Kurzskript Lineare Algebra II

Immi Halupczok

12. Mai 2025

Inhaltsverzeichnis

Lineare Algebra I

Mi 9.10.

1 Mathematische Grundbegriffe

1.1 Lineare Gleichungssysteme

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* $n \geq 1$ *eine natürliche Zahl und seien* $a_1, \ldots, a_n$ *und* b *reelle Zahlen. Einen Ausdruck der Form*

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

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

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.*

[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.

(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*** $(a_1, \ldots, a_n)$ *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*

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

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

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

gilt.

Lemma 1.1.7 (a) *Sei* $L :=$ „$a_1x_1 + \cdots + a_nx_n = b$“ *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*

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

(b) *Wir nehmen nun außerdem an, dass* $L' :=$ „$a'_1x_1 + \cdots + a'_nx_n = b'$“ *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*

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

Definition 1.1.8 *Seien* $m \geq 1$ *und* $n \geq 1$ *natürliche Zahlen. Ein* ***lineares Gleichungssystem*** *in einem Variablentupel* $\underline{x} = (x_1, \ldots, x_n)$ *ist ein Tupel* $\underline{L} = (L_1, \ldots, L_m)$*, 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* $L_1, \ldots, L_m$ *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:*

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

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

$$\underline{L} := \left(\begin{array}{ccccccc} a_{1,1}x_1 & + a_{1,2}x_2 & + \cdots + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + a_{2,2}x_2 & + \cdots + & a_{2,n}x_n & = & b_2 \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m,1}x_1 & + a_{m,2}x_2 & + \cdots + & a_{m,n}x_n & = & b_m \end{array} \right) \tag{1}$$

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

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

(Der senkrechte Strich hat formal keine Bedeutung. Er dient nur dazu, optisch sichtbar zu machen, das 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*

$$\begin{pmatrix} ra_{i,1} & ra_{i,2} & \dots & ra_{i,n} \end{pmatrix}.$$

(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*

$$\begin{pmatrix} a_{i,1} + ra_{j,1} & a_{i,2} + ra_{j,2} & \dots & a_{i,n} + ra_{j,n} \end{pmatrix}.$$

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:*

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

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-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 enhält. Insbesondere haben wir die entsprechenden x_k bereits in Schritt (i) gewählt. Diese Gleichung legt also x_j eindeutig fest, nämlich: $x_j = b_i - a_{i,j+1}x_{j+1} - a_{i,j+2}x_{j+2} - \cdots - a_{i,n}x_n$.

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

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.*

(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) *„$\forall x \in M\colon A$" 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) *„$\exists x \in M\colon A$" 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) *„$\exists^{=1} x \in M\colon A$" 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 „$\exists! x \in M\colon A$"

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

[2] Achtung: 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.

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

Statt „$\forall x \in M\colon \forall y \in M\colon A$" schreibt man auch „$\forall x, y \in M\colon A$", 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 „$\forall x \in M\colon A$" 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 veschiedene 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 scheiben 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:*

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

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:*

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

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 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.*

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

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

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 $\mathrm{Abb}(A, B)$ die Menge aller Abbildungen von A nach B.*

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

$$f\colon A \to B, a \mapsto T,$$

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

Konvention 1.3.5 *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.*

Definition 1.3.6 *Die **Identität** auf einer Menge A ist die Abbildung $\mathrm{id}_A\colon A \to A, a \mapsto a$.*

Definition 1.3.7 *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 1.3.8 *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 $f^0 := \mathrm{id}_A$.*

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

Notation 1.3.9 *Ist A eine Aussage, in der eine Variable x vorkommt und $f\colon B \to C$ 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:*

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

Definition 1.3.10 *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:* $\operatorname{im} f := f(A)$.
(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 $f\colon A \to B$.*

(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 „$f\colon A \xrightarrow{1:1} B$“.*

Satz 1.3.12 *Seien A und B Mengen und sei $f\colon A \to B$ eine Abbildung.*

(a) *Die Abbildung f ist bijektiv genau dann, wenn eine Abbildung $g\colon B \to A$ existiert, so dass $f \circ g = \mathrm{id}_B$ und $g \circ f = \mathrm{id}_A$ 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 $f\colon A \to B$ 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 $f\colon A \to B$ 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 $f\colon A \to B$ eine Abbildung und $A' \subseteq A$ eine Teilmenge, so schreiben wir $f|_{A'}$ für die* ***Einschränkung*** *von f auf A', d. h. $f|_{A'}\colon A' \to B, a \mapsto f(a)$.*

Satz 1.3.16 *Seien A und B endliche Mengen gleicher Kardinalität. Dann gilt für Abbildungen $f \in \mathrm{Abb}(A, B)$: Ist f injektiv <u>oder</u> surjektiv, so ist f bereits bijektiv.*

1.4 Partitionen und Äquivalenzrelationen

Definition 1.4.1 *Eine* ***Partition*** *einer Menge M ist eine Menge P von nichtleeren 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) $\forall a \in M\colon a \sim a$ *(**Reflexivität**)*
   (ii) $\forall a, b \in M\colon (a \sim b \Rightarrow b \sim a)$ *(**Symmetrie**)*
   (iii) $\forall a, b, c \in M\colon (a \sim b \wedge b \sim c \Rightarrow a \sim c)$ *(**Transitivität**)*
   Ist dies der Fall, so wird „$a \sim b$“ oft ausgesprochen als „a ist ***äquivalent*** *zu b“ oder „a und b sind* ***äquivalent***“.
(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.)

Mo 4.11.

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 „$a \equiv b \mod m$"; 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 $M \to M/\sim, a \mapsto a/\sim$ 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

Definition 2.1.1 (a) *Eine **Gruppe** ist gegeben durch eine Menge G, eine Abbildung $\circ\colon G \times G \to G$ und ein Element $e \in G$ mit folgenden Eigenschaften:*
   (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**. Man sagt „G ist eine Gruppe" oder „$(G, \circ)$ ist eine Gruppe" oder „$(G, \circ, e)$ ist eine Gruppe", je nachem, was aus dem Kontext klar ist.*
(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 **Verknüpfung**.*

Beispiel 2.1.3 *Ist M eine beliebige Menge, so bildet die Menge aller Bijektion von von M nach M eine Gruppe, mit der Verkettung von Abbildungen als Verknüpfung und id_M als neutralem Element. Diese Gruppe wird auch mit $\mathrm{Sym}(M)$ 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) $a \circ b = a' \circ b \quad \Rightarrow \quad a = a'$ *und*
$a \circ b = a \circ b' \quad \Rightarrow \quad b = b'$

(b) $a \circ b = b \quad \Rightarrow \quad a = e$ *und*
$a \circ b = a \quad \Rightarrow \quad b = e$

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 $a^0 := e$, $a^n := \underbrace{a \circ \cdots \circ a}_{n \text{ mal}}$, $a^{-n} := (a^{-1})^n$*

(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 2.1.7 *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 $+\colon R \times R \to R$ 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**.*

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 „$a_1x_1 + \cdots + a_nx_n = b$“ 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 Tranformationen 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

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*

$$a_1x_1 + \cdots + a_nx_n = 0$$

(für $a_1, \dots, a_n \in K$). Ihre Lösungsmenge $\{(c_1, \dots, c_n) \in K^n \mid a_1c_1 + \cdots + a_nc_n = 0\}$ 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 definert 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 $G/H := G/\!\sim$ (Ausssprache: „G* ***modulo*** *H“), wobei $\sim$ die Äquivalenzrelation ist, die definiert ist durch*

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

Für die Äquivalenzklasse

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

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

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

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

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

$$a_1 x_1 + \cdots + a_n x_n = 0.$$

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 $0, 1, \dots, n-1$ bezeichnet (statt mit $\bar{0}$, $\bar{1}$, $\dots$, $\overline{n-1}$).*

Mi 13.11.

