Lineare Algebra II

Bernd Ammann, SS 2008

KAPITEL 1

Polynome

1. Vorbemerkungen

Eines der zentralen Themen der Linearen Algebra 2 ist die Theorie der Normalformen von Endomorphismen, in anderen Worten: Sei ein Endomorphismus $f : V \to V$ gegeben. Unter welchen Bedingungen können wir eine geschickte Basis von V finden, so dass die zugehörige Matrix besonders einfach ist. Wir haben zum Beispiel am Ende des Wintersemesters gesehen, dass es zu jedem selbstadjungierten Endomorphismus eine Orthonormalbasis gibt, so dass die zugehörige Matrix Diagonalgestalt hat (Satz 10.5, Orthonormale Hauptachsentransformation von selbstadjungierten Endomorphismen). Wir werden u.a. sehen: Zu jedem Endomorphismus eines komplexen Vektorraums finden wir einen Basis, so dass die zugehörige Matrix Dreiecksgestalt hat (= trigonal ist).

Wenn wir mit dem Körper der reellen Zahlen arbeiten, ist die Situation etwas komplizierter. Und man möchte die Aussagen so formulieren, dass auch endliche Körper wie $\mathbb{Z}/p\mathbb{Z}$, p Primzahl, eingeschlossen sind, da solche Körper u.a. in der Kryptographie wichtig sind.

Sei $A \in \mathrm{Mat}(n, n; \mathbb{K})$ (ähnliches gilt für Endomorphismen). Wir haben im Wintersemester die charakteristische Polynom-Funktion kennengelernt.

$$\chi_A(\lambda) = \det_n(\lambda \mathbb{1}_n - A).$$

Dies ist eine Funktion $\chi_A : \mathbb{K} \to \mathbb{K}$.

Wir wissen auch schon, dass die Eigenwerte von A gerade die Nullstellen von χ_A sind. Wenn wir genügend viele Eigenwerte kennen, so können wir die Matrix durch Basiswechsel auf Diagonalgestalt bringen.

Beispiel.

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

Wir betrachten A zunächst als komplexe Matrix, also $A \in \mathrm{Mat}(3,3;\mathbb{C})$. Die charakteristische Polynomfunktion ist dann

$$\chi_A(\lambda) = \det_3 \begin{pmatrix} \lambda-1 & 0 & 0 \\ 0 & \lambda & -1 \\ 0 & 1 & \lambda \end{pmatrix} = (\lambda-1)(\lambda^2+1).$$

$$\chi_A : \mathbb{C} \to \mathbb{C}.$$

Wir haben die Nullstellen $\lambda_1 = 1$, $\lambda_2 = i$, $\lambda_3 = -i$ und die zugehörigen Eigenvektoren

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad v_2 = \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix}, \qquad v_3 = \begin{pmatrix} 0 \\ 1 \\ -i \end{pmatrix}.$$

Die Eigenvektoren v_1, v_2 und v_3 bilden eine Basis von $\mathbb{C}^3$ und in dieser Basis hat der Endomorphismus $\mathcal{L}_A$ die Gestalt

$$\mathrm{Mat}_{(v_i)}^{(v_i)}(\mathcal{L}_A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{pmatrix}.$$

Wir können A aber auch als Element in $\mathrm{Mat}(n,n;\mathbb{R})$ betrachten, dann erhalten wir eine charakteristische Polynom-Funktion χ_A, die auch durch die Formel $\chi_A(\lambda) = (\lambda-1)(\lambda^2+1)$ beschrieben wird, aber nun haben wir $\chi_A : \mathbb{R} \to \mathbb{R}$. Diese Funktion hat nur die Nullstelle 1, wir finden nur einen einzigen Eigenwert mit Multiplizität 1. Als reelle Matrix ist A nicht diagonalisierbar. Um A gut beschreiben zu können, muss man auch die "komplexen Nullstellen" der Funktion $\chi_A : \mathbb{R} \to \mathbb{R}$ betrachten. Wir stecken uns deswegen das folgende Ziel:

Ziel Nr. 1. Sei K ein Körper und R ein Unterkörper von K. Wir wollen aus einem Polynom in R ein Polynom in K machen.

In der Schule ist es üblich, Polynome (über $\mathbb{K}$) als Funktionen $\mathbb{K} \to \mathbb{K}$ der Form $x \mapsto a_0 + a_1 x + \cdots a_m x^m$ zu definieren. In anderen Worten: der in der Schule benutzte Begriff "Polynom" entspricht genau dem, was wir in LA1, Kapitel 2, Abschnitt 2 als "Polynom-Funktion" bezeichnet haben. Solch eine Definition ist für uns nicht sinnvoll, wir werden Polynome anders definieren.

Um die Schwierigkeiten mit den Polynom-Funktionen zu verdeutlichen, betrachten wir den endlichen Körper $\mathbb{Z}/2\mathbb{Z}$, d.h. einen Körper mit den Elementen $\bar{0}$ und $\bar{1}$. Dieser Körper ist ein Unterkörper von einem Körper $\mathbb{K}_4 = \{\bar{0}, \bar{1}, a, b\}$ mit 4 Elementen, der durch die Tabellen

$+$	$\bar{0}$	$\bar{1}$	a	b
$\bar{0}$	$\bar{0}$	$\bar{1}$	a	b
$\bar{1}$	$\bar{1}$	$\bar{0}$	b	a
a	a	b	$\bar{0}$	$\bar{1}$
b	b	a	$\bar{1}$	$\bar{0}$

$\bullet$	$\bar{0}$	$\bar{1}$	a	b
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	a	b
a	$\bar{0}$	a	b	$\bar{1}$
b	$\bar{0}$	b	$\bar{1}$	a

beschrieben wird.

Wir setzen $R = \mathbb{Z}/2\mathbb{Z}$ und $K = \mathbb{K}_4$ und betrachten die Polynom-Funktion $x \mapsto P(x) = x(x + \bar{1})$. Wir interpretieren diesen Ausdruck zunächst als eine Funktion $P : R \to R$. Es gilt $P(\bar{0}) = \bar{0}$ und $P(\bar{1}) = \bar{0}$, die Funktion $P : R \to R$ ist also die Null-Funktion. Es ist sehr naheliegend die Null-Funktion $R \to R$ zur Null-Funktion $K \to K, x \mapsto 0$ fortzusetzen.

Wir können aber P auch gleich als Polynom in K interpretieren, als $K \to K : x \mapsto P(x) = x(x+\bar{1})$. Insbesondere $a \mapsto a(a+\bar{1}) = ab = \bar{1}$. Die Fortsetzung auf K ist somit nicht eindeutig, es ist unklar, ob a eine Nullstelle der Polynom-Funktion $P : R \to R$ ist oder nicht. Abhilfe schafft die Definition des Polynoms im nächsten Abschnitt.

Ein zweiter Grund motiviert die folgende Definition von Polynomen: Auf dem Weg zu unseren Normalformen wird der Satz von Hamilton-Cayley wichtig sein. Er besagt

$$\chi_A(A) = 0.$$

Damit dieser Ausdruck überhaupt definiert ist, muss man Matrizen in Polynome einsetzen können.

Ziel Nr. 2. Sei R ein Körper. Wir wollen Matrizen $A \in \mathrm{Mat}(n, n; R)$ in Polynome in einsetzen können.

Wir können beide Ziele vereinigen.

Vereinigtes Ziel. Sei S ein Ring mit 1 und R ein Unterring mit 1 von S, so dass $rs = sr$ für alle $r \in R$ und $s \in S$. Wir wollen aus einem Polynom über R ein Polynom über S machen.

Ziel Nr. 1 erhalten wir daraus direkt, $S = K$: Jeder Körper ist ein kommutativer Ring mit 1. Um Ziel Nr. 2 zu erhalten, setzen wir $S := \mathrm{Mat}(n, n; R)$.

Die Menge aller Polynome ist wiederum ein Ring. Er hat ähnliche Eigenschaften wie der Ring der ganzen Zahlen, u.a. erlaubt er eine Division mit Rest und eine im wesentlichen eindeutige Primfaktorzerlegung.

2. Definition der Polynome

Im folgenden sei R ein kommutativer Ring mit 1. Alle Ringe in diesem Kapitel sind Ringe mit 1, und alle Unterringe sind Unterringe mit derselben 1.

Bevor wir eine formale Defintion von Polynomen angeben, wollen wir ein anschauliches Bild erklären.

Eine Polynom über R stellt man sich am besten als einen Ausdruck der Art $P = a_0 + a_1X + a_2X^2 + \cdots a_mX^m$ (mit $m \in \mathbb{N} \cup \{0\}$ und $a_0, \ldots, a_m \in R$) vor, den wir als Rechenvorschrift interpretieren wollen. Genauer: sei S ein (nicht unbedingt kommutativer) Ring, der R als Unterring enthält. Wenn zugegebenem $A \in S$ ersetzen jedes X im Ausdruck P durch A. Das Ergebnis nennen wir $P(A)$. Wir erhalten eine Funktion $S \to S$, $A \mapsto P(A)$, wir sagen: wir setzen A in P ein. Im Spezialfall $S = R$ nennen wir die so erhaltene Funktion $\hat{P} : R \to R, r \to P(r)$ die *assoziierte Polynom-Funktion.* Die Faktoren a_i heißem *Koeffizienten von* P, genauer a_i heißt der Koeffizient vom Grad i.

Wir sagen, zwei Polynome $P = a_0 + a_1X + a_2X^2 + \cdots a_mX^m$ und $Q = b_0 + b_1X + b_2X^2 + \cdots b_rX^r$ sind gleich, wenn

(1.) $a_i = b_i$ für alle $i \in \{0, 1, \ldots, \min\{m, r\}\}$,
(2.) $a_i = 0$ für alle i mit $r < i \leq m$,
(3.) $b_i = 0$ für alle i mit $m < i \leq r$.

Offensichtlich gilt dann auch $P(A) = Q(A)$ für alle A.

Beispiele. (1) $R = \mathbb{R}$: Die Polynome $P = 2 + 3X + 0X^2$ und $Q = 2 + 3X$ sind gleich.
(2) $R = \mathbb{Z}/2\mathbb{Z}$: Die Polynome $P = X(X - 1)$ und $Q = 0$ sind nicht gleich, aber die assoziierten Polynomfunktionen sind gleich: $P(r) = Q(r)$ für alle $r \in R = \{0, 1\}$. Wenn man aber $a \in \mathbb{K}_4$ einsetzt, erhalten wir $P(a) = 1 \neq 0 = Q(a)$.

Wir werden später sehen, dass verschiedene Polynome verschiedene Rechenvorschriften darstellen, genauer:

Lemma 2.1. *Seien P und Q Polynome über R, die nicht gleich sind. Dann gibt es einen Ring S, der R als Unterring enthält, und ein $A \in S$, so dass $P(A) \neq Q(A)$.*

Die Addition und Multiplikation von Polynomen macht man nach den naheliegenden Regeln, z.B.

$$(1 + 3X) + (2 + 5X^3) = (3 + 3X + 5X^3 \qquad (1 + X)(2 + 3X + 4X^2) = (2 + 5X + 7X^2 + 4X^3).$$

Konvention $X^0 := 1$.

Wiederholung: $\mathrm{Abb}_e(\mathbb{N}_0, R)$ ist der Raum aller Abbildungen $\mathbb{N}_0 \to R$, die nur endlich viele Elemente auf etwas von Null verschiedenes abbilden. Die Menge $\mathrm{Abb}_e(\mathbb{N}_0, R)$ sind also genau die quasi-endlichen Familien von Elementen in R. Wir schreiben sie in der Form $(a_0, a_1, a_2, \ldots, a_m, 0, 0, \ldots)$ oder $(a_i)_{i \in \mathbb{N}_0}$.

Formale Definition von Polynomen.

Definition 2.2. Sei R ein kommutativer Ring. Wir definieren

$$R[X] := \mathrm{Abb}_e(\mathbb{N}_0, R).$$

Wir addieren Elemente von $R[X]$ wie Elemente von $\mathrm{Abb}_e(\mathbb{N}_0, R)$, d.h. komponentenweise

$$(a_i)_{i \in \mathbb{N}_0} + (b_i)_{i \in \mathbb{N}_0} := (a_i + b_i)_{i \in \mathbb{N}_0}.$$

Wir definieren aber eine andere Multiplikation

$$(a_i)_{i \in \mathbb{N}_0} \cdot (b_i)_{i \in \mathbb{N}_0} := (c_i)_{i \in \mathbb{N}_0},$$

wobei $c_i := \sum_{j=0}^{i} a_j b_{i-j}$.

Man rechnet leicht nach, dass $R[X]$ ein kommutativer Ring ist, das Nullelement ist $(0, 0, 0, \ldots)$ und das Einselement ist $(1, 0, 0, \ldots)$.

Beispiele: $(0, 1, 0, \ldots)^2 = (0, 0, 1, 0, \ldots)$, $(0, 1, 0, \ldots)^3 = (0, 0, 0, 1, 0, \ldots)$, etc.

$(r_1, 0, 0, \ldots) \cdot (r_2, 0, 0, \ldots) = (r_1 r_2, 0, 0 \ldots)$.

Zu jedem $(i \mapsto a_i) \in \mathrm{Abb}_e(\mathbb{N}_0, R)$ erhält man ein Polynom $\sum_{i \in \mathbb{N}_0} a_i X^i$. Umgekehrt lässt sich jedes Polynom in eindeutiger Art so schreiben. Außerdem ist die Addition und Multiplikation auf $R[X]$ genau die oben angedeutete intuitiv definierte Addition und Multiplikation von Polynomen. Wir definieren deswegen.

