Eigenwerte & Diagonalisierbarkeit

Def: Ein Endomorphismus $\varphi: V \to V$ heißt **diagonalisierbar**, wenn es eine Basis von V bestehend aus Eigenvektoren von φ gibt.

Bem: Ist $\dim V = n < \infty$, so ist φ genau dann diagonalisierbar, wenn es eine Basis $B = (v_1, \dots, v_n)$ von V gibt, so dass gilt

$$M_B^B(\varphi) = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$$

mit $\lambda_1, \dots, \lambda_n \in K$.

Dann sind $\lambda_1, \dots, \lambda_n$ EW von φ und v_i ist EV zum EW λ_i.

Def: Eine Matrix $A \in M_{n \times n}(K)$ ist **diagonalisierbar**, wenn der durch A beschriebene Endomorphismus $x \mapsto Ax$ von K^n diagonalisierbar ist.

$\Leftrightarrow \exists S \in Gl_n(K): \quad SAS^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ mit $\lambda_1, \dots, \lambda_n \in K$.

Bsp: Nicht jede Matrix ist diagonalisierbar!

$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\qquad$ $\ker(A - \lambda E) = \ker\begin{pmatrix} -\lambda & 1 \\ 0 & -\lambda \end{pmatrix} = \begin{cases} \langle e_1 \rangle & \text{falls } \lambda = 0 \\ 0 & \text{falls } \lambda \neq 0 \end{cases}$

$\Rightarrow$ 0 ist der einzige EW von A

Wäre A diagonalisierbar, so müsste A ähnlich sein zu $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

$\lightning$ zu $\ker A = \langle e_1 \rangle$, $\quad \ker\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = K^2$.

Lemma: Sei V ein K-VR und $\varphi: V \to V$ ein Endomorphismus. Sind $v_1, \dots, v_m$ Eigenvektoren zu paarweise verschiedenen Eigenwerten $\lambda_1, \dots, \lambda_m$ von φ, dann sind $v_1, \dots, v_m$ linear unabhängig.

Insbesondere: $m \leq \dim V$.

Beweis: Induktion nach m. $\underline{m=1}$: ✓ da $v_1 \neq 0$

$\underline{m \geq 2,\ m-1 \to m}$ Seien $\alpha_1, \dots, \alpha_m \in K$: $\alpha_1 v_1 + \_\_ + \alpha_m v_m = 0$ $(*)$

$$0 = \varphi(\underbrace{\alpha_1 v_1 + \_\_ + \alpha_m v_m}_{=0}) = \alpha_1 \varphi(v_1) + \_\_ + \alpha_m \varphi(v_m) = \alpha_1 \lambda_1 v_1 + \alpha_2 \lambda_2 v_2 + \dots + \alpha_m \lambda_m v_m$$

$$\longrightarrow \quad \cancel{\alpha_1 \lambda_1 v_1} + \alpha_2 \lambda_2 v_2 + \_\_ + \alpha_m \lambda_m v_m = 0$$

$$\cancel{\alpha_1 \lambda_1 v_1} + \alpha_2 \lambda_1 v_2 + \_\_ + \alpha_m \lambda_1 v_m = 0$$

$$\Longrightarrow \quad \alpha_2(\lambda_2 - \lambda_1) v_2 + \alpha_3(\lambda_3 - \lambda_1) v_3 + \dots + \alpha_m(\lambda_m - \lambda_1) v_m = 0$$

$$\overset{IV}{\Longrightarrow} \quad \alpha_2 \underbrace{(\lambda_2 - \lambda_1)}_{\neq 0} = \alpha_3 \underbrace{(\lambda_3 - \lambda_1)}_{\neq 0} = \_\_ = \alpha_m \underbrace{(\lambda_m - \lambda_1)}_{\neq 0} = 0$$

$$\longrightarrow \quad \alpha_2 = \alpha_3 = \_\_ = \alpha_m = 0 \overset{(*)}{\Longrightarrow} \alpha_1 v_1 = 0 \underset{v_1 \neq 0}{\Longrightarrow} \alpha_1 = 0.$$

$\square$

Lemma: Sei V ein K-VR und $\varphi: V \to V$ ein Endomorphismus. Sind $v_1, \dots, v_m$ Eigenvektoren zu paarweise verschiedenen Eigenwerten $\lambda_1, \dots, \lambda_m$ von φ, dann sind $\lambda_1, \dots, \lambda_m$ linear unabhängig.

