n$ ist injektiv.*
(e) *Die Abbildung $A\colon K^n \to K^n$ ist surjektiv.*

Wenn diese Bedingungen gelten, dann sind die Matrizen B aus (b) und (c) eindeutig und entsprechen beide der Umkehrabbildung von A.

Definition 4.3.6 *Sind die Bedingungen aus dem obigen Satz erfüllt, so nennt man A invertierbar. Die Matrix B nennt man dann das **Inverse** von A, und man schreibt A^{-1} dafür.*

Bemerkung 4.3.7 *Ist A eine beliebige Matrix und S eine invertierbare (quadratische) Matrix geeigneter Größe, so ist $\operatorname{rk} A = \operatorname{rk}(AS)$ bzw. $\operatorname{rk} A = \operatorname{rk}(SA)$.*

Bemerkung 4.3.8 *Sind $A, B \in K^{n\times n}$ beide invertierbar, so ist auch AB invertierbar, und es gilt $(AB)^{-1} = B^{-1}A^{-1}$.*

4.4 Anwendung auf lineare Gleichungssysteme

Sei weiterhin K ein Körper.

Satz 4.4.1 *Für jede Matrix $A = (a_{ij})_{ij} \in K^{m\times n}$ sind die folgenden Zahlen gleich:*

(a) *der Rang von A;*

(b) *der **Spaltenrang** von A, d. h. die Dimension des Erzeugnisses*

$$\langle \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix}, \dots, \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix} \rangle_K$$

der Spalten von A;

(c) *der **Zeilenrang** von A, d. h. die Dimension des Erzeugnisses*

$$\langle (a_{1,1}, \dots, a_{1,n}), \dots, (a_{m,1}, \dots, a_{m,n}) \rangle_K$$

der Zeilen von A.

Inbesondere ist die Dimension des Lösungsraums von $A\underline{x} = 0$ gleich n (Anzahl der Variablen) minus der maximalen Anzahl linear unabhängiger Zeilen von A.

Bemerkung 4.4.2 *Jede Zeile eines Matrix-Produkts BA (für $A \in K^{m\times n}$, $B \in K^{\ell\times m}$) ist eine Linearkombination der Zeilen von A: Sind $z_1, \dots, z_m \in K^{1\times n}$ die Zeilen von A und ist $(b_{i,1}, \dots, b_{i,m})$ die i-te Zeile von B, so ist die i-te Zeile von BA gleich*

$$b_{i,1}z_1 + \cdots + b_{i,m}z_m.$$

Insbesondere: Ist $\underline{L}$ ein lineares Gleichungssystem mit Koeffizientenmatrix $(A \mid \underline{b})$ und ist $\underline{L}'$ eine elementare Transformation von $\underline{L}$, so ist die Koeffizientenmatrix $(A' \mid \underline{b}')$ von $\underline{L}'$ gegeben durch $A' = EA$ und $\underline{b}' = E\underline{b}$ für eine Matrix $E \in K^{m\times m}$.

Definition 4.4.3 *Die Matrizen E aus Bemerkung 4.4.2, die elementaren Transformationen entsprechen, nennt man **Elementarmatrizen**, und EA nennt man eine **elementare Zeilentransformation** von A. Die Elementarmatrizen sind also die Matrizen $E = (e_{ij})_{ij}$ mit:*

(a) *Gleichungen k und ℓ vertauschen (für $1 \le k, \ell \le m$, $k \neq \ell$): $e_{ii} = 1$ falls $i \neq k, \ell$; $e_{k\ell} = e_{\ell k} = 1$; alle anderen e_{ij} sind 0;*

(b) *Gleichung k mit $r \in K^\times$ multiplizieren ($1 \le k \le m$): $e_{ii} = 1$ falls $i \neq k$ $e_{kk} = r$; alle anderen e_{ij} sind 0;*

(c) *das r-fache von Gleichung k zu Gleichung ℓ addieren (für $r \in K$ und $1 \le k, \ell \le m$, $k \neq \ell$): $e_{ii} = 1$; $e_{\ell k} = r$; alle anderen e_{ij} sind 0.*

Satz 4.4.4 *Elementarmatrizen sind invertierbar, und das Inverse einer Elementarmatrix ist auch eine Elementarmatrix.*