2.3 Polynomringe

Definition 2.3.1 *Eine **Folge** von Elementen einer Menge M ist eine Funktion $a\colon \mathbb{N} \to M$, 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 $\sum_{i=0}^n a_ix^i$ auch $\sum_{i\in\mathbb{N}} a_ix^i$.*

Definition 2.3.5 *Sind $f = \sum_{i\in\mathbb{N}} a_ix^i$ und $g = \sum_{i\in\mathbb{N}} b_ix^i$ 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:*

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

$$f \cdot g := \sum_{i\in\mathbb{N}} \Big(\sum_{j=0}^{i} a_jb_{i-j}\Big)x^i$$

Satz 2.3.6 *Ist R ein kommutativer Ring, so ist auch $R[x]$ ist 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 nichtkonstante 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 $\cdot\colon K \times V \to V$, 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 neutrale Element $0 \in V$ der Vektoraddition nennt man **Nullvektor**.*

In Abschnitt 3.1 habe ich die Vektorraddition, 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 $\mathrm{Abb}(M, K)$ 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 $a \in M$.*

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

3.2 Untervektorräume

Sei weiterhin K ein Körper.

Definition 3.2.1 *Sei $(V, +, \cdot)$ 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 $v_1, \ldots, v_n \in V$ ist ein Vektor der Form*

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

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

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

für die Menge aller Linearkombinationen von $v_1, \ldots, v_n$.
Ist allgemeiner $A \subseteq V$ eine beliebige Teilmenge von V, so schreibt man

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

für die Menge aller Linearkombinationen von (jeweils endlich vielen) Vektoren aus A.
Man nennt $\langle v_1, \ldots, v_n \rangle_K$ bzw. $\langle A \rangle_K$ die ***lineare Hülle*** *(oder den* ***Span*** *oder das* ***Erzeugnis****) von $v_1, \ldots, v_n$ bzw. von A.*
Das Erzeugnis der leere 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 unabghängig 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:*

(a) *$(v_1, \dots, v_n)$ ist eine Basis von V.*
(b) *$(v_1, \dots, v_n)$ ist ein minimales Erzeugendensystem von V, d. h. $\langle v_1, \dots, v_n \rangle_K = V$, aber für jedes $i \le n$ gilt: $\langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n \rangle_K \neq V$.*
(c) *$(v_1, \dots, v_n)$ ist ein maximales linear unabhängiges Tupel, d. h. $(v_1, \dots, v_n)$ ist linear unabhängig, aber für jeden weiteren Vektor $v_{n+1} \in V$ ist das Tupel $(v_1, \dots, v_{n+1})$ linear abhängig.*
(d) *Jeder Vektor $v \in V$ lässt sich auf eindeutige Weise als Linearkombintation 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 $\{v_i \mid i \in \mathbb{N}_{\ge 1}\} \subseteq V$. 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 $M \to M'$ 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 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 $(v_1 \mid \cdots \mid v_n)$ 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 $A = (v_1 \mid \cdots \mid v_n) \in K^{m\times n}$ 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 $\operatorname{im} A$ (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*
$$\left(A \,\middle|\, \underline{b} \right) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$
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 4.1.7 *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:*

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

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* $AI_\ell = A$.
(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 2.1.4 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.*

Notation 4.1.11 *Ist $A \in K^{n\times n}$ und $k \in \mathbb{N}$, so setzen wir $A^m := \underbrace{A \cdot A \cdots A}_{k \text{ mal}}$ falls $k \geq 1$ und $A^0 := I_n$.*

4.2 Lineare Abbildungen

Sei weiterhin K ein Körper.

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

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

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

Beispiel 4.2.2 *Jede durch eine Matrix $A \in K^{m\times n}$ gegebene Abbildung von K^n nach K^m ist linear.*

Bemerkung 4.2.3 (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 $f(0) = 0$.*

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

Satz 4.2.5 *Sind V und W K-Vektorräume, ist $v_1, \ldots, v_n$ eine Basis von V und sind $w_1, \ldots, w_n$ 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 4.2.6 *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 $\mathrm{Hom}(K^n, K^m)$ (die einer Matrix die zugehörige Abbildung zuordnet).*

Mi 11.12.

Korollar 4.2.7 *Seien V und W K-Vektorräume, sei $v_1, \ldots, v_n$ eine Basis von V und sei $w_1, \ldots, w_m$ eine Basis von W. Dann erhalten wir eine Bijektion*

$$K^{m\times n} \to \mathrm{Hom}(V, W),$$

die eine Matrix $A := (a_{ij})_{ij}$ abbildet auf die lineare Abbildung $f\colon V \to W$, die definiert ist durch

$$f(\sum_{j=1}^{n} r_j v_j) = \sum_{i=1}^{m} s_i w_i \text{ für } \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in K^n \text{ beliebig und } \begin{pmatrix} s_1 \\ \vdots \\ s_m \end{pmatrix} = A \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}.$$

Definition 4.2.8 *Die Matrix A aus Korollar 4.2.7 nennt man die* ***Matrix von*** *f bezüglich der Basen $(v_j)_j$ und $(w_i)_i$.*

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) *Das Bild* $\operatorname{im} f$ *ist ein Untervektorraum von* W *(vgl. Definition 1.3.10).*
(b) *Der Kern* $\ker f$ *ist ein Untervektorraum von* V*.*
(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 4.2.12 *Seien* V *und* W K*-Vektorräume.*

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

Beispiel 4.2.13 *Ist* V *ein* K*-Vektorraum und* $v_1, \dots, v_n$ *eine Basis von* V*, so ist*

$$K^n \to V, \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \mapsto \sum_{i=1}^{n} r_i v_i$$

ein Isomorphismus von Vektorräumen.

Satz 4.2.14 *Seien* V *und* W K*-Vektorräume und sei* $f \colon V \to W$ *ein Isomorphismus. Dann ist die inverse Abbildung* $f^{-1} \colon W \to V$ *auch ein Isomorphismus.*

Bemerkung 4.2.15 *Ist* $f \in \operatorname{Hom}(V, W)$ *ein Isomorphismus von Vektorräumen, so lassen sich mit* f *„Eigenschaften zwischen* V *und* W *übertragen“, z. B. gilt:*

(a) *Seien* $v_1, \dots, v_n \in V$ *und* $w_1 := f(v_1), \dots, w_n := f(v_n)$*. Dann sind* $v_1, \dots, v_n$ *linear unabhängig / ein Erzeugendensystem von* V */ eine Basis von* V *genau dann, wenn* $w_1, \dots, w_n$ *linear unabhängig / ein Erzeugendensystem von* W */ eine Basis von* W *sind.*
(b) $\dim V = \dim W$*.*
(c) *Für* $U_V \subseteq V$ *und* $U_W := f(U_V) \subseteq W$ *gilt:* U_V *ist ein Untervektorraum von* V *genau dann, wenn* U_W *ein Untervektorraum von* W *ist.*

Mo 16.12.