Insbesondere: $m \leq \dim V$.

Satz: Ist $\dim V = n < \infty$ und $\varphi: V \to V$ ein Endomorphismus mit n paarweise verschiedenen Eigenwerten, so ist φ diagonalisierbar.

Beweis: Seien $\lambda_1, \dots, \lambda_n$ die EW von φ und $v_1, \dots, v_n$ zugehörige EV.
Nach dem vorhergehenden Lemma sind $v_1, \dots, v_n$ linear unabhängig.
Wegen $n = \dim V$ ist somit $(v_1, \dots, v_n)$ eine Basis von V. $\square$

Lemma: Sei V ein K-VR und $\varphi: V \to V$ ein Endomorphismus. Sind $\lambda_1, \dots, \lambda_m$ paarweise verschiedene EW von φ so ist die Summe

$$\mathrm{Eig}(\varphi;\lambda_1) \oplus \dots \oplus \mathrm{Eig}(\varphi;\lambda_m) \subseteq V.$$

direkt.

Erinnerung: Seien $U_1, \dots, U_m \subseteq V$ Unterräume. Die Summe $U_1 + \dots + U_m \subseteq V$ ist eine direkte Summe wenn gilt:

$$\forall i \in \{1, \dots, m\}: \quad U_i \cap \Big(\sum_{\substack{j=1 \\ j \neq i}}^{m} U_j \Big) = 0$$

$\iff$ Ist $u \in U_1 + \dots + U_m$ so gibt es eindeutig bestimmte $u_1 \in U_1, \dots, u_m \in U_m$ mit $u = u_1 + \dots + u_m$.

Dann gilt: Sind $B_i = (u_{i,j})_{j \in I_i}$ Basen der U_i, so ist

$$B = (u_{i,j})_{\substack{i \in \{1, \dots, m\}, \\ j \in I_i}}$$ eine Basis von $U_1 \oplus \dots \oplus U_m$.

Lemma: Sei V ein K-VR und $\varphi: V \to V$ ein Endomorphismus. Sind $\lambda_1, \dots, \lambda_m$ paarweise verschiedene EW von φ so ist die Summe

$$\mathrm{Eig}(\varphi; \lambda_1) \oplus \dots \oplus \mathrm{Eig}(\varphi; \lambda_m) \subseteq V.$$

direkt.

Beweis: Angenommen $\mathrm{Eig}(\varphi, \lambda_i) \cap \left(\sum_{\substack{j=1 \\ j \neq i}}^{m} \mathrm{Eig}(\varphi; \lambda_j) \right) \neq 0$ für ein $i \in \{1, \dots, m\}$

$$\Rightarrow \exists v_i \in \mathrm{Eig}(\varphi; \lambda_i) \setminus \{0\}: \quad v_i = \sum_{\substack{j=1 \\ j \neq i}}^{m} v_j \quad , v_j \in \mathrm{Eig}(\varphi, \lambda_j) \quad (j \neq i).$$

$$\Rightarrow v_i - \sum_{\substack{j=1 \\ j \neq i}}^{m} v_j = 0 \qquad \lightning. \qquad \square$$

Bemerkung: Ist $\dim V = n < \infty$, so ist $\sum_{i=1}^{m} \dim(\mathrm{Eig}(\varphi; \lambda_i)) \leq n$.

D.h. die Summe der geometrischen Vielfachheiten der EW von φ ist höchstens n.