Satz 4.4.5 (Gauß-Algorithmus; vgl. Satz 1.1.16) *Zu jeder Matrix A existieren Elementarmatrizen $E_1, \dots, E_k$, so dass das Produkt $E_k \cdots E_1 A$ die folgende*

Form hat:

$$\begin{pmatrix}
0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * & 0 & * & \cdots & 0 & * & \cdots & * \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & 0 & * & \cdots & * \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & * & & \vdots & \vdots & & \vdots \\
\vdots & & & & & & & & & & & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots \\
\vdots & & & & & & & & & & & & \ddots & \ddots & 0 & * & \cdots & * \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & & & & & & & & & & & & & & & & & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0
\end{pmatrix}.$$

Hierbei stehen die „$*$“ für beliege Skalare.

Definition 4.4.6 *Die obige Form von Matrizen nennt man* ***Normalform****.*

Lemma 4.4.7 *Für eine Matrix in Normalform gilt: Zeilenrang = (Spalten)rang = Anzahl der Pivot-Elemente*

Definition 4.4.8 *Die* ***Transponierte*** *einer Matrix $A = (a_{ij})_{1\le i\le m, 1\le j\le n} \in K^{m\times n}$ ist die Matrix $A^T := (a_{ji})_{1\le j\le n, 1\le i\le m} \in K^{n\times m}$.*

Bemerkung 4.4.9

(a) *Für $A \in K^{m\times n}$ gilt: $(A^T)^T = A$*

(b) *Für $A, B \in K^{m\times n}$ gilt: $(A+B)^T = A^T + B^T$*

(c) *Für $A \in K^{\ell\times m}$ und $B \in K^{m\times n}$ gilt: $(AB)^T = B^T A^T$.*

(d) *Eine Matrix $A \in K^{n\times n}$ ist invertierbar genau dann, wenn A^T invertierbar ist, und ist dies der Fall, so gilt $(A^T)^{-1} = (A^{-1})^T$.*

(e) *Ist $E \in K^{n\times n}$ eine Elementarmatrix, so ist auch E^T eine Elementarmatrix. Für $A \in K^{m\times n}$ erhält man AE aus A durch eine* ***elementare Spaltentransformation****, d. h. Tauschen von Spalten bzw. Multiplikation einer Spalte mit $r \in K^\times$ bzw. Addition des r-fachen einer Spalte zu einer anderen Spalte.*

Satz 4.4.10 *Ist $A \in K^{n\times n}$, und wendet man auf die (erweiterte) Matrix $(A \mid I_n)$ Zeilentransformationen so an, dass beim Ergebnis $(A' \mid B')$ die Matrix A' in Normalform ist, so gilt:*

(a) *A ist invertierbar genau dann wenn $A' = I_n$; insbesondere lässt sich jede invertierbare Matrix als Produkt von Elementarmatrizen schreiben.*

(b) *Ist A invertierbar, so ist $B' = A^{-1}$.*

5 Endomorphismen

Im ganzen Kapitel sei weiterhin K ein Körper.

Definition 5.0.1 *Sei V ein K-Vektorraum.*

(a) *Eine lineare Abbildung von V in sich selbst nennt man auch einen* ***Endomorphismus*** *von V. Man setzt* $\mathrm{End}(V) := \mathrm{Hom}(V, V)$.

(b) *Die invertierbaren Endomorphismen von V bilden (mit der Verkettung von Abbildungen) eine Gruppe; diese Gruppe wird mit* $\mathrm{Aut}(V)$ *(oder manchmal auch* $\mathrm{GL}(V)$*) bezeichnet. Im Fall $V = K^n$ besteht* $\mathrm{Aut}(V)$ *aus den invertierbaren Matrizen in $K^{n\times n}$, und man schreibt auch* $\mathrm{GL}_n(K)$ *dafür.*

5.1 Determinanten

Satz 5.1.1 *Sind $v_1, \dots, v_n \in K^n$, so schreiben wir im Folgenden $(v_1 \mid \cdots \mid v_n) \in K^{n\times n}$ für die Matrix mit den Spalten $v_1, \dots, v_n$.*

Es existiert genau eine Abbildung $f\colon K^{n\times n} \to K$, so dass für alle $v_1, \dots, v_n \in K^n$ gilt:

(a) *f ist* ***multilinear****, d. h. für alle $j = 1, \dots, n$ ist die Abbildung*

$$K^n \to K, w \mapsto f((v_1 \mid \cdots \mid v_{j-1} \mid w \mid v_{j+1} \mid \cdots \mid v_n))$$

linear.