Definition 2.3 (Formal korrekte Definition von Polynomen). Sei R ein kommutativer Ring. Der Ring $R[X]$ heißt der *Ring der Polynome* über R, die Elemente heißen *Polynome* über R. Wir schreiben $X := (0, 1, 0, 0, \ldots)$. Somit ist $\sum_{i=0}^{m} a_m X^m = (a_0, a_1, \ldots, a_m, 0, 0, \ldots)$. Wir identifizieren ausserdem $r \in R$ mit $(r, 0, 0, \ldots) = r + 0X^1 + 0X^2 \ldots$.

Mit dieser Definition ist R ein Unterring von $R[X]$.

Beweis von Lemma 2.1. Wir setzen $S := R[X]$, $A := X$. Dann gilt $P(X) = P$, $Q(X) = Q$. □

3. Ringe (Fortsetzung)

Bevor wir mit Polynomen fortfahren, müssen wir noch ein paar Begriffe über Ringe einführen.

Seien R und S Ringe. Wir benutzen in diesem Semester den Begriff "Ring" immer im Sinne von "Ring mit 1". Unterringe sind immer als Unterringe mit 1 zu verstehen, die 1 ist in allen Unterringen enthalten. Eine Abbildung $\phi : R \to S$ heißt Homomorphismus von Ringen (mit 1), falls für alle $x, y \in R$ gilt

$$\phi(x+y) = \phi(x) + \phi(y) \qquad \phi(xy) = \phi(x)\phi(y) \qquad \phi(1_R) = 1_S.$$

Falls ϕ surjektiv, bzw. injektiv, bzw. bijektiv ist, so nennt man ϕ einen Epi-, bzw. Mono-, bzw. Isomorphismus von Ringen. Ein Endomorphismus von Ringen ist ein Homomorphismus von einem Ring in sich selbst, und ein Automorphismus von Ringen ist wieder ein bijektiver Endomorphismus von Ringen.

Beispiele.

(1) Die komplexe Konjugation $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ ist ein Isomorphismus von Ringen, sogar ein Automorphismus.
(2) Die Abbildung $R \to \mathrm{Mat}(n, n; R)$, $R \mapsto r\mathbb{1}_n$ ist ein Monomorphismus von Ringen.
(3) Seien $n, m \in \mathbb{N}$. Die Abbildung

$$\phi : \mathrm{Mat}(n, n; R) \to \mathrm{Mat}(n+m, n+m; R), \qquad A \mapsto \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$$

erfüllt $\phi(A + B) = \phi(A) + \phi(B)$ und $\phi(AB) = \phi(A)\phi(B)$ für alle $A, B \in \mathrm{Mat}(n, n; R)$, aber nicht $\phi(1_n) = 1_{n+m}$. Sie ist also kein Homomorphismus von Ringen (mit 1).

Definition 3.1 (Wiederholung). Ein Element a eines kommuativen Rings R heißt Nullteiler, falls $a \neq 0$ und falls es ein $b \in R \setminus \{0\}$ gibt mit $ab = 0$.

Definition 3.2. Ein Ring R (mit 1) heißt *Integritätsring* (oder auch *Integritätsbereich*), falls R kommutativ ist, $1 \neq 0$ und falls R keine Nullteiler besitzt.

Jeder Unterring eines Integritätsringes ist wieder ein Integritätsring.

Beispiele.

(1) $\mathbb{Z}$ ist ein Integritätsring.
(2) Alle Körper sind Integritätsringe.
(3) Der Nullring $(\{0\}, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring mit 1, aber $1 = 0$, deswegen ist es kein Integritätsring.
(4) Der Ring $\mathbb{Z} \oplus \mathbb{Z}$, versehen mit der komponentenweisen Multiplikation und komponentenweisen Addition ist ein kommutativer Ring mit $1 = (1,1) \neq 0 = (0,0)$, aber er hat Nullteiler: $(0,1) \cdot (1,0) = (0,0)$. Es ist kein Integritätsring.

4. Elementare Eigenschaften von Polynomen

Nachtrag und Wiederholung: Ein Monom ist ein Polynom der Form aX^n, $a \in R$, $n \in \mathbb{N}_0$. Das X in $R[X]$ nennt man auch die *Unbestimmte* des Polynomring. $R[X]$ ist der Polynomring in der Unbestimmten X über R. Ein Polynom $a_0 + a_1X + a_2X^2 + \ldots$ ist *konstant*, falls $a_n = 0$ für alle $n \geq 1$. Man identifiziert $r \in R$ mit dem konstanten Polynom $r + 0X + 0X^2 + \cdots$.

Ist $P = \sum_{i \in \mathbb{N}_0} a_i X^i \in R[X]$ ein Polynom $\neq 0$, dann ist die Menge $\{i \in \mathbb{N}_0 \,|\, a_i \neq 0\}$ endlich und nicht-leer und besitzt deswegen ein Maximum, das wir n nennen. Man nennt dann n den Grad von P und schreibt hierfür kurz $\deg P$. Für das Nullpolynom $P = 0$ definieren wir $\deg(0) = -\infty$.

Beispiel: $\deg(1 + 0X + 3X^2 + 0X^3 + 0X^4 \ldots) = \deg(1 + 3X^2) = 2$

Beispiele: X^2 und $2 + X + 0X^2$ sind unitär, $1 + 2X$ ist nicht unitär.

Proposition 4.1. *Sei R ein Ring, $P, Q \in R[X]$.*

$$\deg(P + Q) \leq \max\{\deg P, \deg Q\}$$

$$\deg(P \cdot Q) \leq \deg P + \deg Q$$

Ist R ein Integritätsring, dann gilt sogar

$$\deg(P \cdot Q) = \deg P + \deg Q.$$

Hierbei nutzen wir die Konventionen

$$n + (-\infty) := -\infty + n := -\infty \qquad (-\infty) + (-\infty) := -\infty.$$

Beweis. Die Aussage ist klar, falls $P = 0$ oder $Q = 0$.

Seien nun $P, Q \in R[X] \setminus \{0\}$, $n = \deg P$ und $m = \deg Q$. Wir schreiben

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \qquad Q = b_0 + b_1 X + b_2 X^2 + \cdots + b_m X^m,$$

wobei $a_n \neq 0$ und $b_m \neq 0$. Ohne Beschränkung der Allgemeinheit sei $n \geq m$. Wir setzen $b_i = 0$ für $i \in \{m+1, \ldots, n\}$. Dann gilt

$$P + Q = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \cdots + (a_n + b_n)X^n,$$

und deswegen ist $\deg(P+Q) \leq n = \max\{\deg P, \deg Q\}$. Außerdem gilt

$$P \cdot Q = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + (a_0 b_2 + a_1 b_1 + a_2 b_0)X^2 + \cdots + (a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0)X^m + \cdots + a_n b_m X^{n+m}.$$

Hieraus sieht man $\deg(PQ) \leq n+m$ und wir haben $\deg(PQ) < n+m$ genau dann, wenn $a_n b_m = 0$. Ist also R nullteilerfremd, so gilt $\deg(PQ) = \deg P + \deg Q$. □

Ähnlich sieht man: Das Produkt von unitären Polynomen ist wiederum unitär.

Korollar 4.2. *Ein Ring R ist nullteilerfrei genau dann, wenn $R[X]$ nullteilerfrei ist. Also ist R ein Intergritätsring genau dann, wenn $R[X]$ ein Integritätsring ist.*

Beweis. Sei R nullteilerfrei. Angenommen $PQ = 0$ für $P, Q \in R[X]$. Dann gilt

$$-\infty = \deg(PQ) = \deg P + \deg Q.$$

Wegen $\deg P, \deg Q \in \{-\infty\} \cup \mathbb{N}_0$ folgt $\deg P = -\infty$ oder $\deg Q = -\infty$, also $P = 0$ oder $Q = 0$. Somit ist auch $R[X]$ nullteilerfrei.

Ein Unterring eines nullteilerfreien Ringes ist ebenfalls nullteilerfrei. Aus der Nullteilerfreiheit von $R[X]$ folgt also auch die Nullteilerfreiheit von R. □

Proposition 4.3. *Sei R ein Integritätsring. Dann gilt*

$$(R[X])^* = R^*.$$

In anderen Worten: Ein Polynom ist genau dann invertierbar, wenn es konstant ist und der Wert des Polynoms invertierbar in R ist.

Beweis: Anwesenheitsübungen.

Definition 4.4 (Einsetzen in Polynome). Sei $\phi : R \to S$ ein Homomorphismus von Ringen. Für $A \in S$ definieren wir die *Einsetzungabbildung* (auch manchmal Auswertungsabbildung, engl. evaluation, genannt)

$$\mathrm{ev}_A^\phi : R[X] \to S, \quad P = \sum_{i=0}^m a_i X^i \mapsto \sum_{i=0}^m \phi(a_i) A^i.$$

Hierbei ist wieder nach Definition $A^0 := 1_S$. Wenn ϕ aus dem Kontext heraus klar ist, so schreiben wir auch $P(A)$ an Stelle von $\mathrm{ev}_A^\phi(P)$. Man nennt auch $P(A)$ den *Wert von P an der Stelle A.*

Beispiele.

(1) Falls $S = R[X]$, $\iota : R \to R[X]$ die Inklusion und $A = X$, so ist $\mathrm{ev}^\iota_X : R[X] \to R[X]$ die Identität.
(2) Ist $R = \mathbb{R}$, $S = \mathbb{C}[X]$ $\iota : \mathbb{R} \to \mathbb{C}[X]$ die Verkettung der Inklusionen $\mathbb{R} \to \mathbb{C}$ und $\mathbb{C} \to \mathbb{C}[X]$, $A = X$, dann macht ev^ι_A aus dem Polynom $P = \sum_{i=0}^m a_i X^i$ über $\mathbb{R}$ das Polynome über $\mathbb{C}$ mit derselben Formel $P = \sum_{i=0}^m a_i X^i$.
(3) Allgemein bekommen wir zu einem Unterring R von S, einen injektiven Homomorphismus $\mathrm{ev}^\iota_X : R[X] \to S[X]$, der uns erlaubt, $R[X]$ als Unterring von $S[X]$ zu betrachten.
(4) Ist $\kappa : \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation, und $\iota : \mathbb{C} \to \mathbb{C}[X]$, so ist $\mathrm{ev}^{\iota\circ\kappa}_X : \mathbb{C}[X] \to \mathbb{C}[X]$, die Abbildung, die alle Koeffizienten komplex konjugiert. Wir schreiben $\bar{P} := \mathrm{ev}^\kappa_X(P)$, also
$$\overline{a_0 + a_1 X + a_2 X^2 + \cdots} = \bar{a}_0 + \bar{a}_1 X + \bar{a}_2 X^2 + \cdots$$
(5) Ist $A \in \mathrm{Mat}(n, n; R)$, $\phi : R \to \mathrm{Mat}(n, n; R)$, $r \mapsto r\mathbb{1}_n$, so gilt
$$\mathrm{ev}^\phi_A(a_0 + a_1 X + a_2 X^2 + \cdots) = a_0 + a_1 A + a_2 A^2 + \cdots .$$
(6) Ist $S = R[X]$, $\iota : R \to R[X]$ die Inklusion und $A = X^2$, dann gilt
$$\mathrm{ev}^\iota_{X^2}(a_0 + a_1 X + a_2 X^2 + \cdots) = a_0 + a_1 X^2 + a_2 X^4 + \cdots$$
(7) Ist $S = R[X]$, $\iota : R \to R[X]$ die Inklusion und $Q \in R[X]$, so schreibt man oft $P \circ Q$ für $\mathrm{ev}^\iota_Q(P)$. So ergibt $P = X^2 + X + 1$, $Q = X^3 + 1$ dann $P \circ Q = (x^3 + 1)^2 + (X^3 + 1) + 1 = X^6 + 3X^3 + 3$. Die Notation ist motiviert durch die Identität
$$\widehat{P \circ Q} = \hat{P} \circ \hat{Q}.$$
(8) Sei $S = \mathrm{Abb}(R, R)$, versehen mit der komponentenweisen Addition und der komponentenweisen Multiplikation. Die Abbildung $\phi : R \to S$ bilde $a \in R$ auf die konstante Funktion $(R \to R, r \mapsto a) \in \mathrm{Abb}(R, R)$ ab. Weiter sei $A = \mathrm{Id} : R \to R$ die Identität. Wir berechnen $\mathrm{ev}^\phi_{\mathrm{Id}}(a_m X^m) \in \mathrm{Abb}(R, R)$. Sei dazu $b \in R$:
$$(\mathrm{ev}^\phi_{\mathrm{Id}}(a_m X^m))(b) = (\phi(a_m)\underbrace{\mathrm{Id} \cdot \ldots \cdot \mathrm{Id}}_{m-\text{mal}})(b) = a_m \underbrace{b \cdot \ldots \cdot b}_{m-\text{mal}}) = \widehat{a_m X^m}(b).$$
Und deswegen gilt für alle Polynome $P \in R[X]$
$$\mathrm{ev}^\phi_{\mathrm{Id}}(P) = \widehat{P}.$$

Proposition 4.5. *Sei $\phi : R \to S$ ein Homomorphismus von Ringen, $A \in S$. Dann gilt für die oben definierte Einsetzungsabbildung $\mathrm{ev}^\phi_A : R[X] \to S$:*

(a) $\mathrm{ev}^\phi_A|_R = \phi$, *insbesondere* $\mathrm{ev}^\phi_A(1_R) = 1_S$,
(b) $\mathrm{ev}^\phi_A(X) = A$,
(c) $\mathrm{ev}^\phi_A(P + Q) = \mathrm{ev}^\phi_A(P) + \mathrm{ev}^\phi_A(Q)$ *für alle* $P, Q \in R[X]$,
(d) ev^ϕ_A *ist ein Homomorphismus von Ringen, gdw für alle* $r \in R$ *gilt* $\phi(r)A = A\phi(r)$.