Satz: Sei V ein K-VR mit $\dim V = n < \infty$ und $\varphi: V \to V$ ein Endomorphismus.
Seien $\lambda_1, \dots, \lambda_m$ die paarweise verschiedenen EW von φ $(m \geq 0)$, und
$n_j := \dim \mathrm{Eig}(\varphi; \lambda_j)$ für $j \in \{1, \dots, m\}$.

Dann ist $n_1 + \dots + n_m \leq n$ und φ ist diagonalisierbar $\Leftrightarrow n_1 + \dots + n_m = n$.

Beweis: $n_1 + \dots + n_m \leq n$ haben wir soeben gezeigt.

zz: φ diagonalisierbar $\Leftrightarrow n_1 + \dots + n_m = n$.

„$\Rightarrow$“ Sei B eine Basis von V bestehend aus EV von φ. Seien die Vektoren in B benannt durch:

$$\begin{aligned}
v_{1,1}, \dots, v_{1,e_1} &\in \mathrm{Eig}(\varphi; \lambda_1)\\
v_{2,1}, \dots, v_{2,e_2} &\in \mathrm{Eig}(\varphi; \lambda_2)\\
\vdots \qquad\quad \vdots \quad &\\
v_{m,1}, \dots, v_{m,e_m} &\in \mathrm{Eig}(\varphi, \lambda_m)
\end{aligned}$$

mit $\forall i \in \{1, \dots, m\}\ \forall j \in \{1, \dots, \cancel{e_m}\, e_i\}: \varphi(v_{i,j}) = \lambda_i v_{i,j}$

$\Rightarrow \forall i \in \{1, \dots, m\}: e_j \leq n_j$

$n = e_1 + \dots + e_m \leq n_1 + \dots + n_m \leq n. \quad \Rightarrow n_1 + \dots + n_m = n.$

Satz: Sei V ein K-VR mit $\dim V = n < \infty$ und $\varphi: V \to V$ ein Endomorphismus. Seien $\lambda_1, \ldots, \lambda_m$ die paarweise verschiedenen EW von φ $(m \geq 0)$, und $n_j := \dim \mathrm{Eig}(\varphi; \lambda_j)$ für $j \in \{1, \ldots, m\}$.

Dann ist $n_1 + \ldots + n_m \leq n$ und φ ist diagonalisierbar $\Leftrightarrow n_1 + \ldots + n_m = n$.

Beweis: $n_1 + \ldots + n_m \leq n$ haben wir soeben gezeigt.

ZZ: φ diagonalisierbar $\Leftarrow n_1 + \ldots + n_m = n$.

„$\Leftarrow$": Für $i \in \{1, \ldots, m\}$ sei $(b_{i,1}, \ldots, b_{i,n_i})$ Basis von $\mathrm{Eig}(\varphi; \lambda_i)$

$B = (b_{1,1}, \ldots, b_{1,n_1}, b_{2,1}, \ldots, b_{2,n_2}, \ldots, b_{m,1}, \ldots, b_{m,n_m})$ ist linear unabhängig

$\overset{n_1 + \ldots + n_m = n}{\Longrightarrow}$ B ist Basis von V.

$\square$

Verfahren zur Diagonalisierung einer Matrix $A \in M_{n\times n}(K)$

(1) Eigenwerte $\lambda_1, \dots, \lambda_m$ bestimmen: $\lambda \in K$ ist EW $\Leftrightarrow \det(A - \lambda E) = 0$

Nullstellen der Funktion $K \to K$, $\lambda \longmapsto \det(A - \lambda E) = \det \begin{pmatrix} a_{11}-\lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-\lambda & a_{23} \dots & a_{2n} \\ \vdots & & & \\ a_{n1} & \dots & a_{n,n-1} & a_{nn}-\lambda \end{pmatrix}$

berechnen.