Bemerkung 4.2.16 *Seien* V *und* W K*-Vektorräume, sei* $v_1, \dots, v_n$ *eine Basis von* V*, sei* $w_1, \dots, w_m$ *eine Basis von* W*, und sei* $f \colon V \to W$ *eine lineare Abbildung. Die Matrix von* f *bezüglich der Basen* $(v_i)_i$ *und* $(w_j)_j$ *(aus Korollar 4.2.7) ist gerade die Matrix der Verknüpfung* $g_W^{-1} \circ f \circ g_V \colon K^n \to K^m$*, wobei* $g_V \colon K^n \to V$ *und* $g_W \colon K^m \to W$ *die Isomorphismen aus Beispiel 4.2.13 sind (angewandt auf die Basis* $(v_i)_i$ *von* V *und die Basis* $(w_j)_j$ *von* W*).*

Definition 4.2.17 *Eine Matrix $A \in K^{n\times n}$ heißt* ***invertierbar****, wenn die durch A definierte Abbildung $K^n \to K^n$ ein Isomorphismus ist. Die Matrix, die die inverse Abbildung definiert, heißt zu A* ***inverse Matrix****; Notation dafür: A^{-1}.*

Bemerkung 4.2.18 *Eine Matrix $A \in K^{n\times n}$ ist also invertierbar genau dann, wenn eine Matrix $B \in K^{n\times n}$ existiert mit $AB = BA = I_n$. Ist dies der Fall, so ist $A^{-1} = B$.*

Satz 4.2.19 *Sind $v_1, \dots, v_n$ und $v'_1, \dots, v'_n$ zwei Basen des selben K-Vektorraums V, so existiert eine invertierbare Matrix $A \in K^{n\times n}$ mit der folgenden Eigenschaft: Ist $v \in V$ beliebig, und schreiben wir v als Linearkombintationen*

$$v = \sum_{i=1}^{n} r_i v_i = \sum_{i=1}^{n} r'_i v'_i$$

(für $r_i, r'_i \in K$), so gilt

$$A \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} r'_1 \\ \vdots \\ r'_n \end{pmatrix}.$$

(Man nennt A die ***Basiswechselmatrix*** *zwischen den Basen $(v_i)_i$ und $(v'_i)_i$.)*

4.3 Homomorphiesatz und Rang

Sei weiterhin K ein Körper.

Satz 4.3.1 *Sei V ein K-Vektorraum und $U \subseteq V$ ein Untervektorraum. Dann wird die Quotientengruppe V/U aus Satz 2.2.7 mit der folgenden Skalarmultiplikation zu einem K-Vektorraum:*

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

(Man nennt V/U einen ***Quotientenvektorraum*** *oder* ***Faktorvektorraum****.)*

Bemerkung 4.3.2 *Die kanonische Abbildung $V \to V/U, v \mapsto \bar{v}$ (vgl. Definition 1.4.7) ist linear.*

Satz 4.3.3 *Ist V ein endlich-dimensionaler Vektorraum und $U \subseteq V$ ein Untervektorraum, so gilt $\dim V = \dim U + \dim(V/U)$.*

Mi 18.12.

Satz 4.3.4 *Seien V und W K-Vektorräume, sei $f \in \mathrm{Hom}(V, W)$, sei $U \subseteq V$ ein Untervektorraum, und sei $\mathrm{can}\colon V \to V/U$ die kanonische Abbildung. Es existiert genau dann ein $g \in \mathrm{Hom}(V/U, W)$ mit $f = g \circ \mathrm{can}$, wenn $U \subseteq \ker f$ ist.*

Satz 4.3.5 (Homomorphiesatz) *Sind V und W K-Vektorräume und ist $f \in \operatorname{Hom}(V,W)$, so erhält man einen Isomorphismus*

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

Definition 4.3.6 (a) *Seien V und W endlich-dimensionale Vektorräume. Der **Rang** einer linearen Abbildung $f \in \operatorname{Hom}(V,W)$ ist*

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

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

Bemerkung 4.3.7 *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 $\operatorname{rk} f = \dim V$; ist f nicht injektiv, so ist $\operatorname{rk} f < \dim V$.*
(b) *Die Abbildung f ist surjektiv genau dann, wenn $\operatorname{rk} f = \dim W$; ist f nicht surjektiv, so ist $\operatorname{rk} f < \dim W$.*

Satz 4.3.8 (Sylvesters Rang-Ungleichung) *Sind U, V und W endlich-dimensionale K-Vektorräume und $U \xrightarrow{f} V \xrightarrow{g} W$ lineare Abbildungen, so gilt*

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

Insbesondere: Ist f surjektiv, so ist $\operatorname{rk}(g\circ f) = \operatorname{rk} g$; und: Ist g injektiv, so ist $\operatorname{rk}(g \circ f) = \operatorname{rk} f$.

Mo 6.1.

Bemerkung 4.3.9 *Die Menge der invertierbaren $n \times n$-Matrizen über K bildet eine Gruppe, mit der Matrix-Multiplikation als Verknüpfung und I_n als neutralem Element. Diese Gruppe wird mit $\mathrm{GL}_n(K)$ bezeichnet.*[5]

Korollar 4.3.10 *Sind $A, B \in K^{n\times n}$ Matrizen mit $AB = I_n$, so sind beide Matrizen invertierbar, und invers zueinander (d. h. es gilt $A^{-1} = B$).*

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:*

[5] Auf englisch heißt sie „general linear group"; daher „GL"

(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 A eine Matrix und erhält man A' aus A durch eine elementare Zeilentransformation (siehe Definition 1.1.10), so gilt $A' = EA$ 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**. Die Elementarmatrizen sind also die Matrizen $E = (e_{ij})_{ij}$ mit:*

(TAU) Zeilen k und ℓ vertauschen (für $1 \leq k, \ell \leq m$, $k \neq \ell$): $e_{ii} = 1$ falls $i \notin \{k, \ell\}$; $e_{k\ell} = e_{\ell k} = 1$; alle anderen e_{ij} sind 0;

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

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

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

Definition 4.4.5 *Die **Transponierte** einer Matrix $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in K^{m\times n}$ ist die Matrix $A^T := (a_{ji})_{1\leq j\leq n, 1\leq i\leq m} \in K^{n\times m}$.*

Bemerkung 4.4.6 (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.*

Bemerkung 4.4.7 *Ist* $A \in K^{m\times n}$ *beliebig und* $E \in K^{n\times n}$ *eine Elementarmatrix, so 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.*

Mi 8.1.

Bemerkung 4.4.8 *Ist* $A \in K^{n\times n}$ *eine quadratische Matrix in Normalform mit* $\operatorname{rk} A = n$, *so ist bereits* $A = I_n$.

Satz 4.4.9 *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 *ist invertierbar genau dann wenn* $A' = I_n$; *insbesondere lässt sich jede invertierbare Matrix als Produkt von Elementarmatrizen schreiben. Außerdem ist dann* $B' = A^{-1}$.

5 Endomorphismen

Im ganzen Kapitel sei weiterhin K ein Körper.

5.1 Determinanten

Definition 5.1.1 *Seien* $V_1, \dots, V_n$ *und* W K*-Vektorräume. Eine Abbildung* $f\colon V_1 \times \cdots \times V_n \to W$ *heißt* ***multilinear****, wenn für alle* $v_1 \in V_1, \dots, v_n \in V_n$ *und alle* $1 \le i \le n$ *die Abbildung*

$$V_i \to W, v' \mapsto f(v_1, \dots, v_{i-1}, v', v_{i+1}, \dots, v_n)$$

linear ist. Im Fall $n = 2$ *nennt man* f *auch* ***bilinear****.*

Satz 5.1.2 *Es existiert genau eine Abbildung* $f\colon K^{n\times n} \to K$ *mit den folgenden Eigenschaften:*

(a) *Die Abbildung*

$$K^n \times \cdots \times K^n \to K, (v_1, \dots, v_n) \mapsto f((v_1 \mid \cdots \mid v_n))$$

ist multilinear.

(b) *f ist **alternierend**, d. h. falls $A \in K^{n\times n}$ zwei gleiche Spalten hat, so ist $f(A) = 0$.*
(c) *f ist **normiert**, d. h. $f(I_n) = 1$.*

Definition 5.1.3 *Die Abbildung f aus Satz 5.1.2 wird mit* det *bezeichnet. Ist $A \in K^{n\times n}$, so nennt man* $\det A$ *die **Determinante** von A.*

Beispiel 5.1.4 *Im Fall $n = 2$ erfüllt*

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

die Eigenschaften aus Satz 5.1.2.

