7.5 Irreduzible Polynome

$\deg(F \cdot G) = \deg(F) + \deg(G)$

Sei K ein Körper.

Definition: Ein Polynom in $K[X]$, welches sich als Produkt zweier Polynome in $K[X]$ vom Grad $\geqslant 1$ schreiben lässt, heisst *reduzibel*. Ein Polynom in $K[X]$ vom Grad $\geqslant 1$, welches nicht reduzibel ist, heisst *irreduzibel*.

Beispiel: (a) Jedes Polynom vom Grad 1 ist irreduzibel.

(b) Ein Polynom vom Grad 2 oder 3 ist irreduzibel genau dann, wenn es keine Nullstelle hat.

F reduzibel $\Rightarrow F = G \cdot H$, $\deg(G) = 1 \Rightarrow G(X) = aX + b$ für $a, b \in K$ und $a \neq 0 \Rightarrow G = a \cdot (X + \frac{b}{a})$ und $F(-\frac{b}{a}) = 0$.

Beispiel: Die irreduziblen Polynome in $\mathbb{R}[X]$ sind genau

(a) die Polynome vom Grad 1, also $aX + b$ für alle $a, b \in \mathbb{R}$ mit $a \neq 0$, sowie

(b) die Polynome vom Grad 2 ohne reelle Nullstellen, also $aX^2 + bX + c$ für alle $a, b, c \in \mathbb{R}$ mit $a \neq 0$ und $b^2 - 4ac < 0$.

$K = \mathbb{R}$, $\deg(F) \geq 3 \Rightarrow F$ reduzibel.

Bsp.: $(X^2+1)^2$ über $\mathbb{R}$ reduzibel.

Beispiel: (a) Das Polynom X^2+1 ist irreduzibel in $\mathbb{R}[X]$ und reduzibel in $\mathbb{C}[X]$.

(b) Das Polynom X^2-2 ist irreduzibel in $\mathbb{Q}[X]$ und reduzibel in $\mathbb{R}[X]$.

(c) Das Polynom X^7-3X^2+12 ist irreduzibel in $\mathbb{Q}[X]$ und reduzibel in $\mathbb{R}[X]$.

(d) Das Polynom $X^{65536}+X^{65535}+\ldots+X^2+X+1$ ist irreduzibel in $\mathbb{Q}[X]$.

(e) Das Polynom X^3+X+1 ist irreduzibel in $\mathbb{F}_2[X]$.

Proposition: Für jedes irreduzible Polynom $p(X)\in K[X]$ und je zwei Polynome $F', F''\in K[X]$ gilt:

$$p \text{ teilt } F'F'' \iff p \text{ teilt } F' \text{ oder } F''.$$

Beweis siehe Algebra I.

Satz: Jedes normierte Polynom in $K[X]$ ist ein Produkt von normierten irreduziblen Polynomen in $K[X]$, und diese sind bis auf Vertauschung eindeutig bestimmt.

Beweis siehe Algebra I.

Bemerkung: Ob und wie man diese Faktorisierung konkret bestimmen kann, hängt vom Körper K ab. Ist K endlich, so gibt es überhaupt nur endlich viele Polynome von kleinerem Grad, und es genügt, jedes davon auf Teilbarkeit zu überprüfen. Für ein effektives Verfahren z.B. im Fall $K=\mathbb{Q}$ siehe Algebra II.

8 Endomorphismen I

8.1 Charakteristisches Polynom

$A = (a_{ij})_{ij}$ $\Rightarrow$ $X \cdot I_n - A =$

$$\begin{pmatrix} X-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & X-a_{22} & & \vdots \\ \vdots & & \ddots & -a_{n-1,n} \\ -a_{n1} & \cdots & & X-a_{nn} \end{pmatrix}$$

Definition: Das *charakteristische Polynom* einer $n \times n$-Matrix A über K ist

$$\mathrm{char}_A(X) := \det(X \cdot I_n - A) \in K[X].$$

Proposition: Das Polynom $\mathrm{char}_A(X)$ ist normiert vom Grad n, und sein konstanter Koeffizient ist $(-1)^n \cdot \det(A)$.

Bemerkung: Das charakteristische Polynom kann man auch bestimmen aus der Formel $\det(A - X \cdot I_n) = \pm \mathrm{char}_A(X)$.

