

8. Das Polynomring

Stets sei k ein Körper.

Definition k -Algebra, k -Algebrenhomomorphismen.

Beispiel End $_k V \cong M_n(k)$ ist eine k -Algebra, $\dim_k V = n$.
 $f \mapsto M_\varphi(f)$ ist Algebrenhomomorphismen.

Lemma 1 a) Der k -Vektorraum $k^{(N)}$ wird durch
 $(f \cdot g)(k) = \sum_{i+j=k} f(i)g(j)$ zu einer Algebra mit 1.

b) Für $X = e_1$ liefern die Potenzen X^i $i=0, \dots$ die kanonische Basis. Es ist also $P = P(X) = \sum_{i=0}^m a_i X^i$ für ein m und $a_i \in k$.

c) $P+Q, \lambda P, P \cdot Q$ werden auf die übliche Art berechnet.

Definition a) Obige Algebra heißt Polynomalgebra in der Variablen X . Man schreibt dafür $k[X]$. $P = P(X) \in k[X]$ heißt Polynom in X . Statt Variablen sagt man auch Unbekannte.

b) $\text{grad } P$, Höchstkoeffizient, konstanter Term, normiertes Polynom.
 $\text{grad } 0 = -\infty$.

Lemma 2 Sei A eine k -Algebra. Dann gibt es genau einen k -Algebrenhomomorphismus $\varphi: k[X] \rightarrow A$ mit $\varphi(1)=1$ und $\varphi(X)=a$, den Einsetzungshomomorphismen. Ist $P = P(X) = r_0 + r_1 X + \dots + r_m X^m$, so ist $\varphi(P) = P(a) = r_0 + r_1 a + \dots + r_m a^m$.

Definition $P(a)$ heißt Wert von P an der Stelle a .
 a heißt Nullstelle, falls $P(a)=0$.

Beispiel: $P(X) = X^2, k = \mathbb{R}, \begin{bmatrix} 0 & \lambda \\ 0 & 0 \end{bmatrix}$ ist Nullstelle von P in $\mathbb{R}^{2 \times 2}$ für jedes $\lambda \in \mathbb{R}$.

Definition Sei R ein kommut. Ring.

a) R heißt nullteilerfrei oder Integritätsbereich $\Leftrightarrow (xy=0 \Rightarrow x=0 \text{ oder } y=0)$

b) $x \in R$ heißt Einheit $\Leftrightarrow \exists y \in R$ mit $xy=1$.

$R^* = \{x \in R \mid x \text{ Einheit}\}$

- Lemma 3 a) $\text{grad } PQ = \text{grad } P + \text{grad } Q$, $\text{grad } (P+Q) \leq \max(\text{grad } P, \text{grad } Q)$.
b) $k[X]$ ist Integritätsbereich. Also folgt aus $0 \neq P$ und $PQ_1 = PQ_2$ stets $Q_1 = Q_2$.
c) $k[X]^* = \{a_0 \neq 0\} = \{\text{konstante Polynome} \neq 0\}$.

Satz 4 (Division mit Rest) Für $P, Q \in k[X]$ mit $Q \neq 0$ existieren $S, R \in k[X]$ mit $P = QS + R$ und $\text{grad } R < \text{grad } Q$. Dabei sind Q und R eindeutig bestimmt.

Bem: R heißt Rest von P bei Division durch Q .

Beispiel im Nekt:

- Definitionen a) $P|Q$ in $k[X] \Leftrightarrow \exists S$ mit $PS = Q$
b) P irreduzibel $\Leftrightarrow P$ normiert, $\text{grad } P \geq 1$ und aus $P = Q_1 Q_2$ folgt $Q_1 \in k[X]^*$ oder $Q_2 \in k[X]^*$.

Beispiel: $X - a$ ist irreduzibel für jedes a .

Satz 5 Sei $P \in k[X]$, $a \in k$. Dann gilt: $P(a) \neq 0 \Leftrightarrow X - a \nmid P$.

Definition: Seien $P, Q \in k[X] \setminus \{0\}$.
 $TC(P, Q) = \{H \mid H|P \text{ und } H|Q\}$ - Menge der gemeinsamen Teiler.
 H heißt ggT von P und Q , d.h. $H = \text{ggT}(P, Q)$, falls $H \in TC(P, Q)$, H normiert und $H'|H$ für alle $H' \in TC(P, Q)$.

Satz 6 Für $P, Q \in k[X] \setminus \{0\}$ existiert ein ggT H . Er ist eindeutig bestimmt. Ferner $\exists U, V$ mit $H = UP + VQ$. Dabei können H, U, V mit dem Eukl. Alg. rekursiv berechnet werden.

Satz 7 Ist P irreduzibel mit $P|Q_1 Q_2 \dots Q_r$ so folgt $P|Q_i$ für mindestens ein i .