(b) *f ist* ***alternierend****, d. h. falls $j \neq k$ existieren mit $v_j = v_k$, dann ist $f((v_1 \mid \cdots \mid v_n)) = 0$.*

(c) *f ist* ***normiert****, d. h. $f(I_n) = 1$.*

Definition 5.1.2 *Die Abbildung f aus Satz 5.1.1 wird mit* $\det$ *bezeichnet. Ist $A \in K^{n\times n}$, so nennt man $\det A$ die* ***Determinante*** *von A.*

Lemma 5.1.3 *Im Folgenden sei $A \in K^{n\times n}$ beliebig und $E \in K^{n\times n}$ eine Elementarmatrix. Wir nehmen an, dass $\det\colon K^{n\times n} \to K$ eine Abbildung mit den Eigenschaften aus Satz 5.1.1 ist. Dann gilt:*

(a) $\det(AE) = \det A \cdot \det E$

(b)
$$\det E = \begin{cases} -1 & \text{falls } E \text{ zwei Spalten tauscht} \\ r & \text{falls } E \text{ eine Spalte mit } r \in K^\times \text{ multipliziert} \\ 1 & \text{falls } E \text{ das } r\text{-fache einer Spalte zu einer} \\ & \text{anderen Spalte addiert } (r \in K) \end{cases}$$

(c) *Enthält A eine Spalte, die nur aus 0en besteht, so ist $\det A = 0$.*

Bemerkung 5.1.4 *Aus dem Lemma ergibt sich eine Möglichkeit, $\det A$ zu berechnen:*

(a) *Forme A durch Spaltentransformationen zu einer Matrix $A' = AE_1 \cdots E_k$ in transponierter Normalform um (für Elementarmatrizen E_i). Es folgt: $\det A' = \det A \cdot \det E_1 \cdots \det E_k$.*

(b) *Wenn A' eine Nullspalte enthält, ist* $\det A = \det A' = 0$.
Wenn A' keine Nullspalten enthält, ist $A' = I_n$, und es folgt $\det A = (\det E_1 \cdots \det E_k)^{-1}$.
Außerdem gibt Lemma 5.1.3 (b) an, was $\det E_i$ *ist.*

Korollar 5.1.5 *Sei* $\det\colon K^{n\times n} \to K$ *eine Abbildung mit den Eigenschaften aus Satz 5.1.1. Dann gilt für beliebige Matrizen $A, B \in K^{n\times n}$:*

(a) *A ist invertierbar genau dann, wenn* $\det A \neq 0$ *ist. Ist dies der Fall, so gilt* $\det(A^{-1}) = (\det A)^{-1}$.
(b) $\det AB = \det A \cdot \det B$.
(c) $\det A = \det A^T$. *Insbesondere gelten die Eigenschaften aus Satz 5.1.1 und Lemma 5.1.3 auch für Zeilen statt Spalten, und Determinanten können auch mit Zeilentransformationen berechnet werden.*

Satz 5.1.6 (Laplacescher Entwicklungssatz) *Sei $n \geq 2$ und sei $A = (a_{ij})_{1\leq i,j\leq n} \in K^{n\times n}$. Wir schreiben $A_{(k,\ell)}$ für die $(n-1)\times(n-1)$-Matrix, die man aus A erhält, indem man die k-te Zeile und die ℓ-te Spalte rausstreicht. Dann gilt für jedes $\ell \leq n$:*

$$\det A = \sum_{k=1}^{n} (-1)^{k+\ell} \cdot a_{k,\ell} \cdot \det A_{(k,\ell)}.$$

(Man nennt diese Art, $\det A$ *zu berechnen, die „**Entwicklung** nach der ℓ-ten Spalte“.)*

Bemerkung 5.1.7 *Da* $\det A = \det A^T$, *gilt auch die analoge Formel mit Zeilen statt Spalten, d. h. für jedes $k \leq n$ gilt:*

$$\det A = \sum_{\ell=1}^{n} (-1)^{k+\ell} \cdot a_{k,\ell} \cdot \det A_{(k,\ell)}.$$