Beispiele. (Fortsetzung)
In den Beispielen (1)–(3) und (5)–(7) ist der Zielring S kommutativ, deswegen gilt dann für alle $r \in R$: $\phi(r)A = A\phi(r)$. In Beispiel (4) gilt für alle $r \in R$ und alle $A \in \mathrm{Mat}(n,n;R)$

$$\phi(r)A = (r\mathbb{1}_n)A = rA\mathbb{1}_n = A(r\mathbb{1}_n) = A\phi(r).$$

Somit ist in allen obigen Beispielen ev_A^ϕ ein Ringhomomorphismus.

Beweis der Proposition. (a) und (b) sind offensichtlich.

Für (c) schreiben wir $P = \sum_{i=0}^m a_i X^i$ und $Q = \sum_{i=0}^m b_i X^i$, $M = \max\{\deg P, \deg Q\}$. Dann gilt

$$\begin{aligned}
\mathrm{ev}_A^\phi(P+Q) &= \mathrm{ev}_A^\phi\Big(\sum_{i=0}^m (a_i+b_i)X^i\Big) \\
&= \sum_{i=0}^m \phi(a_i+b_i)A^i \\
&= \sum_{i=0}^m \phi(a_i)A^i + \sum_{i=0}^m \phi(a_i)A^i \\
&= \mathrm{ev}_A^\phi(P) + \mathrm{ev}_A^\phi(Q)
\end{aligned}$$

Für (d) schreiben wir $P = \sum_{i=0}^n a_i X^i$ und $Q = \sum_{i=0}^m b_i X^i$. Dann gilt

$$\begin{aligned}
\mathrm{ev}_A^\phi(PQ) &= \mathrm{ev}_A^\phi\Big(\sum_{i=0}^{n+m}\Big(\sum_{k+j=i} a_k b_j\Big)X^i\Big) \\
&= \sum_{i=0}^{n+m}\sum_{k+j=i} \phi(a_k b_j)A^{k+j} \\
&= \sum_{i=0}^{n+m}\sum_{k+j=i} \phi(a_k)\phi(b_j)A^k A^j \\
&\overset{*}{=} \sum_{i=0}^{n+m}\sum_{k+j=i} \phi(a_k)A^k\phi(b_j)A^j \\
&= \Big(\sum_{k=0}^n \phi(a_k)A^k\Big)\Big(\sum_{j=0}^m \phi(b_j)A^j\Big) \\
&= \mathrm{ev}_A^\phi(P)\ \mathrm{ev}_A^\phi(Q)
\end{aligned}$$

Hierbei benötigen wir bei dem Gleichheitszeichen $\overset{*}{=}$, dass A mit dem Bild von ϕ kommutiert. □

Wir haben unter anderem gezeigt:

PROPOSITION 4.6 (Universelle Eigenschaft des Polynomrings $R[X]$)**.** *Seien R und S Ringe (mit 1), R kommutativ, $A \in S$, und $\phi : R \to S$ ein Homomorphismus von Ringen. Dann gibt es einen eindeutig bestimmten Homomorphismus von Ringen $\mathrm{ev}_A^\phi : R[X] \to S$ so dass $\mathrm{ev}_A^\phi(X) = A$ und so dass das Diagramm*

$$\begin{tikzcd}
R \arrow[r] \arrow[dr] & R[X] \arrow[d] \\
 & S
\end{tikzcd}$$

kommutiert.

Bemerkung zu Beginn der dritten Vorlesung:

In den letzten Stunden haben wir den Polynomring $R[X]$ betrachtet, wobei R kommutativer Ring (mit Eins) ist. Der wichtigste Fall ist, wenn R ein Körper ist. Wenn R ein Körper ist, hat man sehr weitgehende Aussagen, u.a. gibt es eine Polynomdivision mit Rest, siehe unten. Andere Aussagen wiederum gelten auch unter der Voraussetzung, wenn R ein etwas allgemeinerer kommutativer Ring ist. Um zu erklären, wieso es wichtig ist, auch Ringe zuzulassen, die kein Körper sind, gebe ich ein Beispiel: Den Ring der reellen Polynome in 2 Variablen X und Y definiert man als $(\mathbb{R}[X])[Y]$, d.h. man startet mit dem Körper $\mathbb{R}$, geht dann in einem ersten Schritt über zum Polynomring über dem Ring $\mathbb{R}$, den wir mit $\mathbb{R}[X]$ notieren, und dann in einem zweiten Schritt betrachten wir Polynome über dem Ring $\mathbb{R}[X]$, dessen Unbekannte wir mit Y bezeichnen. man zeigt, dass $\mathbb{R}[X])[Y]$ und $\mathbb{R}[Y])[X]$ isomorphe Ringe sind, und nennt ihn. $\mathbb{R}[X,Y]$. Man kann zeigen, dass auch in diesem Ring eine bis auf Einheiten eindeutige Primfaktorzerlegung existiert. Es würde aber zu weit führen, dies alles in diesem Semester zu machen. Wir wollen deswegen annehmen, dass R ein Körper ist, wenn dies die Aussagen oder Beweise vereinfacht, und bei anderen Aussagen beliebige kommutative Ringe (mit 1) zulassen.

5. Polynomdivision

In diesem Abschnitt sei K immer ein Körper

PROPOSITION 5.1 (Polynomdivision)**.** *Seien $P, Q \in K[X], Q \neq 0$.*
Dann gibt es (eindeutige) $S, T \in K[X]$, so dass $P = QS + T$ mit $deg(T) < deg(Q)$.

Beweis der Existenz.

(a) $P = 0$, dann erfüllen $S := T := 0$ das Gewünschte.

(b) Wir setzen $k := \deg P - \deg Q$.
Wenn $k < 0$, dann $S := 0$, $T := P$.
Wenn $k \geq 0$, so zeigen wir die Existenz mit Induktion über k
<u>Induktionsanfang $k = 0$</u>: $n = \deg P = \deg Q$
$P = \sum_{i=0}^{n} a_i X^i, Q = \sum_{i=0}^{n} b_i X^i, a_n \neq 0, b_n \neq 0$
$s = \frac{a_n}{b_n}$ konstantes Polynom
$T = P - QS = \sum_{i=0}^{n}(a_i - \frac{a_n}{b_n} b_i) X^i = \sum_{i=0}^{n-1}(a_i - \frac{a_n}{b_n} b_i) X^i$
$\deg T \leq n - 1 < \deg Q$

<u>Induktionsschritt von $k-1$ nach k</u>:
$n = \deg Q$
$P = \sum_{i=0}^{n+k} a_i X^i, a_{n+k} \neq 0$
$Q = \sum_{i=0}^{n} b_i X^i, b_n \neq 0$
Setze $\widehat{S} := \frac{a_{n+k}}{b_n} X^k$

$$\begin{aligned}
\widehat{T} &= P - \widehat{S}Q \\
&= \sum_{i=0}^{n+k} a_i X^i - \sum_{i=0}^{n} \frac{a_{n+k}}{b_n} b_i X^i X^k \\
&= P - \widehat{S}Q = \sum_{i=0}^{n+k} a_i X^i - \sum_{i=k}^{n+k} \frac{a_{n+k}}{b_n} b_{i-k} X^i \\
&= \sum_{i=k}^{n+k} \underbrace{\left(a_i - \frac{a_{n+k}}{b_n} b_{i-k}\right)}_{\substack{\text{für } i=n+k: \\ a_{n+k} - b_n \frac{a_{n+k}}{b_n} = 0}} X^i + \sum_{i=0}^{k-1} a_i X^i
\end{aligned}$$

Also $\deg \widehat{T} \leq n + k - 1$.
Nach Induktionsvorraussetzung existieren $\tilde{S}$ und $\tilde{T}$, so dass

$$\widehat{T} = Q\tilde{S} + \tilde{T}, \qquad \deg \tilde{T} < \deg Q$$

Also: $P = Q\widehat{S} + \widehat{T} = Q(\widehat{S} + \tilde{S}) + \tilde{T}$, $\deg \tilde{T} < \deg Q$
$S := \widehat{S} + \tilde{S}$, $T := \tilde{T}$. Die Existenz folgt.

Beweis der Eindeutigkeit. Wird dem Leser als Übungsaufgabe überlassen. □

Beispiel. Polynom-Division
$P = X^4 + 2X^3 + X^2 + 2X + 1$
$Q = X^2 + X + 1$

$$
\begin{array}{l}
(X^4 + 2X^3 + X^2 + 2X + 1) = (X^2 + X + 1)(1 \cdot X^2 + 1 \cdot X - 1) + (2X + 2) \\
\underline{-X^4 - X^3 - X^2} \\
\qquad\quad X^3 + 0 + 2X \\
\qquad \underline{-X^3 - X^2 - X^1} \\
\qquad\qquad - X^2 + X + 1 \\
\qquad\qquad \underline{+X^2 + X^1 + 1} \\
\qquad\qquad\qquad 2X + 2
\end{array}
$$

Definition 5.2. $P \in K[X], \alpha \in K$ heißt Nullstelle von P, falls $P(\alpha) = 0$.

Proposition 5.3. *Sei $P \in K[X]$, $\alpha \in K$. Dann ist α eine Nullstelle genau dann, wenn*

$$\exists Q \in K[X] : Q(X - \alpha) = P$$

Beweis. $\Leftarrow$: Sei $P = Q(X - \alpha)$. Dann gilt $P(\alpha) = Q(\alpha)(\alpha - \alpha) = 0$
$\Rightarrow$: Sei $P(\alpha) = 0$
Dividiere P durch $(X - \alpha)$
$P = S(X - \alpha) + T$, $\deg T < \deg(X - \alpha) = 1$
$\Rightarrow \exists c \in K : T = c$
$0 = P(\alpha) = S(\alpha) \underbrace{(\alpha - \alpha)}_{=0} + \underbrace{T(\alpha)}_{=c} = c$
$\Rightarrow T = 0 \in K[X]$ □

6. Ideale und Hauptideale

Sei R immer ein Ring.

Definition 6.1. $I \in R$ heißt Ideal, falls

(1) $(I, +)$ ist eine Untergruppe von $(R, +)$
(2) $x \cdot a \in I \quad \forall x \in R \ \forall a \in I$
(3) $a \cdot x \in I \quad \forall x \in R \ \forall a \in I$

Man schreibt dann kurz $I \triangleleft R$.
Insbesondere ist I abgeschlossen unter Addition, unter der Abbildung $x \mapsto -x$ und der Multiplikation.

Beispiele.

(1) $R = \mathbb{Z}, k \in \mathbb{Z}$
(2) $R = \mathbb{R}[X]$
$I := \{\sum_{i=1}^{m} a_i X^i | a_i \in \mathbb{R}, m \in \mathbb{N}\ \} \triangleleft \mathbb{R}[X]$
(3) Sei $I \triangleleft R$
$I = R \Leftrightarrow 1 \in I$

Lemma 6.2. *Sei $f : R \to S$ ein Homomorphismus von Ringen. Dann ist* $\text{Bild}f$ *ein Unterring und*
$Kernf$ *ist ein Ideal.*

Beweis. $\text{Bild}f$ ist Unterring :

- $f(0) = 0 \in \text{Bild}f \Rightarrow \text{Bild}f \neq \emptyset$
- $\forall a, b \in \text{Bild}f : \exists s, t \in R : \quad f(s) = a, f(t) = b$
  $\underbrace{f(s+t)}_{\in \text{Bild}f} = f(s) + f(t) = a + b$
- $\underbrace{f(-s)}_{\in \text{Bild}f} = -a$
- $\forall a, b \in \text{Bild}f : \exists s, t \in R : \quad f(s) = a, f(t) = b$
  $\underbrace{f(st)}_{\in \text{Bild}f} = f(s)f(t) = ab$
- $f(1_R) = 1_S$

$\Rightarrow \text{Bild}f$ ist Unterring

Beweis. Kern f ist Ideal:

- $\forall a, b \in \text{Kern } f : \quad f(a-b) = f(a) - f(b) = 0 - 0 = 0$
  $\Rightarrow a - b \in \text{Kern } f$. Außerdem ist $0 \in \text{Kern } f$. Also ist $(\text{Kern } f, +)$ eine Untergruppe von $(R, +)$.
- $\forall x \in R, \forall a \in \text{Kern } f : \ f(xa) = f(x)\underbrace{f(a)}_{=0} = 0$
  $\Rightarrow xa \in \text{Kern } f$
- Analog : $ax \in \text{Kern } f$

$\Rightarrow$ Kern f ist Ideal □

Lemma 6.3.
Sei $(\mathfrak{a}_i)_{i \in I}$ eine Familie von Idealen in R, $I \neq \emptyset$.
Dann ist $\bigcap_{i \in I} \mathfrak{a}_i$ ein Ideal.

Beweis.