Proposition: Je zwei ähnliche Matrizen über K haben dasselbe charakteristische Polynom.

Beweis:

$$\det(X I_n - A) = \det\left((X \cdot \delta_{ij} - a_{ij})_{ij}\right) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \cdot \prod_{i=1}^{n} (X \cdot \delta_{i,\sigma i} - a_{i,\sigma i})$$

$\deg = n$ wenn $\sigma = \mathrm{id}$

$< n$ sonst.

$$= \prod_{i=1}^{n} (X - a_{ii}) + \text{kleinere Terme} = X^n + \text{kleinere}$$

Konstanter Koeffizient $= \det(0 \cdot I_n - A) = \det(-A) = (-1)^n \cdot \det(A)$. qed.

Beweis: $B = UAU^{-1} \Rightarrow$

$$\begin{aligned} \operatorname{char}_B(X) = \det(X \cdot I_n - B) &= \det(X \cdot U \cdot I_n \cdot U^{-1} - U \cdot A \cdot U^{-1}) \\ &= \det(U \cdot (X \cdot I_n - A) \cdot U^{-1}) \\ &= \det(U) \cdot \det(X \cdot I_n - A) \cdot \det(U^{-1}) \\ &= \qquad \operatorname{char}_A(X) \end{aligned}$$

$\det(U)^{-1}$

qed.

Sei nun f ein Endomorphismus eines endlich-dimensionalen K-Vektorraums V, und sei B eine geordnete Basis von V.

Proposition: Das charakteristische Polynom von ${}_B[f]_B$ ist unabhängig von B.

Beweis: $\forall$ Basis B, B' : ${}_B[f]_B$ und ${}_{B'}[f]_{B'}$ ähnlich. geeh.

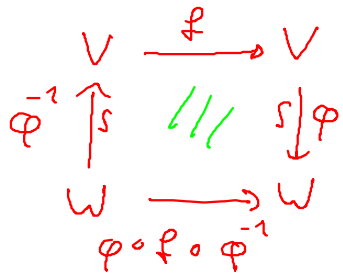
Definition: Dieses heisst das *charakteristische Polynom von f*, bezeichnet mit

$$\mathrm{char}_f(X) \;:=\; \mathrm{char}_{{}_B[f]_B}(X).$$

Dies ist ein normiertes Polynom vom Grad $\dim_K(V)$ über K, und sein konstanter Koeffizient ist $(-1)^n \cdot \det(f)$.

Proposition: Für jeden Isomorphismus von Vektorräumen $\varphi\colon V \xrightarrow{\sim} W$ gilt

$$\operatorname{char}_{\varphi\circ f\circ\varphi^{-1}}(X) \;=\; \operatorname{char}_f(X).$$



Bew.: $\mathcal{B}, \mathcal{B}'$ geordnete Basen von V, W

$$\Rightarrow \quad {}_{\mathcal{B}'}[\varphi\circ f\circ\varphi^{-1}]_{\mathcal{B}'} = {}_{\mathcal{B}'}[\varphi]_{\mathcal{B}} \cdot {}_{\mathcal{B}}[f]_{\mathcal{B}} \cdot {}_{\mathcal{B}'}[\varphi]_{\mathcal{B}}^{-1}$$

ähnlich.

qed.

Proposition: Für jedes $\lambda \in K$ gilt

$$\operatorname{char}_f(\lambda) \;=\; \det(\lambda\cdot \mathrm{id}_V - f).$$

Bew.: $\operatorname{char}_f(\lambda) = \operatorname{char}_f(X)\Big|_{X=\lambda} = \det\left(X\cdot I_n - {}_{\mathcal{B}}[f]_{\mathcal{B}}\right)\Big|_{X=\lambda}$

$= \det\left(\lambda\cdot I_n - {}_{\mathcal{B}}[f]_{\mathcal{B}}\right)$

$= \det\left(\lambda\cdot {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{B}} - {}_{\mathcal{B}}[f]_{\mathcal{B}}\right)$

$= \det\left({}_{\mathcal{B}}[\lambda\cdot \mathrm{id} - f]_{\mathcal{B}}\right)$

$= \det(\lambda\cdot \mathrm{id} - f)$. qed.

