

## IX POLYNOME UND ALGEBREN

### 9.1 DEFINITION

$\mathbb{K}$  Körper. Eine  $\mathbb{K}$ -Algebra ist ein Vektorraum  $A$  über  $\mathbb{K}$  mit Multiplikation  $*: A \times A \rightarrow A$ , so dass

$$i) \quad a * (b + c) = a * b + a * c \quad \text{Distributivit\"at}$$

$$ii) \quad (a + b) * c = a * c + b * c$$

$$iii) \quad \lambda(a * b) = (\lambda a) * b = a * (\lambda b) \quad \text{Assoziativit\"at}$$

### 9.2 BEHERKUNG

- Wenn zusätzlich gilt  $(a * (b * c)) = ((a * b) * c)$  dann heißt  $A$  assoziativ
- Wenn zusätzlich gilt  $a * b = b * a$ , dann heißt  $A$  kommutativ

### 9.3 BEISPIELE

a)  $(\mathbb{K}, +, \cdot)$  assoziativ, kommutativ

b)  $\text{Hom}(V, V) = \text{End}(V)$

$$f * g := f \circ g \quad \text{nichtkommutativ, assoziativ, Algebra}$$

$$(\mathbb{K}^{n \times n}, +, \cdot) \quad \text{Matrixmultiplikation}$$

$$\text{Hadamard oder Schurprodukt } [a_{ij}] \cdot [b_{ij}] = [a_{ij} b_{ij}]$$

c)  $C[0, 1]$  kommutativ, assoziativ

$$(f * g)(t) = f(t) g(t)$$

$$(f * g)(t) = \int f(t-s) g(s) ds \quad \text{Faltung}$$

d)  $(\mathbb{R}^3, +, \times)$ , Kreuzprodukt  $a \times b = -b \times a$

$$(a \times b) \times c \neq a \times (b \times c)$$

$\rightarrow$  nicht assoziativ, nichtkommutativ - Quaternionen

e)  $(K^{n \times n} +, [ ])$

$$[A, B] = A \cdot B - B \cdot A$$

Lie - Produkt

Kommatorprodukt

nichtkommutativ, nicht assoziativ

→ Jacobi - Identität

f)  $A = K^{n \times n}$  symm. =  $\{A \mid A = A^T\}$

$$A * B = \frac{AB + BA}{2} \quad \text{jordan - Produkt}$$

assoziativ, kommutativ

### 9.4 DEFINITION

$K^\infty = \{(a_0, a_1, a_2, \dots) \mid a_i \in K\}$  Vektoren aller Folgen

$P_K = \{(a_0, a_1, \dots, a_n, 0, 0, \dots) \mid a_i \in K\}$

Unterraum der endlichen Folgen

Basis von  $P_K$ :  $(e_i)_{i \geq 0}$

$$(a_n) * (b_n) = (c_n)$$

$$c_n = \sum_{k=0}^n a_k b_{n-k} = \sum_{k=0}^n a_{n-k} b_k \quad \text{Cauchy - Produkt}$$

### 9.5 SATZ

i)  $(P_K, *)$  ist eine assoziative, kommutative  $K[G]$ -Algebra

mit Einselement  $(1, 0, 0, \dots) = e_0$

$$x^k := e_k \quad e_i * e_j = e_{i+j}$$

ii)  $[K[x]] = \left\{ \sum_{k=0}^{\infty} a_k x^k \mid a_k \in K \right\}$  formale Potenzreihen

bilden kommutative, assoziative Algebra

ad ii)) Sei  $a_i = 0$  für  $i > m$ ,  $b_j = 0$  für  $j > n$

$$\sum_{i=0}^n a_i b_{n-i} = \sum_{i=0}^m a_i b_{n-i} = 0 \quad k > m+n$$

$$\begin{array}{ccccc} & & & & \\ & \overbrace{\phantom{aaaaaaa}}^{\substack{a_0 \quad a_1 \quad \dots \quad a_m}} & & & \\ & & & & \\ & i < m & & n & \\ & & & k-i > m+n-i & \end{array}$$

