LINEARE ALGEBRA II, SS 2011.
NOTIZEN ZUR VORLESUNG.

ULRICH GÖRTZ

1. Ringe

Referenz: [Bosch, Lineare Algebra, Kapitel 5]

4.4.

1.1. **Definition und erste Eigenschaften. Definitionen.** Ring (immer mit 1), kommutativer Ring, Einheit, Einheitengruppe $R^\times$.

Rechenregeln. $0a = 0$ für alle $a \in R$. Kürzungsregel gilt im allg. nicht.

Beispiele. $\mathbb{Z}$, Körper, $M_{n\times n}(K)$ (K Körper).

1.2. **Der Polynomring über einem (kommutativen) Ring.** R kommutativer Ring.

Definition. Der *Polynomring* $R[X]$ über R in der Unbestimmten X ist der Ring aller Folgen $(a_i)_{i\in\mathbb{N}}$ mit nur endlich vielen Einträgen $\neq 0$, mit elementweiser Addition und der Multiplikation

$$(a_i)_i \cdot (b_i)_i = \left(\sum_{j+k=i} a_j b_k \right)_i .$$

Dies ist ein kommutativer Ring mit $1 = (1, 0, 0, \dots)$ (und $0 = (0, 0, \dots)$).

Wir setzen $X := (0, 1, 0, 0, \dots)$ und können dann jedes Element in eindeutiger Weise als $\sum_{i\geq 0} a_i X^i$ schreiben (fast alle $a_i = 0$). 6.4.

Die Abbildung $R \to R[X]$, $a \mapsto (a, 0, 0, \dots)$ ist ein injektiver Ringhomomorphismus und wir fassen vermöge dieses Homomorphismus Elemente von R als Elemente von $R[X]$ auf. Diese Elemente heißen *konstante Polynome*.

Satz 1.1 (Einsetzungshomomorphismus)**.** *Sei R ein kommutativer Ring, $\varphi\colon R \to R'$ ein Ringhomomorphismus und $x \in R'$. Dann existiert ein eindeutig bestimmter Ringhomomorphismus $\Phi\colon R[X] \to R'$ mit $\Phi(a) = \varphi(a)$ für alle $a \in R$ und $\Phi(X) = x$, nämlich*

$$\sum_i a_i X^i \mapsto \sum_i \varphi(a_i) x^i.$$

Wir schreiben in der Situation des Satzes auch ev_x für Φ und $f(x) = \Phi(f)$.

Definition 1.2. Sei R ein kommutativer Ring, $f = \sum_{i=0}^N a_i X^i \in R[X]$ mit $a_N \neq 0$. Dann heißt a_N der *Leitkoeffizient* von f und N der Grad von f, in Zeichen $\deg f$. Das Element a_0 heißt der *Absolutkoeffizient* von f. Ist $a_N = 1$, so bezeichnet man f als *normiertes* Polynom.

Wir setzen $\deg 0 = -\infty$.

Definition 1.3. Ein kommutativer Ring R heißt *Integritätsbereich*, wenn $R \neq \{0\}$ und für alle $x, y \in R$ mit $xy = 0$ gilt: $x = 0$ oder $y = 0$.

Lemma 1.4. *Sei R ein kommutativer Ring, $f, g \in R[X]$.*

(1) $\deg(f+g) \leq \max(\deg f, \deg g)$,
(2) $\deg(fg) \leq \deg f + \deg g$, *und falls R ein Integritätsbereich ist, so gilt sogar* $=$.

Korollar 1.5. *Sei R ein Integritätsring. Dann ist auch $R[X]$ ein Integritätsring. Es gilt $R[X]^\times = R^\times$.*

Definition 1.6. Sei $\varphi\colon R \to R'$ ein Ringhomomorphismus. Dann heißen

$$\operatorname{Im} f := f(R)$$

das Bild, und

$$\operatorname{Ker} f := f^{-1}(\{0\})$$

der Kern des Ringhomomorphismus f.

Es ist leicht zu sehen, dass in dieser Situation $\operatorname{Im} f$ wieder ein Ring ist. Weil in aller Regel $1 \notin \operatorname{Ker} f$ gilt, ist der Kern eines Ringhomomorphismus in der Regel kein Ring in unserem Sinne, allerdings stets ein sogenanntes Ideal:

Definition 1.7. Sei R ein Ring. Eine Teilmenge $\mathfrak{a} \subseteq R$ heißt *Ideal* von R, falls $\mathfrak{a}$ eine Untergruppe von $(R, +)$ ist und falls für alle $a \in \mathfrak{a}$ und $x \in R$ gilt: $xa \in \mathfrak{a}$ und $ax \in \mathfrak{a}$.

Beispiel: Ist $d \in \mathbb{Z}$, so ist die Menge $(d) := \{xd;\ x \in \mathbb{Z}\}$ aller Vielfachen von d ein Ideal (und wir werden sehen, dass im Ring $\mathbb{Z}$ alle Ideale diese Form haben).

11.4.

1.3. **Teilbarkeit in Integritätsringen.** Bemerkung: Ist R ein Integritätsring, so gilt für $a \neq 0$ die Kürzungsregel: $ab = ac \Rightarrow b = c$.

Erinnerung: Division mit Rest in $\mathbb{Z}$.

Satz 1.8. *Sei K ein Körper, seien $f, g \in K[X]$, $g \neq 0$. Dann existieren eindeutig bestimmte Polynome $q, r \in K[X]$ mit $\deg r < \deg g$ und so dass*

$$f = qg + r.$$

Definition 1.9. Ein Integritätsring R heißt *euklidischer Ring*, falls eine Abbildung $\delta\colon R \setminus \{0\} \to \mathbb{N}$ ("Gradabbildung") existiert, so dass für alle $a, b \in R$, $b \neq 0$, (nicht notwendig eindeutig bestimmte) Elemente $q, r \in R$ existieren, so dass $r = 0$ oder $\delta(r) < \delta(b)$ und $a = qb + r$.

Beispiele. $\mathbb{Z}$ mit $\delta(a) = |a|$; $K[X]$ (K Körper) mit $\delta(f) = \deg(f)$.

Definition 1.10. Ein Ideal $\mathfrak{a}$ in einem Ring R heißt *Hauptideal*, wenn ein Element $a \in R$ existiert, so dass $\mathfrak{a} = (a) := \{xa;\ x \in R\}$.

Ein Integritätsring R heißt *Hauptidealring*, wenn jedes Ideal in R ein Hauptideal ist.

Satz 1.11. *Jeder euklidische Ring ist ein Hauptidealring. Insbesondere sind $\mathbb{Z}$ und $K[X]$ (K Körper) Hauptidealringe.*

Teilbarkeit, Primfaktorzerlegung.

Definition 1.12. Sei R ein Integritätsring. Seien $a, b \in R$

(1) Wir sagen, a sei ein Teiler von b (in Zeichen $a|b$), falls $c \in R$ existiert mit $ac = b$. Andernfalls schreiben wir $a \nmid b$.
(2) Wir nennen a, b zueinander assoziiert, falls $c \in R^\times$ existiert mit $ac = b$.

Bemerkung 1.13. (1) $a|b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$,
(2) a, b assoziiert $\Leftrightarrow$ ($a|b$ und $b|a$) $\Leftrightarrow (a) = (b)$.

Definition 1.14. Sei R ein Integritätsring.

(1) Ein Element $p \in R \setminus (R^\times \cup \{0\})$ heißt *irreduzibel*, falls für alle $a, b \in R$ mit $p = ab$ gilt: $a \in R^\times$ oder $b \in R^\times$.
(2) Ein Element $p \in R \setminus (R^\times \cup \{0\})$ heißt *prim* (oder *Primelement*), falls für alle $a, b \in R$ mit $p|ab$ gilt: $p|a$ oder $p|b$.

13.4.

Satz 1.15. *Sei R ein Integritätsring. Ist $p \in R$ prim, so ist p irreduzibel. Ist R ein Hauptidealring, so gilt auch die Umkehrung.*

Satz 1.16. *Sei R ein Hauptidealring. Dann lässt sich jedes Element aus $R \setminus (R^\times \cup \{0\})$ als Produkt von Primelementen schreiben.*

Lemma 1.17. *Sei R ein Integritätsring, seien $p_1, \ldots, p_r \in R$ prim und seien $q_1, \ldots, q_s \in R$ irreduzibel. Gilt*

$$p_1 \cdot \cdots \cdot p_r = q_1 \cdot \cdots \cdot q_s,$$

so gilt $r = s$ und nach einer eventuellen Umnummerierung der q_i gilt für alle $i = 1, \ldots, r$: Es gibt $\varepsilon_i \in R^\times$ mit $p_i = \varepsilon_i q_i$.

Definition 1.18. Ein Integritätsring R heißt *faktoriell*, wenn sich jedes Element aus $R \setminus (R^\times \cup \{0\})$ als Produkt von Primelementen schreiben lässt.

Man sagt in der Situation dieser Definition auch, in R gelte die "eindeutige Zerlegung in Primfaktoren".

Beispiel 1.19. Da $\mathbb{Z}$ ein Hauptidealring ist, ist $\mathbb{Z}$ faktoriell. Wegen $\mathbb{Z}^\times = \{1, -1\}$ gilt auch die folgende, etwas präzisere Aussage: Jede ganze Zahl $a \in \mathbb{Z}$, $a \neq 0$, lässt sich schreiben als $a = \varepsilon p_1 \cdot \cdots \cdot p_r$ mit $\varepsilon \in \{1, -1\}$ und (positiven) Primzahlen p_i. Dabei ist ε eindeutig bestimmt (nämlich gleich dem Vorzeichen von a), und die p_i sind eindeutig bestimmt bis auf die Reihenfolge.

Beispiel 1.20. Sei K ein Körper. Nach dem Gezeigten ist der Polynomring $R = K[X]$ faktoriell. Es gilt $R^\times = K^\times$ und wir erhalten: Jedes Polynom $f \in K[X]$, $f \neq 0$, lässt sich schreiben als Produkt $f = uf_1 \cdot \cdots \cdot f_r$, wobei $u \in K^\times$, $f_i \in K[X]$ irreduzibel und normiert.

Dabei ist u eindeutig bestimmt (u ist der Leitkoeffizient von f), und die f_i sind eindeutig bestimmt bis auf ihre Reihenfolge. (Da die f_i irreduzibel sind, gilt $\deg f_i > 0$.)

18.4.

Nullstellen von Polynomen. Sei K ein Körper.

Definition 1.21. Sei $f \in K[X]$. Ein Element $\alpha \in K$ heißt *Nullstelle* von f, falls $f(\alpha) = 0$.

Bemerkung 1.22. Ein Element $\alpha \in K$ ist genau dann Nullstelle eines Polynoms $f \in K[X] \setminus \{0\}$, wenn $X - \alpha$ das Polynom f teilt. Insbesondere sehen wir, dass ein Polynom vom Grad n höchstens n verschiedene Nullstellen haben kann.

Ist α eine Nullstelle des Polynoms f, und gilt $(X-\alpha)^m | f$, aber $(X-\alpha)^{m+1} | f$, so sagen wir, α sei eine Nullstelle der Vielfachheit m und schreiben $\mathrm{mult}_\alpha(f) := m$.

Wir sagen, ein Polynom $f \in K[X] \setminus \{0\}$ zerfalle vollständig in Linearfaktoren, wenn f Produkt von linearen Polynomen (d.h. von Polynomen vom Grad 1) ist.

Definition 1.23. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes Polynom in $K[X] \setminus K$ eine Nullstelle besitzt. (Äquivalent: wenn jedes Polynom in $K[X] \setminus K$ vollständig in Linearfaktoren zerfällt.)

Theorem 1.24. *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Dieses schwierige Theorem beweisen wir nicht im Rahmen der Vorlesung über lineare Algebra. Es wird üblicherweise in den Vorlesungen *Algebra* und *Funktionentheorie* bewiesen, kann aber auch mit Mitteln der Analysis I bewiesen werden.

Der chinesische Restsatz. Sei R ein Ring, $\mathfrak{a} \subset R$ ein Ideal. Für Elemente $x, y \in R$ schreiben wir

$$x \equiv y \mod \mathfrak{a}, \text{ wenn } x - y \in \mathfrak{a}.$$

In den meisten Fällen ist $\mathfrak{a} = (a)$ ein Hauptideal; dann schreiben wir auch $x \equiv y \mod a$, und dies ist gerade äquivalent zu $a | x - y$. Man sagt, x sei *kongruent* zu y *modulo* $\mathfrak{a}$. Kongruenz ist eine "Äquivalenzrelation" (siehe unten).

Definition 1.25. Sei R ein Integritätsring, seien $a, b \in R$.

(1) Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von a, b, in Zeichen: $d = \mathrm{ggT}(a,b)$, wenn $d|a$, $d|b$, und für jedes Element d', das a und b teilt, $d'|d$.
(2) Ein Element $d \in R$ heißt *kleinstes gemeinsames Vielfaches* von a, b, in Zeichen $d = \mathrm{kgV}(a,b)$, wenn $a|d$, $b|d$, und für jedes Element d', das von a und b geteilt wird, $d|d'$.
(3) Die Elemente a, b heißen *teilerfremd*, falls $(a,b) := \{xa + yb;\ x, y \in R\} = R$.

Bemerkung 1.26.
(1) Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches sind (nur) eindeutig bestimmt bis auf Multiplikation mit Einheiten aus R, die Notationen $\mathrm{ggT}(a,b)$, $\mathrm{kgV}(a,b)$ sind mit entsprechender Vorsicht zu gebrauchen!
(2) Ist R ein Hauptidealring, so ist d genau dann ein größter gemeinsamer Teiler von a, b, falls $(d) = (a,b)$. Insbesondere sind in diesem Fall a und b genau dann teilerfremd, wenn 1 größter gemeinsamer Teiler von a und b ist.

Exkurs. Die abc-Vermutung. Der Satz von Mason-Stothers.

Satz 1.27 (Chinesischer Restsatz)**.** *Seien R ein Integritätsring und $a_1, \ldots, a_r \in R$ paarweise teilerfremde Elemente. Sei $a = a_1 \cdot \cdots \cdot a_r$.*

Seien $b_1, \ldots, b_r \in R$. Dann existiert ein Element $b \in R$, so dass für alle $i = 1, \ldots, r$ gilt: $b \equiv b_i \mod a_i$. Ist b' ein weiteres solches Element, so gilt $b \equiv b' \mod a$.

20.4.