- Der Schnitt von Untergruppen ist wieder eine Untergruppe (siehe Vektorraumtheorie).
- Sei $a \in \bigcap_{i \in I} \mathfrak{a}_i, x \in R$
  $\Rightarrow \forall i \in I : \ a \in \mathfrak{a}_i, x \in R \underbrace{\Rightarrow}_{\mathfrak{a}_i \text{Ideal}} ax, xa \in \mathfrak{a}_i \Rightarrow ax, xa \in \bigcap_{i \in I} \mathfrak{a}_i$ □

Definition 6.4. Sei $M \subseteq R$, $(M) = \bigcap_{M \subset \mathfrak{a} \triangleleft R} \mathfrak{a} \triangleleft R$ das kleinste Ideal von R, das M enthält.
(M) heißt das von M erzeugte Ideal in R. M heißt Erzeugendensystem von (M). Falls M endlich ist, $M = \{a_1, ..., a_n\}$, dann schreibt man $(a_1, ..., a_n) = (\{a_1, ..., a_n\})$
Ein Ideal $a \triangleleft R$ heißt
- endlich erzeugt, falls, $\exists a_1, .., a_n \in \mathfrak{a}$ mit $\mathfrak{a} = (a_1, .., a_n)$
- Hauptideal, falls $\exists a \in \mathfrak{a}$ mit $\mathfrak{a} = (a)$

Bemerkung 6.5. Sei R kommutativ. Dann gilt $b \in R$, $(b) = \{b \cdot r | r \in R\}$
$b_1, ..., b_n \in R$, $(b_1, ..., b_n) = \{\sum_{i=1}^{n} b_i r_i | r_i \in R\}$

Definition 6.6. Ein Ring R heißt Hauptidealring (HIR), falls

(a) R ist ein Integritätsring
(b) Jedes Ideal von R sei ein Hauptideal

Ziel: Beweisen, dass $\mathbb{Z}$ und $K[X]$ HIR sind

Definition 6.7. Ein euklidischer Ring ist ein Integritätsring mit einer Abbildung

$$d : R \setminus \{0\} \to \mathbb{N}_0,$$

so dass $\forall p, q \in R$, $q \neq 0$ Elemente $s, t \in R$ existieren mit $p = qs + t$ und $\{t = 0$ oder $d(t) < d(q)\}$.

Beispiele. Euklidische Ringe sind:

(1) $R = \mathbb{Z}, d : \mathbb{Z} \to \mathbb{N}_0, z \mapsto |z|$
(2) Proposition 5.1 besagt, dass $(R = \mathbb{K}, d := \deg)$ ein euklidischer Ring ist.

Proposition 6.8. *Alle euklidischen Ringe sind Hauptidealringe.*

Beweis. Sei (R, d) ein euklidischer Ring, $\mathfrak{a} \triangleleft R$.
Falls $\mathfrak{a} = \{0\}$, dann $\mathfrak{a} = (0)$.
Sei $\mathfrak{a} \cap (R \setminus \{0\}) \neq \emptyset$.
Wir setzen $n := \min\{d(x) | x \in \mathfrak{a} \cap (R \setminus \{0\})\}$.
Wähle $b \in \mathfrak{a} \cap (R \setminus \{0\})$, so dass $d(b) = n$.

<u>Beh.:</u> $(b) = \mathfrak{a}$, denn

(1) $b \in \mathfrak{a} \Rightarrow (b) \subseteq \mathfrak{a}$
(2) Sei $v \in \mathfrak{a}$:
Dividiere v durch b: $v = sb + t$ mit $t = 0$ oder $d(t) < d(s)$. Somit haben wir

$$t = \underbrace{v}_{\in \mathfrak{a}} - \underbrace{s}_{\in R} \underbrace{b}_{\in \mathfrak{a}} \in \mathfrak{a} \Rightarrow d(t) = 0 \text{ oder } d(t) \geq d(q)$$

Also $t = 0$. Also ist $v = sb \in (b) \Rightarrow \mathfrak{a}$ Hauptideal. Also ist R ein Hauptidealring. $\square$

Anwendung. Zu Beginn der heutigen Vorlesung wollen wir kurz motivieren, wieso wir Hauptidealringe studieren. Wir betrachten dazu folgende Anwendung.

Sei $K = R$ ein Körper, $A \in S = Mat(n, n; K)$. Wir wählen den Homomorphismus von Ringen $\varphi : K \to S$, $a \mapsto a \cdot 1_n$. Nach Proposition 4.6 existiert dann ein Homomorphismus $ev_A^{\varphi} : K[X] \to S, P \mapsto P(A)$, so dass das Diagramm

$$\begin{tikzcd}
K \arrow[r] \arrow[dr, "\varphi"] & K[X] \arrow[d, "\mathrm{ev}_A^{\varphi}"] \\
& \mathrm{Mat}(n, n; K)
\end{tikzcd}$$

kommutiert.

Dann ist $\ker(ev_A^{\varphi})$ ein Ideal in $K[X]$, also ein Hauptideal, das heißt es existiert ein Polynom $P_0 \in K[X]$, so dass $(P_0) = \ker(ev_A^{\varphi})$. Dabei ist $(P_0) = \{P_0 Q | Q \in K[X]\}$, $P_0 = a_0 + a_1 X + ... + a_m X^m$, $a_m \neq 0$, Wir setzen $P_A = \frac{1}{a_m} P_0 = \frac{a_0}{a_m} + ... + 1 \cdot X^m$, $(P_A) = (P_0) = \ker(ev_A^{\varphi})$ heißt *das* Minimalpolynom von A. Es ist das „kleinste“ nicht-triviale Polynom mit $P_A(A) = 0$.

7. Teiler, irreduzible Elemente, Primelemente

In diesem Abschnitt sind R, S Integritätsringe.

$$R^* = \{\text{invertierbare Elemente in } R\} = \{\text{Einheiten von } R\},$$

Also zum Beispiel $(\mathbb{Z})^* = \{\pm 1\}$ und $(\mathbb{R}[X])^* = \mathbb{R}\backslash\{0\}$.

Definition 7.1. $a, b \in R, a \mid b :\Leftrightarrow a$ teilt $b :\Leftrightarrow \exists c \in R : b = ac$.
Sprich: „b ist Vielfaches von a“ oder „a teilt b“ oder „a ist Teiler von “.

Beispiele.

- $7 \mid 14$ in $\mathbb{Z}$
- $2 \nmid 3$ in $\mathbb{Z}$, $2 \mid 3$ in $\mathbb{R}$
- $(X - 2) \mid X^2 - 4 = (X + 2)(X - 2)$ in $R[X]$
- $r \mid 0 \quad \forall r \in R$, $1 \mid r \quad \forall r \in R$

Definition 7.2. Seien $a, b \in R\backslash\{0\}$.

(1) Es heißen a und b assoziiert $:\Leftrightarrow a \sim b \Leftrightarrow a \mid b$ und $b \mid a :\Leftrightarrow \exists c \in R^* : b = ac$. Die Relation „assoziiert“ ist eine Äquivalenzrelation.
(2) a ist echter Teiler von b, genau dann wenn
    (a) $a \mid b$ und
    (b) $a \notin R^*$ und
    (c) $a \nsim b$
(3) a ist irreduzibel, genau dann wenn
    (a) $a \notin R^*$ und
    (b) a hat keine echten Teiler
    Dies wiederum gilt genau dann, wenn
    (a) $a \notin R^*$ und
    (b') a hat keine echten Teiler.
(4) a ist reduzibel $\Leftrightarrow \exists b, c \in R \backslash (R^* \cup \{0\})$, so dass $a = bc$.
(5) a prim (in R), genau dann wenn
    (a) $a \notin R^*$
    (b) $\forall b, c \in R$ gilt: $a \mid bc \Rightarrow a \mid b \vee a \mid c$

Man zeigt leicht, dass ein $a \in R \setminus (R^* \cup \{0\})$ genau dann reduzibel ist, wenn es nicht irrdezibel ist.

Insbesondere haben wir also

$$R = \{0\} \dot{\cup} R^* \dot{\cup} \{\text{reduzible Elmte}\} \dot{\cup} \{\text{irreduzible Elmte}\}$$

Beispiele.

(1) $R = \mathbb{Z}$, $5 \sim -5$
    2 ist echter Teiler von 12.
    $2, 3, 5, -2, -3, -5$ prim und irreduzibel.
(2) R Körper, $r, s \in R^* \Rightarrow r \sim s$
(3) K Körper, $R = K[X]$, $R^* = K^* = \{\text{konstante Polynome} \neq 0\}$. Es gilt dann für alle $\alpha \in K$, dass $(X - \alpha)$ irreduzibel in $K[X]$ ist.
    Um dies zu begründen, nehmen wir an, dass $X - \alpha = PQ$, $P, Q \in K[X] \backslash \{0\}$, $1 = \deg(PQ) = \deg(P) + \deg(Q)$
    $\Rightarrow \deg(P) = 0$ oder $\deg(Q) = 0$
    $\Rightarrow P \in (K[X])^*$ oder $Q \in (K[X])^*$.
    Also ist $(X - \alpha)$ irreduzibel.
(4) $\forall P \in K[X], K$ Körper. $(X - \alpha) \mid P \Leftrightarrow \alpha$ Nullstelle von P.
(5) K Körper, $P \in K[X]$, $\deg(P) \in \{2, 3\}$. Dann gilt:

$$\exists \alpha \in K \text{ mit } P(\alpha) = 0 \Leftrightarrow P \text{ reduzibel.}$$

Begründung.

(a) Falls es $\alpha \in K$ gibt mit $P(\alpha) = 0 \Rightarrow \exists Q \in K[X]$ mit $P = (X - \alpha)Q \Rightarrow P$ reduzibel ($\deg(X - \alpha) = 1$, $\deg(Q) \in \{1, 2\}$).
(b) Sei P reduzibel $\Rightarrow \exists Q, T \in K[X]\backslash K$, $P = QT$, $\deg(P) \leq 3$, $\deg(Q) \geq 1$, $\deg(T) \geq 1$. Ohne Beschränkung der Allgemeinheit können wir annehmen: $\deg(Q) = 1 \Rightarrow Q = aX + b$ mit $a \neq 0$, $Q(\alpha) = 0$, $\alpha = -\frac{b}{a} \in K \Rightarrow P(\alpha) = 0$

Lemma 7.3. *Sei R ein Integritätsring, $a \in R$. Aus a prim folgt, dass a irreduzibel ist.*

Beweis.

(1) a prim $\Rightarrow a \notin R^* \cup \{0\}$
(2) Falls a reduzibel ist, so $\exists b, c \in R\backslash R^* : a = bc$. Offensichtlich $a \mid a = bc$. Wir behaupten nun $a \nmid b$. Um diese Behauptung zu zeigen, nehmen wir an $a \mid b$. Daraus folgt $\exists d \in R$, so dass $b = ad \Rightarrow a = bc = adc \Rightarrow a(1 - dc) = 0 \Rightarrow dc = 1 \Rightarrow c \in R^* \Rightarrow$ Widerspruch.
Analog zeigen wir $a \nmid c$.
$\Rightarrow a$ ist nicht prim.

□

Lemma 7.4. *Sei $a \in R, (a) := \{ar | r \in R\}, 1 \in (a), (1) \subseteq (a)$.*

(1) a invertierbar $\Leftrightarrow (a) = R$
(2) $a \mid b \Leftrightarrow (b) \subseteq (a)$
(3) a ist echter Teiler von $b \Leftrightarrow (b) \subsetneqq (a) und (a) \neq R$
(4) $a \sim b \Leftrightarrow (b) = (a)$
(5) Sei $p \in R\backslash(R^* \cup \{0\})$. p irreduzibel $\Leftrightarrow$ es existiert kein Hauptideal $(b) \subsetneqq R$ mit $(p) \subsetneqq (b)$.

Begrüdung.

(1) a invertierbar $\Leftrightarrow 1 \in (a) \Leftrightarrow (a) = R$
(2) $a \mid b \Leftrightarrow \exists r \in R, b = ra \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$
(3) a ist echter Teiler von b, genau dann wenn $a \mid b, b \nmid a$ und $a \notin R^* \cup \{0\}$. Dies gilt genau dann wenn $(b) \subsetneqq (a), (a) \neq R$ ist.

Definition 7.5. Ein Polynom $a_0 + a_1X + ... + a_mX^m, a_m \neq 0$ heit *normiert*, falls $a_m = 1$.

Korollar 7.6. *Sei K ein Körper, $\{0\} \neq \mathfrak{a} \lhd K[X]$. Dann existiert ein eindeutiges* normiertes *Polynom $P_0 \in K[X]$, so dass $(P_0) = \mathfrak{a}$.*

Beweis. Da $K[X]$ ein Hauptidealring ist, gibt es ein $P_1 \in K[X]$ mit $(P_1) = \mathfrak{a}, P_1 \neq 0$. $P_1 = a_0 + a_1X + ... + a_mX^m$, $a_m \neq 0$, $P_0 = \frac{a_0}{a_m} + \frac{a_1}{a_m}X + ... + 1 \cdot X^m$ normiert.
$P_0 \sim P_1 \Rightarrow (P_0) = (P_1) = \mathfrak{a} \rightsquigarrow$ Existenz von P_0. Sei $Q \in K[X]$ normiert $(Q) = \mathfrak{a} = (P_0) \Rightarrow Q \sim P \Rightarrow \exists r \in K^* : Q = rP \Rightarrow \deg(Q) = \deg(P)$, $Q = b_0 + ... + 1 \cdot X^m \Rightarrow r \cdot P = r\frac{a_0}{a_m} + ... + r \cdot 1 \cdot X^m$, $r = r \cdot 1 = 1 \Rightarrow Q = P_0 \rightsquigarrow$ Eindeutigkeit. □

Größter gemeinsamer Teiler (ggT) und kleinstes gemeinsames Vielfaches (kgV). Sei R ein Hauptidealring. $a, b \in R$.