$$\text{W.R.: } \int \frac{1}{x} = \log|x|$$

$$\log(-1) = e^{\log(-1)} = -1$$

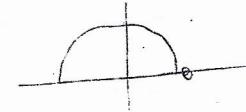
$$e^{i\varphi} = \cos \varphi + i \sin \varphi$$

$$e^{i\pi} = -1$$

$$1 + e^{i\pi} = 0$$

$$\log(-1) = i\pi$$

$$\sqrt{-1} = \pm i$$



$$\sqrt[3]{-1} = 1, e^{\frac{2\pi i}{3}}, e^{-\frac{2\pi i}{3}} \quad \sqrt{e^{ix}} = e^{\frac{ix}{2}}$$

$$(\mathbb{P}_K, *) \quad \mathbb{P}_K = \{ (a_0, a_1, \dots, a_n, 0, \dots) \mid a_k \in K, n \in \mathbb{N}_0 \}$$

$$\text{mit } (a_i) * (b_j) = c_k$$

ist eine assoziative, kommutative  $\mathbb{K}$ -Algebra

$$c_k = \sum_{j=1}^k a_j b_{k-j} = \sum_{j=0}^k a_{k-j} b_j$$

$$e_i * e_j = e_{i+j} \quad x^i := e_i$$

$$\text{Sei } a_i = 0 \text{ für } i > m, \quad b_j = 0 \text{ für } j > n$$

$$\begin{array}{ccccccc} & & & & & & \\ \hline & & & & & & \\ & & & & & & \\ \hline & & & & & & \\ a_0 & a_1 & \dots & a_m & & & m+n \\ & & & & & & \end{array}$$

$$c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^m a_i \underbrace{b_{k-i}}_{=0} = 0$$

$$k > m+n$$

$$i < m$$

$$k-i > m+n-i > n$$

$$\deg(p(x)q(x)) \leq \deg p(x) + \deg q(x)$$

$$p(x) = a_0 + a_1 x + \dots + a_m x^m$$

$$\deg p(x) = \max \{ i \mid a_i \neq 0 \}$$

$$\text{Distributivgesetze } (a * (b+c))_k = \sum_{i=0}^k a_i (b_{k-i} + c_{k-i})$$

$$= \sum_{i=0}^k a_i b_{k-i} + \sum_{i=0}^k a_i c_{k-i} = (a * b)_k + (a * c)_k$$

→ funktioniert auch für beliebige Folgen:

$$(a * b)_k = \sum a_i b_{k-i} \text{ ist endl für alle } k$$

## 9.6 DEFINITION

$$x^0 := (1, 0, \dots, 0) =: 1$$

$$x^k := (0, \dots, 0, 1, 0, \dots, 0)$$

$$x^k \cdot x^\ell = x^{k+\ell}$$

wir schreiben  $\mathbb{K}[x]$  anstelle von  $\mathbb{P}_\mathbb{K}$

$$p(x) = \sum_{i=0}^m a_i x^i$$

$$\Rightarrow \deg p(x) = \max \{i \mid a_i \neq 0\}$$

$$\deg 0 := -\infty$$

## 9.7 LEMMA

i)  $\deg(p(x) \cdot q(x)) = \deg p(x) + \deg q(x)$

ii)  $\mathbb{K}[x]$  ist nullteilerfrei

$$p(x) \cdot q(x) = 0 \Rightarrow p(x) = 0 \vee q(x) = 0$$

$$\text{Zn und P } n = p \cdot q \Rightarrow p \neq 0 \text{ mod n } q \neq 0 \text{ mod n}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

## 9.8 DEFINITION

Jedes Polynom  $p(x) \in \mathbb{K}[x]$  induziert eine Funktion

$$p: \mathbb{K} \rightarrow \mathbb{K}$$

$$\alpha \mapsto p(\alpha) = \sum_{k=0}^n a_k \alpha^k$$

$$(\lambda p + \mu q)(\alpha) = \lambda p(\alpha) + \mu q(\alpha)$$

$$(p \cdot q)(\alpha) = p(\alpha) \cdot q(\alpha)$$

$\mathbb{K}[x] \rightarrow \mathbb{K}^\mathbb{K}$  ist ein Algebra-Homomorphismus

- injektiv?