1.4. **Quotientenkörper.**

Definition 1.28. Sei M eine Menge. Eine Teilmenge $R \subseteq M \times M$ heißt *Äquivalenzrelation*, wenn gilt

(1) (reflexiv) Für alle $x \in M$ ist $(x, x) \in R$.
(2) (symmetrisch) Für alle $x, y \in M$ ist $(x, y) \in R$ genau dann, wenn $(y, x) \in R$.
(3) (transitiv) Für alle $x, y, z \in M$ mit $(x, y) \in R$, $(y, z) \in R$ gilt $(x, z) \in R$.

Üblicherweise schreibt man $x \sim y$ statt $(x, y) \in R$.

Definition 1.29. Sei R eine Äquivalenzrelation auf M. Die Teilmengen von M der Form $[m] := \{m' \in M;\ m' \sim m\}$ für ein $m \in M$ heißen die *Äquivalenzklassen* von R.

Die Menge aller Äquivalenzklassen bezeichnen wir mit $M/\sim$.

Zwei Äquivalenzklassen in M sind entweder disjunkt oder gleich.

Sei nun A ein Integritätsring, und $M = A \times (A \setminus \{0\})$. Betrachte die folgende Äquivalenzrelation R auf M:

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc.$$

Satz 1.30. *Sei $K := M/\sim$. Wir schreiben $\frac{a}{b}$ für die Äquivalenzklasse eines Elementes $(a, b) \in M$. Es gilt dann also*

$$\frac{a}{b} = \frac{c}{d} \quad \Leftrightarrow \quad ad = bc.$$

Dann ist K mit der Addition

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

und der Multiplikation

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

ein Körper, der sogenannte Quotientenkörper *von A.*

Die Abbildung $A \to K$, $a \mapsto \frac{a}{1}$ ist ein injektiver Ringhomomorphismus. Man schreibt oft a statt $\frac{a}{1}$ und fasst R als Teilmenge von K auf.

Beispiel 1.31. Der Quotientenkörper von $\mathbb{Z}$ ist der Körper $\mathbb{Q}$ der rationalen Zahlen.

1.5. **Determinanten über Ringen.** Sei R ein Ring. Wir bezeichnen mit $M_{n\times n}(R)$ die Menge aller $n \times n$-Matrizen mit Einträgen in R. Mit der üblichen Addition und Multiplikation von Matrizen ist dies wieder ein Ring.

Sei nun speziell R ein Integritätsring, K sein Quotientenkörper. Wir betrachten $M_{n\times n}(R)$ als Teilmenge von $\subset M_{n\times n}(K)$. Die Leibniz-Formel zeigt, dass für alle $A \in M_{n\times n}(R)$ die Determinante $\det(A)$ (die wir definiert haben für Matrizen mit Einträgen in einem Körper; wir fassen also A auf als Element von $M_{n\times n}(K)$) ein Element von R ist. Es gelten, wie über jedem Körper, auch über K die üblichen Rechenregeln, zum Beispiel:

Satz 1.32. *Seien $A, B \in M_{n\times n}(R)$. Dann gilt $\det(AB) = \det(A)\det(B)$. (Da beide Seiten dieser Gleichung Elemente von R sind, gilt diese Gleichheit auch in R.)*

Die Cramersche Regel zeigt:

Satz 1.33. *Sei $A \in M_{n\times n}(R)$. Es existiert genau dann eine Matrix $B \in M_{n\times n}(R)$ mit $AB = BA = E_n$ (also ein multiplikatives Inverses von A in dem Ring $M_{n\times n}(R)$), wenn* $\det(A) \in R^\times$.

Es ist nicht schwer zu zeigen (durch Reduktion auf den "universellen" Fall $R = \mathbb{Z}[X_{ij};\ i,j = 1,\dots,n]$), dass beide Sätze auch über beliebigen kommutativen Ringen gelten.

2. Charakteristisches Polynom und Minimalpolynom

K Körper, V endlich-dimenionaler K-VR.

2.1. Charakteristisches Polynom.

Definition 2.1. (1) Sei $n \geq 0$ und $A \in M_{n\times n}(K)$. Dann heißt das Polynom $\operatorname{charpol}_A(X) := \det(XE_n - A) \in K[X]$ das *charakteristische Polynom* der Matrix A.

(2) Sei $f\colon V \to V$ ein Endomorphismus von V, $\mathscr{B}$ eine Basis von V, $A = M^{\mathscr{B}}_{\mathscr{B}}(f)$. Dann ist $\operatorname{charpol}_A(X)$ unabhängig von der Wahl der Basis $\mathscr{B}$ und heißt das *charakteristische Polynom* des Endomorphismus f.

27.4.

Satz 2.2. *Sei $f\colon V \to V$ ein Endomorphismus von V, χ sein charakteristisches Polynom. Dann ist $\alpha \in K$ genau dann eine Nullstelle von χ, wenn α ein Eigenwert von f ist.*

Sei $n = \dim V$, $f \in \operatorname{End}_K(V)$ mit charakteristischem Polynom χ. Dann gilt

$$\chi = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0,$$

d.h. χ ist normiert vom Grad n. Außerdem ist $a_0 = \det(-f) = (-1)^n \det f$.

Definition 2.3. Eine Matrix $A \in M_{n\times n}(K)$ heißt trigonalisierbar, wenn A zu einer oberen Dreiecksmatrix konjugiert ist. Ein Endomorphismus von V heißt trigonalisierbar, wenn eine Basis von V existiert, so dass die beschreibende Matrix bezüglich dieser Basis eine obere Dreiecksmatrix ist.

Satz 2.4. *Eine Matrix (ein Endomorphismus) ist genau dann trigonalisierbar, wenn ihr (sein) charakteristisches Polynom vollständig in Linearfaktoren zerfällt.*

Spur einer Matrix, eines Endomorphismus. Sei $n = \dim V$, $f \in \operatorname{End}_K(V)$ mit charakteristischem Polynom χ, und schreibe

$$\chi = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

Dann heißt das Element $-a_{n-1} \in K$ die *Spur* des Endomorphismus f. Für eine Matrix $A = (a_{ij})_{i,j} \in M_{n\times n}(K)$ nennt man entsprechend das Negative des Koeffizienten von X^{n-1} im charakteristischen Polynom von A die *Spur*, $\operatorname{Spur}(A)$, von A. Es gilt

$$\operatorname{Spur}(A) = \sum_{i=1}^{n} a_{ii}.$$

2.5.

2.2. **Minimalpolynom.** Sei $A \in M_{n\times n}(K)$, und sei $\Phi\colon K[X] \to M_{n\times n}(K)$ der Ringhomorphismus mit $\Phi(a) = aE_n$ für alle $a \in K$ und $\Phi(X) = A$. Wir schreiben $K[A]$ für das Bild von Φ—dies ist ein kommutativer Unterring von $M_{n\times n}(K)$, der K enthält (und auch ein K-Vektorraum ist).

Definition 2.5. Mit den obigen Notationen definieren wir: Das Minimalpolynom minpol_A von A ist das eindeutig bestimmte normierte Polynom $p \in K[X]$ mit $\operatorname{Ker}\Phi = (p)$.

Ist $f \in \operatorname{End}_K(V)$, so haben alle Matrizen, die f bezüglich einer Basis von V beschreiben, dasselbe Minimalpolynom. Wir nennen dieses Polynom das *Minimalpolynom* von f und bezeichnen es mit minpol_f.

2.3. **Der Satz von Cayley-Hamilton.**

Definition 2.6. Sei $f \in \operatorname{End}_K(V)$. Ein Unterverktorraum $U \subseteq V$ heißt *f-invariant*, wenn $f(U) \subseteq U$.

Definition 2.7. Sei $f \in \operatorname{End}_K(V)$. Ein Untervektorraum $U \subseteq V$ heißt f-zyklischer Unterraum, falls $u \in U$ existiert mit $U = \langle u, f(u), f^2(u), \dots\rangle$.

Lemma 2.8. *Sei $U \subseteq V$ ein f-zyklischer Unterraum, u wie in der Definition und $i = \dim U$. Dann ist $u, f(u), \dots, f^{i-1}(u)$ eine Basis von U.*

Definition 2.9. Sei $f = X^n + \sum_{i=0}^{n-1} a_i X^i \in K[X]$ ein normiertes Polynom vom Grad n. Dann heißt die Matrix

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -a_{n-1} \end{pmatrix}$$

die *Begleitmatrix von f*.

Bemerkung. Ein Untervektorraum $U \subseteq V$ ist genau dann f-zyklisch, wenn $f(U) \subseteq U$ und eine Basis von U existiert, so dass die Matrix von $f_{|U}$ bezüglich dieser Basis die Form einer Begleitmatrix hat.

Lemma 2.10. *Sei $A \in M_{n\times n}(K)$ die Begleitmatrix des normierten Polynoms f (vom Grad n). Dann gilt* $\operatorname{charpol}_A = f$.

Übung. Das Minimalpolynom der Begleitmatrix von f ist f. 4.5.

Satz 2.11 (Cayley-Hamilton)**.** *Ist $A \in M_{n\times n}(K)$, so gilt* $\operatorname{charpol}_A(A) = 0 (\in M_{n\times n}(K))$. *Ist f ein Endomorphismus des endlich-dimensionalen K-Vektorraums V, so gilt* $\operatorname{charpol}_f(f) = 0 (\in \operatorname{End}_K(V))$.

Beweis. Sei $f \in \operatorname{End}_K(V)$, $\chi = \operatorname{charpol}_f$. Zu zeigen ist $\chi(f)(v) = 0$ für alle $v \in V$. Zu $v \in V$ betrachte den f-zyklischen Unterraum $U = \langle v, f(v), f^2(f), \dots\rangle$. Es gilt dann $f(U) \subseteq U$ und bezüglich der Basis $v, f(v), \dots, f^{i-1}(v)$, $i = \dim U$, hat $f_{|U}$ als beschreibende Matrix eine Begleitmatrix. Das charakteristische Polynom von f ist ein Vielfaches des charakteristischen Polynoms dieser Begleitmatrix. Daran sehen wir: es genügt, $\chi(f)(v) = 0$ in dem speziellen Fall zu zeigen, dass V ein f-zyklischer Vektorraum mit Basis $v, f(v), \dots, f^{n-1}(v)$ ist.

In diesem Fall ist $\chi(f)(v) = 0$ aber leicht nachzurechnen. Ist nämlich $\chi = X^n + \sum_{i=0}^{n-1} a_i X^i$, so lesen wir aus der letzten Spalte der Begleitmatrix ab, dass

$$f^n(v) = f(f^{n-1}(v)) = \sum_{i=0}^{n-1} -a_i f^i(v),$$

also

$$\chi(f)(v) = f^n(v) + \sum_{i=0}^{n-1} a_i f^i(v) = 0.$$

□

Korollar 2.12. *Ist $A \in M_{n\times n}(K)$, so gilt* $\operatorname{minpol}_A \mid \operatorname{charpol}_A$.

- Für $A \in M_{2\times 2}(K)$ sei p_A das Polynom
$$p_A := \det(X \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - A) \in K[X].$$
Zeige, dass für alle A gilt: $\det(A \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - A) = 0 (\in K)$ (hier bezeichne $A \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ das Matrizenprodukt), und finde ein A mit $p_A(A) \neq 0 (\in M_{2\times 2}(K))$.

3. Die Jordansche Normalform

Referenzen: Ich habe keine genaue Vorlage, aber die Bücher [Brieskorn, Lineare Algebra und Analytische Geoetrie II], [Fischer, Lernbuch Lineare Algebra und Analytische Geometrie] sind vermutlich hilfreich. Ebenso kann ich das Buch [Vinberg, A Course in Algebra], Kap. 6.4, empfehlen. Zum konzeptionellen Verständnis ist auch das Buch von Bosch nützlich, es benutzt aber einen anderen (komplizierteren) Zugang.

3.1. Aussage und Eindeutigkeit.

Definition 3.1. Für $\lambda \in K$, $r \geq 1$, bezeichne mit $J_{r,\lambda} \in M_{r\times r}(K)$ den *Jordan-Block* der Größe $r \times r$ mit Diagonaleintrag λ (und 1en direkt oberhalb der Diagonalen, 0en sonst). Wir sagen, eine Matrix $A \in M_{n\times n}(K)$ habe Jordansche Normalform (JNF), falls $r_1, \ldots, r_k \geq 1$ und $\lambda_1, \ldots \lambda_k \in K$ existieren, so dass

$$A = \operatorname{diag}(J_{r_1,\lambda_1}, \ldots, J_{r_k,\lambda_k}) \quad \text{(Block-Diagonalmatrix)}$$

ist.

Theorem 3.2. *Sei $A \in M_{n\times n}(K)$ eine Matrix, deren charakteristisches Polynom vollständig in Linearfaktoren zerfällt. Dann existieren $S \in GL_n(K)$ und $r_1, \ldots, r_k \geq 1$, $\lambda_1, \ldots \lambda_k \in K$, so dass*

$$SAS^{-1} = \operatorname{diag}(J_{r_1,\lambda_1}, \ldots, J_{r_k,\lambda_k})$$

und die Paare $(r_1, \lambda_1), \ldots, (r_k, \lambda_k)$ sind eindeutig bestimmt bis auf die Reihenfolge (auch die Vielfachheit, mit der ein Paar auftritt, ist eindeutig bestimmt).

Bemerkung 3.3.
(1) Wie oben bemerkt, zerfällt $\operatorname{charpol}_A$ genau dann vollständig in Linearfaktoren, wenn A trigonalisierbar ist.
(2) Eine entsprechende Aussage gilt für trigonalisierbare Endomorphismen endlich-dimensionaler Vektorräume.

(3) Ist $A = \operatorname{diag}(J_{r_1,\lambda_1}, \ldots, J_{r_k,\lambda_k})$, so gilt

$$\operatorname{charpol}_A = \prod_{i=1}^{k} (X - \lambda_i)^{r_i}$$

und wenn $\mu_1, \ldots, \mu_s$ die paarweise verschiedenen Eigenwerte von A und m_i die Größe des größten Jordan-Blocks zu μ_i bezeichnen:

$$\operatorname{minpol}_A = \prod_{i=1}^{s} (X - \mu_i)^{m_i}.$$

Korollar 3.4. *Sei $A \in M_{n\times n}(K)$ eine Matrix, deren charakteristisches Polynom vollständig in Linearfaktoren zerfällt. Dann sind alle Nullstellen des charakteristischen Polynoms von A auch Nullstellen des Minimalpolynoms von A (und umgekehrt).*

9.5.

Korollar 3.5. *Sei $A \in M_{n\times n}(K)$ eine Matrix, deren charakteristisches Polynom vollständig in Linearfaktoren zerfällt. Die Matrix A ist genau dann diagonalisierbar, wenn das Minimalpolynom nur einfache Nullstellen hat.*

Bemerkung 3.6. Mit etwas mehr Anstrengung kann man zeigen: $A \in M_{n\times n}(K)$ ist genau dann diagonalisierbar, wenn minpol_A vollständig in Linearfaktoren zerfällt und nur einfache Nullstellen hat, siehe Korollar 3.19.