*(Man nennt dies die „**Entwicklung** nach der k-ten Zeile“.)*

Korollar 5.1.8 *Die Determinanten von 2×2- bzw. 3×3-Matrizen lassen sich wie folgt berechnen:*

(a)

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

(b) ***Regel von Sarrus****:*

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

Definition 5.1.9 *Zwei Matrizen $A, A' \in K^{n\times n}$ heißen **ähnlich** (zueinander), wenn eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$ existiert mit $A' = SAS^{-1}$.*

Bemerkung 5.1.10 *Ähnlichkeit von Matrizen ist eine Äquivalenzrelation.*

Bemerkung 5.1.11 *Seien V und W endlich-dimensionale K-Vektorräume und sei $f \in \mathrm{Hom}(V, W)$. Wir wählen Isomorphismen $\alpha\colon K^n \to V$ und $\beta\colon K^m \to W$.*

(a) *Wenn wir V und K^n mit Hilfe von α identifizieren und W und K^m mit Hilfe von β, so lässt sich f durch eine Matrix $A = (a_{ij})_{ij} \in K^{m\times n}$ beschreiben:*

$$A = \beta^{-1} \circ f \circ \alpha\colon K^n \to K^m.$$

(b) *α bildet die Standardbasis von K^n auf eine Basis $v_1, \ldots, v_n$ von V ab, und β bildet die Standardbasis von K^m auf eine Basis $w_1, \ldots, w_m$ von W ab. Mit dieser Notation gilt, für $1 \le j \le n$:*

$$f(v_j) = \sum_{i=1}^{m} a_{ij} w_i$$

(c) *Wählt man andere Isomorphismen $\alpha'\colon K^n \to V$ und $\beta'\colon K^m \to W$, so erhält man eine (möglicherweise) andere Matrix $A' = (\beta')^{-1} \circ f \circ \alpha'$, die f beschreibt. Es gilt jedoch $A' = SAT$, für $S = (\beta')^{-1} \circ \beta \in \mathrm{GL}_m(K)$ und $T = \alpha^{-1} \circ \alpha' \in \mathrm{GL}_n(K)$.*

(d) *Wendet man (c) auf den Fall $V = W$, $\beta = \alpha$ und $\beta' = \alpha'$ an, so erhält man: Die Matrizen $A = \alpha^{-1} \circ f \circ \alpha$ und $A' = (\alpha')^{-1} \circ f \circ \alpha'$ sind ähnlich zueinander.*

Definition 5.1.12 *Ist V ein endlich-dimensionaler K-Vektorraum und $f \in \mathrm{End}(V)$ ein Endomorphismus, so definieren wir $\det f$, indem wir einen Isomorphismus $\alpha\colon K^n \to V$ wählen und $\det f := \det A$ setzen für $A = \alpha^{-1} \circ f \circ \alpha \in K^{n\times n}$.*

Bemerkung 5.1.13 *Ähnliche Matrizen haben die gleiche Determinante. Insbesondere hängt $\det f$ in Definition 5.1.12 nicht von der Wahl von α ab.*

Nachtrag: In einer Übungsaufgabe wird noch gezeigt: Für Matrizen der Form

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

gilt: $\det A = a_{11} a_{22} \cdots a_{nn}$.

5.2 Eigenwerte und Eigenvektoren

Definition 5.2.1 *Sei V ein K-Vektorraum und $f \in \operatorname{End}(V)$ ein Endomorphismus. Ein Skalar $\lambda \in K$ heißt* ***Eigenwert*** *von f wenn es einen Vektor $v \in V \setminus \{0\}$ gibt mit $f(v) = \lambda v$. In diesem Fall nennt man v einen* ***Eigenvektor*** *von f zum Eigenwert λ.*

Satz 5.2.2 *Ist $A \in K^{n \times n}$ und x eine Variable, so ist $\chi_A(x) := \det(xI_n - A)$ ein Polynom in x. Die Nullstellen von χ_A sind genau die Eigenwerte von A.*

Definition 5.2.3 *Das Polynom $\chi_A(x) := \det(xI_n - A)$ aus Satz 5.2.2 nennt man das* ***charakteristische Polynom***[5] *der Matrix $A \in K^{n \times n}$.*

Bemerkung 5.2.4 *Das charakteristische Polynom $\chi_A(x)$ einer Matrix $A \in K^{n \times n}$ ist ein normiertes Polynom vom Grad n:*

$$\chi_A(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n.$$

Außerdem ist $a_0 = (-1)^n \cdot \det A$.