Wem  $|\mathbb{K}| < \infty$

$$\dim \mathbb{K}[x] = \infty$$

$$\dim \mathbb{K}^\mathbb{K} = |\mathbb{K}|$$

$p(x) = (x - \xi_1)(x - \xi_2) \dots (x - \xi_n)$  hat Grad n

$$\mathbb{K} = \{\xi_1, \dots, \xi_n\} \quad f \mapsto = \int_{\mathbb{K}} f(\xi) d\xi$$

$$\text{wobei } \delta_\xi(x) = \begin{cases} 0 & x \neq \xi \\ 1 & x = \xi \end{cases}$$

surjektiv?  $\rightarrow$  (ii)

9.9

Jede Funktion  $f: \mathbb{K} \rightarrow \mathbb{K}$  ist Polynomfunktion, d.h.  
 $\exists$  Polynom  $p(x) \in \mathbb{K}[x]$  sodass  $p(z) = f(z) \quad \forall z \in \mathbb{K}$

9.10 DEFINITION

Eine Abbildung  $\psi: A \rightarrow B$  zwischen zwei  $\mathbb{K}$ -Algebren  
heißt Algebrahomomorphismus, wenn  $\psi$  linear  
und multiplikativ ist:

$$(\forall a, b \in A): \psi(a *_A b) = \psi(a) *_B \psi(b)$$

9.11 BEISPIEL

a)  $\mathbb{K}[x] \rightarrow \mathbb{K}^{\mathbb{K}}$

$p(x) \mapsto$  Polynomfunktion

b) Für  $x \in \mathbb{K}$

$\forall a: \mathbb{K}[x] \rightarrow \mathbb{K}$  ist Algebrahomomorphismus  
 $p(x) \mapsto p(a)$

c)  $\mathbb{K} \rightarrow \mathbb{K}[x]$

Einbettung, Algebrahomomorphismus

$x \mapsto x \cdot 1$

9.12 Einsetzungssatz

Sei  $A$  associative Algebra über  $\mathbb{K}$  mit  
Einselement  $1_A$

i)  $\psi: \mathbb{K} \rightarrow A$  ist Algebrahomomorphismus  
 $a \mapsto a \cdot 1_A$

ii) Für jedes  $a \in A$  ist die Abbildung

$$\psi_a: \mathbb{K}[x] \rightarrow A$$

$$\sum_{n=0}^{\infty} c_n x^n \mapsto \sum_{n=0}^{\infty} c_n a^n$$

wobei  $a^0 := 1$  und  $a^{k+1} := a * a^k$

der eindeutige Algebrahomomorphismus

$\psi: \mathbb{K}[x] \rightarrow A$  mit der Eigenschaft  $\psi(x) = a$

iii) Jeder Algebrahomomorphismus  $\varphi: \mathbb{K}[x] \rightarrow A$   
hat diese Form

Beweis

Wenn  $a = \varphi(k) \Rightarrow a^k = \varphi(x)^k = \varphi(x^k)$

Wenn  $\varphi(x)$  bekannt ist, dann ist  $\varphi(x^k)$  festgelegt  
für alle  $k \Rightarrow \varphi(p(x))$  ist festgelegt für  
alle  $p(x) \in \mathbb{K}[x]$  (Fortsatzungssatz)