- Erstelle weitere Aufgaben vom Typ der Präsenzaufgabe auf Blatt 7.
- Was ist die JNF von $J_{r,\lambda}^t$, wobei A^t die zu A transponierte Matrix bezeichnet?
- Finde Matrizen $A, B \in M_{n\times n}(K)$, die nicht zueinander konjugiert sind, aber so dass $\operatorname{charpol}_A = \operatorname{charpol}_B$, $\operatorname{minpol}_A = \operatorname{minpol}_B$. Wie groß muss n mindestens sein, damit solche A, B existieren?
- Sei $v \in \mathbb{R}^2$ und sei $f \in \operatorname{End}_{\mathbb{R}}(\mathbb{R}^2)$ die Spiegelung an der Geraden $\langle v\rangle$. Bestimme die Jordansche Normalform von f.

Die duale Partition einer Partition. Ein Tupel $r_1 \geq r_2 \geq r_3 \geq \cdots$ natürlicher Zahlen heißt *Partition* von $n \in \mathbb{N}$, falls $n = \sum r_i$. (Insbesondere dürfen nur endlich viele $r_i \neq 0$ sein.)

Definition 3.7. Sei $r_1 \geq r_2 \geq r_3 \geq \cdots$ eine Partition von n. Dann ist auch $s_1 \geq s_2 \geq \cdots$ mit

$$s_i = \#\{j;\ r_j \geq i\}$$

eine Partition von n. Sie wird als die *zu* $(r_\bullet)_\bullet$ *duale Partition* bezeichnet.

Lemma 3.8. *Sei $r_1 \geq r_2 \geq r_3 \geq \cdots$ eine Partition von n, $s_1 \geq s_2 \geq \cdots$ ihre duale Partition. Dann ist $r_1 \geq r_2 \geq r_3 \geq \cdots$ die duale Partition von $(s_\bullet)_\bullet$.*

Eindeutigkeit der Jordanschen Normalform. Sei A eine Matrix in Jordanscher Normalform. Das charakteristische Polynom von A bestimmt die Diagonaleinträge zusammen mit ihrer Vielfachheit. Die Größe der Jordan-Blöcke lässt sich wie folgt beschreiben:

Sei μ einer der Eigenwerte von A, und seien $r_1 \geq r_2 \geq \cdots$ die Größen der Jordan-Blöcke mit Diagonaleintrag μ. Sei $s_1 \geq s_2 \geq \cdots$ die zu $(r_\bullet)_\bullet$ duale Partition. Dann gilt

$$s_i = \dim \operatorname{Ker}(A - \mu)^i - \dim \operatorname{Ker}(A - \mu)^{i-1}.$$

Die Zahlen $\dim \mathrm{Ker}(A-\mu)^i$ ändern sich nicht, wenn man A durch eine zu A konjugierte Matrix ersetzt. Dies beweist, dass die Größen der Jordan-Blöcke in der Jordanschen Normalform einer trigonalisierbaren Matrix eindeutig bestimmt sind.

3.2. **Zerlegung in verallgemeinerte Eigenräume, Jordan-Zerlegung.**

Definition 3.9. Sei $f \in \mathrm{End}_K(V)$, sei μ ein Eigenwert von f, und sei m die Vielfachheit der Nullstelle μ von minpol_f. Der Untervektorraum

$$\tilde{V}_\mu := \bigcup_{i\geq 0} \mathrm{Ker}(f-\mu\,\mathrm{id})^i = \mathrm{Ker}(f-\mu\,\mathrm{id})^m \tag{1}$$

heißt der *verallgemeinerte Eigenraum* (oder: *Hauptraum*) von f zum Eigenwert μ.

Bemerkung 3.10. Wir sehen insbesondere: Der Eigenraum von f zum Eigenwert μ ist im verallgemeinerten Eigenraum enthalten. Jede Nullstelle des charakteristischen Polynoms ist auch eine Nullstelle des Minimalpolynoms.

Ist $f \in \mathrm{End}_K(V)$ und $\tilde{V}$ der verallgemeinerte Eigenraum von f zum Eigenwert μ, so gilt $f(\tilde{V}) \subseteq \tilde{V}$ und der einzige Eigenwert von $f_{|\tilde{V}}$ ist μ.

11.5.

Satz 3.11. *Sei $f \in \mathrm{End}(V)$, $\chi = \mathrm{charpol}_f$, und χ zerfalle vollständig in Linearfaktoren. Seien $\mu_1, \ldots, \mu_s$ die Eigenwerte von f (μ_i paarweise verschieden). Sei $\tilde{V}_i$ der verallgemeinerte Eigenraum von f zum Eigenwert μ_i.*

Dann gilt $V = \bigoplus_{i=1}^s \tilde{V}_i$ und $\dim \tilde{V}_i = \mathrm{mult}_{\mu_i}(\mathrm{charpol}_f)$.

Beweis. **I. Die Summe ist direkt.** Sei $m_i = \mathrm{mult}_{\mu_i}(\mathrm{minpol}_f)$, d.h.

$$\mathrm{minpol}_f = \prod_{i=1}^s (X-\mu_i)^{m_i}.$$

Wir zeigen $\tilde{V}_1 \cap (\sum_{i>1} \tilde{V}_i) = 0$. Aus Symmetriegründen impliziert das die Behauptung. Sei nun $v \in \tilde{V}_1 \cap (\sum_{i>1} \tilde{V}_i)$. Wegen $v \in \tilde{V}_1$ gilt $(f-\mu_1\,\mathrm{id})^{m_1}(v) = 0$, wegen $v \in \sum_{i>1} \tilde{V}_i$ gilt $(\prod_{i>1}(f-\mu_i\,\mathrm{id})^{m_i})(v) = 0$ (wobei das Produkt als Produkt in $\mathrm{End}_K(V)$ zu verstehen ist, d.h. als Verkettung von Abbildungen). Beachte, dass die Abbildungen $(f-\mu_i\,\mathrm{id})^{m_i}$ alle miteinander (und mit f) kommutieren.

Weil die Polynome $p_1 := (X-\mu_1)^{m_1}$ und $q_1 := \prod_{i>1}(X-\mu_i)^{m_i}$ teilerfremd sind, existieren $a, b \in K[X]$ mit $ap_1 + bq_1 = 1$. Dann folgt $v = \mathrm{id}(v) = a(f)(p_1(f)(v)) + b(f)(q_1(f)(v)) = 0$.

II. $V = \sum_{i=1}^s \tilde{V}_i$. Die Polynome $q_j := \prod_{i\neq j}(X-\mu_i)^{m_i}$, $j = 1, \ldots, n$, haben keinen nicht-trivialen gemeinsamen Teiler, das kleinste Ideal in $K[X]$, das alle q_j enthält, ist daher $= (1) = K[X]$. Insbesondere existieren Polynome a_j mit

$$\sum_{j=1}^n a_j q_j = 1.$$

Ist $v \in V$, so ist offenbar $q_j(f)(v) \in \tilde{V}_j$. Außerdem gilt $f(\tilde{V}_j) \subseteq \tilde{V}_j$ und deshalb auch $a(f)(\tilde{V}_j) \subseteq \tilde{V}_j$ für jedes Polynom $a \in K[X]$. Insgesamt erhalten wir

$$v = \sum_j a_j(f)(q_j(f)(v)) \in \sum_{j=1}^s \tilde{V}_j.$$

III. $\dim \tilde{V}_i = \mathrm{mult}_{\mu_i}(\mathrm{charpol}_f)$**.** Es gilt $\mathrm{charpol}_f = \prod_i \mathrm{charpol}_{f_{|\tilde{V}_i}}$. Da μ_i der einzige Eigenwert von $f_{|\tilde{V}_i}$ ist, folgt, dass

$$\mathrm{charpol}_{f_{|\tilde{V}_i}} = (X-\mu_i)^{\mathrm{mult}_{\mu_i}(\mathrm{charpol}_f)}$$

und wegen $\deg \mathrm{charpol}_{f_{|\tilde{V}_i}} = \dim \tilde{V}_i$ die Behauptung. □

Definition 3.12. Ein Endomorphismus $f \in \mathrm{End}_K(V)$ heißt *nilpotent*, falls die folgenden äquivalenten Bedingungen erfüllt sind:

(1) Es existiert i, so dass $f^i = 0$.
(2) $f^n = 0$ $(n = \dim V)$,
(3) $\mathrm{charpol}_f = X^n$
(4) $\mathrm{minpol}_f \,|X^n$.
(5) Bezüglich einer geeigneten Basis von V wird f durch eine obere Dreiecksmatrix beschrieben, deren Diagonaleinträge alle $= 0$ sind.

16.5.

Lemma 3.13. *Seien $f_1, f_2 \in \mathrm{End}_K(V)$ Endomorphismen mit $f_1 \circ f_2 = f_2 \circ f_1$.*

(1) *Sind f_1 und f_2 diagonalisierbar, so ist $f_1 + f_2$ diagonalisierbar.*
(2) *Sind f_1 und f_2 nilpotent, so ist $f_1 + f_2$ nilpotent.*

Satz 3.14 (Jordan-Zerlegung)**.** *Sei $f \in \mathrm{End}(V)$ ein Endomorphismus, dessen charakteristisches Polynom vollständig in Linearfaktoren zerfällt. Dann existieren eindeutig bestimmte Endomorphismen D und N von V mit den folgenden Eigenschaften: D ist diagonalisierbar, N ist nilpotent,*

$$f = D + N, \qquad \text{und } DN = ND.$$

Ferner existieren Polynome $p_d, p_n \in K[X]$ mit Absolutterm 0, so dass $D = p_d(f)$, $N = p_n(f)$.

Beweis. Sei $V = \bigoplus_{i=1}^s \tilde{V}_{\mu_i}$ die Zerlegung in verallgemeinerte Eigenräume und $\mathrm{charpol}_f = \prod_{i=1}^s (X-\mu_i)^{n_i}$. Mit dem chinesischen Restsatz finden wir ein Polynom p_d, so dass

$$p_d \equiv \mu_i \mod (X-\mu_i)^{n_i},\ i = 1, \ldots, s, \quad p_d \equiv 0 \mod X.$$

Beachte, dass die letzte Bedingung aus den vorherigen folgt, falls 0 ein Eigenwert von f ist, und dass ansonsten X mit allen $(X-\mu_i)^{n_i}$ teilerfremd ist.

Dann gilt $p_d(f)_{|\tilde{V}_{\mu_i}} = \mu_i \,\mathrm{id}$ für alle i, also ist $D := p_d(f)$ diagonalisierbar. Andererseits sei $p_n := X - p_d$ und $N := p_n(f)$. Dann hat $N_{|\tilde{V}_{\mu_i}}$ nur den Eigenwert 0, ist daher nilpotent, also ist N nilpotent. Offenbar gilt $DN = ND$, da sich D und N als Polynome in f ausdrücken lassen.

Eindeutigkeit. Sei $f = D + N$ die soeben konstruierte Zerlegung und $f = D' + N'$ eine weitere. Wir zeigen $D = D'$, $N = N'$. Auch wenn wir nicht voraussetzen, dass sich D' und N' als Polynome in f schreiben lassen, gilt das, wie wir gesehen haben, für D und N und es folgt, dass f, D, N, D', N' alle miteinander kommutieren. Insbesondere ist in der Gleichung

$$D - D' = N' - N$$

die linke Seite diagonalisierbar und die rechte Seite nilpotent. Es folgt $D - D' = 0 = N' - N$, wie gewünscht. □

Bemerkung 3.15. Um den Satz über die Jordan-Zerlegung ohne die Eindeutigkeitsaussage und ohne die Aussage, dass sich D und N als Polynome in f ausdrücken lassen, zu beweisen, kann man elementarer vorgehen: Man definiere D als die eindeutig bestimmt Abbildung mit $D_{|\tilde{V}_{\mu_i}} = \mu_i \operatorname{id}_{\tilde{V}_{\mu_i}}$ und $N = f - D$. Es lässt sich dann leicht prüfen, dass D diagonalisierbar, N nilpotent und $DN = ND$.

- Wiederhole die äquivalenten Charakterisierungen nilpotenter Endomorphismen aus der Vorlesung und den Übungen. Wiederhole die Definition diagonalisierbarer Endomorphismen aus LA 1. Beispiele? Beispiele nicht nilpotenter Endomorphismen, nicht diagonalisierbarer Endomorphismen?
- Formuliere den Satz über die Jordanzerlegung für Matrizen statt für Endomorphismen. Was ist die Jordanzerlegung einer Matrix in JNF? Beweise die Existenz der Jordanzerlegung als Korollar des Satzes über die JNF.
- Was ist die Jordanzerlegung von

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 5 & -2 \\ 4 & -1 \end{pmatrix} \quad \in M_{2\times 2}(\mathbb{Q})?$$

- Seien $A_1, \dots, A_s$ quadratische obere Dreiecksmatrizen, so dass für alle i alle Diagonaleinträge von A_i gleich sind. Was ist die Jordanzerlegung der Diagonal-Blockmatrix $\operatorname{diag}(A_1, \dots, A_s)$?

18.5.

3.3. **Nilpotente Endomorphismen.**

Lemma 3.16. *Sei $f \in \operatorname{End}_K(V)$ ein nilpotenter Endomorphismus und sei $U = \langle u, f(u), \dots \rangle$ ein zyklischer Unterraum. Dann ist $\dim U = \min\{m; f^m(u) = 0\}$. Ist $u' \in U \setminus f(U)$, so gilt*

$$U = \langle u', f(u'), f^2(u'), \dots \rangle.$$

Satz 3.17 (Normalform für nilpotente Endomorphismen/Matrizen)**.** *Es sei f ein nilpotenter Endomorphismus von V. Dann existieren eine Basis $\mathscr{B}$ von V und natürliche Zahlen $r_1 \geq \dots \geq r_k \geq 1$, so dass*

$$M_{\mathscr{B}}^{\mathscr{B}}(f) = \operatorname{diag}(J_{r_1,0}, \dots, J_{r_k,0}).$$

Eine entsprechende Aussage gilt für nilpotente Matrizen in $M_{n\times n}(K)$.

(Dies ist gerade die Existenzaussage des Satzes über die Jordansche Normalform im speziellen Fall nilpotenter Endomorphismen. Wegen der Eindeutigkeitsaussage im Satz über die Jordansche Normalform, die wir bereits bewiesen haben, sind die r_i eindeutig bestimmt. Wir haben auch bereits gesehen, dass die Anzahl der Jordan-Blöcke gleich der Dimension des Eigenraums von f zum Eigenwert 0, also gleich $\dim \operatorname{Ker} f$ sein muss.)