$I_n = {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{B}}$

~~$\operatorname{char}_f(X) = \det(X\cdot \mathrm{id} - f)$~~ ergibt keinen Sinn.

$X = \lambda \Rightarrow$ ~~$\operatorname{char}_f(\lambda) = \det(\lambda\cdot \mathrm{id} - f)$~~.

8.2 Eigenwerte und Eigenvektoren

Sei f ein Endomorphismus eines K-Vektorraums V.

$\in V$

Definition: Ein Vektor $v \in V$ heisst *Eigenvektor von f zum Eigenwert* $\lambda \in K$, falls $v \neq 0$ ist und $f(v) = \lambda \cdot v$. Ein Element $\lambda \in K$, welches als Eigenwert zu einem geeigneten Eigenvektor von f auftritt, heisst schlechthin ein *Eigenwert von f*.

EW

Proposition-Definition: Ein Element $\lambda \in K$ ist Eigenwert von f genau dann, wenn der Endomorphismus $\lambda \cdot \mathrm{id}_V - f \colon V \to V$ nicht injektiv ist. Der von Null verschiedene Unterraum

$$\mathrm{Eig}_{\lambda,f} := \mathrm{Kern}(\lambda \cdot \mathrm{id}_V - f) \subset V$$

heisst dann der zu λ gehörende *Eigenraum von f*. Seine von Null verschiedenen Elemente sind genau die Eigenvektoren von f zum Eigenwert λ.

Bew.: λ ist EW $\Leftrightarrow \exists\, v \in V \setminus \{0\} : f(v) = \lambda v$

$\Leftrightarrow (\lambda \cdot id_V - f)(v) = \lambda \cdot v - f(v) = 0$

$\Leftrightarrow v \in \mathrm{Kern}(\lambda \cdot id_V - f)$.

$\Leftrightarrow \mathrm{Kern}(\lambda \cdot id_V - f) \neq 0$. q.e.d.

Definition: Die *geometrische Vielfachheit* eines Eigenwerts $\lambda \in K$ von f ist die Dimension des zugehörigen Eigenraums $\mathrm{Eig}_{\lambda,f}$.

Proposition: Seien $\lambda_1, \ldots, \lambda_r \in K$ paarweise verschiedene Eigenwerte von f. Dann ist die folgende lineare Abbildung injektiv:

$$\mathrm{Eig}_{\lambda_1,f} \times \ldots \times \mathrm{Eig}_{\lambda_r,f} \longrightarrow V, \quad (v_1, \ldots, v_r) \mapsto v_1 + \ldots + v_r.$$

Beweis: Induktion über r.

$r = 0$ ✓

$r > 0 \Rightarrow$ Sei $(v_1, \ldots, v_r)$ im Kern, also $v_1 + \ldots + v_r = 0$

$\Rightarrow f(v_1) + \ldots + f(v_r) = f(v_1 + \ldots + v_r) = f(0) = 0$

$\lambda_1 \cdot v_1 + \ldots + \lambda_r \cdot v_r = 0$

$\Rightarrow \lambda_r \cdot (v_1 + \ldots + v_r) - (\lambda_1 v_1 + \ldots + \lambda_r v_r) = \lambda_r \cdot 0 - 0 = 0$

$\Rightarrow \underbrace{(\lambda_r - \lambda_1) \cdot v_1}_{\in \mathrm{Eig}_{\lambda_1,f}} + \ldots + \underbrace{(\lambda_r - \lambda_{r-1}) \cdot v_{r-1}}_{\in \mathrm{Eig}_{\lambda_{r-1}}(f)} = 0$

IV $\Rightarrow \forall 1 \le i \le r-1 : (\lambda_r - \lambda_i) v_i = 0 \Rightarrow v_i = 0 \Rightarrow v_r = -v_1 - \ldots - v_{r-1} = 0$ qed.

Folge: $\sum_{i=1}^{r} \dim \mathrm{Eig}_{\lambda_i}(\varphi) = \dim\left(\bigoplus_{i=1}^{r} \mathrm{Eig}_{\lambda_i}(\varphi)\right) \leq \dim(V)$.

Die Summe der geom. Multiplizitäten der EWe ist $\leq \dim(V)$.

Folge: Anzahl der EWe $\leq \dim(V)$.