(2) Zu jedem EW λ_i eine Basis $v_{i,1}, \dots, v_{i,n_i}$ des Eigenraums $\mathrm{Eig}(\varphi, \lambda_i) = \ker(A - \lambda_i E)$ bestimmen.

(3) Ist $n_1 + \dots + n_m = n$: Basen der Eigenräume zu einer Basis $\mathcal{B}$ von V vereinigen.

$$T_{\mathcal{E}}^{\mathcal{B}} = \left(v_{1,1} \dots v_{1,n_1} \; v_{2,1} \dots v_{2,n_2} \dots\dots v_{m,1} \dots v_{m,n_m} \right)$$

$\Longrightarrow \quad (T_{\mathcal{E}}^{\mathcal{B}})^{-1} A \, T_{\mathcal{E}}^{\mathcal{B}}$ ist Diagonalmatrix.

Einschub: Polynome & Polynomfunktionen

Eine Funktion $F: K \to K$ heißt **Polynomfunktion**, wenn es $a_0, \dots, a_n \in K$ gibt, so dass für alle $x \in K$ gilt:

$$F(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Ist G eine Polynomfunktion mit $G(x) = \sum_{j=0}^{m} b_j x^j$, so sind auch FG und $F+G$ Polynomfunktionen:

$$(F+G)(x) = \sum_{i=0}^{n} (a_i + b_i) x^i \qquad (\text{o.E. } m \leq n,\ b_{m+1} = \dots = b_n = 0)$$

$$(FG)(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{m+n} \left(\sum_{l=0}^{k} a_l b_{k-l}\right) x^k$$

Die Polynomfunktionen (über einem festen Körper K) bilden einen kommutativen Ring (mit Eins)

<u>Def:</u> Eine Menge R mit Verknüpfungen $+, \cdot : R \times R \to R$ heißt **Ring** (mit Eins) wenn gilt:

- $(R, +)$ ist eine abelsche Gruppe
- $\forall a, b, c \in R: \quad (ab)c = a(bc)$
- $\forall a, b, c \in R: \quad a(b+c) = ab + ac$ und $(a+b)c = ac + bc$.
- Es gibt ein (eindeutig bestimmtes) Einselement $1 \in R$ mit $1a = a1 = a$ für alle $a \in R$.

R ist **kommutativ** wenn für alle $a, b \in R$ gilt $ab = ba$.

Satz [Analysis] Sei $K=\mathbb{R}$ oder $K=\mathbb{C}$. Sind F, G Polynomfunktionen mit $F(x)=\sum_{i=0}^{n} a_i x^i$, $G(x)=\sum_{i=0}^{n} b_i x^i$ für $x\in K$ so gilt: $a_i=b_i$ für $0\leq i\leq n$.

Dieser Satz gilt nicht über endlichen Körpern!

Bsp: $K=\mathbb{Z}/2\mathbb{Z}=\{\bar{0},\bar{1}\}$

$\bar{0}+\bar{0}=\bar{0}$ $\quad \bar{1}+\bar{0}=\bar{0}+\bar{1}=\bar{1}$ $\quad \bar{1}+\bar{1}=\bar{0}$

$\bar{0}\cdot\bar{1}=\bar{1}\cdot\bar{0}=\bar{0}\cdot\bar{0}=\bar{0}$ $\quad \bar{1}\cdot\bar{1}=\bar{1}$

$F(x)=x^2+x+\bar{1}$ $\qquad G(x)=\bar{1}$

$F(\bar{0})=\bar{0}^2+\bar{0}+\bar{1}=\bar{0}+\bar{0}+\bar{1}=\bar{1}$ $\qquad G(\bar{0})=\bar{1}$

$F(\bar{1})=\bar{1}+\bar{1}+\bar{1}=\bar{0}+\bar{1}=\bar{1}$ $\qquad G(\bar{1})=\bar{1}$ $\qquad \rightarrow F=G$

Insb. die Definition der Vielfachheit von Nullstellen einer Polynomfunktion stellt über endlichen Körpern ein Problem dar!