Bemerkung 5.2.5 *Ähnliche Matrizen haben das gleiche charakteristische Polynom. Man kann deshalb für beliebige endlich-dimensionale Vektorräume V das* ***charakteristische Polynom*** *χ_f eines Endomorphismus $f \in \operatorname{End}(V)$ definieren, indem man einen Isomorphismus $\alpha \colon K^n \to V$ wählt und $\chi_f := \chi_A$ setzt, für $A = \alpha^{-1} \circ f \circ \alpha$. Auch hier gilt: Die Nullstellen von χ_f sind genau die Eigenwerte von f.*

Definition 5.2.6 (a) *Eine Matrix der Form*

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix} \in K^{n \times n}$$

für $\lambda_1, \ldots, \lambda_n \in K$ heißt ***Diagonalmatrix*** *(„mit* ***Diagonaleinträgen*** *$\lambda_1, \ldots, \lambda_n$“).*

(b) *Eine Matrix $A \in K^{n \times n}$ heißt* ***diagonalisierbar****, wenn sie zu einer Diagonalmatrix ähnlich ist.*

Satz 5.2.7 *Eine Matrix $A \in K^{n \times n}$ ist diagonalisierbar genau dann, wenn eine Basis von K^n aus Eigenvektoren von A existiert. Genauer:*

(a) *Ist $S^{-1}AS$ eine Diagonalmatrix (für $S \in \mathrm{GL}_n(K)$), so bilden die Spalten von S eine Basis von V aus Eigenvektoren von A, und die zugehörigen Eigenwerte sind die entsprechenden Diagonaleinträge von $S^{-1}AS$,*

[5] Manche Autoren verwenden ein anderes Vorzeichen in der Definition des charakteristischen Polynoms: $\chi_A := \det(A - xI_n)$.

(b) *Ist umgekehrt $S \in \mathrm{GL}_n(K)$ eine Matrix, deren Spalten eine Basis von V aus Eigenvektoren von A zu den Eigenwerten $\lambda_1, \ldots, \lambda_n$ bilden, so ist $S^{-1}AS$ eine Diagonalmatrix mit Diagonaleinträgen $\lambda_1, \ldots, \lambda_n$.*

Bemerkung 5.2.8 *Für Endomorphismen f eines endlich-dimensionalen Vektorraums V erhält man: V hat eine Basis aus Eigenvektoren von f genau dann, wenn ein Isomorphismus $\alpha \colon K^n \to V$ existiert, so dass $\alpha^{-1} \circ f \circ \alpha$ eine Diagonalmatrix ist. Ist dies der Fall, so nennt man f* ***diagonalisierbar***

Ist $A \in K^{n \times n}$, so lässt sich wie folgt bestimmen, ob A diagonalisierbar ist:

(a) Bestimme die Eigenwerte $\lambda_1, \ldots, \lambda_k$ von A (als Nullstellen des charakteristischen Polynoms χ_A).

(b) Sei $U_i := \ker(\lambda_i I_n - A)$; die Elemente von $U_i \backslash \{0\}$ sind genau die Eigenvektoren von A zum Eigenwert λ_i.

(c) A ist diagonalisierbar genau dann, wennn $U_1 + \cdots + U_\ell = K^n$ ist. Ist dies der Fall, so lässt sich eine Basis $v_1, \ldots, v_n$ von K^n aus Eigenvektoren zu A finden. Sei S die Matrix mit Spalten $v_1, \ldots, v_n$. Dann ist $S^{-1}AS$ eine Diagonalmatrix.

6 Euklidische und unitäre Vektorräume

In diesem ganzen Kapitel sei $\mathbb{K}$ entweder $\mathbb{R}$ oder $\mathbb{C}$.