Mo 13.1.

Lemma 5.1.5 *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 5.1.2 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 5.1.6 *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 5.1.5 (b) an, was $\det E_i$ *ist.*

Korollar 5.1.7 *Sei* $\det\colon K^{n\times n} \to K$ *eine Abbildung mit den Eigenschaften aus Satz 5.1.2. 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 5.1.2 und Lemma 5.1.5 auch für Zeilen statt Spalten, und Determinanten können auch mit Zeilentransformationen berechnet werden.*

Satz 5.1.8 (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 $k \leq n$:*

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

*(Man nennt diese Art, $\det A$ zu berechnen, die „**Entwicklung** nach der k-ten Zeile".)*

Beispiel 5.1.9 *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: $\det A = a_{11}a_{22}\cdots a_{nn}$. (Matritzen dieser Form nennt man **obere Dreiecksmatrizen**.)*

Bemerkung 5.1.10 *Da $\det A = \det A^T$, gilt auch die analoge Formel mit Zeilen statt Spalten, d. h. für jedes $\ell \leq n$ gilt:*

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

*(Man nennt dies die „**Entwicklung** nach der ℓ-ten Spalte".)*

Korollar 5.1.11 (Regel von Sarrus) *Die Determinante einer 3×3-Matrix lässt sich wie folgt berechnen:*

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

Bemerkung 5.1.12 (Leibniz-Formel) *Im Allgmeinen lässt sich die Determinante einer $n\times n$-Matrix $A = (a_{ij})_{ij}$ ausdrücken als eine Summe von Produkten der Form $\pm a_{i_1,j_1}\cdots a_{i_n,j_n}$, wobei es je einen Summenden gibt für jede Möglichkeit, aus jeder Zeile und jeder Spalte genau einen Matrix-Koeffizienten auszuwählen. Genauer:*

$$\det A = \sum_{\sigma\in \mathrm{Sym}(\{1,\ldots,n\})} \mathrm{sgn}(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)}\cdots a_{n,\sigma(n)},$$

wobei $\mathrm{Sym}(\{1,\dots,n\})$ *die Menge der Bijektionen* $\{1,\dots,n\} \to \{1,\dots,n\}$ *ist (siehe Beispiel 2.1.3), und wobei das* ***Signum*** $\mathrm{sgn}(\sigma)$ *von* σ *wie folgt definiert ist: Wir betrachten die Matrix* $B_\sigma = (b_{ij})_{ij}$ *mit* $b_{i,\sigma(i)} = 1$ *und allen anderen Koeffizienten* 0 *und setzen* $\mathrm{sgn}(\sigma) := \det(B_\sigma) \in \{1,-1\}$.

Definition 5.1.13 *Sei* V *ein* K*-Vektorraum.*

(a) *Eine lineare Abbildung von* V *in sich selbst nennt man auch einen* ***Endomorphismus*** *von* V*. Die Menge aller Endomorphismen von* V *wird mit* $\mathrm{End}(V)$ *bezeichnet.*
(b) *Ein* ***Automorphismus*** *ist ein bijektiver Endomorphismus. Die Menge aller Automorphismen von* V *bildet eine Gruppe (mit der Verkettung von Abbildungen als Verknüpfung); diese wird mit* $\mathrm{Aut}(V)$ *(oder manchmal auch mit* $\mathrm{GL}(V)$*) bezeichnet.*

Mo 20.1.

Definition 5.1.14 *Sei* V *ein endlich-dimensionaler* K*-Vektorraum und* $f \in \mathrm{End}(V)$ *ein Endomorphismus. Die* ***Determinante*** *von* f *wird wie folgt definiert. Sei* $g\colon K^n \to V$ *ein beliebiger Isomorphismus und sei* $A \in K^{n\times n}$ *die Matrix zur Abbildung* $g^{-1} \circ f \circ g$*. Dann definiert man* $\det f := \det A$.

Lemma 5.1.15 *In Definition 5.1.14 hängt die Determinante* $\det A$ *nicht von der Wahl von* g *ab.*

5.2 Eigenwerte und Eigenvektoren

Definition 5.2.1 *Sei* V *ein* K*-Vektorraum und sei* $f \in \mathrm{End}(V)$ *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.

Definition 5.2.2 *Sei* $A \in K^{n\times n}$ *und* x *eine Variable. Nach Bemerkung 5.1.12 ist die Determinante* $\chi_A(x) := \det(xI_n - A)$ *ein Polynom in* x*. Dieses Polynom nennt man das* ***charakteristische Polynom***[6] *der Matrix* A.

Bemerkung 5.2.3 *Das charakteristische Polynom* $\chi_A(x)$ *einer Matrix* $A \in K^{n\times n}$ *hat die Form*

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

wobei $a_0 = (-1)^n \cdot \det A$ *ist. (Ein Polynom, bei dem – wie hier – die höchste* x*-Potenz mit dem Faktor* 1 *vorkommt, nennt man* ***normiert****.)*

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

Satz 5.2.4 *Sei $A \in K^{n\times n}$. Die Nullstellen von χ_A sind genau die Eigenwerte von A. Ist $\lambda \in K$ eine solche Nullstelle, so sind die Eigenvektoren von A zum Eigenwert λ genau die Elemente von $\ker(\lambda I_n - A) \setminus \{0\}$.*

Definition 5.2.5 *Analog zu Definition 5.1.14 kann man das **charakteristische Polynom** auch für Endomorphismen f von endlich-dimensionalen Vektorräumen V definieren: Ist $g\colon K^n \to V$ ein Isomorphismus und $A \in K^{n\times n}$ die Matrix zur Abbildung $g^{-1} \circ f \circ g$, so definiert man $\chi_f := \chi_A$.*

Mi 22.1.

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

(b) *Ein Endomorphismus $f \in \mathrm{End}(V)$ heißt **diagonalisierbar**, wenn ein Isomorphismus $g\colon K^n \to V$ existiert, so dass $g^{-1} \circ f \circ g$ durch eine Diagonalmatrix gegeben ist.*

(c) *Eine Matrix $A \in K^{n\times n}$ heißt **diagonalisierbar**, wenn der entsprechende Endomorphismus diagonalisierbar ist, d. h. wenn eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$ existiert, so dass $S^{-1}AS$ eine Diagonalmatrix ist.*

Bemerkung 5.2.7 *Sei V ein endlich-dimensionaler K-Vektorraum. Ein Endomorphismus $f \in \mathrm{End}(V)$ ist diagonalisierbar genau dann, wenn eine Basis von V aus Eigenvektoren von f existiert. Genauer:*

(a) *Ist $g\colon K^n \to V$ ein Isomorphismus, so dass $g^{-1} \circ f \circ g$ durch eine Diagonalmatrix mit Diagonaeinträgen $\lambda_1, \dots, \lambda_n$ gegeben ist, so ist $g(e_1), \dots, g(e_n)$ eine Basis von V, und $g(e_i)$ ist ein Eigenvektor zum Eigenwert λ_i. (Hierbei ist $e_1, \dots, e_n$ die Standardbasis von K^n.)*

(b) *Ist umgekehrt $v_1, \dots, v_n$ eine Basis von V so, dass v_i ein Eigenvektor zum Eigenwert λ_i ist, so wählen wir den Isomorphismus $g\colon K^n \to V$ so, dass $g(e_i) = v_i$ ist. Dann ist $g^{-1} \circ f \circ g$ gegeben durch die Diagonalmatrix mit Diagonaleinträgen $\lambda_1, \dots, \lambda_n$.*

(c) *Im Fall $V = K^n$ ist g durch eine Matrix $S \in \mathrm{GL}_n(K)$ gegeben, und die obigen $g(e_i)$ sind die Spalten von S.*

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 $\langle v, w\rangle_{\mathbb{K}}$ 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 $\|v\| := \sqrt{\langle v, v\rangle} \in \mathbb{R}_{\geq 0}$. (Hierbei ist $\mathbb{R}_{\geq 0}$ eine Kurzschreibweise für $\{r \in \mathbb{R} \mid r \geq 0\}$.)*

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:*

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

Die Norm eines Vektors ist dann

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

Mo 27.1.