Def: (1) Ein Polynom über K ist eine Folge $(a_i)_{i\geq 0}$ von Elementen $a_i \in K$, bei der nur endlich viele Glieder $\neq 0$ sind.

(2) Auf der Menge der Polynome definiert man:

$$(a_i)_{i\geq 0} + (b_i)_{i\geq 0} := (a_i + b_i)_{i\geq 0}$$

$$(a_i)_{i\geq 0} \cdot (b_i)_{i\geq 0} := \left(\sum_{l=0}^{k} a_{k-l} b_l \right)_{k\geq 0}$$

(3) Das Nullpolynom $0 := (0)_{i\geq 0}$, das Einspolynom $1 := (1, 0, 0, \ldots\ldots)$

(4) Ist $f = (a_i)_{i\geq 0}$, so sei der Grad

$$\deg f = \operatorname{gr} f := \begin{cases} \max\{n \geq 0 : a_n \neq 0\} & \text{falls } f \neq 0 \\ -\infty & \text{falls } f = 0 \end{cases}$$

(5) Polynome von Grad ≤ 0 heißen konstante Polynome.

Polynome vom Grad ≤ 1 heißen lineare Polynome.

Satz: Sei $K[X]$ die Menge aller Polynome über K.

(1) $(K[X], +, \cdot)$ ist ein kommutativer Ring (mit Eins).

(2) $(K[X], +)$ gemeinsam mit dem Produkt

$$\lambda (a_i)_{i \geq 0} = (\lambda a_i)_{i \geq 0} \qquad (\lambda \in K)$$

bildet einen K-VR.

(Beweis durch langwieriges Nachrechnen.)

Bemerkung: $K[X]$ ist damit auch eine K-Algebra.

Sei $X := (0, 1, 0, \ldots) \in K[X]$.

$\Rightarrow X^0 = 1, \quad X^n = (0, \ldots, 0, \underset{\uparrow\, n\text{-te Stelle}}{1}, 0, \ldots) \quad (n \geq 0)$

$(X^n)_{n \geq 0}$ ist eine Basis von $K[X]$:

Ist $f = (a_i)_{i \geq 0} \in K[X]$ und $n = \deg f$

$$\Rightarrow \quad f = \sum_{i=0}^{n} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 .$$

X bezeichnet man als Unbestimmte.

Def: Für $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ und $\lambda \in K$ sei $f(\lambda) := \sum_{i=0}^{n} a_i \lambda^i$

Sind $f, g \in K[X]$, so gilt $(f+g)(\lambda) = f(\lambda) + g(\lambda)$, $(fg)(\lambda) = f(\lambda) g(\lambda)$

(Beweis durch Nachrechnen)

Sind $f, g \in K[X]$, so gilt $(f+g)(\lambda) = f(\lambda) + g(\lambda)$, $(fg)(\lambda) = f(\lambda) g(\lambda)$
(Beweis durch Nachrechnen)

Def: Für $f \in K[X]$ sei $\tilde{f}: K \to K$, $\lambda \mapsto f(\lambda)$ $\in \mathrm{Abb}(K, K)$ die
durch f bestimmte Polynomfunktion.

Damit ist $\sim: \begin{cases} K[X] \longrightarrow \mathrm{Abb}(K,K) \\ f \longmapsto \tilde{f} \end{cases}$ eine Abbildung, die jedem
Polynom eine Polynomabbildung zuweist.

Bem: Es gilt $\widetilde{f+g} = \tilde{f} + \tilde{g}$, $\widetilde{fg} = \tilde{f}\tilde{g}$, $\tilde{1} = 1$, d.h. $\sim$ ist ein Ringhomomorphismus.

Bsp: $K = \mathbb{Z}/2\mathbb{Z}$. $f = X^2 + X + \bar{1}$, $g = \bar{1} \in \mathbb{Z}/2\mathbb{Z}[X]$ $f \neq g$ aber $\tilde{f} = \tilde{g}$!