Satz 8 Jedes $0 \neq P$ ist endliches Produkt $P = a P_1 P_2 \dots P_r$ mit $a \in k$, P_i irreduzibel. Dabei sind a, r und die P_i eindeutig bis auf die Reihenfolge der Faktoren.

Bem: Polynom von Grad n hat in k höchstens n Nullstellen.

9. Eigenwerte und Eigenvektoren

Definitionen: Sei $f \in \text{End}_k V$. Ein Skalar $\lambda \in k$ heißt Eigenwert von f in k , falls ein Vektor $0 \neq v \in V$ existiert mit $fv = \lambda v$, d.h. falls $\text{Kern}(\lambda \text{id}_V - f) \neq 0$. Man nennt $E(f, \lambda) := \text{Kern}(\lambda \text{id}_V - f)$ den Eigenraum zum Eigenwert λ und jeden Vektor $0 \neq v$ in $E(f, \lambda)$ einen Eigenvektor von f zum Eigenwert λ .

Bemerkungen und Beispiele: 1) Analoge Definitionen für $A: k^n \rightarrow k^n$ mit $x \mapsto Ax$.

2) Die Nulleabbildung $0: V \rightarrow V$ mit $0(v) = 0 \forall v \in V$ hat als einzigen E.W. 0. Jeder Vektor $0 \neq v$ ist Eigenvektor.

3) Für $V = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ bel. oft differenzierbar}\}$ sei $D \in \text{End}_{\mathbb{R}} V$ definiert durch $D(f) = f' = \text{Ableitungsfunktion von } f$. Dann ist für jedes $\lambda \in \mathbb{R}$ die Funktion $f_\lambda \in V$ mit $f_\lambda(x) = \lambda x$ ein Eigenvektor von D zum E.W. λ .

Definitionen: a) Für $A \in k^{n \times n}$ ist das charakteristische Polynom χ_A definiert als $\chi_A(X) = \det_n(XE_n - A)$.

b) $A, B \in k^{n \times n}$ heißen ähnlich über k , falls ein $S \in GL_n(k)$ existiert mit $S^{-1}AS = B$.

Beispiel: Ist $f \in \text{End}_k V$ und sind φ, ψ Koordinatensysteme von V , so sind $M_\varphi(f)$ und $M_\psi(f)$ ähnlich über k nach dem Satz über Koordinatenwechsel.

Lemma: Seien $A, B \in k^{n \times n}$.

- a) $\chi_A(X) = X^n - (\sum_{i=1}^n a_{ii})X^{n-1} + \dots + (-1)^n \det_n A \in k[X]$
 b) falls A und B ähnlich sind über k , gilt $\chi_A = \chi_B$.

Definition: Sei $f \in \text{End}_k V$, $\dim_k V = n < \infty$. Das charakteristische Polynom von f ist definiert als $\chi_f = \chi_{M_\varphi(f)}$,

wobei $\varphi: k^n \xrightarrow{\sim} V$ ein K.O.S. ist. (Dies ist unabhängig von der Wahl nach Teil b) des Lemmas).

Satz 2 Sei $\dim_k V = n < \infty$, $f \in \text{End}_k V$.

Die Eigenwerte von f in k sind gerade die Nullstellen von χ_f in k . Insbesondere gibt es höchstens n Eigenwerte.

Beispiel:

$$D(\alpha) = \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \in \mathbb{R}^{2 \times 2} \subseteq \mathbb{C}^{2 \times 2}$$

hat in $\mathbb{C}$ die Eigenwerte $e^{i\alpha} = \cos \alpha + i \sin \alpha$ und $e^{-i\alpha} = \cos \alpha - i \sin \alpha$. Für $\alpha \notin \mathbb{Z}\pi$ hat also $D(\alpha)$ keinen Eigenwert in $\mathbb{R}$.

Zerlegungslemma: Seien Q_1, Q_2 in $k[X]$ teilerfremd (d.h. 1 ist der größte gemeinsame Teiler). Dann gilt für jedes $f \in \text{End}_k V$

$$\text{Kern}(Q_1 Q_2)(f) = \text{Kern } Q_1(f) \oplus \text{Kern } Q_2(f) = \text{Kern } Q_1(f) + \text{Kern } Q_2(f)$$

Bem. 1) Per Induktion erhält man sogar:

Sei $Q = Q_1 Q_2 \dots Q_r$ mit paarweise teilerfremden Q_i für $i \neq j$, so gilt $\text{Kern } Q(f) = \bigoplus \text{Kern } Q_i(f) = \sum \text{Kern } Q_i(f)$

2) Für $Q_i = (X - \lambda_i)$ mit $\lambda_i \neq \lambda_j$ für $i \neq j$ findet man $\sum E(f, \lambda_i) = \bigoplus E(f, \lambda_i)$. Insbesondere sind

Eigenvektoren zu verschiedenen Eigenwerten immer l.u.