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.*

Mi 29.1.

6.2 Isometrien und Orthonormalbasen

In diesem gesamten Aschnitt sei V ein endlich-dimensionaler euklidischer oder unitärer $\mathbb{K}$-Vektorraum. Auf $\mathbb{K}^n$ verwenden wir immer das Standard-Skalarprodukt.

Definition 6.2.1 (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 6.2.2 *Die orthogonalen bzw. unitären Matrizen bilden eine Untergruppe von $\mathrm{GL}_n(\mathbb{K})$.*

Definition 6.2.3 (a) *Ein Vektor $v \in V$ heißt* ***normiert***[7]*, 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 6.2.4 *Eine* ***Orthonormalbasis*** *von V ist eine Basis $v_1, \dots, v_n$ mit folgenden Eigenschaften:*

(a) *v_i ist normiert für alle i.*

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

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

Beispiel 6.2.5 *Die Standardbasis von* $\mathbb{K}^n$ *ist eine Orthonormalbasis.*

Bemerkung 6.2.6 *Ist* $v_1, \ldots, v_n$ *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* $a_i, b_i \in \mathbb{K}$*):* $\langle v, w\rangle = \sum_i a_i \bar{b}_i$.

Satz 6.2.7 *Sei* $v_1, \ldots, v_n$ *eine Orthonormalbasis von* V *und sei* $v \in V$. *Dann gilt* $v = \sum_{i=1}^n \langle v, v_i\rangle v_i$.

Satz 6.2.8 *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.*

Bemerkung 6.2.9 *Sine* $v_1, \ldots, v_k \in V\setminus\{0\}$ *paarweise orthogonal zueinander (d. h.* $v_i \perp v_j$ *für alle* $i \neq j$*), so sind sie bereits linear unabhängig.*

Satz 6.2.10 (Gram-Schmidt-Orthogonalisierung) *V besitzt eine Orthonormalbasis. Sind bereits* $v_1, \ldots, v_k \in V$ *gegeben, die normiert und paarweise orthogonal zueinander sind, so lassen sich* $v_1, \ldots, v_k$ *zu einer Orthonormalbasis von V ergänzen.*

Korollar 6.2.11 *Ist V ein n-dimensionaler euklidischer oder unitärer Vektorraum, so existiert eine Isometrie* $g\colon \mathbb{K}^n \to V$ *(wobei* $\mathbb{K}^n$ *mit dem Standard-Skalarprodukt versehen ist).*

Lineare Algebra II

Mo 7.4.

6.3 Orthogonale Komplemente

Sei weiterhin $\mathbb{K}$ entweder $\mathbb{R}$ oder $\mathbb{C}$, und V sei ein euklidischer bzw. unitärer $\mathbb{K}$-Vektorraum.

Definition 6.3.1 *Das* ***orthogonale Komplement*** *eines Untervektorraums $U \subseteq V$ ist*

$$U^\perp := \{v \in V \mid \forall u \in U : v \perp u\}.$$

Für Vektoren $u \in V$ schreibt man auch $u^\perp := \langle u \rangle_{\mathbb{K}}^\perp = \{v \in V \mid v \perp u\}$.

Bemerkung 6.3.2 *Sei $u_1, \ldots, u_m$ ein Erzeugendensystem von U und sei $v \in V$. Dann ist $v \in U^\perp$ genau dann, wenn $v \perp u_1, \ldots, v \perp u_m$.*

Satz 6.3.3 *Sei $U \subseteq V$ ein Untervektorraum. Dann gilt:*

(a) *$U^\perp$ ist auch ein Untervektorraum von V, und es gilt $U \cap U^\perp = \{0\}$.*
(b) *$U \subseteq (U^\perp)^\perp$.*

Ist V endlich-dimensional, so gilt außerdem:

(c) *Ist $u_1, \ldots, u_m$ eine Orthonormalbasis von U und $w_1 \ldots, w_n$ eine Orthonormalbasis von $U^\perp$, so ist $u_1, \ldots, u_m, w_1, \ldots, w_n$ eine Orthonormalbasis von V. Insbesondere gilt $\dim U + \dim U^\perp = \dim V$.*
(d) *$U = (U^\perp)^\perp$*

Do 10.4.

6.4 Bilinear- und Sesquilinearformen

Definition 6.4.1 *Sei K ein beliebiger Körper und V ein K-Vektorraum.*

(a) *Eine* ***Bilinearform*** *auf V ist eine bilineare Abbildung $\beta\colon V \times V \to K$ (siehe Definition 5.1.1), d. h. für alle $v, v', w, w' \in V$ und alle $r \in K$ gilt: $\beta(rv + v', w) = r\beta(v, w) + \beta(v', w)$ und $\beta(v, rw + w') = r\beta(v, w) + \beta(v, w')$.*
(b) *Eine Bilinearform $\beta\colon V \times V \to K$ heißt* ***symmetrisch****, wenn für alle $v, w \in V$ gilt: $\beta(v, w) = \beta(w, v)$.*

Definition 6.4.2 *Sei V ein $\mathbb{C}$-Vektorraum.*

(a) *Eine* ***Sesquilinearform*** *auf V ist eine Abbildung $\beta\colon V \times V \to \mathbb{C}$, so dass für alle $v, v', w, w' \in V$ und alle $r \in K$ gilt: $\beta(rv + v', w) = r\beta(v, w) + \beta(v', w)$ und $\beta(v, rw + w') = \bar{r}\beta(v, w) + \beta(v, w')$.*
(b) *Eine Sesquilinearform $\beta\colon V \times V \to \mathbb{C}$ heißt* ***hermitesch****, wenn für alle $v, w \in V$ gilt: $\beta(v, w) = \overline{\beta(w, v)}$.*

Lemma 6.4.3 (a) *Ist $v_1, \dots, v_n$ eine Basis von V und ist $A = (a_{ij})_{ij} \in K^{n\times n}$ eine Matrix, so existiert genau eine Bilinearform $\beta\colon V \times V \to K$, so dass $\beta(v_i, v_j) = a_{ij}$ gilt für alle i, j.*

(b) *Im Fall $K = \mathbb{C}$ gilt die gleiche Aussage auch für Sequilinearformen.*

Von nun an sei $\mathbb{K}$ entweder $\mathbb{R}$ oder $\mathbb{C}$, und V sei ein euklidischer bzw. unitärer $\mathbb{K}$-Vektorraum.

Satz 6.4.4 *Ist $f \in \mathrm{End}(V)$ ein Endomorphismus, so ist*

$$\beta_f\colon V \times V \to \mathbb{K}, (v, w) \mapsto \langle v, f(w)\rangle$$

eine Bilinearform (im Fall $\mathbb{K} = \mathbb{R}$) bzw. eine Sesquilinearform (im Fall $\mathbb{K} = \mathbb{C}$), und zu jeder Bilinearform/Sequilinearform β existiert genau ein Endomorphismus $f \in \mathrm{End}(V)$, so dass $\beta = \beta_f$ gilt.