- Linearität von  $\varphi_a$ :  $\textcircled{u}$

- Multiplikativität

$$\varphi_a(p(x)q(x)) \stackrel{!}{=} \varphi_a(p(x)) + \varphi_a(q(x))$$

$$\text{Sei } p(x) = \sum_{i=0}^m a_i x^i \quad q(x) = \sum_{j=0}^n b_j x^j$$

$$p(x) \cdot q(x) = \sum_{k=0}^{m+n} \gamma_k x^k \quad \text{wobei } \gamma_k = \sum_{i+j=k} a_i b_{j-i}$$

$$\varphi_a(p(x)q(x)) = \sum_{k=0}^{m+n} \gamma_k a^k$$

$$\varphi_a(p(x)) * \varphi_a(q(x)) = \left( \sum_{i=0}^m x_i a_i \right) \left( \sum_{j=0}^n x_j b_j \right)$$

$$= \sum_{i=0}^m \sum_{j=0}^n x_i b_j x_i + j$$

$$= \sum_{k=0}^{m+n} \underbrace{\sum_{\substack{i,j \geq 0 \\ i+j=k}} a_i b_j}_{\gamma_k} x^k = \sum_{k=0}^{m+n} \gamma_k x^k$$

$$= \sum_{i=0}^k a_i b_{k-i} = \gamma_k$$

Schreibweise:  $\varphi_a(p(x)) =: p(a)$

### 9.13 BEISPIEL

a)  $A = \mathbb{K}$

$$\varphi_\alpha(p(x)) = p(\alpha)$$

b)  $A = \text{Hom}(V, V) \quad \ell: \mathbb{K} \rightarrow \text{Hom}(V, V)$

$$f^0 = \text{id}, f^k = \underbrace{f \circ \dots \circ f}_{k \text{ mal}} \quad \lambda \mapsto \lambda \cdot \text{id}$$

$$\Rightarrow \varphi_f\left(\sum_{k=0}^n a_k x^k\right) = \sum_{k=0}^n a_k f^k$$

c)  $A = \mathbb{K}^{n \times n}$

$$\forall_A f(p(x)) = p(A) = \sum_{k=0}^n x_k A^k$$

9.14 BEMERKUNG

$\mathbb{K}[x]$  ist die "freie assoziative Algebra mit einem Erzeuger" über  $A$

Jede Abbildung  $f: \{x\} \rightarrow A$  hat eine eindeutige Fortsetzung zu einem Algebrahomomorphismus

$$\psi: \mathbb{K}[x] \rightarrow A$$

$\mathbb{K}[x]$  ... kleinste Algebra über  $\mathbb{K}$ , die  $x$  enthält für zwei Erzeuger?

$$f: \{x, y\} \rightarrow A$$

$$\downarrow \\ \psi: \mathbb{K}\langle x, y \rangle \rightarrow A$$

nichtkommutative Polynome in  $x, y$

analog: freie Gruppe, freies Monoid

jeder Vektorraum ist frei über seiner Basis

9.15 Def

Sei  $p(x) \in \mathbb{K}[x]$

Eine Nullstelle von  $p(x)$  ist ein  $\gamma \in \mathbb{K}$

sodass  $p(\gamma) = 0 \quad (\Leftrightarrow p(x) \in \ker \psi_\gamma)$

Beispiele •  $p(x) = a_0$  ... keine nichttriviale Nullstelle

$$\bullet p(x) = a_0 + a_1 x \rightarrow \gamma = \frac{-a_0}{a_1}$$

$$\bullet p(x) = a_0 + a_1 x + a_2 x^2 \rightarrow \text{Formel 2000 v. Chr}$$

$$\bullet p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \rightarrow \text{Formel von Cardano}$$

Gerolamo Cardano 1501 - 1576

→ Ars Magna 1545

Nicolo Tartaglia 1499 - 1557, Scipione dal Ferro 1465 - 1526

$\deg p(x) = 4 \rightarrow L. Ferrari$

→ Antonio Fiore

$\deg p(x) \geq 5 \rightarrow 1826$  Abel → keine allg. Formel

### 9.16 BEM

Die Methode von Cardano und Tartaglia

cub p:b reb equalis 20

$$x^3 + 6x = 20$$

• Ansatz:  $x = u + v$

$$(u+v)^3 + 6(u+v) = 20$$

$$u^3 + 3u^2v + 3uv^2 + v^3 + 6(u+v) = 20$$

$$u^3 + v^3 + (3uv + 6)(u+v) = 20$$

• Wähle  $v$  so, dass  $3uv + 6 = 0$

$$\Rightarrow uv = -2 \Rightarrow u^3 v^3 = -8$$

$$u^3 + v^3 = 20$$

$$a = u^3, b = v^3$$

$$\begin{array}{l} ab = -8 \\ a+b = 20 \end{array} \quad \left. \begin{array}{l} \Rightarrow \\ \Rightarrow \end{array} \right. a(20-a) = -8$$