Lemma: Seien $f, g \in K[X]$.

(1) Es ist $\deg(f+g) \leq \max\{\deg f, \deg g\}$.

degree

Ist $\deg f \neq \deg g$, so gilt $\deg(f+g) = \max\{\deg f, \deg g\}$

(2) $\deg(fg) = \deg f + \deg g$

(mit $n + (-\infty) = -\infty$, $(-\infty) + (-\infty) = -\infty$, $\max\{n, -\infty\} = n$)

Beweis: (1) Sei $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{n} b_i X^i$ mit $n = \operatorname{gr} f$ $(a_n \neq 0)$, $\operatorname{gr} f \geq \operatorname{gr} g$.

$$f+g = (a_n + b_n) X^n + \sum_{i=0}^{n-1} (a_i + b_i) X^i$$

$\Rightarrow \deg(f+g) \leq n = \max\{\deg f, \deg g\}$

Ist $\deg f \neq \deg g \Rightarrow b_n = 0 \rightarrow a_n + b_n = a_n \neq 0 \Rightarrow \deg(f+g) = n$.

Lemma: Seien $f, g \in K[X]$.

(1) Es ist $\deg(f+g) \leq \max\{\deg f, \deg g\}$.

Ist $\deg f \neq \deg g$, so gilt $\deg(f+g) = \deg f + \deg g$

(2) $\deg(fg) = \deg f + \deg g$ (mit $n + (-\infty) = -\infty$, $(-\infty) + (-\infty) = -\infty$, $\max\{n, -\infty\} = n$)

Beweis: (2) Sei $n = \deg f$, $m = \deg g$ oE: $n, m \neq -\infty$.

Sei $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{m} b_i X^i$ mit $a_n \neq 0$, $b_m \neq 0$.

$fg = \sum_{k \geq 0} c_k X^k$ mit $c_k = \sum_{\ell=0}^{k} a_\ell b_{k-\ell}$

$k > m+n$: $\Rightarrow 0 \leq \ell \leq k$: $\ell > n$ oder $k - \ell > m$ $\Rightarrow c_k = 0$
$\ell > n \Rightarrow a_\ell = 0$, $k-\ell > m \Rightarrow b_{k-\ell} = 0$

$\Rightarrow \deg(fg) \leq m+n$.

$k = m+n$: $c_{m+n} = a_n b_m + \sum_{\ell=0}^{n-1} a_\ell \underbrace{b_{m+n-\ell}}_{\neq 0} + \sum_{\ell=n+1}^{m+n} \underbrace{a_\ell}_{=0} b_{m+n-\ell} = a_n b_m \neq 0$.

$\Rightarrow \deg(fg) = m+n$.

Bem: Es gilt $\forall m, n \geq 0$: $X^m X^n = X^{m+n}$

Bemerkung: Der kommutative Ring $K[X]$ ist nullteilerfrei,
d.h. sind $f, g \in K[X]$ mit $fg = 0 \Rightarrow f = 0$ oder $g = 0$

(denn: sind $f, g \neq 0$, so ist $\deg(fg) = \deg f + \deg g \geq 0$.)

Satz (Polynomdivision) Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q, r \in K[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.

Beweis: **Existenz:** Induktion nach $n = \deg f$

$\underline{n < \deg(g)}$: $q = 0$, $r = f$ ✓

$\underline{n \geq \deg(g)}$: Die Aussage gelte für $n' < n$.

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0, \quad g = b_m X^m + \ldots + b_0, \quad a_n \neq 0, \ b_m \neq 0, \quad n \geq m$$

$$h := f - \frac{a_n}{b_m} X^{n-m} g \implies \deg(h) < n$$

$$\overset{IV}{\implies} h = q' g + r' \quad \text{mit} \quad q', r' \in K[X] \quad \text{und} \quad \deg(r') < \deg(g) = m.$$

$$\longrightarrow \quad f = \underbrace{\left(q' + \frac{a_n}{b_m} X^{n-m} \right)}_{=: q} g + \underbrace{r'}_{=: r} \quad \text{mit} \quad \deg(r') < \deg(g)$$

Satz (Polynomdivision) Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q, r \in K[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.