Satz 6.4.5 *Zu jedem Endomorphismus $f \in \mathrm{End}(V)$ existiert genau ein Endomorphismus $g \in \mathrm{End}(V)$, so dass für alle $v, w \in V$ gilt: $\langle f(v), w\rangle = \langle v, g(w)\rangle$.*

Definition 6.4.6 (a) *Ist $f \in \mathrm{End}(V)$, so wird die Abbildung g aus Satz 6.4.5 die zu f* ***adjungierte Abbildung*** *genannt. Notation dafür: f^*.*

(b) *Ein Endomorphismus f heißt* ***selbstadjungiert****, wenn $f = f^*$ gilt.*

Bemerkung 6.4.7 *Es gilt $f^{**} = f$.*

Bemerkung 6.4.8 *Ein Endomorphismus $f \in \mathrm{End}(V)$ is genau dann eine orthogonale Transformation, wenn $f^* = f^{-1}$ gilt.*

Bemerkung 6.4.9 *Angewandt auf Matrizen $A \in \mathbb{K}^{n\times n}$ (aufgefasst als Endomorphismen von $\mathbb{K}^n$ mit dem Standard-Skalarprodukt) erhält man:*

- *Die zu A adjungierte Abbildung ist gegeben durch $A^* = \bar{A}^T$*
- *A ist selbstadjungiert genau dann, wenn A symmetrisch (im Fall $\mathbb{K} = \mathbb{R}$) bzw. hermitesch (im Fall $\mathbb{K} = \mathbb{C}$) ist.*
- *A ist orthogonal (im Sinne von Definition 6.2.1) genau dann, wenn $\bar{A}^T = A^{-1}$ ist; vgl. Satz 6.2.8.*

Mo 14.4.

Bemerkung 6.4.10 *Sei $\beta\colon V \times V \to \mathbb{K}$ eine Bilinearform (im Fall $\mathbb{K} = \mathbb{R}$) bzw. eine Sequilinearform (im Fall $\mathbb{K} = \mathbb{C}$) und sei $f \in \mathrm{End}(V)$ der entprechende Endomorphismus aus Satz 6.4.4. Dann gilt: β is symmetrisch bzw. hermitesch genau dann, wenn f selbstadjungiert ist.*

6.5 Der Spektralsatz und Folgerungen

Sei weiterhin $\mathbb{K}$ entweder $\mathbb{R}$ oder $\mathbb{C}$, und V sei ein euklidischer bzw. unitärer $\mathbb{K}$-Vektorraum.

Definition 6.5.1 *Ein Endomorphismus $f\colon V \to V$ heißt **normal**, wenn gilt: $f \circ f^* = f^* \circ f$.*

Beispiel 6.5.2 (a) *Ist f selbstadjungiert, so ist f normal.*

(b) *Ist f orthogonal (im Fall $\mathbb{K} = \mathbb{R}$) bzw. unitär (im Fall $\mathbb{K} = \mathbb{C}$), so ist f normal.*

Satz 6.5.3 (Spektralsatz für normale Endomorphismen über $\mathbb{C}$) *Sei V ein endlich-dimensionaler unitärer $\mathbb{C}$-Vektorraum. Ein Endomorphismus $f \in \operatorname{End}(V)$ ist normal genau dann, wenn V eine Orthonormalbasis aus Eigenvektoren von f besitzt.*

Satz 6.5.4 (Spektralsatz für normale Endomorphismen über $\mathbb{R}$) *Sei V ein endlich-dimensionaler euklidischer $\mathbb{R}$-Vektorraum, und sei $f \in \operatorname{End}(V)$ ein Endomorphismus mit der folgenden Eigenschaft:*

($\star$) *Ist $U \subseteq V$ ein nicht-trivialer[8] Untervektorraum mit $f(U) \subseteq U$, so hat die Einschränkung $f|_U$ mindestens einen Eigenwert (in $\mathbb{R}$).*

Unter dieser Annahme ($\star$) ist f normal genau dann, wenn V eine Orthonormalbasis aus Eigenvektoren von f besitzt.

Korollar 6.5.5 (Hauptachsentransformation für Endomorphismen) *Sei V endlich-dimensional und sei $f \in \operatorname{End}(V)$ selbstadjungiert. Dann existiert eine Orthonormalbasis $v_1, \dots, v_n$ von V aus Eigenvektoren von f, und alle Eigenwerte von f sind reell.*

Do 17.4.

Bemerkung 6.5.6 *Für Matrizen besagt Korollar 6.5.5: Ist $A \in \mathbb{K}^{n\times n}$ symmetrisch bzw. hermitesch, so existiert eine orthogonale bzw. unitäre Matrix S, so dass $S^{-1}AS$ eine Diagonalmatrix mit reellen Einträgen ist.*

Korollar 6.5.7 *Eine symmetrische bzw. hermitesche Matrix $A \in \mathbb{K}^{n\times n}$ ist genau dann positiv definit, wenn alle ihre Eigenwerte positiv sind.*

Korollar 6.5.8 *Sei $A \in \mathbb{K}^{n\times n}$ symmetrisch bzw. hermitesch, und sei $S \in \mathrm{GL}_n(\mathbb{K})$ so, dass $D := S^*AS$ eine Diagonalmatrix ist. (Solche S existieren immer, nach Bemerkung 6.5.6.) Dann ist A positiv definit genau dann, wenn alle Diagonaleinträge von D positive reelle Zahlen sind.*

[8] also $U \neq \{0\}$

Satz 6.5.9 (Hauptminoren-Kriterium) *Sei $A \in \mathbb{K}^{n\times n}$ symmetrisch bzw. hermitesch. Für $k \leq n$ sei $A_k \in \mathbb{K}^{k\times k}$ die Matrix, die aus den ersten k Zeilen und ersten k Spalten von A besteht. (Diese A_k nennt man die **Hauptminoren** von A.) Dann gilt: A ist positiv definit genau dann, wenn $\det A_k > 0$ ist für $k = 1, \dots, n$.*

Do 24.4.

Korollar 6.5.10 *Seien $b_{ij} \in \mathbb{R}$ für $1 \leq i \leq j \leq n$ und sei $f(x_1, \dots, x_n) = \sum_{1\leq i\leq j\leq n} b_{ij}x_ix_j$. (Eine solche Funktion nennt man eine **quadratische Form**.) Definiere $A = (a_{ij})_{ij} \in \mathbb{R}^{n\times n}$ durch: $a_{ij} = a_{ji} = \frac{1}{2}b_{ij}$ falls $i \neq j$ und $a_{ii} = b_{ii}$. Dann hat f ein Minimum bei 0 genau dann, wenn das Hauptminoren-Kriterium erfüllt ist (d. h. wenn A positiv definit ist).*

Korollar 6.5.11 (Hauptachsentransformation für Bilinearformen) *Sei V endlich-dimensional und sei $\beta\colon V \times V \to \mathbb{K}$ eine symmetrische (im Fall $\mathbb{K} = \mathbb{R}$) bzw. hermitesche (im Fall $\mathbb{K} = \mathbb{C}$) Bilinearform. Dann existiert eine Orthonormalbasis $v_1, \dots, v_n$ von V, so dass $\beta(v_i, v_j) = 0$ gilt für $i \neq j$. Außerdem gilt $\beta(v_i, v_i) \in \mathbb{R}$ für alle i.*

Satz 6.5.12 (Sylvesters Trägheitssatz) *Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum und $\beta\colon V \times V \to \mathbb{K}$ eine symmetrische (im Fall $\mathbb{K} = \mathbb{R}$) bzw. hermitesche (im Fall $\mathbb{K} = \mathbb{C}$) Bilinearform. Dann existiert eine Basis $v_1, \dots, v_n$ von V, so dass für $1 \leq i, j \leq n$ gilt: $\beta(v_i, v_j) = 0$ falls $i \neq j$, und $\beta(v_i, v_i) \in \{-1, 0, 1\}$. Außerdem sind die Anzahlen*

$$n_a = \#\{i \mid \beta(v_i, v_i) = a\}$$

(für $a = -1, 0, 1$) durch β eindeutig festgelegt, d. h. sie hängen nicht von der Wahl der Basis ab.