$$a^2 - 20a - 8 = 0$$

$$a = \frac{20 \pm \sqrt{400+32}}{2} = 10 \pm \sqrt{108}$$

$$\rightarrow u^3 = 10 + \sqrt{108}, v^3 = 10 - \sqrt{108}$$

$$x = u+v = \sqrt[3]{10+\sqrt{108}} + \sqrt[3]{10-\sqrt{108}}$$

### 9.17 · Satz: Satz mit Fakt

Seien  $p(x), q(x) \in K[x]$ ,  $q(x) \neq 0$

Dann  $\exists! s(x), r(x) \in K[x]$

sodass  $\deg r(x) < \deg q(x)$

und  $p(x) = s(x) \cdot q(x) + r(x)$

Vgl N:  $m, n \in \mathbb{N}$

$m \in \mathbb{K}$ ,  $n \in \mathbb{N}$

$\Rightarrow \exists! a, b : m = a \cdot n + b$

wobei  $0 \leq b < n$

## Beweis

Induktion nach  $\deg p(x)$

Fall 1:  $\deg p(x) < \deg q(x)$

$$\rightarrow p(x) = 0 \cdot q(x) + p(x) \rightarrow \text{endlich}$$

Fall 2:  $\deg p(x) \geq \deg q(x)$

$$p(x) = \sum_{k=0}^m a_k x^k \quad q(x) = \sum_{l=0}^n b_l x^l \quad m \geq n$$

$$\begin{aligned} \text{Sei } p_m(x) &= p(x) - \frac{a_m}{b_n} x^{m-n} q(x) \\ &= \sum_{k=0}^m a_k x^k - \sum_{l=0}^n \frac{a_m}{b_n} b_l x^{m-n+l} \\ &= \sum_{k=0}^{m-1} a_k x^k - \sum_{l=0}^{n-1} \frac{a_m}{b_n} x^{m-n+l} \end{aligned}$$

$$\deg p_m(x) < \deg p(x)$$

$$A \rightarrow p_m(x) = s_1(x) \cdot q(x) + r_1(x)$$

$$\Rightarrow p(x) = \left( \frac{a_m}{b_n} x^{m-n} + s_1(x) \right) q(x) + r_1(x)$$

$$p_1(x) + \frac{a_m}{b_n} x^{m-n} q(x)$$

9.12 BSP

$$\begin{array}{r} 3x^5 - x^4 + 2x^3 + x^2 \\ - (3x^5 - 8x^4 + 3x^3) \\ \hline 0 \quad 8x^4 - x^3 + x^2 \end{array} \quad + 1: x^2 - 3x + 1 = \underbrace{3x^3 + 8x^2 + 23x + 61}_{s(x)}$$

$$\underline{- (8x^4 - 24x^3 + 8x^2)}$$

$$0 \quad 23x^3 - 7x^2 + 1$$

$$\underline{- (23x^3 - 69x^2 + 23x)}$$

$$0 \quad 62x^2 - 23x + 1$$

$$\underline{- (62x^2 - 186x + 62)}$$

$$0 \quad \underbrace{163x - 61}_{r(x)}$$

### 9.19 DEF:

$q(x)$  teilt  $p(x) \dots q(x) | p(x)$  wenn  
 $\exists s(x): p(x) = s(x) q(x)$   
(d.h. Division geht ohne Rest auf)

### 9.20

$$\begin{aligned} q(x) &= x - \zeta \\ \rightarrow p(x) &= s(x)(x - \zeta) + r \\ \Rightarrow p(\zeta) &= r \end{aligned}$$