Beweis. (nach [Vinberg, A Course in Algebra]) Offenbar ist die Aussage des Satzes äquivalent dazu, dass V die direkte Summe von f-zyklischen Unterräumen ist.

Wir zeigen das durch Induktion nach $n = \dim V$. Für $n = 1$ ist nichts zu zeigen, sei also nun $n > 1$. Sei $U \subseteq V$ ein Unterraum der Dimension $n - 1$ mit $\operatorname{Im} f \subseteq U$. Insbesondere gilt $f(U) \subset U$ und nach Induktion zerlegt sich $U = U_1 \oplus \cdots U_\ell$ als direkte Summe f-zyklischer Unterräume.

Sei $v \in V \setminus U$ und schreibe $f(v) = \sum_{i=1}^{\ell} u_i \in U$. Indem wir gegebenenfalls von v geeignete Elemente der U_i abziehen, können wir erreichen, dass für alle i gilt: $u_i = 0$ oder $u_i \notin f(U_i)$.

1. Fall: $f(v) = 0$. Dann ist

$$V = \langle v \rangle \oplus U_1 \oplus \cdots \oplus U_\ell$$

eine Zerlegung in zyklische Unterräume.

2. Fall: $f(v) \neq 0$. Sei m minimal mit der Eigenschaft, dass $f^{m+1}(v) = f^m(f(v)) = 0$. Nach Umnummerieren der U_i (und entsprechend der u_i) können wir annehmen, dass m auch minimal ist mit $f^m(u_1) = 0$. Wegen $f(v) \neq 0$ ist dann $u_1 \neq 0$, nach unserer Vorüberlegung also $u_1 \notin f(U_1)$. Weil U_1 ein f-zyklischer Unterraum ist, folgt daraus $U_1 = \langle u_1, f(u_1), \dots, f^{m-1}(u_1)\rangle$ und $\dim U_1 = m$. Andererseits hat $W := \langle v, f(v), \dots, f^m(v)\rangle$ die Dimension $m+1$.

Behauptung. $V = W \oplus U_2 \oplus \cdots \oplus U_\ell$.

Begründung. Da $\dim V = \dim W + \dim \sum_{i>1} U_i$, genügt es zu zeigen, dass

$$W \cap (U_2 \oplus \cdots \oplus U_\ell) = 0.$$

Nehmen wir also an, dass $a_i \in K$ sind mit

$$\sum_{i=0}^{m} a_i f^i(v) \in U_2 \oplus \cdots \oplus U_\ell.$$

Weil $v \notin U$, muss $a_0 = 0$ sein. Indem wir wieder $f(v) = \sum u_i$ schreiben und ausnutzen, dass $U_1 \cap (U_2 \oplus \cdots \oplus U_\ell) = 0$ ist, erhalten wir

$$\sum_{i=1}^{m} a_i f^i(u_1) = 0,$$

und das impliziert $a_1 = \cdots = a_m = 0$. □

3.4. **Beweis des Satzes über die Jordansche Normalform.** Ist $f \in \mathrm{End}_K(V)$ gegeben, so zerlegen wir $V = \bigoplus \tilde{V}_i$ in die direkte Summe der verallgemeinerten Eigenräume. Wir wählen mit Hilfe von Satz 3.17 Basen der $\tilde{V}_i$, so dass der nilpotente Endomorphismus $f_{|\tilde{V}_i} - \mu_i \,\mathrm{id}_{\tilde{V}_i}$ von $\tilde{V}_i$ durch eine Matrix in Jordanscher Normalform beschrieben wird. Hier bezeichnet μ_i den Eigenwert von f auf $\tilde{V}_i$. Insgesamt erhalten wir so eine Basis von V, bezüglich derer f durch eine Matrix in Jordanscher Normalform beschrieben wird.

Um die Jordansche Normalform eines Endomorphismus (einer Matrix) zu finden, genügt es die Dimensionen $\dim \mathrm{Ker}(f - \lambda \,\mathrm{id})^i$ zu berechnen. Daraus findet man, wie der Eindeutigkeitsbeweis zeigt, die Jordansche Normalform. Oft kann man einen Großteil dieser Berechnungen sparen, wenn man zunächst das charakteristische Polynom und das Minimalpolynom berechnet und in Linearfaktoren zerlegt, weil das gewissen Einschränkungen an die Jordansche Normalform mit sich bringt.

Wesentlich aufwändiger ist es in der Regel, eine Basis von V zu finden, bezüglich derer ein gegebenener Endomorphismus sich durch eine Matrix in Jordanscher Normalform beschreiben lässt. Dazu muss man geeignete Basen der verallgemeinerten Eigenräume bestimmen, die jeweils eine Zerlegung des verallgemeinerten Eigenraums in zyklische Unterräume bezüglich des nilpotenten Anteils beschreiben.

3.5. **Die rationale Normalform.** Wir beschließen das Kapitel über die Jordansche Normalform mit dem folgenden Satz, der auch ohne die Trigonalisierbarkeitsvoraussetzung gilt und insbesondere zeigt, dass jeder Endomorphismus, dessen Minimalpolynom vollständig in Linearfaktoren zerfällt, trigonalisierbar ist.

Satz 3.18. *Sei $f \in \mathrm{End}_K(V)$, und sei $p \in K[X]$ ein irreduzibles Polynom, das* $\mathrm{charpol}_f$ *teilt. Dann ist p ein Teiler von* minpol_f.

Beweis. Weil sich der Beweis mit Hilfe des Begriffs des Quotientenvektorraums übersichtlicher formulieren lässt, benutzen wir diese Konstruktion hier. Vergleiche die Hausaufgaben 2 und 3 auf Blatt 8.

Beweis durch Induktion nach $\dim V$. Ist $\dim V = 1$, so ist notwendigerweise $\operatorname{charpol}_f = \operatorname{minpol}_f$. Seien nun $\dim V > 1$, $v \in V \setminus \{0\}$, $U = \langle v, f(v), f^2(v), \dots \rangle$, sei $g = f_{|U} \in \operatorname{End}_K(U)$ und sei $h \in \operatorname{End}_K(V/U)$ der von f induzierte Endomorphismus auf V/U.

Dann gilt $\operatorname{charpol}_f = \operatorname{charpol}_g \operatorname{charpol}_h$, also gilt $p | \operatorname{charpol}_g$ oder $p | \operatorname{charpol}_h$. Im ersten Fall folgt direkt der Satz: Weil U ein f-zyklischer Untervektorraum ist, ist nämlich $\operatorname{charpol}_g = \operatorname{minpol}_g$, und weil $\operatorname{minpol}_f(g) = 0$, gilt $\operatorname{minpol}_g \mid \operatorname{minpol}_f$.

Wenn $p | \operatorname{charpol}_h$, so folgt mit Induktionsvoraussetzung, dass $p | \operatorname{minpol}_h$, und wieder gilt $\operatorname{minpol}_f(h) = 0$, also $\operatorname{minpol}_h \mid \operatorname{minpol}_f$. □

Korollar 3.19. *Sei $f \in \operatorname{End}_K(V)$. Dann gilt: f ist genau dann trigonalisierbar, wenn minpol_f vollständig in Linearfaktoren zerfällt, und f ist genau dann diagonalisierbar, wenn minpol_f vollständig in Linearfaktoren zerfällt und nur einfache Nullstellen besitzt.*

Darüberhinaus gilt das folgende Theorem, das eine Normalform für Endomorphismen angibt, ohne dass man die Trigonalisierbarkeit annehmen muss.

Theorem 3.20 (Rationale Normalform)**.** *Sei $f \in \operatorname{End}_K(V)$, und sei*

$$\operatorname{charpol}_f = \prod_{i=1}^{s} p_i^{n_i}$$

die Zerlegung in ein Produkt irreduzibler normierter Polynome ($p_i \in K[X]$ paarweise verschieden). Dann existieren für jedes $i \in \{1, \dots, s\}$ natürliche Zahlen $r_{i,1} \geq r_{i,2} \geq \cdots$ mit $\sum_j r_{i,j} = n_i$ und eine Basis $\mathscr{B}$ von V, so dass

$$M_{\mathscr{B}}^{\mathscr{B}}(f) = \operatorname{diag}(A_1, \dots, A_s)$$

eine Diagonal-Blockmatrix ist, und für jedes i die Matrix $A_i \in M_{N_i \times N_i}$, $N_i := n_i \deg p_i$, selbst eine Diagonal-Blockmatrix ist, die zusammengesetzt ist aus den Begleitmatrizen der Polynome $p_i^{r_{i,1}}$, $p_i^{r_{i,2}}$, ... Dabei sind die p_i als die irreduziblen Teiler von $\operatorname{charpol}_f$ bis auf ihre Reihenfolge und die Zahlen $r_{i,j}$ eindeutig bestimmt.

Für alle i ist p_i ein Teiler von minpol_f, und $p_i^{r_{i,1}}$ ist die maximale Potenz von p_i, die minpol_f teilt.

- Was ist die JNF der Matrix $A = (a_{ij}) \in M_{n \times n}(K)$ mit $a_{ij} = 0$ für $i \geq j$, $a_{ij} = 1$ für $i < j$?
- Prüfe, dass die Matrix

$$A = \begin{pmatrix} 4 & -4 & 2 \\ 6 & -6 & 3 \\ 4 & -4 & 2 \end{pmatrix} \in M_{3\times 3}(\mathbb{Q})$$

nilpotent ist und finde eine Zerlegung von $\mathbb{Q}^3$ in zyklische Unterräume bezüglich des zugehörigen Endomorphismus. Löse diese Aufgabe auf verschiedene Art und Weise: Einerseits durch "Anwendung" des Beweises von Satz 3.17 in dieser Situation, andererseits durch Betrachtung der Filtrierung

$$0 \subseteq \operatorname{Ker} A \subseteq \operatorname{Ker} A^2 \subseteq \mathbb{Q}^3.$$

Erstelle weitere Aufgaben dieses Typs, in denen die gegebene Matrix teils denselben Jordantyp wie A, teils einen anderen Jordantyp hat.

• Was bedeutet es für einen nilpotenten Endomorphismus $f \in \mathrm{End}_K(V)$, dass alle Jordanblöcke in der JNF von f Größe 1 haben? Versuche ein Kriterium anzugeben, das dazu äquivalent ist, dass alle Jordanblöcke von f dieselbe Größe haben. Versuche ein Kriterium dafür zu geben, das dazu äquivalent ist, dass keine zwei Jordanblöcke derselben Größe existieren. Versuche ein Kriterium dafür zu geben, dass nur ein einzige Jordanblock existiert.
• Sei $f \in \mathrm{End}_K(V)$ ein nilpotenter Endomorphismus, und seien $r_1 \geq r_2 \geq \cdots$ die Größen der Jordanblöcke von f. Zeige, dass $\mathrm{Ker}\, f^{r_1} = 0$. Sei $g_i = f_{|\,\mathrm{Ker}\, f^{r_i}}$. Welche Größen haben die Jordanblöcke in der JNF von $g_i \in \mathrm{End}_K(\mathrm{Ker}\, f^{r_i})$?
Sei W ein Komplementärraum von $\mathrm{Ker}\, f^{r_1-1}$, und sei $w \in W \setminus \{0\}$. Zeige, dass der Untervektorraum $\langle w, f(w), f^2(w), \dots \rangle$ Dimension r_1 hat.
Sei $\mathscr{B} = (b_1, \dots, b_n)$ eine Basis bezüglich derer f JNF hat. Zeige, dass genau r_1 der Basisvektoren nicht in $\mathrm{Ker}\, f^{r_1-1}$ liegen.
• Sei f ein nilpotenter Endomorphismus von V und $v \in V$ mit $V = \langle v, f(v), f^2(v), \dots \rangle$. Zeige, dass $v \notin \mathrm{Im}\, f$. Gilt diese Aussage auch, wenn f nicht nilpotent ist?
• Sei $A \in M_{2\times 2}(\mathbb{R})$ eine Drehung. Wann ist A konjugiert zu einer Matrix in JNF? Finde die rationale Normalform von A. Finde die JNF von A, aufgefasst als Element von $M_{2\times 2}(\mathbb{C})$.
• Welche Drehungen von $\mathbb{R}^3$ besitzen eine JNF? Welche JNF kommen vor?
• Sei $f \in \mathrm{End}_K(V)$ ein Endomorphismus mit $f^2 = 3\,\mathrm{id}_V$. Wann besitzt f eine JNF? Falls ja: welche JNF kann f haben? Finde und diskutiere ähnliche Aufgaben dieses Typs.

4. Konstruktionen von Vektorräumen

23.5.

Sei K ein Körper. Alle in diesem Kapitel betrachteten Vektorräume sind Vektorräume über K.

Sprechweise: Kommutatives Diagramm. Ein "Diagramm" von Abbildungen (von Vektorräumen, Gruppen, Mengen, ...) heißt *kommutativ*, wenn für je zwei Objekte in dem Diagramm alle Verkettungen entlang verschiedener Wege vom ersten zum zweiten Objekt dieselbe Abbildung beschreiben. Zum Beispiel sind die folgenden beiden Diagramme

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle t} \\ C & \xrightarrow{g} & D \end{array} \qquad\qquad \begin{array}{ccc} A & & \xrightarrow{f} \quad B \\ & {\scriptstyle h}\searrow \quad \swarrow{\scriptstyle g} & \\ & C & \end{array}$$

genau dann kommutativ, wenn $t \circ f = g \circ s$ bzw. $g \circ f = h$.

4.1. **Produkt, direkte Summe von VR.** Sei I eine Menge ("Indexmenge"), und sei für jedes $i \in I$ ein Vektorraum V_i gegeben.

Erinnerung: Das Produkt $\prod_{i\in I} V_i$ ist definiert als die Menge aller Familien $(v_i)_{i\in I}$, $v_i \in V_i$.

Definition 4.1. (1) Das Produkt $\prod_{i\in I} V_i$ ist zusammen mit komponentenweiser Addition und Skalarmultiplikation ein Vektorraum und heißt das *Produkt der Vektorräume* V_i.

(2) Die Menge

$$\coprod_{i\in I} V_i := \{(v_i)_i \in \prod_{i\in I} V_i;\ v_i = 0 \text{ für alle bis auf endlich viele} i\}$$

ist ein Untervektorraum von $\prod_{i\in I} V_i$ und heißt das *Koprodukt* oder die *(äußere) direkte Summe der* V_i.

Ist $I = \{1, \dots n\}$, so schreiben wir auch $\prod_{i=1}^n V_i$ oder $V_1 \times \cdots \times V_n$ statt $\prod_{i\in I} V_i$.