Mo 28.4.

Korollar 6.5.13 *Die Lösungsmenge (in $\mathbb{R}^2$) einer Gleichung der Form $ax^2 + bxy + cy^2 + dx + ey + f = 0$ ist ein Kreis, eine Ellipse, eine Parabel, eine Hyperbel, zwei Geraden, eine Gerade, ein Punkt oder leer.*

7 Die Jordansche Normalform

7.1 Direkte Summen und Komplemente

Sei K ein beliebiger Körper.

Definition 7.1.1 (a) *Sind V und V' K-Vektorräume, so schreiben wir $V \oplus V'$ für die Menge $V \times V'$, aufgefasst als K-Vektorraum mit komponentenweiser Addition und Skalarmultiplikation. Wir nennen $V \oplus V'$ die **(äußere) direkte Summe** von V und V'.*

(b) *Sind U und U' Untervektorräume eines K-Vektorraums V mit $U \cap U' = \{0\}$, so identifizieren wir $U \oplus U'$ mit $U + U'$, indem wir $(u, u') \in U \times U'$ mit $u + u' \in U + U'$ identifizieren, d. h. statt $U + U'$ schreibt man $U \oplus U'$, wenn man zusätzlich ausdrücken will, dass $U \cap U' = \{0\}$ gilt, und man nennt dies die **(innere) direkte Summe** von U und U'.*

Satz 7.1.2 *Sei V ein K-Vektorraum und seien $U_1, \dots, U_n \subseteq V$ Untervektorräume. Dann sind äquivalent:*

(a) $V = ((\cdots(U_1 \oplus U_2) \oplus \dots) \oplus U_{n-1}) \oplus U_n$

(b) *Jeder Vektor $v \in V$ lässt sich auf eindeutige Weise als Summe $v = v_1 + \cdots + v_n$ schreiben mit $v_i \in U_i$.*

Ist $u_{i,1}, \dots, u_{i,m_i}$ eine Basis von U_i für jedes i, so ist auch die folgende Bedingung zu den obigen Bedingungen äquivalent:

(c) $(u_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m_i}$ *ist eine Basis von V.*

Bemerkung 7.1.3 *Aus dem Satz folgt auch, dass die Klammerung bei (a) egal ist; wir schreiben in Zukunft einfach $V = U_1 \oplus \cdots \oplus U_n$.*

Mo 5.5.

Definition 7.1.4 *Sei V ein K-Vektorraum und U ein Untervektorraum. Ein **Komplement** von U (in V) ist ein Untervektorraum $U' \subseteq V$, so dass $U \oplus U' = V$ gilt.*

Bemerkung 7.1.5 *Komplemente existieren immer, sind aber nicht eindeutig. Ist V endlich-dimensional, $U \subseteq V$ und $U' \subseteq V$ ein Komplement von U, so gilt* $\dim U' = \dim V - \dim U$.

Bemerkung 7.1.6 *Ist V ein K-Vektorraum, $U \subseteq V$ ein Untervektoraum und $U' \subseteq V$ ein Komplement von U, so ist die Abbildung $U' \to V/U, u' \mapsto \bar{u}' = u' + U$ ein Isomorphismus von Vektorräumen.*

7.2 Nilpotente Endomorphismen

Im Folgenden sei K ein beliebiger Körper und V ein K-Vektorraum.

Definition 7.2.1 *Ein Endomorphismus $f \in \operatorname{End}(V)$ heißt **nilpotent**, wenn es ein $k \in \mathbb{N}$ gibt, so dass $f^k = 0$ ist. Eine Matrix $A \in K^{n \times n}$ heißt **nilpotent**, wenn sie als Endomorphismus von K^n nilpotent ist, d. h. wenn es ein $k \in \mathbb{N}$ gibt, so dass $A^k = 0$ ist. Das kleinste solche k heißt **Nilpotenzgrad** (auch: **Nilpotenzindex**) von f bzw. A.*

Von nun an nehmen wir an, dass V endlich-dimensional ist.

Satz 7.2.2 *Sei $f \in \operatorname{End}(V)$ nilpotent, und sei $k \in \mathbb{N}$ der Nilpotenzgrad von f. Setze $U_\ell := \ker(f^\ell)$ und $W_\ell := \operatorname{im}(f^\ell)$ für $\ell \in \mathbb{N}$. Dann gilt:*

(a) $\{0\} = U_0 \subsetneq U_1 \subsetneq \cdots \subsetneq U_{k-1} \subsetneq U_k = V$
(b) $V = W_0 \supsetneq W_1 \supsetneq \cdots \supsetneq W_{k-1} \supsetneq W_k = \{0\}$

Insbesondere ist $k \leq \dim V$.

Beispiel 7.2.3 *Die Matrix*

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

nilpotent, und für $\ell = 0, \ldots, n$ gilt:

$$\ker(A^\ell) = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_\ell \\ 0 \\ \vdots \\ 0 \end{pmatrix} \mid a_i \in K \right\} \qquad \textit{und} \qquad \operatorname{im}(A^\ell) = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_{n-\ell} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \mid a_i \in K \right\}.$$

Satz 7.2.4 (Jordansche Normalform von nilpotenten Matrizen) *Ist $f \in \operatorname{End}(V)$ ein nilpotenter Endomorphismus, so existiert ein Isomorphismus $g\colon K^n \to V$ (für $n = \dim V$), so dass die Matrix von $g^{-1} \circ f \circ g$ die Form*

$$\begin{pmatrix} \left.\boxed{\begin{matrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{matrix}}\right\} r_1 \times r_1 & & & \Huge 0 \\ & \left.\boxed{\begin{matrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{matrix}}\right\} r_2 \times r_2 & & \\ & & \ddots & \\ \Huge 0 & & & \left.\boxed{\begin{matrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{matrix}}\right\} r_\ell \times r_\ell \end{pmatrix}$$

hat für $r_1, \ldots, r_\ell \geq 1$. (Im Fall $r_i = 1$ ist gemeint, dass der entsprechende Block einfach nur $\boxed{0}$ ist.) Hierbei sind $r_1, \ldots, r_\ell$ bis auf Reihenfolge durch f eindeutig bestimmt.

Do 8.5.

Bemerkung: Setzt man $d_m := \dim \operatorname{im} f^m$, so ist die Anzahl der Blöcke der Größe $r \times r$ gegeben durch $d_{r-1} - 2d_r + d_{r+1}$.

Bemerkung 7.2.5 *In Satz 7.2.4 ist der Nilpotenzgrad von f das Maximum $\max\{r_1, \ldots, r_\ell\}$.*

Korollar 7.2.6 *Ist $f \in \operatorname{End}(V)$ nilpotent und $n = \dim V$, so gilt für das charakteristische Polynom von f: $\chi_f(x) = x^n$. Insbesondere ist 0 der einzige Eigenwert von f.*

Lemma 7.2.7 *Ist $f \in \operatorname{End}(V)$ nilpotent und $\lambda \in K^\times$, so ist $f + \lambda \operatorname{id}_V$ invertierbar.*

Mo 12.5.

7.3 Die Hauptraumzerlegung

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

Definition 7.3.1 *Sei $f \in \operatorname{End}(V)$. Ein Untervektorraum $U \subseteq V$ heißt **f-invariant**, wenn $f(U) \subseteq U$ gilt. Ist dies der Fall, so fassen wir $f|_U$ oft als Endomorphismus von U auf.*

Lemma 7.3.2 *Sei $f \in \operatorname{End}(V)$.*

(a) *Es existiert ein $N \in \mathbb{N}$, so dass für jedes $N' \geq N$ gilt: $\operatorname{im} f^N = \operatorname{im} f^{N'}$ und $\ker f^N = \ker f^{N'}$.*

Für N wie in (a) gilt außerdem:

(b) $V = \operatorname{im} f^N \oplus \ker f^N$.