6.1 Skalarprodukte

Definition 6.1.1 *Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum. Ein* ***Skalarprodukt*** *auf V ist eine Abbildung $V \times V \to \mathbb{K}, (v, w) \mapsto \langle v, w \rangle$, so dass für alle $v, v', w, w' \in V$ und alle $r \in \mathbb{K}$ folgendes gilt:*

(a) *$\langle rv + v', w \rangle = r\langle v, w \rangle + \langle v', w \rangle$ und $\langle v, rw + w' \rangle = \bar{r}\langle v, w \rangle + \langle v, w' \rangle$ (**Sesquilinearität** im Fall $\mathbb{K} = \mathbb{C}$; **Bilinearität** im Fall $\mathbb{K} = \mathbb{R}$).*

(b) *$\langle v, w \rangle = \overline{\langle w, v \rangle}$ (**Hermitezität** im Fall $\mathbb{K} = \mathbb{C}$; **Symmetrie** im Fall $\mathbb{K} = \mathbb{R}$)*

(c) *Ist $v \neq 0$, so ist $\langle v, v \rangle$ eine reelle Zahl größer als 0 (**positive Definitheit**).*

Vorsicht: Die Notation $\langle v, w \rangle$ für das Skalarprodukt sieht (dummerweise) fast genauso aus wie die Notation für das Erzeugnis von v und w (Definition 3.2.5).

Definition 6.1.2 *Ein* ***euklidischer Vektorraum*** *ist ein $\mathbb{R}$-Vektorraum zusammen mit einem Skalarprodukt; ein* ***unitärer Vektorraum*** *ist ein $\mathbb{C}$-Vektorraum zusammen mit einem Skalarprodukt.*

Definition 6.1.3 *Sei V ein euklidischer oder unitärer Vektorraum. Die* ***Norm*** *eines Vektors $v \in V$ definiert durch $\|v\| := \sqrt{\langle v, v \rangle} \in \mathbb{R}_{\geq 0}$.*

Beispiel 6.1.4 *Wir fassen $\mathbb{R}^n$ als euklidischen Vektorraum und $\mathbb{C}^n$ als unitären Vektorraum auf, indem wir das folgende* ***Standard-Skalarprodukt*** *verwenden:*

$$\langle \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \rangle := a_1\bar{b}_1 + \cdots + a_n\bar{b}_n.$$

Die Norm eines Vektors ist dann

$$\| \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \| = \sqrt{|a_1|^2 + \cdots + |a_n|^2}.$$

Satz 6.1.5 *Sei V ein euklidischer bzw. unitärer $\mathbb{K}$-Vektorraum, seien $v, w \in V$ und sei $r \in \mathbb{K}$. Dann gilt:*

(a) $\|v\| = 0 \iff v = 0$
(b) $\|rv\| = |r| \cdot \|v\|$
(c) $|\langle v, w\rangle| \leq \|v\| \cdot \|w\|$ *(**Cauchy-Schwarz-Ungleichung**), und Gleichheit gilt genau dann, wenn v und w linear abhängig sind.*
(d) $\|v + w\| \leq \|v\| + \|w\|$ *(**Dreiecksungleichung**)*

Definition 6.1.6 *Sei $A \in \mathbb{K}^{n\times n}$.*

(a) *Wir schreiben $\bar{A}$ für die Matrix, die man aus A erhält, indem man alle Einträge komplex konjugiert.*
(b) *Gilt $A^T = A$, so nennt man A* ***symmetrisch****. Gilt $A^T = \bar{A}$, so nennt man A* ***hermitesch****.*
(c) *Eine hermitesche Matrix heißt* ***positiv definit****, wenn für alle $v \in \mathbb{K}^n \setminus \{0\}$ gilt: $v^T A\bar{v}$ ist eine reelle Zahl größer als 0.*

Satz 6.1.7 (a) *Zu jedem Skalarprodukt $\langle\cdot,\cdot\rangle$ auf $\mathbb{K}^n$ existiert genau eine Matrix $A \in \mathbb{K}^{n\times n}$, so dass*

$$\langle v, w\rangle = v^T A\bar{w}$$

gilt.

(b) *Eine Matrix $A \in \mathbb{K}^{n\times n}$ entspricht auf die obige Art einem Skalarprodukt genau dann, wenn sie hermitesch und positiv definit ist.*

6.2 Orthonormalbasen

In diesem gesamten Aschnitt sei V ein endlich-dimensionaler euklidischer oder unitärer $\mathbb{K}$-Vektorraum.