Satz 4.2 (Universelle Eigenschaft des Produkts)**.** (1) *Mit den obigen Notationen sei* $V := \prod_{i\in I} V_i$*. Die* Projektionen $\pi_i\colon V \to V_i$, $(v_i)_i \mapsto v_i$, *sind Vektorraumhomomorphismen.*

(2) *Sei* W *ein Vektorraum zusammen mit Homomorphismen* $p_i\colon W \to V_i$*. Dann gibt es genau einen Homomorphismus* $\varphi\colon W \to V$*, so dass für alle* $i \in I$*:* $p_i = \pi_i \circ \varphi$*.*

(3) *Sei* V' *ein Vektorraum zusammen mit Homomorphismen* $\pi'_i\colon V' \to V_i$*, der auch die Eigenschaft in (2) hat. Dann gibt es einen eindeutig bestimmten Isomorphismus* $\varphi\colon V \to V'$*, so dass für alle* i*:* $\pi_i = \pi'_i \circ \varphi$*.*

Satz 4.3 (Universelle Eigenschaft des Koprodukts)**.** (1) *Mit den obigen Notationen sei* $V := \coprod_{i\in I} V_i$*. Die Inklusionen* $\iota_i\colon V_i \to V$, $v \mapsto (\dots, 0, v, 0, \dots)$ *(v steht an der Stelle I) sind Homomorphismen.*

(2) *Sei* W *ein Vektorraum zusammen mit Homomorphismen* $f_i\colon V_i \to W$*. Dann gibt es genau einen Homomorphismus* $\varphi\colon \coprod_{i\in I} V_i \to W$*, so dass für alle* $i \in I$*:* $f_i = \varphi \circ \iota_i$*.*

(3) *Sei* V' *ein Vektorraum zusammen mit Homomorphismen* $\iota'_i\colon V_i \to V'$*, der auch die Eigenschaft in (2) hat. Dann gibt es einen eindeutig bestimmten Isomorphismus* $\varphi\colon V \to V'$*, so dass für alle* i*:* $\iota'_i = \varphi \circ \iota_i$*.*

Definition 4.4. Seien I eine Menge, V ein K-Vektorraum, und seien $V_i \subseteq V$, $i \in I$, Untervektorräume. Wir sagen, V sei die *(innere) direkte Summe* der Untervektorräume V_i, wenn gilt

(1) Für jedes $v \in V$ gibt es $n \geq 0$, $i_1, \dots, i_n \in I$ und $v_1 \in V_{i_1}, \dots, v_n \in V_{i_n}$ mit $v = \sum_{j=1}^n v_j$.

(2) Sind $n \geq 0$, $i_1, \dots, i_n \in I$ paarweise verschieden und $v_1 \in V_{i_1}, \dots, v_n \in V_{i_n}$ mit $\sum_{j=1}^n v_j = 0$, so gilt $v_1 = 0, \dots, v_n = 0$.

Notation: $V = \bigoplus_{i\in I} V_i$.

Wegen des folgenden Satzes macht man in der Regel keinen großen Unterschied zwischen Koprodukt und innerer direkter Summe von Vektorräumen (und bezeichnet oft auch das Koprodukt mit $\bigoplus$).

Satz 4.5. (1) *Seien* V_i, $i \in I$ *Vektorräume. Sei* ι_i *die Inklusion* $V_i \to \coprod_I V_i$*. Dann ist* $\coprod_{i\in I} V_i = \bigoplus_{i\in I} \iota_i(V_i)$*.*

(2) *Sei* V *ein Vektorraum,* V_i, $i \in I$*, Untervektorräume von* V *mit* $V = \bigoplus V_i$*. Bezeichne mit* ι_i *die Inklusion* $V_i \to \coprod_{i\in I} V_i$*. Dann gibt es einen eindeutig bestimmten Isomorphismus* $\varphi\colon \coprod_{i\in I} V_i \to V$*, so dass für alle* i *und* $v \in V_i$*:* $\varphi(\iota_i(v)) = v$*.*

- Vergleiche die Definition des Produktes mit den Definitionen von K^n, V^n, $V_1 \times V_2$, $\mathrm{Abb}(M, K)$ (M eine Menge) aus der LA 1. Vergleiche die Definition der inneren direkten Summe mit dem in LA 1 eingeführten Begriff der direkten Summe.
- Sei I eine Menge, V ein Vektorraum und setze $V_i := V$ für alle i. Welcher Homomorphismus $\coprod_I V \to V$ korrespondiert im Sinne der universellen Eigenschaft des Koprodukts zu den Abbildungen id_V (für alle i)?

• Diskutiere an Beispielen, dass (für unendliches I) das Produkt nicht die universelle Eigenschaft des Koproduktes, und das Koprodukt nicht die universelle Eigenschaft des Produkts hat.
• Sei V ein VR. Begründe, warum die Wahl einer Basis (mit Indexmenge I) dasselbe ist wie die Wahl eines Isomorphismus $V \cong \bigoplus_{i\in I} K$.
• Seien I eine Menge, V_i, $i \in I$, Vektorräume. Zeige, dass für jeden VR W gilt:

$$\mathrm{Hom}_K(\coprod_{i\in I} V_i, W) = \prod_{i\in I} \mathrm{Hom}(V_i, W)$$

(was ist hier mit = gemeint?). Zeige, dass die obige Aussage eine Umformulierung der universelles Eigenschaft des Koprodukts ist. Handelt es sich sogar um einen Isomorphismus von Vektorräumen?

Formuliere und löse eine analoge Aufgabe für das Produkt.

25.5.

4.2. **Quotientenvektorraum.** Sei V ein K-Vektorraum, und sei $U \subseteq V$ ein Untervektorraum. Betrachte auf V die folgende Äquivalenzrelation:

$$v \sim w \quad :\Longleftrightarrow \quad v - w \in U.$$

Wir bezeichnen die Menge der Äquivalenzklassen mit V/U.

Die Äquivalenzklasse von $v \in V$ bezüglich dieser Äquivalenzrelation ist die Menge

$$v + U = \{v + u;\ u \in U\}.$$

In diesem Fall nennt man die Äquivalenzklassen oft *Nebenklassen (von U).*

Wir machen V/U zu einem K-Vektorraum, indem wir Addition und Skalarmultiplikation definieren durch

$$(v + U) + (w + U) := (v + w) + U, \quad \alpha(v + U) := (\alpha v + U), \qquad v, w \in V,\ \alpha \in K.$$

Diese Verknüpfungen sind *wohldefiniert*!

Die Abbildung $\pi\colon V \to V/U$, $v \mapsto v + U$, ist ein surjektiver Vektorraumhomomorphismus und wird als die *kanonische Projektion* oder *Quotientenabbildung* bezeichnet. Der Vektorraum V/U zusammen mit der kanonischen Projektion π heißt der *Quotientenvektorraum* oder einfach der Quotient von V nach U.

Der Kern der kanonischen Projektion $\pi\colon V \to V/U$ ist $\operatorname{Ker}\pi = U$.

Wie der folgende Satz zeigt, lässt sich auch der Quotientenvektorraum durch eine universelle Eigenschaft beschreiben. Wie im Fall von Produkt und Koprodukt charakterisiert die universelle Eigenschaft den Quotientenvektorraum (zusammen mit der kanonischen Projektion) eindeutig bis auf eindeutigen Isomorphismus. Zusammen mit der Präzisierung in Teil (2) wird der Satz oft als Homomorphiesatz bezeichnet.

Satz 4.6. (1) *(Universelle Eigenschaft des Quotienten) Sei W ein K-Vektorraum und $p\colon V \to W$ ein Homomorphismus. Wenn $U \subseteq \operatorname{Ker} p$, dann existiert ein eindeutig bestimmter Homomorphismus $f\colon V/U \to W$ mit $f \circ \pi = p$.*

(2) *Existiert f mit $f \circ \pi = p$, so folgt $U \subseteq \operatorname{Ker} p$. Sind p mit $U \subseteq \operatorname{Ker} p$ und f wie in (1), so gilt: $\operatorname{Im} f = \operatorname{Im} p$. Die Abbildung f ist genau dann injektiv wenn $U = \operatorname{Ker} p$, genauer gilt stets $\operatorname{Ker} f = \operatorname{Ker} p/U$.*

30.5.

Korollar 4.7. *Sei $f\colon V \to W$ ein Vektorraumhomomorphismus, $\pi\colon V \to V/\operatorname{Ker} f$ die kanonische Projektion, $\iota\colon \operatorname{Im} f \to W$ die Inklusion. Dann faktorisiert f eindeutig als $f = \iota \circ g \circ \pi$ mit einem Isomorphismus $g\colon V/\operatorname{Ker} f \to \operatorname{Im} f$.*

Bemerkung 4.8. Sei $f \in \mathrm{End}_K(V)$ und sei $U \subseteq V$ ein f-invarianter Untervektorraum. Dann induziert f einen Homomorphismus $V/U \to V/U$, $v + U \mapsto f(v) + U$.

Satz 4.9. *Sei V endlich-dimensional, $U \subseteq V$ ein Untervektorraum. Dann ist* $\dim U + \dim V/U = \dim V$.

- Wiederhole die Definition des Begriffs *Äquivalenzrelation*. Überprüfe, dass die oben betrachtete Relation $\sim$ (für $U \subseteq V$) tatsächlich eine Äquivalenzrelation ist.
- Wähle einen eindimensionalen Untervektorraum U von $\mathbb{R}^2$ und veranschauliche die Äquivalenzklassen $v + U$ geometrisch.
- Was ist $V/\{0\}$? Was ist V/V Was ist $(U_1 \oplus U_2)/U_2$?
- Begründe anhand der universellen Eigenschaft des Quotienten, dass die kanonische Projektion $V \to V/U$ surjektiv ist.
- Sei $f \in \mathrm{End}_K(V)$ und sei $U \subseteq V$ ein f-invarianter Untervektorraum. Sei $\mathscr{B} = (b_1, \dots, b_n)$ eine Basis von V, die durch Ergänzen einer Basis $(b_1, \dots, b_d)$ von U entsteht. Was bedeutet es für die Form von $A := M^{\mathscr{B}}_{\mathscr{B}}$, dass $f(U) \subseteq U$? Zeige, dass unter der kanonischen Projektion π die Vektoren $b_{d+1}, \dots, b_n$ auf eine Basis von V/U abgebildet werden. Was ist die Matrix, die den von f induzierten Endomorphismus $V/U \to V/U$ bezüglich dieser Basis beschreibt?
- Begründe, dass Satz 4.9 auch ohne die Voraussetzung, dass V endlich-dimensional ist, als korrekt angesehen werden kann.
- Wann gibt es einen nichttrivialen VR-Homomorphismus $\prod_{i\in I} K / \coprod_{i\in I} K \to K$? Kann man einen solchen explizit angeben?

4.3. **Quotienten abelscher Gruppen.** Sei G eine Gruppe (wir schreiben die Verknüpfung als $\cdot$) und $H \subseteq G$ eine Untergruppe. Für $x, y \in G$ sei $x \sim y :\Leftrightarrow y^{-1}x \in H$. Dies ist eine Äquivalenzrelation und wir bezeichnen mit G/H die Menge der Äquivalenzklassen (*H-Linksnebenklassen*). Die Nebenklasse von $x \in G$ ist

$$xH = \{xh;\ h \in H\}.$$

(Schreibt man G additiv, so wird die Nebenklasse mit $x + H$ bezeichnet. Analog zu Linksnebenklassen kann man von Rechtsnebenklassen sprechen. Ist G kommutativ, so muss man nicht zwischen der Linksnebenklasse xH und der Rechtsnebenklasse Hx unterscheiden.)

Weil G die disjunkte Vereinigung der H-Nebenklassen ist (wie bei jeder Äquivalenzrelation), erhalten wir im endlichen Fall den

Satz 4.10 (Euler-Lagrange)**.** *Sei G eine endliche (kommutative) Gruppe, $H \subseteq G$ eine Untergruppe und $[G : H] := \#(G/H)$ die Anzahl der Äquivalenzklassen in G bezüglich der oben definierten Äquivalenzrelation. Dann gilt*

$$\#G = \#H \cdot [G : H].$$

Insbesondere gilt $\#H | \#G$.

Lemma 4.11. *Sei G eine (multiplikativ geschriebene) endliche Gruppe mit n Elementen und neutralem Element e, und sei $g \in G$. Dann gilt $g^n = e$.*

Sei nun G abelsch. Mit der Verknüpfung

$$(xH) + (yH) := (xy) + H$$

ist G/H eine abelsche Gruppe. Die kanonische Abbildung $\pi\colon G \to G/H$, die jedem $x \in G$ seine Äquivalenzklasse zuordnet, ist ein surjektiver Gruppenhomomorphismus und heißt die *kanonische Projektion*. Analog zum Vektorraumfall haben wir.

Satz 4.12. (1) *(Universelle Eigenschaft des Quotienten) Sei T eine abelsche Gruppe und $p\colon G \to T$ ein Gruppenhomomorphismus mit $H \subseteq \operatorname{Ker} p$. Dann existiert ein Gruppenhomomorphismus $f\colon G/H \to T$ mit $f \circ \pi = p$.*

(2) *(Homomorphiesatz) Sei T eine abelsche Gruppe und $p\colon G \to T$ ein Gruppenhomomorphismus. Es existiert ein Gruppenhomomorphismus $f\colon G/H \to T$ mit $f \circ \pi = p$ genau dann, wenn $H \subseteq \operatorname{Ker} p$. In diesem Fall ist f eindeutig bestimmt und es gilt $\operatorname{Im} f = \operatorname{Im} p$, und die Abbildung f ist genau dann injektiv wenn $H = \operatorname{Ker} p$.*

- Sei G eine (multiplikativ geschriebene, nicht notwendig kommutative) Gruppe und $H \subseteq G$ eine Untergruppe. Zeige, dass durch $x \sim y :\Leftrightarrow xy^{-1} \in H$ eine Äquivalenzrelation definiert wird.
- Zeige am Beispiel $G = GL_2(K)$, $B \subset G$ die Untergruppe der oberen Dreiecksmatrizen, dass man die obige Definition nicht einfach auf den nichtkommutativen Fall übertragen kann, weil es keine wohldefinierte Multiplikation auf der Menge der B-Nebenklassen gibt.
- Vollziehe den Satz von Euler-Lagrange in konkreten Beispielen nach. (Zum Beispiel: K ein endlicher Körper, $G = GL_n(K)$, B die Untergruppe der oberen Dreiecksmatrizen.)

1.6.