### 9.21 FOLGERUNG

$\zeta$  ist Nullstelle von  $p(x) \Leftrightarrow (x - \zeta) | p(x)$

### 9.22 HORNER-SCHÉMA

$p(x) \in K[x], \lambda \in K, p(\lambda) = ?$

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$p(\lambda) = a_n \lambda^n + a_{n-1} \lambda^{n-1} + \dots + a_1 \lambda + a_0 = \frac{n(n+1)}{2} \lambda^{n-2}$$

Man braucht  $\approx n^2$  Multiplikationen,

Besser  $\rightarrow n$  Multiplikationen:

$$\begin{aligned} p(\lambda) &= (a_n \lambda^{n-1} + a_{n-1} \lambda^{n-2} + \dots + a_1) \lambda + a_0 \\ &= ((a_n \lambda^{n-2} + a_{n-1} \lambda^{n-3} + \dots + a_2) \lambda + a_1) \lambda + a_0 \\ &\dots \text{ usw.} \end{aligned}$$

### BEISPIEL

$$\begin{aligned} p(x) &= a_3 x^3 + a_2 x^2 + a_1 x + a_0 \\ &= (a_3 x^2 + a_2 x + a_1) x + a_0 \\ &= ((a_3 x + a_2) x + a_1) x + a_0 \end{aligned}$$

a3

$$a_3 x + a_2$$

$$(a_3 x + a_2) x + a_1$$

$$((a_3 x + a_2) x + a_1) + a_0$$

## ALGORITHMUS:

$$\begin{aligned} \gamma_n &= a_n \quad \text{für } k \\ \text{für } k &= n-1, \dots, 0 \quad \gamma_n = 2\gamma_{n+1} + a_n \\ \Rightarrow p(\lambda) &= \gamma_0 \end{aligned}$$

$$p(x) = 3x^5 - x^4 + 2x^3 + x^2 + 1 \quad \lambda = 5$$

$$\gamma_5 = 3$$

$$\gamma_4 = 5 \cdot 3 + (-1) = 14$$

$$\gamma_3 = 5 \cdot 14 + 2 = 72$$

$$\gamma_2 = 5 \cdot 72 + 1 = 361$$

$$\gamma_1 = 5 \cdot 361 = 1805$$

$$\gamma_0 = 5 \cdot 1805 + 1 =$$

vgl. Division

$$\begin{array}{r}
 3x^5 - x^4 + 2x^3 + x^2 + 1 : x - 5 = 3x^4 + 14x^3 + 72x^2 + 361x + 1805 \\
 \underline{- (3x^5 - 15x^4)} \\
 \hline
 14x^4 + 2x^3 + x^2 + 1 \\
 \underline{- (14x^4 - 70x^3)} \\
 \hline
 72x^3 + x^2 + 1 \\
 \underline{- (72x^3 - 360x^2)} \\
 \hline
 361x^2 + 1 \\
 \underline{- (361x^2 - 1805x)} \\
 \hline
 1805x + 1 \\
 \underline{- (1805x - 9025)} \\
 \hline
 9026
 \end{array}$$

Ein Polynom  $p(x)$  heißt wenn

$$\exists p_1(x), p_2(x) \in K[x] : \deg p_1(x), \deg p_2(x) < \deg p(x) \wedge p(x) = p_1(x) \cdot p_2(x)$$

d.h. es gibt edle Teiler

Sonst heißt  $p(x)$  irreduzibel

Q. 2.4 BEM

- i) konstante und lineare Polynome sind irreduzibel
- ii) irreduzible Polynome vom Grad  $\geq 2$  haben keine Nullstellen (sonst ist  $x-\gamma$  Faktor)