Definition 6.2.1 (a) *Ein Vektor $v \in V$ heißt **normiert**[6], wenn $\|v\| = 1$.*

(b) *Zwei Vektoren $v, w \in V$ heißen **orthogonal** (zueinander), wenn $\langle v, w\rangle = 0$ ist. Man schreibt $v \perp w$.*

Definition 6.2.2 *Eine **Orthonormalbasis** von V ist eine Basis $v_1, \dots, v_n$ mit folgenden Eigenschaften:*

(a) *v_i ist normiert für alle i.*

(b) *$v_i \perp v_j$ für alle i, j mit $i \neq j$.*

Beispiel 6.2.3 *Die Standardbasis von $\mathbb{K}^n$ ist eine Orthonormalbasis.*

Bemerkung 6.2.4 *Sie $v_1, \dots, v_n$ eine Orthonormalbasis von V, so gilt für beliebige Vektoren $v = \sum_i a_i v_i$ und $w = \sum_i b_i v_i$ (mit $a_i, b_i \in \mathbb{K}$): $\langle v, w\rangle = \sum_i a_i b_i$.*

Satz 6.2.5 *Sei $v_1, \dots, v_n$ eine Orthonormalbasis von V und sei $v \in V$. Dann gilt $v = \sum_{i=1}^{n} \langle v, v_i\rangle v_i$.*

Satz 6.2.6 (Gram-Schmidt-Orthogonalisierung) *V besitzt eine Orthonormalbasis. Sind bereits $v_1, \dots, v_k \in V$ gegeben, die normiert und paarweise orthogonal zueinander sind, so lassen sich $v_1, \dots, v_k$ zu einer Orthonormalbasis von V ergänzen.*

6.3 Isometrien

In diesem gesamten Aschnitt sei V ein endlich-dimensionaler euklidischer oder unitärer $\mathbb{K}$-Vektorraum.

Definition 6.3.1 (a) *Seien V und W endlich-dimensionale euklidische oder unitäre Vektorräume. Ein Isomorphismus $f \in \mathrm{Hom}(V, W)$ heißt **Isometrie**, wenn für alle $v, v' \in V$ gilt: $\langle v, v'\rangle = \langle f(v), f(v')\rangle$.*

(b) *Ist $W = V$, so nennt man f auch eine **orthogonale Transformation** (falls $\mathbb{K} = \mathbb{R}$) bzw. eine **unitäre Transformation** (falls $\mathbb{K} = \mathbb{C}$).*

(c) *Man nennt eine Matrix $A \in \mathbb{K}^{n\times n}$ **orthogonal** bzw. **unitär**, wenn der entsprechende Endomorphismus von $\mathbb{K}^n$ (mit dem Standard-Skalarprodukt) eine orthogonale bzw. unitäre Transformation ist.*

Bemerkung 6.3.2 *Die orthogonalen bzw. unitären Matrizen bilden eine Untergruppe von $\mathrm{GL}_n(\mathbb{K})$.*

[6] Nicht verwechseln mit einem „normierten Polynom“.

Korollar 6.3.3 *Ist V ein n-dimensionaler euklidischer oder unitärer Vektorraum, so existiert ein Isomorphismus $g\colon \mathbb{K}^n \to V$ (wobei $\mathbb{K}^n$ mit dem Standard-Skalarprodukt versehen ist).*

Satz 6.3.4 *Für eine Matrix $A \in \mathbb{K}^{n\times n}$ sind äquivalent:*

(a) *A ist orthogonal bzw. unitär.*
(b) *A ist invertierbar und es gilt $A^T = \bar{A}^{-1}$.*
(c) *Die Spalten von A bilden eine Orthonormalbasis.*

Satz 6.3.5 (Hauptachsentransformation) *Eine Matrix $A \in \mathbb{K}^{n\times n}$ ist symmetrisch bzw. hermitesch genau dann wenn alle Eigenwerte reell sind und eine Orthonormalbasis aus Eigenvektoren existiert. Dies ist auch äquivalent dazu, dass eine orthogonale bzw. unitäre Matrix $S \in \mathbb{K}^{n\times n}$ existiert, so dass $S^T A\bar{S}$ eine Diagonalmatrix mit reellen Einträgen ist.*