4.4. **Quotienten von Ringen nach Idealen.** Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Für $x, y \in R$ definiere $x \sim y :\Leftrightarrow x - y \in I$. Dies ist eine Äquivalenzrelation, wir nennen die Äquivalenzklassen auch als I-Nebenklassen und bezeichnen die Menge aller I-Nebenklassen mit R/I. Die Nebenklasse von $x \in R$ ist

$$x + I = \{x + y;\ y \in I\}.$$

Mit den Verknüpfungen

$$(x + I) + (y + I) := (x + y) + I, \quad (x + I) \cdot (y + I) := (xy) + I, \qquad x, y \in R$$

ist R ein kommutativer Ring mit Einselement $1 + I$. Er wird als *Restklassenring* oder *Quotient* von R modulo I bezeichnet.

Beispiel 4.13. (1) $R = \mathbb{Z}$ der Ring der ganzen Zahlen, $m \in \mathbb{Z}$. Das Rechnen im Restklassenring $\mathbb{Z}/(m)$ ist gerade das Rechnen modulo (Division mit Rest durch) m.

(2) Der Restklassenring $\mathbb{Q}[X]/(X^2 - 2)$ ist isomorph zum Körper $\mathbb{Q}(\sqrt{2})$.

Satz 4.14. (1) *(Universelle Eigenschaft des Quotienten) Sei T ein kommutativer Ring und $p\colon R \to T$ ein Ringhomomorphismus mit $I \subseteq \operatorname{Ker} p$. Dann existiert ein Ringhomomorphismus $f\colon R/I \to T$ mit $f \circ \pi = p$.*

(2) *(Homomorphiesatz) Sei T ein kommutativer Ring und sei $p\colon R \to T$ ein Ringhomomorphismus. Es existiert genau dann ein Ringhomomorphismus $f\colon R/I \to T$ mit $f \circ \pi = p$, wenn $I \subseteq \operatorname{Ker} p$. In diesem Fall ist f eindeutig bestimmt und es gilt: $\operatorname{Im} f = \operatorname{Im} p$. Die Abbildung f ist genau dann injektiv wenn $I = \operatorname{Ker} p$.*

- Sei $R = \mathbb{Q}$ der Ring der rationalen Zahlen. Kann man, analog zum Quotienten nach Idealen, den Quotient von $\mathbb{Q}$ nach dem Unterring $\mathbb{Z}$ definieren?
- Vergleiche die Konstruktion des Restklassenrings $\mathbb{Z}/(m)$ mit der Konstruktion in der Übungsaufgabe aus Blatt 3, LA 1.
- Vergleiche die Konstruktionen von Quotienten von Vektorräumen, abelschen Gruppen und kommutativen Ringen. Begründe, dass man in jedem Fall gerade nach *Kernen* von Morphismen den Quotienten bilden kann. Schwieriger: Versuche geeignete Quotientenkonstruktionen im Fall nichtkommutativer Gruppen und nichtkommutativer Ringe zu finden.

4.5. **Das RSA-Verfahren.**

Satz 4.15 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl, und $a \in \mathbb{Z}$. Dann gilt*

$$a^p \equiv a \mod p.$$

Wenn p die Zahl a nicht teilt, so gilt

$$a^{p-1} \equiv 1 \mod p.$$

Seien p, q verschiedene (in der Praxis: große) Primzahlen, sei $N := pq$ und sei e eine Zahl, die teilerfremd ist zu $(p-1)(q-1)$, und sei $d \in \mathbb{Z}$ mit

$$de \equiv 1 \mod (p-1)(q-1).$$

Lemma 4.16. *Mit den obigen Notationen gilt für alle $a \in \mathbb{Z}$:*

$$a^{de} \equiv a \mod N.$$

Das RSA-Verfahren (entwickelt 1977 von Rivest, Shamir und Adleman) ist ein "public key" Verschlüsselungsverfahren, das den Austausch geheimer Nachrichten über nicht abhörsichere Kanäle *ohne* den vorherigen Austausch eines geheimen Schlüssels ermöglicht. Dazu veröffentlicht der spätere Empfänger der Nachricht seinen *öffentlichen Schlüssel*, der dann allgemein bekannt ist, und zum Verschlüsseln von Nachrichten verwendet werden kann. Das Entschlüsseln ist aber nur mit zusätzlichen Informationen möglich, die sich zwar im Prinzip aus dem öffentlichen Schlüssel gewinnen lassen, aber nicht mit akzeptablem Rechenaufwand (d.h. mit heute bekannten Verfahren wüde es Jahre dauern, diese Berechnungen durchzuführen). Der hohe Rechenaufwand resultiert beim RSA-Verfahren daraus, das kein schnelles Verfahren bekannt ist, die Primteiler p und q von N zu bestimmen, wenn nur N gegeben ist und p und q sehr groß sind.

Öffentlicher Schlüssel. Der öffentliche Schlüssel besteht aus N und e.

Verschlüsselung. Der Sender der Nachricht beschreibt seine Nachricht durch natürliche Zahlen $K < N$ und schickt dem Empfänger die kodierte Nachricht $C := K^e \mod N$.

Entschlüsselung. Der Empfänger kennt nicht nur N und e, sondern auch p und q, also auch $(p-1)(q-1)$, und kann damit recht schnell eine Zahl d mit $de \equiv 1 \mod (p-1)(q-1)$ berechnen. Nach Erhalt der kodierten Nachricht C berechnet er C^d und erhält

$$C^d \equiv K^{ed} \equiv K \mod N$$

zurück.

Varianten des Verfahrens kann man statt zur Verschlüsselung auch zum *Signieren* von Nachrichten einsetzen (d.h. um zu Belegen, dass die Nachricht tatsächlich vom Absender kommt und nicht unterwegs verändert wurde).

- Zeige an einem Beispiel, dass man auf die Voraussetzung, dass p prim ist, im kleinen Satz von Fermat nicht verzichten kann.
- Vollziehe das Verfahren an einem konkreten Beispiel nach.

6.6.

4.6. **Der Dualraum.**

Definition 4.17. (1) Sei K ein Körper, V ein Vektorraum. Dann heißt der Vektorraum $V^\vee := \mathrm{Hom}(V, K)$ der *Dualraum* von V.

(2) Sei $f\colon V \to W$ ein Vektorraumhomomorphismus. Dann heißt der Vektorraumhomomorphismus

$$f^\vee\colon W^\vee \to V^\vee, \quad \lambda \mapsto \lambda \circ f,$$

die zu f *duale Abbildung.*

Bemerkung 4.18. (1) Es gilt $(\mathrm{id}_V)^\vee = \mathrm{id}_{V^\vee}$ und $(f \circ g)^\vee = g^\vee \circ f^\vee$. (Man sagt, das Bilden des Dualraums und der dualen Abbildung sei ein *kontravarianter Funktor.*)

(2) $(K^n)^\vee = \mathrm{Hom}(K^n, K) = M_{1\times n}(K)$.

(3) Aus den beiden vorherigen Punkten folgt insbesondere: Ist $\dim V = n < \infty$, so ist $\dim V^\vee = n$.

Lemma 4.19. *Sei $f\colon V \to W$ ein Vektorraumhomomorphismus und $f^\vee\colon W^\vee \to V^\vee$ die duale Abbildung.*

(1) *[Seien V und W endlich-dimensional.[1]] Ist f injektiv, so ist $f^\vee$ surjektiv.*

(2) *Ist f surjektiv, so ist $f^\vee$ injektiv.*

Man kann das Lemma in der folgenden Form verallgemeinern:

Satz 4.20. *Seien V, W [endlich-dimensionale] K-Vektorräume und $f\colon V \to W$ eine lineare Abbildung. Seien $V^\vee$, $W^\vee$ die Dualräume von V und W und sei $f^\vee$ die zu f duale Abbildung.*

(1) *Sei $\iota^\vee\colon V^\vee \to (\mathrm{Ker}\, f)^\vee$ die zur Inklusion $\iota\colon \mathrm{Ker}\, f \to V$ duale Abbildung. Dann faktorisiert $\iota^\vee$ über einen Isomorphismus*

$$V^\vee/f^\vee(W^\vee) \xrightarrow{\sim} (\mathrm{Ker}\, f)^\vee.$$

(2) *Sei $\pi^\vee\colon (W/f(V))^\vee \to W^\vee$ die zur kanonischen Projektion $\pi\colon W \to W/f(V)$ duale Abbildung. Dann ist $\pi^\vee$ injektiv und identifiziert*

$$(W/f(V))^\vee = \mathrm{Ker}(f^\vee)$$

als Teilmengen von $W^\vee$.

Insbesondere gilt $\mathrm{rg}\, f = \mathrm{rg}\, f^\vee$.

8.6.

Lemma 4.21. *Sei V ein Vektorraum. Dann existiert eine natürliche Abbildung*

$$V \to V^{\vee\vee} := (V^\vee)^\vee, \quad v \mapsto (V^\vee \to K,\ \lambda \mapsto \lambda(v)).$$

Diese Abbildung ist ein injektiver Vektoraumhomomorphismus, [sofern V endlich-dimensional ist].

Satz 4.22. *Sei V ein endlich-dimensionaler Vektorraum. Ist $\mathscr{B} = (b_1, \ldots, b_n)$ eine Basis von V, so definiere $b_i^\vee \in V^\vee$ durch*

$$b_i^\vee\colon V \to K,\ v = \sum_{j=1}^{n} a_j b_j \mapsto a_i$$

[1] Hier benutzen wir, dass $f(V) \subseteq W$ einen Komplementärraum besitzt, d.h. letztlich den Basisergänzungssatz, den wir in der LA 1 nur für den Fall bewiesen haben, dass W endlich erzeugt ist.

(also $b_i^\vee(b_j) = \delta_{ij}$ (Kronecker-Symbol)). Dann ist $b_1^\vee, \dots, b_n^\vee$ eine Basis von $V^\vee$, die sogenannte duale Basis zur Basis $\mathscr{B}$. Insbesondere gilt $\dim V = \dim V^\vee$, und die Wahl der Basis $\mathscr{B}$ liefert einen Isomorphismus $V \to V^\vee$, $b_i \mapsto b_i^\vee$.

Die beiden vorhergehenden Sätze liefern einen neuen Beweis dafür, dass der Spaltenrang und der Zeilenrang jeder Matrix übereinstimmen. Dieser Beweis kommt ganz ohne Rechnungen mit Matrizen aus.

Korollar 4.23. *Sei V ein endlich-dimensionaler Vektorraum. Die natürliche Abbildung $V \to V^{\vee\vee}$ ist ein Isomorphismus.*

Satz 4.24. *Seien V, W endlich-dimensionale Vektorräume mit Basen $\mathscr{B}$, $\mathscr{C}$ und sei $f\colon V \to W$ ein Homomorphismus. Seien $\mathscr{B}^\vee$, $\mathscr{C}^\vee$ die dualen Basen von $V^\vee$, $W^\vee$, und sei $f^\vee$ die zu f duale Abbildung. Dann gilt*

$$M_{\mathscr{B}^\vee}^{\mathscr{C}^\vee}(f^\vee) = M_{\mathscr{C}}^{\mathscr{B}}(f)^t,$$

wobei A^t die transponierte Matrix einer Matrix A bezeichnet.

- Überprüfe die Richtigkeit von Bemerkung 4.18.
- Zeige, dass für jeden K-VR V der K-VR $\mathrm{Hom}(K, V)$ "kanonisch" isomorph zu V ist. (Deshalb ist es nicht besonders interessant, diesen VR zu betrachten; er unterscheidet sich nicht von V.)
- Sei W ein K-VR. Welche der Definitionen und Ergebnisse lassen sich auf die Zuordnung $V \mapsto \mathrm{Hom}_K(V, W)$ übertragen?
- Überprüfe, dass die duale Basis der Standardbasis von K^n gerade die "Standardbasis" von $M_{n\times 1}(K)$ ist.
- Belege anhand eines Beispiels, dass der in Satz 4.22 konstruierte Isomorphismus $V \to V^\vee$ abhängig von der Wahl der Basis $\mathscr{B}$ ist.
- Sei V ein endlich-dimensionaler Vektorraum mit Basis $\mathscr{B}$. Wende die Konstruktion von Satz 4.22 auf V und $\mathscr{B}$, und dann auf den Dualraum $V^\vee$ und die duale Basis $\mathscr{B}^\vee$ an. Ist die Verkettung der so erhaltenen Isomorphismen $V \to V^\vee$, $V^\vee \to V^{\vee\vee}$ die natürliche Abbildung $V \to V^{\vee\vee}$?
- Sei $V = \bigoplus_{i\in\mathbb{N}} K$. Zeige, dass die natürliche Abbildung $V \to V^{\vee\vee}$ injektiv, aber nicht surjektiv ist.

5. Bilinearformen, euklidische und unitäre Vekorräume

Referenz: [Bosch, Lineare Algebra, Kapitel 7].

Motivation: Länge von Vektoren, Abstand, Winkel zwischen zwei Vektoren in $\mathbb{R}^2$, $\mathbb{R}^n$. Nullstellenmengen quadratischer Formen, Kegelschnitte, Hauptachsentransformation. (Siehe auch die Einleitung zu Kapitel 7 in [Bosch, Lineare Algebra], und [Fischer, Lernbuch Lineare Algebra und Analytische Geometrie].)

Alle in diesem Kapitel auftretenden Vektorräume seien endlich-dimensional.

15.6.

5.1. **Bilinearformen und Sesquilinearformen.** Erinnerung: Multilineare, bilineare Abbildungen (vgl. LA 1). Bezeichne mit $\mathrm{Bil}(\mathrm{V} \times \mathrm{W}, \mathrm{U})$ den K-Vektorraum aller bilinearen Abbildungen $V \times W \to U$.

Definition 5.1. Sei K ein Körper, sei V ein K-Vektorraum. Eine Bilinearform auf V ist eine bilineare Abbildung $\beta\colon V \times V \to K$, d.h. eine Abbildung $\beta\colon V \times V \to K$, so dass für alle $v \in V$ die Abbildungen

$$V \to V,\ w \mapsto \beta(v, w), \quad \text{und} \quad V \to V,\ w \mapsto \beta(w, v),$$

Vektorraumendomorphismen von V sind.

Eine Bilinearform β heißt symmetrisch, wenn $\beta(v,w) = \beta(w,v)$ für alle $v, w \in V$ gilt.

Eine Bilinearform β heißt nicht-ausgeartet, wenn für alle $v \in V$ die folgenden beiden Bedingungen erfüllt sind:

$$\text{falls } \beta(v,w) = 0 \text{ für alle } w \in W, \text{so gilt } v = 0,$$

und

$$\text{falls } \beta(w,v) = 0 \text{ für alle} w \in W, \text{so gilt } v = 0.$$

Auch wenn der Begriff der Bilinearform über beliebigen Körpern von Interesse ist, werden wir im folgenden den Fall $K = \mathbb{R}$ in das Zentrum unserer Betrachtungen stellen. Allerdings ist es sinnvoll, auch den Körper $\mathbb{C}$ miteinzubeziehen. Hier ist allerdings der zentrale Begriff nicht der der Bilinearform (jedenfalls von unserem Standpunkt aus — konkret zum Beispiel deswegen, weil wir "Skalarprodukte", siehe unten, nutzen wollen, um einem Vektor in V seine *Länge* zuordnen wollen), sondern der in der folgenden Definition beschriebene Begriff der Sesquilinearform. Wir bezeichnen mit $\overline{\alpha}$ das komplex Konjugierte einer komplexen Zahl $\alpha \in \mathbb{C}$.