Q. 2.5 BSP

- $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

$K = \mathbb{Q}$  ... irreduzibel,  $K = \mathbb{R}$  ... reduzibel

- $x^2 + 1 = (x-i)(x+i)$

$K = \mathbb{Q}, K = \mathbb{R}$ , irreduzibel,  $K = \mathbb{C}$  reduzibel

- $x^2 + x + 1 \in \mathbb{K}_2[x]$  ist irreduzibel

$x^3 + x + 1 \in \mathbb{K}_2[x]$  ist irreduzibel

$$x^5 + x + 1 = (x^2 + x + 1)(x^3 - x^2 + 1) \rightarrow \text{reduzibel}$$

$\overline{-1} : (\overline{-1})^2 = 1 \quad (\overline{-1})^2 + 1 = 0$

Körper in dem  $x^2 + x + 1 \in \mathbb{K}_2[x]$  eine Nullstelle hat?

Sei  $\alpha$  eine "Zahl" sodass  $\alpha^2 + \alpha + 1 = 0$

$$\Rightarrow \alpha^2 = -\alpha - 1$$

$$\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$$

$$(\alpha a + b)(\alpha c + d) = ac \cdot \alpha^2 + (bc + ad) \alpha + bd$$

$$= (ac + bc + ad) \alpha + (ad + bd)$$

$\Rightarrow \{\alpha a + b \mid a, b \in \mathbb{K}_2\}$  ist Ring und sogar Körper

$GF(2^2) = GF(4) \dots$  galois field

für alle  $p \in \mathbb{P}, k \in \mathbb{N}$  der  $GF(p^k)$  Körper der Ordnung  $p^k$

## 9.26 Hauptsatz der Algebra

$\mathbb{C}$  ist algebraisch abgeschlossen

d.h. jedes Polynom  $p(x) \in \mathbb{C}[x]$  hat Nullstelle  $\zeta \in \mathbb{C}$

FOLGERUNG

1)  $p(x) \in \mathbb{C}[x]$  ist irreduzibel  $\Leftrightarrow \deg p(x) \leq 1$

2) jedes  $p(x)$  hat eine Faktorisierung

$$p(x) = (x - \zeta_1)(x - \zeta_2) \dots (x - \zeta_n)$$

wobei  $\zeta_i \in \mathbb{C}$ ,  $n = \deg p(x)$

Beweis

Satz von Liouville  $\rightarrow$  jede komplexe, differenzierbare Funktion ist unbeschränkt.

$\rightsquigarrow$  Theorie der komplexen Funktionen

$$f'(z_0) = \lim_{z \rightarrow z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

$\frac{1}{p(z)}$  beschränkt  $\Rightarrow p(z)$  konstanter Wert

## 9.27 SATZ

In beliebigen Körpern gilt: jedes Polynom hat eine (bis auf die Reihenfolge) eindeutige Faktorisierung

$p(x) = p_1(x) \dots p_n(x)$  in irreduzible Faktoren

## 9.28 Satz & Bsp

$$p(x) = (x - \zeta_1) \dots (x - \zeta_n)$$

$p(x), q(x) \in \mathbb{K}[x] \setminus \{0\}$

$$q(x) = (x - \eta_1) \dots (x - \eta_m)$$

"monic"  $\rightarrow$  führender Koeffizient ist 1

Dann gibt es ein eindeutiges, normiertes Polynom

von maximalem Grad  $(p(x), q(x))$

sodass  $\text{ggT}(p(x), q(x)) | p(x) \wedge \text{ggT}(p(x), q(x)) | q(x)$

Dann gilt: alle gemeinsamen Teiler von  $p(x)$  und  $q(x)$  teilen  $\text{ggT}(p(x), q(x))$

Beweis

## • Eindeutigkeit

Sei  $g(x)$  Polynom von maximalen Grad, sodass  $p(x)$  und  $q(x)$  teilt

$$\Rightarrow p(x) = f(x) \cdot g(x) \quad \text{und} \quad q(x) = h(x) \cdot g(x)$$