(c) *Ist $g \in \operatorname{End}(V)$ ein Endomorphismus, der mit f kommutiert, d. h. so dass $f \circ g = g \circ f$ gilt, so sind $\ker f^N$ und $\operatorname{im} f^N$ g-invariant.*

Definition 7.3.3 *Sei $f \in \operatorname{End}(V)$ und $\lambda \in K$. Der **Eigenraum** von f zum Eigenwert λ ist*

$$\operatorname{Eig}_\lambda(f) := \ker(\lambda \operatorname{id}_V - f).$$

*Der **Hauptraum** von f zum Eigenwert λ ist*

$$\operatorname{Hau}_\lambda(f) := \ker(\lambda \operatorname{id}_V - f)^N$$

für „hinreichend große N“, d. h. so dass für alle $N' \geq N$ gilt: $\ker(\lambda \operatorname{id}_V - f)^{N'} = \ker(\lambda \operatorname{id}_V - f)^N$.

Bemerkung 7.3.4 $\mathrm{Eig}_\lambda(f)$ *und* $\mathrm{Hau}_\lambda(f)$ *kann man für beliebige* $\lambda \in K$ *definieren, aber nur wenn* λ *ein Eigenwert von* f *ist, sind diese Räume nicht-trivial. Genauer gilt:*

$$\lambda \text{ ist ein Eigenwert von } f \iff \mathrm{Eig}_\lambda(f) \neq \{0\} \iff \mathrm{Hau}_\lambda(f) \neq \{0\}.$$

Definition 7.3.5 *Wir nennen einen Körper* K ***algebraisch abgeschlossen****, wenn jedes nicht-konstante Polynom* $f \in K[X]$ *mindestens eine Nullstelle besitzt.*

Bemerkung 7.3.6 *Der Fundamentalsatz der Algebra (siehe Bemerkung 2.3.14) besagt also:* $\mathbb{C}$ *ist algebraisch abgeschlossen. Außerdem werden wir in der Algebra-Vorlesung sehen: Jeder beliebige Körper* K *lässt sich zu einem algebraisch abgeschlossenen Körper* $L \supseteq K$ *vergrößern.*

Satz 7.3.7 (Hauptraumzerlegung) *Ist* K *algebraisch abgeschlossen,* V *ein endlich-dimensionaler* K*-Vektorraum,* $f \in \mathrm{End}(V)$ *und sind* $\lambda_1, \dots, \lambda_\ell$ *die Eigenwerte von* f*, so gilt*

$$V = \mathrm{Hau}_{\lambda_1}(f) \oplus \cdots \oplus \mathrm{Hau}_{\lambda_\ell}(f).$$

Lemma 7.3.8 *Sei* $f \in \mathrm{End}(V)$*, seien* $\lambda, \lambda' \in K$*, und sei* $g := \lambda\,\mathrm{id}_V - f$*. Dann gilt:* $H' := \mathrm{Hau}_{\lambda'}(f)$ *ist* g*-invariant, und* $g|_{H'} \in \mathrm{End}(H')$ *ist entweder ein Automorphismus (nämlich falls* $\lambda' \neq \lambda$*) oder nilpotent (nämlich falls* $\lambda' = \lambda$*).*

Do 15.5.

7.4 Die Jordansche Normalform

Wir nehmen in diesem gesamten Abschnitt an, dass K ein algebraisch abgeschlossener Körper ist. Außerdem sei weiterhin V ein endlich-dimensionaler K-Vektorraum.

Satz 7.4.1 (Jordansche Normalform) *Ist* $f \in \mathrm{End}(V)$ *ein Endomorphismus, so existiert ein Isomorphismus* $g\colon K^n \to V$ *(für* $n = \dim V$*), so dass die Matrix* *von $g^{-1} \circ f \circ g$ die Form*

$$\begin{pmatrix} \boxed{\begin{matrix}\lambda_1 & 1 & 0 & \cdots & 0\\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda_1\end{matrix}} \left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\end{matrix}}\right\} r_1 \times r_1 & & & \text{\Huge 0} \\ & \boxed{\begin{matrix}\lambda_2 & 1 & 0 & \cdots & 0\\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda_2\end{matrix}} \left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\end{matrix}}\right\} r_2 \times r_2 & & \\ & & \ddots & \\ \text{\Huge 0} & & & \boxed{\begin{matrix}\lambda_\ell & 1 & 0 & \cdots & 0\\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda_\ell\end{matrix}} \left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\end{matrix}}\right\} \end{pmatrix} r_\ell \times r_\ell$$

hat für $\lambda_1, \dots, \lambda_\ell \in K$ und $r_1, \dots, r_\ell \geq 1$. Hierbei sind die Paare $(\lambda_1, r_1), \dots, (\lambda_\ell, r_\ell)$ bis auf Reihenfolge durch f eindeutig bestimmt. (Die λ_i müssen nicht alle verschieden sein.)

Definition 7.4.2 *Die Matrix aus dem Satz nennt man die* ***jordansche Normalform*** *von f. Man sagt auch, eine Matrix „ist in* ***jordanscher Normalform***“*, wenn sie die obige Form hat. Die obigen $(r_i \times r_i)$-Blöcke dieser Matrix nennt man* ***Jordan-Blöcke****.*

Bemerkung 7.4.3 *Ist $f \in \operatorname{End}(K^n)$, so ist es durch eine Matrix $A \in K^{n \times n}$ gegeben, und wir erhalten: Eine „jordansche Normalform von A“ ist eine Matrix $B \in K^{n \times n}$, die zu A ähnlich ist und die in jordanscher Normalform ist. Und Satz 7.4.1 besagt, dass jede Matrix eine jordansche Normalform besitzt, und dass verschiedene jordansche Normalformen der selben Matrix A (die also zueinander ähnlich sind) sich nur in der Reihenfolge der Blöcke unterscheiden.*

Bemerkung 7.4.4 *Die jordansche Normalform eines Endomorphismus f lässt sich bestimmen, indem man zunächst die Eigenwerte $\lambda_1, \dots, \lambda_\ell$ bestimmt und dann aus den Dimensionen $d_{i,s} := \dim(\ker(f - \lambda_i \operatorname{id}_V)^s)$ die Blockgrößen ableitet: Für $s \geq 1$ gibt $d_{i,s} - d_{i,s-1}$ die Anzahl der Blöcke an, die λ_i auf der Diagonalen haben und mindestens Größe $s \times s$ haben.*

Korollar 7.4.5 *Sei $f \in \operatorname{End}(V)$, seien $\lambda_1, \dots, \lambda_\ell$ die Eigenwerte von f und sei $d_i := \dim \operatorname{Hau}_{\lambda_i}(f)$ die Dimension des entsprechenden Hauptraums, für $1 \leq i \leq \ell$.*

Dann hat das charakteristische Polynom von $f \in \mathrm{End}(V)$ die folgende Form:

$$\chi_f(x) = \prod_{i=1}^{\ell} (\lambda_i - x)^{d_i}$$

Korollar 7.4.6 (Jordanzerlegung) *Jeder Endomorphismus $f \in \mathrm{End}(V)$ lässt sich als Summe $f = f_{\mathrm{diag}} + f_{\mathrm{nilp}}$ schreiben für $f_{\mathrm{diag}}, f_{\mathrm{nilp}} \in \mathrm{End}(V)$ mit folgenden Eigenschaften:*

(a) *f_{diag} ist diagonalisierbar.*
(b) *f_{nilp} ist nilpotent.*
(c) *f_{diag} und f_{nilp} kommutieren, d. h. $f_{\mathrm{diag}} \circ f_{\mathrm{nilp}} = f_{\mathrm{nilp}} \circ f_{\mathrm{diag}}$.*