Definitionen a) $f \in \text{End}_k V$ heißt diagonalisierbar, falls $\exists \varphi: k^n \xrightarrow{\sim} V$ mit $M_\varphi(f) = D = \text{Diagonalmatrix}$.

b) $A \in k^{n \times n}$ heißt diagonalisierbar über k , falls $\exists S \in GL_n(k)$ mit $S^{-1}AS = D = \text{Diagonalmatrix}$.

Bem. $f \in \text{End}_k V$, $\varphi: k^n \xrightarrow{\sim} V$ bel. K.O.S.
 f diag. $\Leftrightarrow M_\varphi(f)$ ist diag. über k .

Definition: Sei $\dim_k V = n < \infty$, $f \in \text{End}_k V$, λ Eigenwert in k .
 a) Die algebraische Vielfachheit $a_\lambda = a(f, \lambda)$ von λ als Eigenwert ist die Vielfachheit von $(X - \lambda)$ als irreduzibler Faktor von χ_f .

b) Die geometrische Vielfachheit $g_\lambda = g(f, \lambda)$ in $g_\lambda = \dim E(f, \lambda)$.

Bem: Stets gilt $1 \leq g_\lambda \leq a_\lambda \leq n$.

Satz 4 Sei $f \in \text{End}_k V$, $\varphi: k^n \xrightarrow{\sim} V$ ein K.O.S., $A = M_\varphi(f)$.
 Dann sind gleichwertig:

- a) f ist diag. a') A ist diag. über k
- b) Es gibt eine Basis aus Eigenvektoren von f .
- c) $V = \bigoplus E(f, \lambda_i)$, wobei $\lambda_1, \dots, \lambda_r$ die E.W. von f .
- d) i) $\chi_A = \prod_{i=1}^r (X - \lambda_i)^{m_i}$ erfüllt in $k[X]$ die Linearfaktoren, d.h. mit $\lambda_i \in k$, $\lambda_i \neq \lambda_j$ für $i \neq j$ und $m_i \geq 1$.
- ii) $\forall i=1, \dots, r$ gilt $g_{\lambda_i} = a_{\lambda_i}$.

Folgerung 5 Hat χ_f n verschiedene Nullstellen in k ,
 so ist f diagonalisierbar.

Man stellt so einen Algorithmus, um die Frage der Diagonalisierbarkeit A zu klären und um gegebenfalls S, D mit $S^{-1}AS = D$ zu finden.

Lemma 6 a) Sei $\dim_k V < \infty$. Dann gibt es zu jedem $f \in \text{End}_k V$ genau ein normiertes Polynom μ_f , so dass für $H \in k[X]$ gilt $H(f) = 0$ genau dann, wenn $\mu_f | H$ gilt.
 b) Analog $\exists$ für $A \in K^{n \times n}$ genau ein norm. Polynom μ_A für das $H(A) = 0$ äquivalent ist zu $\mu_A | H$.

Definition: Mit den Notationen des letzten Semesters
 heißt μ_f bzw. μ_A das Minimalpolynom von
 f bzw. A .

Satz: Sei $A \in K^{n \times n}$. Dann sind gleichwertig:

- a) A ist diag. über K
- b) μ_A zerfällt in $K[X]$ in versch. Linearfaktoren, d.h.
 $\mu_A = \prod_{i=1}^r (X - \lambda_i)$ in $K[X]$ mit $\lambda_i \neq \lambda_j$ für $i \neq j$.

Definition: Für ein mon. Polynom

$P = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in K[X]$ ist die
 Begleitmatrix $B(P)$ definiert als

$$B(P) = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & -a_{n-2} \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix} \in K^{n \times n} \quad \left(\begin{array}{l} \text{Nur Nebendiag.} \\ \text{und letzte Spalte} \\ \text{eventuell } \neq 0 \end{array} \right)$$

Satz 8: Stets gilt $\chi_{B(P)} = \mu_{B(P)} = P$.

Satz 9: Sei $A = \begin{bmatrix} A_1 & A_2 \\ 0 & A_4 \end{bmatrix}$ obere Block-Diagonalmatrix.
 Dann gilt

a) $\chi_A = \chi_{A_1} \cdot \chi_{A_4}$

b) $\forall H \in K[X]$ ist $H(A) = \begin{bmatrix} H(A_1) & * \\ 0 & H(A_4) \end{bmatrix}$

c) Für $i=1,2$ gilt: $\mu_{A_i} \mid \mu_A \mid \mu_{A_i} \cdot \mu_{A_4}$.

Satz von Cayley-Hamilton: Sei $A \in K^{n \times n}$. Dann gilt

Insbesondere haben $\mu_A \mid \chi_A$ und $\chi_A \mid \mu_A$.
 Insbesondere haben μ_A und χ_A die gleichen
 irreduziblen Faktoren und die gleichen Nullstellen.