Definition 7.7.

(1) c ist *ein* kgV von a und b, genau dann wenn $(c) = (a) \cap (b)$.
    Beispiel. $X^4 + X^3 - X - 1$ ist kgV von $(X^3 - 1)$ und $(X^2 - 1)$.
(2) d ist *ein* ggT von a und b, wenn $(d) = (a, b), (a, b) = \{ar_1 + br_2 | r_1, r_2 \in R\}$.
    Beispiel. $R = \mathbb{Z}, a = 6, b = 4 \Leftrightarrow (a, b) = \{6r_1 + 4r_2 | r_1, r_2 \in R\} = 2\mathbb{Z} = (2) = (-2)$.
    Also sind 2 und -2 ggTs von 4 und 6.

VORLESUNG am 28.4.

KOROLLAR 7.8. *Sei $P \in K[X] \setminus \{0\}$ und $\alpha_1, \cdots, \alpha_k$ seien Nullstellen mit Multiplizität $m_1, \cdots, m_k$, dann gilt*

$$\sum_{i=1}^{k} m_i \leq \deg P$$

KOROLLAR 7.9. *K sei ein unendlicher Körper. Seien $P, Q \in K[X]$. Dann gilt*

$$P = Q \Leftrightarrow P(\alpha) = Q(\alpha), \forall \alpha \in K$$

Dies bedeutet, dass zwei Polynome mit Koeffizienten in einem unendlichen Körper genau dann gleich sind, wenn die assoziierten Polynomfunktionen gleich sind. (Bsp. $\mathbb{R}[X], \mathbb{Q}[X]$)

Beweis des Korollars. „$\Rightarrow$“ Ist klar.

„$\Leftarrow$“ Sei $P(\alpha) = Q(\alpha), \forall \alpha \in K$.

Definiere S als $S := P - Q$. Dann sind alle $\alpha \in K$ Nullstellen von S. Da K unendlich ist, folgt dass S unendlich viele Nullstellen hat. Also ist $S = 0$. □

8. Algebraische Abgeschlossenheit

DEFINITION 8.1. Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes $P \in K[X]$ mit $\deg P \geq 1$ mindestens eine Nullstelle besitzt.

Es gilt dann sogar: Zu jedem $P \in K[X] \setminus \{0\}$ gibt es ein $r \in K^*$ und $\alpha_1, \cdots, \alpha_m \in K$ mit

$$P = r(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_m)$$

SATZ 8.2. *Zu jedem Körper L gibt es einen algebraisch abgeschlossenen Körper K, der L als Unterkörper enthält.*

SATZ 8.3. *Fundamentalsatz der Algebra*

$\mathbb{C}$ ist algebraisch abgeschlossen.

Den Beweis dieser Sätze werden Sie später im Studium kennen lernen.

Folgerung. In $\mathbb{C}[X]$ gilt $\forall P \in \mathbb{C}[X]$

$$P \text{ irreduzibel} \Leftrightarrow P \text{prim} \Leftrightarrow \deg P = 1$$

Die Berechnung der Nullstellen von Polynomen bis zu einem Grad von 4 ist durch Formeln möglich. Bei Polynomen von Grad ≥ 5 ist dies im allgemeinen unmöglich (siehe Algebra 1, Galoistheorie).

9. Reelle Polynome

Da die reellen Zahlen nicht algebraisch abgeschlossen sind, finden sich nicht konstante Polynome, die in den reellen Zahlen keine Nullstelle besitzen, so z.B. $P = X^2 + 1$. Wenn man aber $\mathbb{R}[X]$ als Unterring von $\mathbb{C}[X]$ betrachtet, lässt sich eine Zerlegung für reelle Polynome vom Grad ≥ 3 in Polynome vom Grad 1 und 2 herleiten.

Wiederholung. Sei $P = \sum_{j=0}^{m} a_j X^j \in \mathbb{C}[X]$.

Dann ist $\overline{P} := \sum_{j=0}^{m} \overline{a_j} X^j$ und es gilt

- $\overline{P}(\overline{z}) = \overline{P(z)}$
- $\mathbb{R}[X] \subseteq \mathbb{C}[X]$
- $P \in \mathbb{R}[X] \Leftrightarrow P = \overline{P}$

Sei nun $P \in \mathbb{R}[X], \deg P \geq 1$.

Als komplexes Polynom kann P in Primfaktoren vom Grad 1 zerlegt werden. Mit $m = \deg P$ und $\alpha_1, \cdots, \alpha_m \in \mathbb{C}$ ist

$$P = r(X - \alpha_1) \cdots (X - \alpha_m) = \overline{r}(X - \overline{\alpha}_1) \cdots (X - \overline{\alpha}_m)$$

Die Primfaktorzerlegung ist bis auf die Reihenfolge eindeutig. Also ist $r = \overline{r}$ und $\exists \sigma \in S_n$, so dass

$$\alpha_j = \overline{\alpha_{\sigma(j)}}$$

für alle $j \in \{1, \ldots, n\}$. Wir ordnen nun die faktoren um: Wir schieben alle reellen Wurzeln $\alpha_j \in \mathbb{R}$ nach rechts, die imaginaären (=nicht-reellen) Wurzeln nach links. Wenn $\alpha \in \mathbb{C} \setminus \mathbb{R}$ eine Wurzel ist, dann auch $\bar{\alpha}$ und zwar mit derselben Vielfachheit. Wir ordnen jeweils so eine Worzel $\alpha \in \mathbb{C} \setminus \mathbb{R}$ mit $\bar{\alpha}$ zusammen, und erhalten $\beta_j \in \mathbb{C} \setminus \mathbb{R}, \gamma_j \in \mathbb{R}$ mit

$$P = r \quad \underbrace{(X - \beta_1)(X - \overline{\beta}_1)}_{(X^2 - 2(\mathbf{Re}(\beta_1)X + |\beta_1|^2) \in \mathbb{R}[X]} \quad (X - \beta_2)(X - \overline{\beta}_2) \cdots (X - \beta_{r_0})(X - \overline{\beta}_{r_0})(X - \gamma_1) \cdots (X - \gamma_{m-2r_0}),$$

wobei $2r_0$ die Anzahl der imaginären Wurzeln (mit Vielfachheit gezählt) ist.

Folgerung. Sei $P \in \mathbb{R}[X], \deg P \geq 3$. Dann ist P reduzibel.

Theorem 9.1. *Ein Polynom $P \in \mathbb{R}[X]$ ist irreduzibel genau dann, wenn*

(1) $\deg P = 1$ *oder*
(2) $\deg P = 2$ *und P ist von der Form $aX^2 + bX^2 + c$ mit $4ac > b^2$*

Beweis.

(1) $\deg P = 1 \Rightarrow P$ ist irreduzibel.
(2) $\deg P = 2$. Wir schreiben $P = aX^2 + bX + c$. Falls $4ac \leq b^2$, dann sind

$$\alpha_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Nullstellen von P. Also ist P reduzibel.

Sei nun $4ac > b^2$. Angenommen P ist reduzibel, d.h. $P = S_1 \cdot S_2, \deg S_1 = \deg S_2 = 1$ mit $S_1 = p_1X + q_1$ und $S_2 = p_2X + q_2$. Dann folgt

$$P = S_1 \cdot S_2 = p_1p_2X^2 + (p_1q_2 + p_2q_1)X + q_1q_2$$
$$a = p_1p_2 \qquad b = p_1q_2 + p_2q_1 \qquad c = q_1q_2$$

$$\Rightarrow b^2 = (p_1q_2 + p_2q_1)^2 = \underbrace{(p_1q_2 - q_1p_2)^2}_{\geq 0} + 4\underbrace{p_1p_2}_{a}\underbrace{q_1q_2}_{c} \geq 4ac$$

In Widerspruch zur Voraussetzung $4ac < b^2$.

(3) $\deg P \geq 3 \Rightarrow P$ reduzibel.

$\square$

10. Das charakteristische Polynom

Idee. Sei K ein Körper und $A \in \mathrm{Mat}(n,n;K)$. Dann soll das charakteristische Polynom χ_A von A definiert sein durch

$$\chi_A := \det_n(X\mathbb{1}_n - A) \qquad \chi_A \in K[X]$$

Dabei tritt allerdings das Problem auf, dass $X\mathbb{1}_n - A \in \mathrm{Mat}(n,n;K)[X]$, und es stellt sich die Frage, wie die Determinante für Polynoms über dem Matrizenring durch $\det_n$ definiert werden soll.

Bemerkung 10.1.

$$\mathrm{ev}_{\begin{pmatrix} X & & 0 \\ & \ddots & \\ 0 & & X \end{pmatrix}} : (\mathrm{Mat}(n,n;K))[X] \rightarrow \mathrm{Mat}(n,n;K[X])$$

$$\sum_{i=0}^{m} A_iX \mapsto \sum_{i=0}^{m} A_i \begin{pmatrix} X & & 0 \\ & \ddots & \\ 0 & & X \end{pmatrix}^i$$

ist ein Homomorphismus von Ringen und bijektiv (wie in der Vorlesung am 08.05 gezeigt). Dieser Homomorphismus ist eine Variation der Einsetzungsabbildung.

Achtung. Der Ring $\mathrm{Mat}(n,n;K)$ ist nicht kommutativ. Da aber X und $\begin{pmatrix} X & & 0 \\ & \ddots & \\ 0 & & X \end{pmatrix} = X\mathbb{1}_n$ mit allen A kommutieren geht der Beweis von $\mathrm{ev}(P\cdot Q) = ev(P)\cdot \mathrm{ev}(Q)$ genauso wie für kommutative Ringe.

Wir identifizieren ab sofort $(\mathrm{Mat}(n,n;K))[X]$ mit seinem Bild.

Einschub. Determinante in $\mathrm{Mat}(n,n;R)$

Sei R ein kommutativer Ring mit 1, $A = (a_{ij})_{ij} \in \mathrm{Mat}(n,n;R)$.

Wir definieren

$$\det_n A := \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}$$

Es gilt ebenfalls

$$\det_n(A \cdot B) = \det_n(A) \cdot \det_n(B)$$

Auch die Cramer'sche Regel gilt

$$A \cdot A^{ad} = A^{ad} \cdot A = (\det A)\mathbb{1}_n$$

Also ist A invertierbar $\Leftrightarrow \det A \in \mathbb{R}^*$

Beispiel.
(1) Sei $R = \mathbb{Z}$, $A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$, $\det A = 1 \in \{\pm 1\} = (\mathbb{Z})^* \Rightarrow A$ invertierbar in $\mathrm{Mat}(2,2;\mathbb{Z})$
(2) $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ ist nicht invertierbar in $\mathrm{Mat}(2,2;\mathbb{Z})$, da 2 nicht invertierbar in $\mathbb{Z}$.

Definition 10.2. Sei K ein Körper, $A \in \mathrm{Mat}(n,n;K)$. Dann ist das *charakteristische Polynom* definiert durch

$$\chi_A := \det_n(X \cdot \mathbb{1}_n - A)$$

Eigenschaften. Seien $A, B \in \mathrm{Mat}(n,n;K)$

(1) χ_A ist ein normiertes Polynom vom Grad n.
(2) Sind A und B ähnlich, so gilt $\chi_A = \chi_B$.
(3) $\chi_{AB} = \chi_{BA}$
(4) $\chi_{A^T} = \chi_A$
(5) $\chi_A(0) = (-1)^n \det A$

Beweis. $A = (a_{ij})_{ij}$ $\quad X\mathbb{1}_n - A = (\delta_{ij}X - a_{ij})_{ij}$

(1)

$$\chi_A = \det(X\mathbb{1}_n - A) = \sum_{\sigma \in S_n} \left(\operatorname{sgn}\sigma \prod_{j=1}^{n} (\delta_{\sigma(j)j}X - a_{\sigma(j)j}) \right)$$

- **$\sigma \neq$ id:**
$$\deg\left(\prod_{j=1}^{n}(\delta_{\sigma(j)j}X - a_{\sigma(j)j}\right) \leq n-2$$
- **$\sigma =$ id:**
$$\prod_{j=1}^{n}(\delta_{jj}X - a_{jj}) = (X-a_{11})(X-a_{22})\cdots = X^n - \sum_{j=1}^{n} a_{jj}\cdot X^{n-1} + \cdots$$
$$\Rightarrow \chi_A = X^n - \sum_{j=1}^{n} a_{jj}X^{n-1} + \cdots$$

(2) Beweis am 08.05.
(3) am 08.05.
(4)
$$\chi_{A^T} = \det(X\mathbb{1}_n - A^T) = \det((X\mathbb{1}_n - A)^T) = det(X\mathbb{1}_n - A) = \chi_A$$
(5)
$$\chi_A(0) = \det(0\mathbb{1}_n - A) = \det(-A) = (-1)^n \det A$$

□

VORLESUNG am 8.5.

11. Charakteristisches Polynom von Endomorphismen

Sei in diesem Abschnitt V ein n-dimensionaler Vektorraum über dem Körper K. Sei ferner $f : V \to V$ ein Endomorphismus von Vektorräumen. Homomorphismen sind immer Homomorphismen von Vektorräumen.