Beweis: Eindeutigkeit:

Sei $f = qg + r = q'g + r'$ mit $q, q', r, r' \in K[X]$ $\deg(r), \deg(r') < \deg(g)$.

$\Longrightarrow \quad (q-q')g \overset{(*)}{=} r' - r$

$\deg(r'-r) < \deg(g)$

$\deg((q-q')g) = \deg(q-q') + \deg(g) \Rightarrow q - q' = 0 \Rightarrow q = q' \overset{(*)}{\Longrightarrow} r' = r.$

$\square$

Lemma: Sei $f \in K[X]$, $\lambda \in K$.

Dann ist $\tilde{f}(\lambda) = f(\lambda) = 0 \iff \exists q \in K[X]: \quad f = q(X-\lambda)$.

Beweis: Sei $f = q(X-\lambda) + r$ mit $\deg(r) \leq 0$ d.h. r ist konstant $(r \in K)$

$$f(\lambda) = \underbrace{q(\lambda)\,(\lambda-\lambda)}_{=0} + \underbrace{r(\lambda)}_{r} = r$$

$f(\lambda) = 0 \iff r = 0.$ $\square$

Def: Sei $f \in K[X]$ und $\lambda \in K$.

(1) $\lambda \in K$ heißt **Nullstelle** von f, wenn gilt $f(\lambda) = 0$.

(2) Sei $f \neq 0$. Die **Vielfachheit** von λ in f ist die größte Zahl $m \geq 0$ so dass es $g \in K[X]$ gibt mit

$$f = (X-\lambda)^m g$$

Bem: $m > 0 \iff \lambda$ ist Nullstelle von f

Ist m die Vielfachheit von λ in f und $f = (X-\lambda)^m g$, so ist $g(\lambda) \neq 0$

Def: Sei $f \in K[X]$ und $\lambda \in K$.

(1) $\lambda \in K$ heißt Nullstelle von f, wenn gilt $f(\lambda) = 0$.

(2) Sei $f \neq 0$. Die Vielfachheit von λ in f ist die größte Zahl $m \geq 0$ so dass es $g \in K[X]$ gibt mit

$$f = (X - \lambda)^m g$$

Bsp: In $\mathbb{Z}/2\mathbb{Z}$: $f = X(X - \bar{1})$ $\quad g = X^2(X - \bar{1})^2$

$\Rightarrow \tilde{f} = \tilde{g} = \bar{0}$ $\quad f$ hat Nullstellen $\bar{0}, \bar{1}$ mit Vielfachheit 1

g — " — 2

Satz: Sei $0 \neq f \in K[X]$ und $\lambda_1, \dots, \lambda_m$ seien paarweise verschiedene Nullstellen von f, mit Vielfachheiten $n_1, \dots, n_m$.

Dann ist $f = (X-\lambda_1)^{n_1} \cdots (X-\lambda_m)^{n_m} g$ mit $g \in K[X]$, $g(\lambda_j) \neq 0$ für $j \in \{1, \dots, m\}$.

Ist weiters $f = (X-\lambda_1)^{n_1'} \cdots (X-\lambda_m)^{n_m'} g'$ mit $n_1', \dots, n_m' \geq 0$, $g' \in K[X]$ so ist $n_1' = n_1, \dots, n_m' = n_m$ und $g' = g$.

(ohne Beweis: Induktion & Nullteilerfreiheit)

Korollar: $n_1 + \dots + n_m \leq \deg f$.

Insbesondere: Ein von 0 verschiedenes Polynom f hat höchstens $\deg f$ Nullstellen.