Definition 5.2. Sei V ein $\mathbb{C}$-Vektorraum. Eine Sesquilinearform ist eine Abbildung $\beta\colon V \times V \to \mathbb{C}$, für die gilt:

- Für alle $v, w, w' \in V$ gilt

$$\beta(v, w + w') = \beta(v,w) + \beta(v,w') \quad \text{und} \quad \beta(w + w', v) = \beta(w,v) + \beta(w',v).$$

- Für alle $v, w \in V$, $\alpha \in \mathbb{C}$ gilt:

$$\beta(\alpha v, w) = \alpha\beta(v,w), \qquad \beta(v, \alpha w) = \overline{\alpha}\beta(v,w).$$

Eine Sesquilinearform β heißt *hermitesch*, wenn für alle $v, w \in V$ gilt:

$$\beta(v,w) = \overline{\beta(w,v)}.$$

Eine Sesquilinearform β heißt *nicht-ausgeartet*, wenn für alle $v \in V$ die folgenden beiden Bedingungen erfüllt sind:

$$\text{falls } \beta(v,w) = 0 \text{für alle} w \in W, \text{so gilt } v = 0,$$

und

$$\text{falls } \beta(w,v) = 0 \text{für alle} w \in W, \text{so gilt } v = 0.$$

Weil $\overline{\alpha} = \alpha$ für alle $\alpha \in \mathbb{R}$ erhalten wir aus der Definition einer Sesquilinearform für $\mathbb{R}$ als Grundkörper den Begriff der Bilinearform zurück; eine hermitesche Form entspricht gerade einer symmetrischen Bilinearform. Wir können und werden in der Regel beide Fälle simultan abhandeln.

Für eine komplexe Zahl $\alpha \in \mathbb{C}$ verwenden wir die Notation $\alpha > 0$ mit der Bedeutung "$\alpha \in \mathbb{R}$ und $\alpha > 0$". Beachte, dass für eine hermitesche Form β auf V und $v \in V$ stets gilt: $\beta(v,v) \in \mathbb{R}$.

Oft schreiben wir eine BLF/SLF auch einfach als $(\cdot,\cdot)$, d.h. der Wert der Form für Vektoren v, w wird mit $(v,w) \in K$ bezeichnet.

Wir fixieren nun als Grundkörper $\mathbb{K}$ den Körper der reellen Zahlen oder den Körper der komplexen Zahlen. Wir bezeichnen mit $\mathrm{SLF}(V)$ den $\mathbb{K}$-Vektorraum aller Sesquilinearformen auf V. (Im Fall $\mathbb{K} = \mathbb{R}$ wollen wir darunter einfach den $\mathbb{R}$-Vektorraum aller Bilinearformen verstehen.)

Definition 5.3. Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum. Eine sBF/HF β auf V heißt *positiv definit*, wenn für alle $v \in V \setminus \{0\}$ gilt: $\beta(v,v) > 0$. Die Form β heißt positiv semidefinit, wenn für alle $v \in V$ gilt: $\beta(v,v) \geq 0$. Entsprechend: negativ (semi-) definit.

Eine positiv definite sBF/HF heißt auch *Skalarprodukt* auf V. Ein endlich-dimensionaler $\mathbb{R}$-Vektorraum zusammen mit einem Skalarprodukt heißt *euklidischer Vektorraum*, ein endlich-dimensionaler $\mathbb{C}$-Vektorraum mit einem Skalarprodukt heißt *unitärer Vektorraum*.

Beispiel 5.4. Standard-Skalarprodukt auf $\mathbb{K}^n$.

Satz 5.5 (Schwarzsche Ungleichung)**.** *Sei $(\cdot,\cdot)$ eine positiv semi-definite sBF/HF auf dem $\mathbb{K}$-Vektorraum V. Dann gilt für alle $v, w \in V$:*

$$|(v,w)|^2 \leq (v,v)(w,w).$$

Ist die gegebene Form sogar positiv definit, so gilt in der Ungleichung genau dann $=$, wenn v und w linear abhängig sind.

Korollar 5.6. *Sei $(\cdot,\cdot)$ eine positiv semi-definite sBF/HF auf V. Dann ist $(\cdot,\cdot)$ nicht ausgeartet genau dann, wenn $(\cdot,\cdot)$ positiv definit ist.*

Definition 5.7. Sei V ein euklidischer/unitärer Vektorraum mit Skalarprodukt $(\cdot,\cdot)$ (oder allgemeiner ein $\mathbb{K}$-Vektorraum mit einer positiv semi-definiten sBF/HF). Dann definieren wir die Länge eines Vektors $v \in V$ als

$$|v| := \sqrt{(v,v)}.$$

(Beachte, dass $(v,v) \in \mathbb{R}_{\geq 0}$. Unter der Quadratwurzel verstehen wir die eindeutig bestimmte nicht-negative Quadratwurzel.)

Korollar 5.8 (Dreiecksungleichung)**.** *Sei V ein euklidischer/unitärer Vektorraum mit Skalarprodukt $(\cdot,\cdot)$. Für alle $v, w \in V$ gilt*

$$|v+w| \leq |v| + |w|.$$

Definition 5.9.

(1) Sei V ein euklidischer/unitärer Vektorraum mit Skalarprodukt $(\cdot,\cdot)$. Wir nennen Vektoren $v, w \in V$ *orthogonal* zueinander, wenn $(v,w) = 0$.

(2) Sei V ein euklidischer Vektorraum mit Skalarprodukt $(\cdot,\cdot)$. Der Winkel zwischen zwei Vektoren $v, w \in V$ ist die eindeutig bestimmte reelle Zahl $\vartheta \in [0, 2\pi)$, für die gilt

$$\cos\vartheta = \frac{(x,y)}{|x| \cdot |y|}.$$

- Kann man auch für Bilinearformen auf einem $\mathbb{C}$-Vektorraum den Begriff *positiv definit* sinnvoll definieren?
- Begründe anhand einer geometrischen Veranschaulichung, warum die Dreiecksungleichung Dreiecksungleichung heißt.
- Diskutiere die Definition des Winkels zwischen zwei Vektoren anhand der elementaren Definition des Cosinus als Quotient der Längen von Ankathete und Hypotenuse in einem rechtwinkligen Dreieck.

20.6.

5.2. **Existenz von Orthonormalbasen.**

Definition 5.10. Sei $(V, (\cdot,\cdot))$ ein euklidischer/unitärer Vektorraum. Eine Familie $v_1, \dots, v_n \in V$ heißt *Orthogonalsystem*, falls $v_i \neq 0$ für alle i und für alle $i \neq j$ gilt: $(v_i, v_j) = 0$. Gilt zusätzlich $|v_i| = 1$ für alle i, so bezeichnet man die Familie auch als *Orthonormalsystem*.

Sofern die v_i eine Basis von V bilden, spricht man auch von einer *Orthogonalbasis* bzw. *Orthonormalbasis*.

Beispiel 5.11. $\mathbb{K}^n$ mit Standard-Skalarprodukt. Dann bildet die Standardbasis eine Orthonormalbasis.

Lemma 5.12. *Sei $(V, (\cdot,\cdot))$ ein euklidischer/unitärer Vektorraum und sei $v_1, \dots, v_n \in V$ ein Orthogonalsystem. Dann sind $v_1, \dots, v_n$ linear unabhängig.*

Satz 5.13 (Gram-Schmidtsches Orthonormalisierungsverfahren)**.** *Sei $(V, (\cdot,\cdot))$ ein euklidischer/unitärer Vektorraum und sei $\mathscr{B} = (b_1, \dots, b_n)$ eine Basis von V. Dann existiert eine Orthonormalbasis $v_1, \dots, v_n$ von V, für die außerdem gilt:*

(1) *$V_i := \langle v_1, \dots, v_i\rangle = \langle b_1, \dots, b_i\rangle$ für alle i,*
(2) *Für alle i gilt mit $\mathscr{B}_i = (b_1, \dots, b_i)$, $\mathscr{C}_i = (v_1, \dots, v_i)$:*

$$\det M_{\mathscr{C}_i}^{\mathscr{B}_i}(\mathrm{id}_{V_i}) \in \mathbb{R}_{>0}$$

Durch diese Bedingungen sind $v_1, \dots, v_n$ eindeutig bestimmt, und zwar gilt

$$v_i = \frac{v_i'}{|v_i'|} \quad \text{mit} \quad v_i' = b_i - \sum_{k=1}^{i-1} (b_i, v_k) v_k.$$

Definition 5.14. Sei $(V, (\cdot,\cdot))$ ein euklidischer/unitärer Vektorraum. Sei $U \subseteq V$ ein Untervektorraum. Dann heißt

$$U^\perp := \{v \in V;\ \forall u \in U :\ (u, v) = 0\}$$

das *orthogonale Komplement* von U in V.

Satz 5.15. *Sei $(V, (\cdot,\cdot))$ ein euklidischer/unitärer Vektorraum, und $U \subseteq V$ ein Untervektorraum. Dann gilt $V = U \oplus U^\perp$, also insbesondere* $\dim U^\perp = \dim V - \dim U$. *Ferner ist $(U^\perp)^\perp = U$.*

22.6.

5.3. **Bi-/Sesquilinearformen und Matrizen.** Notation. Für eine Matrix $A = (a_{ij})_{i,j} \in M_{m\times n}(K)$ bezeichnen wir wie üblich mit $A^t := (a_{ji})_{i,j} \in M_{n\times m}(K)$ die transponierte Matrix, mit $\overline{A} := (\overline{a_{ij}})_{i,j} \in M_{m\times n}(K)$ die "komplex konjugierte" Matrix, und mit $A^* := \overline{A}^t$ die sogenannte adjungierte Matrix.[2] Entsprechende Bezeichnungen verwenden wir für Elemente von K^n (d.h. für $(n \times 1)$-Matrizen). Eine quadratische Matrix A heißt *symmetrisch*, falls $A = A^t$ und *hermitesch*, falls $A = A^*$.

Satz 5.16. *Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum und $\mathscr{B} = (b_1, \dots, b_n)$ eine Basis von V. Die Abbildung*

$$\mathrm{SLF}(V) \to M_{n\times n}(K), \quad \beta \mapsto M_{\mathscr{B}}(\beta) := (\beta(b_i, b_j))_{i,j}$$

ist ein Isomorphismus von $\mathbb{K}$-Vektorräumen. Ferner gilt:

[2] Der Begriff *adjungiert* hat hier also eine ganz andere Bedeutung als im Zusammenhang mit der Cramerschen Regel.

(1) *Bezeichne* $c_{\mathscr{B}}\colon V \to \mathbb{K}^n$ *die Koordinatenabbildung. Dann gilt für alle* β, $v, w \in V$*:*
$$\beta(v,w) = c_{\mathscr{B}}(v)^t\, M_{\mathscr{B}}(\beta)\, \overline{c_{\mathscr{B}}(w)}$$
(2) *Eine Form* β *ist genau dann symmetrisch/hermitesch, falls* $M_{\mathscr{B}}(\beta)$ *symmetrisch/hermitesch ist.*
(3) *Eine Form* β *ist genau dann nicht-ausgeartet, wenn* $M_{\mathscr{B}}(\beta)$ *invertierbar ist.*

Die Matrix $M_{\mathscr{B}}(\beta)$ *heißt die* Strukturmatrix *der Form* β *(bezüglich der Basis* $\mathscr{B}$*).*

Satz 5.17 (Basiswechsel)**.** *Sei* V *ein endlich-dimensionaler* $\mathbb{K}$*-Vektorraum und seien* $\mathscr{B} = (b_1, \dots, b_n)$, $\mathscr{C} = (c_1, \dots, c_n)$ *Basen von* V*. Sei* β *eine Bilinear-/Sesquilinearform auf* V*. Dann gilt*
$$M_{\mathscr{B}}(\beta) = (M_{\mathscr{C}}^{\mathscr{B}})^t M_{\mathscr{C}}(\beta) \overline{M_{\mathscr{C}}^{\mathscr{B}}}$$

Satz 5.18. *Sei* V *ein endlich-dimensionaler* $\mathbb{K}$*-Vektorraum mit Basis* $b_1, \dots, b_n$ *und* β *eine symmetrische Bilinearform / Hermitesche Form auf* V*. Dann gilt:* β *ist genau dann positiv definit, wenn für alle* $r = 1, \dots, n$
$$\det(\beta(b_i, b_j))_{i=1,\dots,r,\ j=1,\dots,r} > 0.$$

- Zeigen Sie, dass eine SLF, für die eine Orthonormalbasis existiert, notwendigerweise ein Skalarprodukt ist.
- Was heißt es für die Strukturmatrix $M_{\mathscr{B}}(\beta)$ eines Skalarprodukts β, dass $\mathscr{B}$ eine Orthonormalbasis ist?
- Geben Sie ein zu Satz 5.18 analoges Kriterium für den Begriff *negativ definit*. (Die Formulierund ist nicht völlig offensichtlich. Beginnen Sie mit dem Beispiel der durch die Matrix $-E_n$ gegebenen negativ definiten SLF auf $\mathbb{K}^n$.) Wie ist es mit positiv/negativ semidefiniten Formen?

27.6.

5.4. **Die adjungierte Abbildung.**

Satz 5.19. *Sei* V *ein endlich-dimensionaler* $\mathbb{K}$*-Vektorraum mit einer nicht-ausgearteten Sesquilinearform* $(\cdot,\cdot)$*. Sei* $f \in \operatorname{End}_{\mathbb{K}}(V)$*. Dann existiert ein eindeutig bestimmter Endomorphismus* g *von* V*, so dass für alle* $v, w \in V$ *gilt:*
$$(f(v), w) = (v, g(w)).$$

Es heißt g *die zu* f *adjungierte Abbildung; wir bezeichnen die adjungierte Abbildung zu* f *in der Regel mit* f^**.*

Satz 5.20. *Sei* V *ein euklidischer/unitärer* $\mathbb{K}$*-Vektorraum mit Skalarprodukt* $(\cdot,\cdot)$*, und* $f \in \operatorname{End}_{\mathbb{K}}(V)$*. Ist* $\mathscr{B}$ *eine Orthonormalbasis von* V*, so gilt* $M_{\mathscr{B}}^{\mathscr{B}}(f^*) = M_{\mathscr{B}}^{\mathscr{B}}(f)^*$*.*

29.6.