Wir wählen eine Basis $(b_1, \ldots, b_n)$ von V, und setzen

$$A := \mathrm{Mat}_{(b_1,\ldots,b_n)}^{(b_1,\ldots,b_n)}(f).$$

Definition 11.1. Seien f und A wie oben. Wir definieren das charakteristische Polynom von f als

$$\chi_f := \chi_A.$$

Das charakteristische Polynom von f ist unabhängig von der Wahl der Basis. Denn ist $(c_1, \ldots, c_n) = (b_1, \ldots, b_n) \cdot M$ eine andere Basis von V, dann gilt

$$\mathrm{Mat}_{(c_1,\ldots,c_n)}^{(c_1,\ldots,c_n)}(f) := M^{-1}AM.$$

Wegen $\chi_{M^{-1}AM} = \chi_A$ ist somit die Definition von χ_f unabhängig von der Basis.

Analog definieren wir $\mathrm{Spur}(f) := \mathrm{Spur}(A)$. Es ist das Negative des Koeffizients von χ_A von Grad $n-1$ und deswegen auch unabhängig von der Wahl der Basis von V.

Lemma 11.2. *Sei $f : V \to V$ ein Homomorphismus, und $f' : V' \to V'$ die dazu duale Abbildung, dann gilt* $\mathrm{Spur}(f') = \mathrm{Spur}\, f$ *und* $\det f' = \det f$.

Beweis. Sei wieder $(b_1, \ldots, b_n)$ eine Basis von V und $b_1', \ldots, b_n')$ die dazu duale Basis von V'. Dann gilt

$$\mathrm{Mat}_{(b_1',\ldots,b_n')}^{(b_1',\ldots,b_n')}(f') = \left(\mathrm{Mat}_{(b_1,\ldots,b_n)}^{(b_1,\ldots,b_n)}(f)\right)^T.$$

Mit $\mathrm{Spur}\, A = \mathrm{Spur}\, A^T$ und $\det A = \det A^T$ folgt die Aussage. □

12. Das Minimalpolynom

Sei K ein Körper, $n \in \mathbb{N}$, $A \in \mathrm{Mat}(n, n; K)$.

Die Einsetzungsabbildung

$$\mathrm{ev}_A : K[X] \to \mathrm{Mat}(n, n; K), \qquad P \mapsto P(A)$$

ist ein Homomorphismus von Ringen. Der Kern

$$\mathrm{Kern}\ (\mathrm{ev}_A) := \{P \in K[X] \,|\, P(A) = 0\}$$

ist also ein Ideal in $K[X]$. Der Satz von Cayley-Hamilton besagt $\chi_A \in \mathrm{Kern}\ (\mathrm{ev}_A)$, insbesondere $\mathrm{Kern}\ (\mathrm{ev}_A) \neq \{0\}$.

Da $K[X]$ ein Hauptidealring ist, ist Kern (ev_A) ein Hauptideal. Es gibt also ein eindeutiges normiertes Polynom $\mu_A \in K[X]$ so dass Kern (ev_A) das von μ_A erzeugte Polynom ist. Wir nennen μ_A das Minimalpolynom von A.

Der Satz von Cayley-Hamilton besagt $\chi_A \in$ Kern (ev_A). Dies bedeutet dann $\mu_A|\chi_A$, u.a. $0 \leq \deg \mu_A \leq n$.

Um das Minimalpolynom einer Matrix A zu berechnen, bestimmt man zumeist das charakteristische Polynom χ_A. Man zerlegt dann χ_A in irreduzible Polynome, sagen wir

$$\chi_A = P_1^{k_1} \cdot \ldots \cdot P_r^{k_r}$$

und untersucht nun für alle Teiler von χ_A, ob sie im Kern von ev_A liegen. Der kleinste solche Teiler ist das Minimalpolynom.

Beispiele.

(1) Sei $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$. Dann ist $\chi_A = (X-2)^2$. Wegen $\mu_A|\chi_A$ gilt also $\mu_A = 1$, $\mu_A = (X-2)$ oder $\mu_A = \chi_A$. Wegen $\mathrm{ev}_A(1) = \mathbb{1}_2 \neq 0$ und $\mathrm{ev}_A(X-A) = 0$ gilt $\mu_A = (X-2)$.

(2) Ähnlich zeigt man für eine Diagonalmatrix

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix},$$

dass $\chi_D = (X-\lambda_1)^2(X-\lambda_2)$ und $\mu_D = (X-\lambda_1)(X-\lambda_2)$.

(3) Für $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ gilt $\chi_A = (X-1)^3$ und $\mu_A = (X-1)^2$.

Lemma 12.1. *Sind A und B ähnlich, so gilt $\mu_A = \mu_B$.*

Beweis. Wähle ein $M \in \mathrm{GL}(n,k)$, so dass $B = M^{-1}AM$. Dann gilt für $k \in \mathbb{N}_0$:

$$B^k = \underbrace{(M^{-1}AM)(M^{-1}AM)\cdots(M^{-1}AM)}_{k-\text{mal}} = M^{-1}A^kM.$$

Und somit gilt für jedes Polynom $P = \sum_{i=0}^m a_i X^i$:

$$P(B) = \sum_{i=0}^m a_i B^k = \sum_{i=0}^m a_i M^{-1}A^kM = M^{-1}P(A)M.$$

Daraus folgt auch Kern $\mathrm{ev}_B =$ Kern ev_A. $\square$

Sei nun $f : V \to V$ ein Endomorphismus eines endlich dimensionalen Vektorraums. Wir wählen eine Basis $(b_1, \ldots, b_n)$, und nennen die Matrixdarstellung von f in dieser Basis A, also

$$A := \mathrm{Mat}^{(b_1,\ldots,b_n)}_{(b_1,\ldots,b_n)}(f).$$

Man zeigt leicht für $P \in K[X]$:

$$P(A) := \mathrm{Mat}^{(b_1,\ldots,b_n)}_{(b_1,\ldots,b_n)}(f)$$

Es ist also Kern ev_A = Kern ev_f. Wenn wir also das Minimalpolynom von f als $\mu_f := \mu_A$ definieren, so ist μ_f das eindeutige normierte Polynom, das Kern ev_f erzeugt. Insbesondere ist μ_f von der Wahl der Basis unabhängig.

KAPITEL 2

Normalformen von Endomorphismen

1. Zerlegungssatz

Zwei Elemente r, s eines Hauptidealringes R heißen *teilerfremd*, wenn 1 ein ggT von r und s ist. In anderen Worten: wenn es $k, l \in R$ gibt mit $kr + ls = 1$.

Sei U ein Untervektorraum eines Vektorraums V, und $f \in \mathrm{End}(V)$. Dann heißt U invariant unter f, falls $f(U) \subseteq U$.

Ein Endomorphismus $\pi \in \mathrm{End}(V)$ mit $\pi^2 = \pi$ heißt *idempotent*, vgl. LA1, Übungsblatt 8, Aufgabe 31. Es gilt dann

$$V = \mathrm{Bild}\pi \oplus \mathrm{Kern}\ \pi.$$

Die Abbildung π zerlegt sich dann in Blöcke

$$\begin{pmatrix} \mathrm{Id}_{\mathrm{Bild}\pi} & 0 : \mathrm{Kern}\ \pi \to \mathrm{Bild}\pi \\ 0 : \mathrm{Bild}\pi \to \mathrm{Kern}\ \pi & 0 \in \mathrm{End}(\mathrm{Kern}\ \pi) \end{pmatrix}$$

Umgekehrt gibt es zu jeder Zerlegung $V = U_1 \oplus U_2$ eine Abbildung π mit $\pi^2 = \pi$, $\mathrm{Bild}\pi = U_1$, $\mathrm{Kern}\ \pi = U_2$. Man nennt π auch die *Projektion auf* U_1 *mit Kern* U_2.

Satz 1.1 (Zerlegungssatz für 2 Faktoren)**.** *Sei V ein Vektorraum über dem Körper K, $f \in$ End(V), und $P \in K[X] \setminus \{0\}$ ein Polynom mit $P(f) = 0$. Gilt $P = QT$ für teilerfremde Polynome Q und T, so gilt*

(1) $U_Q := \mathrm{Kern}\ Q(f)$ *und* $U_T := \mathrm{Kern}\ T(f)$ *sind invariant unter* f.
(2)
$$V = U_Q \oplus U_T.$$
(3) *Es gibt ein Polynom $P_Q \in K[X]$, so dass $P_Q(f)$ die Projektion auf U_Q mit Kern U_T ist.*
(4) *Es gibt ein Polynom $P_T \in K[X]$, so dass $P_T(f)$ die Projektion auf U_T mit Kern U_Q ist.*

Beispiel. Wir betrachten die reelle Matrix $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$, $f := \mathcal{L}_A : \mathbb{R}^2 \to \mathbb{R}^2$. Man sieht sofort $\chi_f = X^2 - 6X - 8 = (X-2)(X-4)$. Setze $Q := X - 2$, $T := X - 4$. Dann ist U_Q der Eigenraum zum Eigenwert 2 und U_T der zum Eigenwert 4. Setzen wir $P_T = \frac{1}{2}X - 1$ und $P_Q = -\frac{1}{2}X + 2$, so sieht man, dass

$$P_T(A) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

die Matrix der Projektion auf U_T mit Kern U_Q und

$$P_Q(A) = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

die Matrix der Projektion auf U_Q mit Kern U_T ist.

Im Beweis ist das folgende Lemma hilfreich:

Lemma 1.2. *Sei V ein Vektorraum über K, $f \in End(V)$, $P_1, P_2 \in K[X]$. Dann gilt $P_1(f) \circ P_2(f) = (P_1 \cdot P_2)(f) = P_2(f) \circ P_1(f)$. Insbesondere gilt dann* $\text{Kern } P_1(f) \subseteq \text{Kern } (P_1P_2)(f)$.

Beweis des Lemmas. Da $\text{ev}_f : K[X] \to \text{End}(V)$ ein Homomorphismus ist und $K[X]$ kommutativ ist, gilt die obige Aussage. □

Beweis des Satzes. Da Q und T teilerfremd sind, gibt es $\tilde{Q}, \tilde{T} \in K[X]$ mit

$$\tilde{Q}Q + \tilde{T}T = 1.$$

Wir setzen $\pi_T := \tilde{Q}(f)Q(f)$ und $\pi_Q := \tilde{T}(f)T(f)$. Setzen wir $P_T = \tilde{Q}Q$ und $P_Q = \tilde{T}T$ so gilt $\pi_T = P_T(f)$ und $\pi_Q = P_Q(f)$.

Wir wollen zeigen, dass π_T und π_Q die gesuchten Projektionen sind. Man sieht

$$\pi_T + \pi_Q \quad := \quad \text{ev}_f(\tilde{Q}Q + \tilde{T}T) = \text{ev}_f(1) = \text{Id}_V. \tag{1.3}$$

Nach dem Lemma gilt

$$Q(f) \circ \pi_Q = Q(f) \circ \tilde{T}(f) \circ T(f) = \tilde{T}(f) \circ \underbrace{(QT)(f)}_{=P(f)=0} = 0$$

un dann auch $\pi_T \circ \pi_Q = \tilde{Q}(f) \circ Q(f) \circ \pi_Q = 0$.

Dies impliziert

$$\text{Bild}\pi_Q \subseteq U_Q = \text{Kern } Q(f) \subseteq \text{Kern } \pi_T.$$

Sei umgekehrt $v \in \text{Kern } \pi_Q$, dann haben wir

$$v = \text{Id}_V(v) = \pi_T(v) + \pi_Q(v) = \pi_T(v) \in \text{Bild}\pi_T.$$

Also $U_Q = \text{Bild}\pi_Q = \text{Kern } \pi_T$.

Ebenso zeigt man $P(f) \circ \pi_T = 0$, $\pi_Q \circ \pi_T = 0$ und $U_T = \text{Bild}\pi_T = \text{Kern } \pi_Q$. Wir erhalten auch

$$\pi_Q = \text{Id}_V \circ \pi_Q = (\pi_T + \pi_Q) \circ \pi_Q = \pi_T \circ \pi_Q + \pi_Q^2 = \pi_Q^2$$

und ebenso $\pi_T^2 = \pi_T$.

Es bleibt zu zeigen, dass U_Q und U_T invariant unter f sind. Sei $v \in U_Q$, d. h. $Q(f)(v) = 0$. Dann gilt

$$(Q(f))(f(v)) = (Q(f) \circ X(f))(v) = (X(f) \circ Q(f))(v) = f(\underbrace{Q(f)(v)}_{=0}) = 0.$$

Also ist auch $f(v) \in \text{Kern } Q(f) = U_Q$, also ist U_Q invariant unter f. Der Beweis für U_T ist völlig analog. □

Wir zerlegen nun ein beliebiges $P \in K[X] \setminus \{0\}$

$$P = Q_1 \cdot Q_2 \cdots Q_m$$

so dass die Polynome Q_1, Q_2, …, Q_m paarweise teilerfremd sind. Sei $f \in \text{End}(\widetilde{V})$. Wir wenden nun den obigen Satz zunächst für $V = \tilde{V}$, $Q := Q_1$ und $T := Q_1 \cdots Q_m$ und zerlegen

$$\widetilde{V} = \text{Kern } Q_1(f) \oplus \text{Kern } (Q_2 \cdots Q_m)(f).$$

Dann wenden wir den Satz für $V = \text{Kern } (Q_2 \cdots Q_m)(f)$, $Q = Q_2$, $T = Q_3 \cdots Q_m$, und so weiter. Wir erhalten iterativ eine Zerlegung

$$\widetilde{V} = \text{Kern } Q_1(f) \oplus (\text{Kern } Q_2(f) \oplus \cdots (\text{Kern } Q_{m-1}(f) \oplus \text{Kern } Q_m(f)) \cdots)$$

Wir nutzen nun das folgende Lemma, das aus LA1, Satz 7.2 folgt:

Lemma 1.4. *Sei $U_1, U_2, \ldots, U_k$ Untervekorräume von V. Die Summe $U_1 \oplus U_2 \oplus \cdots \oplus U_k$ ist direkt genau dann, wenn alle Summen im Ausdruck $((\ldots(U_1 \oplus U_2) \oplus U_3) \cdots \oplus U_k$ direkt sind.*

Wir somit erhalten den Zerlegungssatz.