Satz (Identitätssatz für Polynome)
Ist K ein unendlicher Körper, so ist die Abbildung

$$\sim : \begin{cases} K[X] \longrightarrow \mathrm{Abb}(K,K) \\ f \longmapsto \tilde{f} \end{cases}$$

injektiv. D.h. sind $f, g \in K[X]$ mit $\tilde{f} = \tilde{g} \Rightarrow f = g$.

Explizit: Seien $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{n} b_i X^i$.

Gilt für alle $\lambda \in K$: $f(\lambda) = g(\lambda) \Rightarrow \forall 0 \leq i \leq n: a_i = b_i$.

Beweis Seien $f, g \in K[X]$ mit $\tilde{f} = \tilde{g} \rightarrow \forall \lambda \in K: \tilde{f}(\lambda) = \tilde{g}(\lambda) \Rightarrow \underbrace{(\tilde{f} - \tilde{g})}_{= \widetilde{f-g}}(\lambda) = 0$

$\rightarrow f - g \in K[X]$ hat unendlich viele Nullstellen.

$\Rightarrow f - g = 0 \Rightarrow f = g$.

$\square$

Def: Ein Körper K ist algebraisch abgeschlossen, wenn jedes nicht-konstante Polynom zumindest eine Nullstelle besitzt.

Bem: K ist algebraisch abgeschlossen, genau dann, wenn jedes $0 \neq f \in K[X]$ in ein Produkt von Linearfaktoren und einen Konstanten zerfällt, d.h.

$$f = \alpha \prod_{j=1}^{m} (X - \lambda_j)^{m_j}$$

Bsp: $\mathbb{R}$ ist nicht algebraisch abgeschlossen: X^2+1 besitzt keine Nullstelle in $\mathbb{R}$!

Satz (Fundamentalsatz der Algebra) $\mathbb{C}$ ist algebraisch abgeschlossen

Bem: Zu jedem Körper K gibt es einen algebraisch abgeschlossenen Oberkörper K'!

Bem: • Der Name der Unbestimmten kann frei gewählt werden: $K[X]$, $K[Y]$, $K[T]$, $K[t]$, $K[u]$, ...

• Rationale Funktionenkörper:

Auf $\{(f,g) : f,g \in K[X],\ g \neq 0\}$ definiert man eine Äquivalenzrelation

$$(f,g) \sim (f',g') \Leftrightarrow fg' = gf'.$$

Für die Äquivalenzklassen schreibt man $\frac{f}{g}$, und definiert

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + f'g}{gg'}, \qquad \frac{f}{g}\,\frac{f'}{g'} = \frac{ff'}{gg'}$$

Damit wird die Menge aller Äquivalenzklassen zu einem Körper, dem rationalen Funktionenkörper

$$K(X) = \left\{\frac{f}{g} : f,g \in K[X],\ g \neq 0\right\} \supseteq \left\{\frac{f}{1} : f \in K[X]\right\} \cong K[X]$$

Damit lässt sich Determinante einer Matrix mit Polynomeinträgen rechtfertigen.

Zusammenfassend:

- Polynome haben die üblichen bekannten Eigenschaften
- Die Unterscheidung von Polynomen und Polynomfunktionen ist nur über endlichen Körpern notwendig.

Das charakteristische Polynom

<u>Def:</u> Sei K ein Körper, $A \in M_{n\times n}(K)$,

Das charakteristische Polynom von A ist das Polynom

$$P_A := \det(A - XE) \underset{\det}{=} \begin{pmatrix} a_{11}-X & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22}-X & a_{23} & \cdots & a_{2n} \\ \vdots & & \ddots & & \vdots \\ a_{n,1} & \cdots & & a_{n,n-1} & a_{nn}-X \end{pmatrix} \in K[X]$$

<u>Bem:</u> λ ist EW von A

$\iff \det(A - \lambda E) = 0$

$\iff P_A(\lambda) = 0.$