Satz 5.21. *Sei* V *ein endlich-dimensionaler* $\mathbb{K}$*-Vektorraum mit einer nicht-ausgearteten symm. BLF/Hermiteschen Form* $(\cdot,\cdot)$*.*

(1) *Die Abbildung* $\operatorname{End}_{\mathbb{K}}(V) \to \operatorname{End}_{\mathbb{K}}(V)$, $f \mapsto f^*$ *ist semilinear (d.h. sie ist ein Homomorphismus abelscher Gruppen (bzgl.* $+$*) und es gilt* $(\alpha f)^* = \overline{\alpha} \cdot f^*$ *für alle* $f \in \operatorname{End}_{\mathbb{K}}(V)$, $\alpha \in \mathbb{K}$*).*
(2) *Es gilt* $\mathrm{id}^* = \mathrm{id}$, $(f^*)^* = f$, $(f \circ g)^* = g^* \circ f^*$*.*
(3) *Es gilt*
$$\operatorname{Ker}(f^*) = (\operatorname{Im} f)^\perp, \qquad \operatorname{Im}(f^*) = (\operatorname{Ker} f)^\perp,$$
und $\operatorname{rg} f = \operatorname{rg} f^*$*.*

Definition 5.22. Sei V ein euklidischer/unitärer Vektorraum. Ein Endomorphismus f von V heißt *selbstadjungiert*, falls $f = f^*$ gilt.

Satz 5.23. *Sei V ein euklidischer/unitärer Vektorraum, $\mathscr{B}$ eine Orthonormalbasis von V und $f \in \mathrm{End}_{\mathbb{K}}(V)$. Dann gilt: Der Endomorphismus f ist genau dann selbstadjungiert, wenn $M_{\mathscr{B}}^{\mathscr{B}}(f)$ symmetrisch bzw. hermitesch ist.*

Definition 5.24.
(1) Sei V ein euklidischer/unitärer $\mathbb{K}$-Vektorraum mit Skalarprodukt $(\cdot,\cdot)$, und $f \in \mathrm{End}_{\mathbb{K}}(V)$. Der Endomorphismus f heißt *normal*, wenn $f \circ f^* = f^* \circ f$ gilt.
(2) Eine Matrix $A \in M_{n\times n}(\mathbb{K})$ heißt *normal*, wenn $AA^* = A^*A$.

Offenbar sind selbstadjungierte Endomorphismen normal.

Lemma 5.25. *Sei V ein euklidischer/unitärer $\mathbb{K}$-Vektorraum mit Skalarprodukt $(\cdot,\cdot)$, und $f \in \mathrm{End}_{\mathbb{K}}(V)$. Sei $\mathscr{B}$ eine Orthonormalbasis von V. Dann gilt: Der Endomorphismus f ist genau dann normal, wenn die Matrix $M_{\mathscr{B}}^{\mathscr{B}}(f)$ normal ist.*

Satz 5.26. *Sei V ein euklidischer/unitärer $\mathbb{K}$-Vektorraum mit Skalarprodukt $(\cdot,\cdot)$, und $f \in \mathrm{End}_{\mathbb{K}}(V)$. Der Endomorphismus f ist genau dann* normal*, wenn für alle $v, w \in V$ gilt:*

$$(f(v), f(w)) = (f^*(v), f^*(w)).$$

Korollar 5.27. *Sei V ein euklidischer/unitärer $\mathbb{K}$-Vektorraum mit Skalarprodukt $(\cdot,\cdot)$, und $f \in \mathrm{End}_{\mathbb{K}}(V)$ normal.*

(1) $\mathrm{Ker}\, f = \mathrm{Ker}\, f^*$
(2) *Ein Element $\lambda \in \mathbb{K}$ ist genau dann ein Eigenwert von f, wenn $\overline{\lambda}$ ein Eigenwert von f^* ist.*

4.7.

Theorem 5.28 (Spektralsatz für normale Endomorphismen)**.** *Sei V ein euklidischer/unitärer $\mathbb{K}$-Vektorraum mit Skalarprodukt $(\cdot,\cdot)$, und $f \in \mathrm{End}_{\mathbb{K}}(V)$ ein Endomorphismus, dessen charakteristisches Polynom vollständig in Linearfaktoren zerfällt. Dann sind äquivalent:*

(1) *f ist normal.*
(2) *Es existiert eine Orthonormalbasis von V, die aus Eigenvektoren von f besteht.*

- Gib ein Beispiel eines normalen Endomorphismus, der nicht selbstadjungiert ist.
- Sind Drehungen, Spiegelungen, Streckungen des $\mathbb{R}^2$ normal? Sind sie selbstadjungiert?

Isometrien. Im folgenden sei V ein euklidischer/unitärer $\mathbb{K}$-Vektorraum mit Skalarprodukt $(\cdot,\cdot)$.

Lemma 5.29. *Sei W ein weiterer eukl./unit. Vektorraum mit Skalarprodukt $\langle\cdot,\cdot\rangle$. Für einen Homomorphismus $f\colon V \to W$ sind äquivalent:*

(1) *Für alle $v, v' \in V$ gilt $(v, v') = \langle f(v), f(v')\rangle$.*
(2) *Für alle $v \in V$ gilt $|v| = |f(v)|$.*
(3) *Für jede Orthonormalbasis $\mathscr{B} = (b_1, \ldots, b_n)$ von V ist $(f(b_1), \ldots, f(b_n))$ eine Orthonormalbasis von* $\mathrm{Im}\, f$ *(mit der Einschränkung von $\langle\cdot,\cdot\rangle$ als Skalarprodukt).*

(4) *Es existiert eine Orthonormalbasis $\mathscr{B} = (b_1, \dots, b_n)$ von V, so dass $(f(b_1), \dots, f(b_n))$ eine Orthonormalbasis von* $\operatorname{Im} f$ *(mit der Einschränkung von $\langle \cdot, \cdot \rangle$ als Skalarprodukt) ist.*

Hat f diese Eigenschaften, so ist f injektiv. Ist f ein Isomorphismus mit diesem Eigenschaften, so nennt man f eine Isometrie*.*

Ist speziell $V = W$, so sind die obigen Aussagen äquivalent dazu, dass f ein Isomorphismus und $f^{-1} = f^*$ ist.

Definition 5.30. (1) Sei V ein euklidischer/unitärer Vektorraum. Ein Automorphismus f von V mit den Eigenschaften des Lemmas heißt *orthogonale Abbildung* (im Fall $\mathbb{K} = \mathbb{R}$) bzw. *unitäre Abbildung* (im Fall $\mathbb{K} = \mathbb{C}$).
(2) Eine Matrix $A \in GL_n(\mathbb{R})$ heißt *orthogonal*, falls $A^{-1} = A^t$. Eine Matrix $A \in GL_n(\mathbb{C})$ heißt *unitär*, falls $A^{-1} = A^*$.

Offenbar sind orthogonale und unitäre Abbildungen normal.

Lemma 5.31. *Sei V ein euklidischer/unitärer Vektorraum und $\mathscr{B}$ eine Orthonormalbasis. Sei $f\colon V \to V$ ein Automorphismus. Dann sind äquivalent:*

(1) *f ist orthogonal/unitär,*
(2) *$M_{\mathscr{B}}^{\mathscr{B}}(f)$ ist orthogonal/unitär.*

Definition 5.32. (1) Die Teilmenge $O(n) \subset GL_n(\mathbb{R})$ der orthogonalen Matrizen ist eine Untergruppe und heißt die *orthogonale Gruppe*.
(2) Die Teilmenge $U(n) \subset GL_n(\mathbb{C})$ der unitären Matrizen ist eine Untergruppe und heißt die *unitäre Gruppe*.

Satz 5.33. *Sei V ein euklidischer/unitärer Vektorraum und $\mathscr{B}$ eine Orthonormalbasis. Sei $\mathscr{C}$ eine weitere Basis von V. Dann gilt: $\mathscr{C}$ ist genau dann eine Orthonormalbasis, wenn die Basiswechselmatrix $M_{\mathscr{B}}^{\mathscr{C}}$ orthogonal bzw. unitär ist.*

Der Stoff bis hier ist relevant für die Klausur zur LA 2. (Für die Nachklausur und für mündliche Prüfungen ist der Stoff der gesamten Vorlesung relevant.)

6.7.

Satz 5.34. *Sei V ein unitärer $\mathbb{C}$-Vektorraum, $f \in \operatorname{End}(V)$. Dann gilt: f ist genau dann eine Isometrie, wenn eine Orthonormalbasis von V existiert, die aus Eigenvektoren von f besteht, und für alle Eigenwerte λ von f der Absolutbetrag $|\lambda| = 1$ ist.*

5.5. **Die Hauptachsentransformation.**

Satz 5.35. *Sei V ein euklidischer/unitärer Vektorraum und $f \in \operatorname{End}_{\mathbb{K}}(V)$ selbstadjungiert. Dann hat das charakteristische Polynom Koeffizienten in $\mathbb{R}$ und zerfällt über $\mathbb{R}$ vollständig in Linearfaktoren.*

Theorem 5.36 (Spektralsatz für selbstadjungierte Abbildungen)**.** *Sei V ein euklidischer/unitärer Vektorraum und $f \in \operatorname{End}_{\mathbb{K}}(V)$ selbstadjungiert. Dann existiert eine Orthonormalbasis von V, die aus Eigenvektoren von f besteht, und alle Eigenwerte von f sind reell.*

Korollar 5.37. *Sei $A \in M_{n\times n}(\mathbb{K})$ eine symmetrische/Hermitesche Matrix. Dann existiert eine orthogonale/unitäre Matrix S, so dass $S^{-1}AS$ eine Diagonalmatrix mit reellen Einträgen ist.*

Korollar 5.38 (Hauptachsentransformation)**.** *Sei V ein euklidischer/unitärer Vektorraum mit Skalarprodukt $(\cdot,\cdot)$. Sei β eine symmetrische Bilinearform/Hermitesche Form auf V. Dann existiert eine Orthonormalbasis $\mathscr{B}$ von V, so dass $M_{\mathscr{B}}(\beta)$ eine Diagonalmatrix mit reellen Einträgen ist.*

Korollar 5.39. *Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum und β eine symmetrische Bilinearform/Hermitesche Form. Dann sind äquivalent:*

1. *β ist positiv definit.*
2. *Es existiert eine Basis $\mathscr{B}$ von V, so dass $M_{\mathscr{B}}(\beta)$ nur positive reelle Eigenwerte hat.*

11.7.

Theorem 5.40 (Sylvesterscher Trägheitssatz)**.** *Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum, $n = \dim V$ und β eine symmetrische Bilinearform/Hermitesche Form auf V. Sei $\mathscr{B}$ eine Basis von V, und seien k_+, k_- bzw. k_0 die Anzahlen der Eigenwerte von $M_{\mathscr{B}}(\beta)$, die positiv, negativ bzw. $= 0$ sind, jeweils gezählt mit der Vielfachheit der entsprechenden Nullstelle des charakteristischen Polynoms.*

Dann ist $k_+ + k_- + k_0 = n$, und die Zahlen k_+, k_- und k_0 sind unabhängig von der Wahl der Basis $\mathscr{B}$.

Es existiert eine Basis $\mathscr{B}$ von V, so dass

$$M_{\mathscr{B}}(\beta) = \operatorname{diag}(1,\dots,1,-1,\dots,-1,0,\dots,0)$$

(mit k_+ Einträgen $= 1$, k_- Einträgen $= -1$ und k_0 Einträgen $= 0$) ist.

13.7.

Bemerkung 5.41. Geometrische Interpretation der Hauptachsentransformation. Kegelschnitte.

Hinweise zum Nachbereiten der Vorlesung

In diesem Abschnitt sammele ich allgemeine Hinweise zum Nachbereiten der Vorlesung. Hinweise zu einzelnen Vorlesungen sind oben in kleiner Schrift in den Text eingefügt.

Definitionen. • Überlege Dir ein Beispiel zu der Definition. Gibt es "triviale" Beispiele? (Zum Beispiel: Ist V ein K-VR, so ist offenbar V ein UVR von V.)

• Falls eine Eigenschaft definiert wird: finde ein Beispiel, in dem die Eigenschaft verletzt ist. Gibt es triviale Beispiele, in denen die Eigenschaft erfüllt ist, oder ist es schwierig, die Existenz von Objekten zu zeigen, die die Definition erfüllen?

• Wenn eine Konstruktion beschrieben wird: Führe die Konstruktion an einem konkreten Beispiel durch. (Zum Beispiel: Berechne zum Verständnis der Definition des charakteristischen Polynoms das charpol einer konkreten 2×2-Matrix, einer konkreten 3×3-Matrix.)

• Hat die Definition einen geometrischen Gehalt? (Zum Beispiel: ein Vektor $v \in V \setminus \{0\}$ ist genau dann ein EV von $f \in \operatorname{End}_K(V)$, wenn die Gerade $\langle v\rangle$ von f in sich selbst abgebildet wird.)

Sätze, Lemmata, ... • Vollziehe die Aussage des Satzes anhand eines konkreten Beispiels nach. (Zum Beispiel: Überprüfe den Satz von Cayley-Hamilton für eine konkrete 2×2-Matrix.)

• Lässt sich sinnvoll eine Umkehrung des Satzes formulieren? Wenn ja: Ist die Umkehrung gültig oder falsch?

• Studiere den Beweis des Satzes — einerseits allgemein, andererseits im Fall eines konkreten Beispiels.

• Versuche, Beispiele zu finden, die zeigen, dass alle Voraussetzungen im Satz wirklich nötig sind. Wo gehen die einzelnen Voraussetzungen im Beweis ein?

• Überlege, ob sich der Beweis vereinfachen lässt. Versuche, alternative Beweise zu finden. Lässt sich der Beweis unter (sinnvollen) zusätzlichen Annahmen vereinfachen?

• Hat der Satz einen geometrischen Gehalt?

• Wird der Satz (das Lemma, ...) in späteren Beweisen benutzt? Ist die Aussage des Satzes ein Spezialfall einer später bewiesenen allgemeineren Aussage?

Sonstiges. • Beschäftige Dich *intensiv* mit den Übungsaufgaben.

• Überlege eigene Übungsaufgaben zum Vorlesungsstoff. Wenn unter den Hausaufgaben "Rechenaufgaben" sind: Überlege, wie man "gut lösbare" Aufgaben dieser Art findet.

• Schaue regelmäßig in Lehrbücher zur Linearen Algebra und vergleiche die entsprechenden Abschnitte dort mit der Vorlesung.