Satz 1.5 (Zerlegungssatz für beliebig viele Faktoren)**.** *Sei V ein Vektorraum über dem Körper K, $f \in End(V)$, und $P \in K[X] \setminus \{0\}$ ein Polynom mit $P(f) = 0$. Gilt $P = Q_1 \cdots Q_m$ für paarweise teilerfremde Polynome $Q_1, \ldots, Q_m \in K[X]$, so gilt*

(1) *$U_i := \text{Kern } Q_i(f)$ sind invariant unter f für alle i.*
(2)
$$V = U_1 \oplus \cdots \oplus U_m.$$
(3) *Es gibt Polynome $R_i \in K[X]$, so dass $R_i(f)$ die Projektion auf U_i mit Kern $\bigoplus_{j \neq i} U_j$ ist.*

Beispiel. Sei $A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \in \text{Mat}(4, 4; \mathbb{R})$.

$$\chi_A = ((X-1)^2 - 1)(X^2+1) = \underbrace{X}_{Q_1:=}\underbrace{(X-2)}_{Q_2:=}\underbrace{(X^2+1)}_{Q_3:=}$$

$$U_1 := \text{Kern } X(A) = \text{Kern } A = \text{span}\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

$$U_2 := \text{Kern } (X-2)(A) = \text{Kern } (A - 2\mathbb{1}_4) = \text{span}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$U_3 := \text{Kern } (X^2+1)(A) = \text{Kern } (A^2 + \mathbb{1}_4) = \text{span}\{e_3, e_4\}$$

Bemerkung 1.6. Ist $A \in \text{Mat}(n, n; K)$ eine quadratische Matrix, so kann man die obigen Ergebnisse auf $\mathcal{L}_A$ anwenden. Die analogen Resultate gelten also auch für quadratische Matrizen.

Weiteres Vorgehen: Sei $f \in \text{End}(V)$, $n = \dim V$. Wir zerlegen das charakteristische Polynom χ_f in Primfaktoren:

$$\chi_f = P_1^{r_1} \cdots P_k^{r_k}.$$

Um die Überlegung einfach zu halten, nehmen wir an, dass alle P_j von der Form $X - \lambda_r$ sind. dies ist im Fall $K = \mathbb{C}$ z.B. immer der Fall. Also

$$\chi_f = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k}.$$

Der Zerlegungssatz besagt dann

$$V = \bigoplus_{i=1}^{k} U_i, \qquad U_i := \text{Kern } (X - \lambda_i)^{r_i}.$$

Und $f(U_i) \subseteq U_i$. Wir haben also f zerlegt

$$f = \begin{pmatrix} f_1 & 0 & \cdots & 0 \\ 0 & f_2 & & 0 \\ & & \ddots & \\ \ldots & & & \ldots \\ 0 & 0 & \cdots & f_k \end{pmatrix}$$

Wenn wir also $f_i := f|_{U_i} \in \text{End}(U_i)$ setzen, so haben wir $(\underbrace{f_i - \lambda_i \text{Id}}_{g_i :=})^{r_i}(x) = 0$ für alle $x \in U_i$.

Ziel: Untersuche Endomorphismen g mit $g^r = 0$.

2. Nilpotente Endomorphismen und Matrizen

Sei K ein Körper, V ein K-Vektorraum.

DEFINITION 2.1. $A \in \mathrm{Mat}(n,n;K)$ (bzw. $f \in \mathrm{End}(V)$) heißt nilpotent, falls $A^k = 0$ für ein $k \in \mathbb{N}$. Falls k minimal gewählt ist, sagt man A ist nilpotent von Stufe k.
Analog: f ist nilpotent von Stufe $\leq k \;\Leftrightarrow\; f^k = 0$.

BEISPIEL.

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad A^3 = 0$$

A ist nilpotent der Stufe 3.

LEMMA 2.2. *Sei* $A = \begin{pmatrix} 0 & & * \\ \vdots & \ddots & \\ 0 & \cdots & 0 \end{pmatrix} = (a_{ij})_{ij} \in \mathrm{Mat}(n,n;K)$ *mit* $a_{ij} = 0$ *falls* $i \geq j$ *(strikte obere Dreiecksmatrix). Dann gilt:* $A^n = 0$.

Beweis. $A^k =: (a_{ijk})_{ij} \quad k \in \mathbb{N}$
Also $a_{ijk} = 0$ falls $i \geq j - k + 1$ für $k = 1$

<u>Behauptung:</u>
Es gilt $\forall ijk$ mit $i > j - k$: $a_{ijk} = 0$.

Aus der Behauptung folgt dann für $k := n$: $\forall i,j : a_{ijn} = 0$, also $A^n = 0$.

<u>Beweis durch Induktion über k:</u>
$k = 1$: siehe oben
$k \to k+1$: Sei $a_{ij(k+1)} \neq 0$

$$a_{ij(k+1)} = \sum_{l=1}^{n} a_{ilk} \cdot a_{lj1}$$
$$\Rightarrow \exists l : \left.\begin{matrix} a_{ilk} \neq 0 & \Rightarrow & i \leq l - k \\ a_{lj1} \neq 0 & \Rightarrow & l \leq j - 1 \end{matrix}\right\} i \leq j - k - 1 = j - (k+1)$$

Somit haben wir $i > j - (k+1) \Rightarrow a_{ij(k+1)} = 0$. □

LEMMA 2.3. *Falls* $A \in \mathrm{Mat}(n,n;K)$ *nilpotent ist, dann ist* $A^n = 0$.

Beweis.

$$\begin{aligned} \exists k: \quad & A^k = 0 \\ & X^k(A) = 0 \\ & \mu_A | X^k \\ & \underline{\text{Also:}}\ \mu_A = X^l \quad l \leq k \\ & \mu_A | \chi_A \quad \text{(Cayley-Hamilton)} \\ & \underline{\text{Also:}}\ l = \deg \mu_A \leq \deg \chi_A = n \\ & X^n(A) = A^n = A^{n-l} \cdot \underbrace{A^l}_{=\mu_A(A)=0} = 0 \end{aligned}$$

□

Lemma 2.4. *Ist A ähnlich zu einer strikten oberen Dreiecksmatrix, so ist A nilpotent.*

Beweis. MAM^{-1} sei obere Dreiecksmatrix , $M \in GL(n, K)$

$(MAM^{-1})^k = 0 = MAM^{-1}MAM^{-1}...MAM^{-1} = MA^kM^{-1}$

$0 = M^{-1}0M = M^{-1}MA^kM^{-1}M = A^k$. □

Analog zeigt man Besitzt $f \in \text{End}(V)$ eine Basis B, so dass $\text{Mat}_B^B(f)$ strikte obere Dreiecksmatrix ist, so ist f nilpotent.

$\text{Mat}_B^B(f^k) = (\text{Mat}_B^B(f))^k = 0$.

Definition 2.5. Eine *nilpotente Matrix in Jordanform* ist eine quadratische Matrix $(a_{lk})_{lk}$, so dass

$a_{lk} = 0\ \forall l \neq k-1$ und $a_{lk} \in \{0, 1\}\ \forall l = k-1$.

Beispiel. $\begin{pmatrix} 0 & 1 & & & & & \\ & 0 & 1 & & & 0 & \\ & & 0 & 0 & & & \\ & & & 0 & 1 & & \\ & & & & 0 & 0 & \\ & 0 & & & & 0 & 1 \\ & & & & & & 0 \end{pmatrix}$ ist eine nilpotente Matrix in Jordanform.

Solche Matrizen sind strikte obere Dreicksmatrizen.

Proposition 2.6. *Sei V ein K-Vektorraum der Dimension n, f ein nilpotenter Endomorphismus von V ($\stackrel{Lemma}{\Longrightarrow}$ $f^n = 0$). Dann gibt es eine Basis $\underline{b} = (b_1, \dots, b_n)$ von V, so dass $\text{Mat}_{\underline{b}}^{\underline{b}}(f)$ eine nilpotente Matrix in Jordanform ist.*

KOROLLAR 2.7. *Sei $A \in \mathrm{Mat}(n,n,K)$. Äquivalent sind:*

(1) *A ist nilpotent*
(2) *A ist ähnlich zu einer strikten oberen Dreiecksmatrix*
(3) *A ist ähnlich zu einer nilpotenten Matrix in Jordanform*

Beweis des Korollars. (2) $\Rightarrow$ (1) : gesehen

(3) $\Rightarrow$ (2) : klar

(1) $\Rightarrow$ (3) : A nilpotent $\Rightarrow \mathcal{L}_A$ nilpotent

Die Proposition zeigt die Existenz einer Basis $\underline{b} = (b_1, ..., b_n)$ von K^n, so dass $\mathrm{Mat}_{\underline{b}}^{\underline{b}}(\mathcal{L}_A)$ eine nilpotente Matrix in Jordanform ist.

Also ist A ähnlich zu einer nilpotenten Matrix in Jordanform □

Beweis der Proposition. Sei $U_k := \text{Kern }(f^k)$, $d_k := \dim U_k$

m sei die kleinste Zahl in $\mathbb{N}$, so dass $f^m = 0$. Insbesondere $m \leq n$.

$U_0 = \{0\} \subseteq U_1 = \text{Kern } f \subseteq U_2 = \text{Kern } f^2 \subseteq ... \subseteq U_m = \text{Kern } f^m = V$

Beh.(a): $f(U_k) \subseteq U_{k-1}$ für alle $k \in \{1, 2, \dots, m\}$.

Denn Sei $v \in U_k \Rightarrow f^k(v) = 0 = f^{k-1}(f(v)) \Rightarrow f(v) \in U_{k-1}$

Beh.(b): Wähle $k \in \{1, ..., m-1\}$. Sei W ein Komplement von U_k in U_{k+1}, d.h. $U_{k+1} = U_k \oplus W$

Dann ist $f_{|W} : W \to U_k$ injektiv und $f(W) \cap U_{k-1} = \{0\}$

Denn: Angenommen $w \in W$, so dass $f(w) \in U_{k-1}$

Dann gilt: $f^k(w) = f^{k-1}(f(w)) = 0$

Also $w \in U_k$. Somit $w \in W \cap U_k = \{0\} \Rightarrow w = 0$

Wir haben somit $f(W) \oplus U_{k-1} \subseteq U_k$. Diese Inklusion ist im allgemeinen keine Gleichheit.

Konstruktion der Basis in der Proposition:

<u>0. Schritt=Vorbereitungsschritt</u> Wir wählen linear unabhängige Vektoren $w_1^{(m-1)}, ..., w_{d_m - d_{m-1}}^{(m-1)}$, so dass
$U_{m-1} \oplus \text{span}\{w_1^{(m-1)}, ..., w_{d_m - d_{m-1}}^{(m-1)}\} = U_m$
Wenn $m = 1$, so ist $d_{m-1} = d_0 = 0$, $f = 0$. Dann ist $\underline{b} := (w_1^{(0)}, ..., w_m^{(0)})$ eine Basis von V, und $\mathrm{Mat}_{\underline{b}}^{\underline{b}}(f)$ ist die Nullmatrix, also insbesondere in der gewünschten Form.
<u>Ab jetzt sei $m \geq 2$:</u>

<u>1. Schritt</u> Seien $w_1^{(m-1)}, ..., w_{d_m-d_{m-1}}^{(m-1)}$ wie oben gegeben. Wende Beh.(b) für $k = m-1$ an.

$W = \operatorname{span}\{w_1^{(m-1)}, ..., w_{d_m-d_{m-1}}^{(m-1)}\}$
Definiere $w_i^{(m-2)} := f(w_i^{(m-1)})$. Behauptung (b) besagt, dass $(w_1^{(m-2)}, ..., w_{d_m-d_{m-1}}^{(m-2)})$ linear unabhängig ist, und ferner haben wir

$$U_{m-2} \oplus \operatorname{span}\{w_1^{(m-2)}, ..., w_{d_m-d_{m-1}}^{(m-2)}\} \subseteq U_{m-1}.$$

Insbesondere sehen wir $d_{m-2} + (d_m - d_{m-1}) \leq d_{m-1}$. Wähle nun weitere Vektoren w_i^{m-2} , $i \in \{d_m - d_{m-1} + 1, ..., d_{m-1} - d_{m-2}\}$, so dass

$$U_{m-2} \oplus \operatorname{span}\{w_1^{(m-2)}, ..., w_{d_{m-1}-d_{m-2}}^{(m-2)}\} = U_{m-1}.$$

Im Fall $m = 2$ sind wir nun fertig, denn $d_{m-2} = d_0 = 0, d_1 \geq n - d_1$.
$(\underbrace{w_1^{(0)}, ...w_{d_1}^{(0)}}_{Basis\ von\ U_1}, \underbrace{w_1^{(1)}, ..., w_{n-d_m}^{(1)}}_{Basis\ von\ W})$ Basis von V
$(b_1, ..., b_n) = (w_1^{(0)}, w_1^{(1)}, w_2^{(0)}, w_2^{(1)}, ..., w_{d_1}^{(0)})$ Basis von V
$f(w_1^{(1)}) = w_1^{(0)}$, $f(w_i^{(0)}) = 0$

$$\operatorname{Mat}_{(b_i)}^{(b_i)}(f) = \left(\begin{array}{cc|cc|cc|c}
0 & 1 & & & & & \\
0 & 0 & & & & & \\
\hline
. & . & 0 & 1 & & & \\
. & . & 0 & 0 & & & \\
\hline
 & & & & \ddots & & \\
 & & & & & \ddots & \\
\hline
 & & & & & & 0
\end{array}\right)$$

Diese Matrix hat auf ihrer diagonalen $n - d_1$ Blöcke der Form $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \operatorname{Mat}(2, 2; K)$ und hat Nullen auf den letzten $2d_1 - n$ Spalten bzw. Zeilen.
<u>Ab jetzt sei $m \geq 3$:</u>

So geht es immer weiter. Wenn man den Beweis völlig sauber formulieren wollten, sollte man hier eine vollständige Induktion benutzen. Wir deuten die Induktion hier an, indem wir den k-ten Schritt angeben.

<u>k-ter Schritt:</u>[1]
Gegeben sei eine linear unabhängige Familie $(w_1^{(m-k)}, ..., w_{d_{m-k+1}-d_{m-k}}^{(m-k)})$, so dass

$$U_{m-k} \oplus \operatorname{span}\{w_1^{(m-k)}, ..., w_{d_{m-k+1}-d_{m-k}}^{(m-k)}\} = U_{m-k+1}.$$

[1] In der Vorlesung waren die Indizes etwas anders, ich habe die Schritte inzwischen etwas umnummeriert.

Wir definieren $w_i^{(m-k-1)} := f(w_i^{(m-k)})$ und sehen mit Behauptung (a) und (b), dass die Familie $(w_1^{(m-k-1)}, \dots, w_{d_{m-k+1}-d_{m-k}}^{(m-k-1)})$ linear unabhängig ist.

$$U_{m-k-1} \oplus \operatorname{span}\{w_1^{(m-k-1)}, ..., w_{d_{m-k+1}-d_{m-k}}^{(m-k-1)}\} \subseteq U_{m-k}$$

Ergänze zu Basis eines Komplements von U_{m-k-1} in U_{m-k} und wir erhalten

$$U_{m-k-1} \oplus \operatorname{span}\{w_1^{(m-k-1)}, ..., w_{d_{m-k}-d_{m-k-1}}^{(m-k-1)}\} = U_{m-k}.$$

Der letzte Schritt ist der Schritt mit $k = m-1$.

$$\underbrace{(\underbrace{w_1^{(0)}, w_2^{(0)}, \dots, w_{d_1}^{(0)}}_{\text{Basis von } U_1}, \dots, w_{d_2-d_1}^{(1)},}_{\text{Basis von } U_2}, \dots, w_{d_m-d_{m-1}}^{(m-1)}) \text{ ist Basis von } V$$

$f(w_i^{(1)}) = w_i^{(0)}$, allgemein $f(w_i^{(j+1)}) = w_i^{(j)}$
Umordnen:

$$(w_1^{(0)}, w_1^{(1)}, \dots, w_2^{(0)}, w_2^{(1)}, ..., w_{d_m-d_{m-1}}^{(m-1)}) =: \underline{b}$$

$\Rightarrow \operatorname{Mat}_{\underline{b}}^{\underline{b}}(f)$ hat ist eine nilpotente Matrix in Jordanform. □

Beispiel. $V := K^3, A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $f = \mathcal{L}_A \in \operatorname{End}(K^3)$

$f^2 = 0 \Rightarrow m = 2$, $\mu_A = X^2$, $\chi_A = X^3$.

$U_0 = \{0\} \subseteq U_1 = \operatorname{Kern} f = \operatorname{span}\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\} \subseteq U_2 = K^3$.

Wähle $w_1^{(1)} := \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}$.

$U_1 \oplus \operatorname{span}\{w_1^{(1)}\} = U_2$.

$w_1^{(0)} := f(w_1^{(1)} = A \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

Wähle nocbh hinzu: $w_2^{(0)} := \begin{pmatrix} 17 \\ 0 \\ 1 \end{pmatrix}$.

$U_0 \oplus \operatorname{span}\{w_1^{(0)}, w_2^{(0)}\} = U_1$

$\underline{b} := (b_1, b_2, b_3) := (w_1^{(0)}, w_1^{(1)}, w_2^{(0)})$ stellt $\mathcal{L}_A$ in Jordan-Normalform da:

$$\mathrm{Mat}_{\underline{b}}^{\underline{b}}(\mathcal{L}_A) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

3. Trigonalisierbarkeit und Jordannormalform

<u>Wdh.:</u> Ein $f \in End(V)$ heißt trigonalisierbar $\Leftrightarrow \exists$ Basis (b_i), so dass $A := \mathrm{Mat}_{(b_i)}^{(b_i)}(f)$ obere Dreiecksmatrix ist.

$$\chi_f = \chi_A = \det(X\mathbb{1} - A) = \det \begin{pmatrix} (X - a_{11} & & * \\ & \ddots & \\ 0 & & X - a_{nn} \end{pmatrix} = (X - a_{11}) \cdots (X - a_{nn})$$

Insbesondere zerfällt in diesem Fall χ_f in Linearfaktoren.

Definition 3.1. Ein Polynom $P \in K[X] \setminus \{0\}$ zerfällt, wenn es $r, a_1, ..., a_n \in K$ gibt, so dass $P = r(X - a_1)...(X - a_n)$

Wir haben bereits gesehen, dass f genau dann trigonalisierbar ist, wenn χ_f zerfällt.

Beispiele. a)$K = \mathbb{C}$: Alle Polynome zerfallen

b)$K = \mathbb{R}$ $X^2 + bX + c$ zerfällt $\Leftrightarrow b^2 - 4c \leq 0$

c) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{Mat}(2, 2, \mathbb{C})$ trigonalisierbar, ähnlich zu $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{Mat}(2, 2, \mathbb{R})$ ist nicht trigonalisierbar

29.5. kein Protokollant gefunden

2.6. kein Protokollant gefunden

5.6. in Bearbeitung

9.6. kein Skript

12.6. kein Skript

16.6. in Bearbeitung

19.6. kein Skript

23.6. in Bearbeitung

Ende des Skripts.

KAPITEL 3

Normalformen in unitären und euklidischen Vektorräumen

1. Definitionen und Grundlegendes

2. Normalformen in unitären Vektorräumen

3. Normalformen in eulidischen Vektorräumen

9.6.2008 Teil 1

In diesem Abschnitt sei immer $K = \mathbb{R}$, V ein euklidischer Vektorraum der Dimension $n := \dim V \in \mathbb{N}$, und $f \in \mathrm{End}(V)$, $A \in Mat(n, n; \mathbb{R})$.

Satz 3.1. *Zerfällt χ_f in $\mathbb{R}[X]$, so ist f orthogonal trigonalisierbar.*

Der Beweis ist geht völlig gleich wie der Beweis der unitären Trigonalisierung im letzten Abschnitt.

Im letzten Semester (Lineare Algebra I) haben wir bereits gesehen.

Satz 3.2. *f ist orthogonal diagonalisierbar, gdw f selbstadjungiert ist.*
A ist orthogonal diagonalisierbar, gdw A symmetrisch ist.

Definition 3.3. f heißt *normal*, falls $f^* f = f f^*$.
A heißt *normal*, falls $A^T A = A A^T$.

Was ist die hier Rolle von normalen Endomorphismen? Orthogonale Matrizen ($A^T = A^{-1}$) und schiefsymmetrische Matrizen ($A^T = -A$) sind normal, aber nur in Ausnahmefällen symmetrisch.

Die beiden folgenden Lemmata lassen sich genau wie im komplexen Fall beweisen.

Lemma 3.4. *Sei f normal. Dann gilt $V = \mathrm{Kern}\ f \oplus \mathrm{Bild} f$ und die Summe ist sogar orthogonal.*

Lemma 3.5. *Set f normal und $P \in \mathbb{R}[X]$. Dann ist auch $P(f)$ normal.*

Lemma 3.6. *Sei A normal mit $A^2 = -\mathbb{1}_n$, dann ist A schiefsymmetrisch (d.h. $A^T = -A$).*

Beweis. Angenommen $A \neq 0$. Wir setzen $B := iA \in \mathrm{Mat}(n, n; \mathbb{C})$. Man rechnet leicht nach, dass B normal ist und $B^2 = \mathbb{1}_n$. B hat somit das Minimalpolynom $\mu_B = (X + 1)(X - 1)$ und die

Eigenwerte ± 1. Daraus folgt, dass B hermitesch ist und deshalb

$$A^T = A^* = ((-i)B)^* = iB^* = iB = -A.$$

□

Aus dem Lemma folgt sofort, dass normale Endomorphismen f mit $f^2 = -\mathrm{Id}$ immer schiefselbstadjungiert sind (d.h. $f^* = -f$).

Proposition 3.7. *Sei f ein Endomorphismus mit $f^2 = -\mathrm{Id}$. Dann gibt es eine Basis $\underline{b} = (b_1, \ldots, b_n)$, so dass*

$$\mathrm{Mat}_{\underline{b}}^{\underline{b}}(f) = \begin{pmatrix} J & 0 & 0 & \cdots & 0 \\ 0 & J & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & J \end{pmatrix}$$

wobei $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Ist f zusätzlich normal, so kann man $\underline{b}$ sogar orthogonal wählen.

Beweis. Wir versehen den reellen Vektorraum V mit der folgenden komplexen Struktur: für $\alpha, \beta \in \mathbb{R}$, $v \in V$ definieren wir:

$$(\alpha + \beta i) \bullet v := \alpha v + \beta f(v).$$

Man überprüft leicht, dass $(V, +, \bullet)$ ein komplexer Vektorraum ist und $f = i \bullet \mathrm{Id}$. Ist $(b_1, \ldots, b_m)$ eine komplexe Basis von V, dann ist $\underline{b} := (b_1, f(b_1), b_2, f(b_2), \ldots, f(b_m))$ eine reelle Basis, in der f die gewünschte Matrixdarstellung hat.

Ist f zusätzlich normal, so definieren wir ein komplexes Skalarprodukt auf V durch

$$\langle v, w \rangle_{\mathbb{C}} := \langle v, w \rangle + i \langle v, f(w) \rangle.$$

Man zeigt leicht, dass diese Abbildung sesquilinear, hermitsch und positiv definit ist. Ausserdem gilt auch im komplexen Sinne $-f = f^*$. Man wählt dann die komplexe Basis als ONB, dann ist die reelle auch eine ONB. □

Proposition 3.8. *Sei f ein normaler Endomorphismus mit $\mu_f = X^2 + bX + c$ mit $b^2 < 4c$, dann gibt es eine Basis $(b_1, \ldots, b_n)$, so dass*

$$\mathrm{Mat}_{\underline{b}}^{\underline{b}}(f) = \begin{pmatrix} M & 0 & 0 & \cdots & 0 \\ 0 & M & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & M \end{pmatrix}$$

wobei $M = \begin{pmatrix} -b/2 & \sqrt{c - b^2/4} \\ -\sqrt{c - b^2/4} & -b/2 \end{pmatrix}$.

Beweis. Zunächst gilt $f^2 + bf = -c\mathrm{Id}$. Wir setzen $g := \frac{1}{\sqrt{c-b^2/4}}(f + \frac{b}{2}\mathrm{Id})$ und rechnen

$$g^2 = \frac{1}{c-4b^2}(f + \frac{b}{2}\mathrm{Id})^2 = \frac{1}{c-b^2/4}(\underbrace{f^2+bf}_{-c\mathrm{Id}} + \frac{b^2}{4}\mathrm{Id}) = -\mathrm{Id}.$$

Nach der vorigen Proposition gibt es eine Basis $\underline{b}$, so dass

$$\mathrm{Mat}_{\underline{b}}^{\underline{b}}(\frac{1}{\sqrt{c-b^2/4}}(f+\frac{b}{2}\mathrm{Id})) = \mathrm{Mat}_{\underline{b}}^{\underline{b}}(g) = \begin{pmatrix} J & 0 & 0 & \cdots & 0 \\ 0 & J & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & J \end{pmatrix}$$

wobei $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Hieraus folgt die Behauptung. □

PROPOSITION 3.9. *In der Primfaktorzerlegung des Minimalpolynoms eines normalen Endomorphismus kommt jeder (normierte) Primfaktor nur einmal vor.*

Beweis. Angenommen P sei ein normierter Primfaktor mit $P^2|\mu_f$. Wir bestimmen $Q \in \mathbb{R}[X]$ mit $\mu_f = P^2Q$. Für ein beliebiges $x \in V$ gilt

$$0 = \mu_f(f)(x) = P(f)\left(P(f)Q(f)(x)\right).$$

Also ist $P(f)Q(f)x \in \mathrm{Bild}P(f) \cap \mathrm{Kern}\ P(f)$. Da $P(f)$ normal ist, folgt $P(f)Q(f)x = 0$ also $\mu_f|PQ$. Dies widerspricht $\mu_f = P^2Q$. □

9.6.2008 Teil 2 kommt evtl. noch.