Sei  $d(x)$  gemeinsamer Teiler  $\Rightarrow \deg d(x) \leq \deg g(x)$

Dividieren  $\Rightarrow g(x) = s(x) \cdot d(x) + r(x)$ ,  $\deg r(x) < \deg d(x)$

$$p(x) = \tilde{f}(x) d(x) \quad q(x) = \tilde{h}(x) d(x)$$

$$f(x) g(x) = \tilde{f}(x) d(x)$$

$$f(x)(s(x) d(x) + r(x))$$

$$(\tilde{f}(x) - f(x)s(x)) d(x) = r(x)$$

$\deg [\text{links}] \geq \deg [\text{rechts}]$

$$\Rightarrow \tilde{f}(x) - f(x)s(x) = 0 \Rightarrow r(x) = 0$$

$$\Rightarrow d(x) | g(x)$$

①  $\rightarrow$  Es kann nur einen ggT geben

9.29 EURE ALG

Wenn  $p(x) = s(x) \cdot q(x) + r(x)$

$$\Rightarrow \text{ggT}(p(x), q(x)) = \text{ggT}(q(x), r(x))$$

$\rightarrow$  wie für ganze Zahlen

9.30 DEF

Eine Nullstelle  $y$  eines Polynoms hat Vielfachheit  $m$   
wenn  $(x-y)^m | p(x)$  aber  $(x-y)^{m+1} \nmid p(x)$

② Nullstellen mit Vielfachheit  $\geq 2$  sind die

Nullstellen des  $\text{ggT}(p(x), p'(x))$

$$(x^n)' = n \cdot x^{n-1}$$

30) a)  $T_g^n(x, 0) = g(0) + \sum_{k=1}^n \frac{g^{(k)}(0)}{k!} (x-0)^k$

$$g(x) = \sin(2x) \rightarrow 0$$

$$g'(x) = 2 \cos(2x)$$

$$g'''(x) = 4 \cdot (-\sin(2x)) \rightarrow 0$$

$$g''''(x) = 8 \cdot (-\cos(2x))$$

$$g''''''(x) = 16 \cdot \sin(2x) \rightarrow 0$$

$$T_g^n(x, 0) = \underbrace{g(0)}_0 + \underbrace{\cos(0) \cdot 2x}_0 + \frac{-\sin(0) 4x^3}{2} + \frac{-\cos(0) 2^3 x^3}{2} \dots$$

$$T_g^n(x, 0) = \sum_{k=0}^m \frac{(-1)^k}{k!} \frac{(2x)^{2k+1}}{(2k+1)!} \text{ sodass } 2m+1 \leq n$$

$$2m+3 \geq n$$

noch einfacher: betrachte

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} + \dots$$

$$\sin(2x) = 2x - \frac{(2x)^3}{3!} + \frac{(2x)^5}{5!} - \dots$$

b)  $R_g^n(x, 0) = \left| \frac{f^{(n+1)}(\zeta)(x-0)^{n+1}}{(n+1)!} \right| < 10^{-6}$ , wobei  $\zeta \in [-\pi, \pi]$   
 (Wähle  $\zeta$  so, dass  $|f^{(n+1)}(\zeta)| \leq 2^{n+1}$ )

$$R_g^n(x, 0) \leq \left| \frac{2^{n+1} x^{n+1}}{(n+1)!} \right| < 10^{-6} \Leftrightarrow 2^{n+1} x^{n+1} / 10^6 < (n+1)!$$

$$\Leftrightarrow 10^6 < \frac{(n+1)!}{2^{n+1} x^{n+1}} < (n+1)!$$

$$\dots |R_g^n| \leq \frac{1}{(n+1)!} 2^{n+1} \pi^{n+1} \leq 10^{-6} \quad \forall x \in [-\pi, \pi]$$

gilt für  $n \geq 26$

X Eigenwert  $\lambda$  zu  $f \in \text{End}(V)$

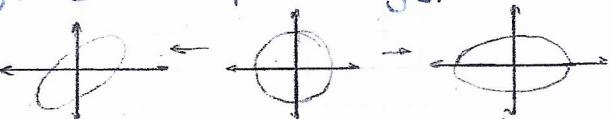
Ziel: finde zu  $f \in \text{End}(V) = \text{Hom}(V, V)$

eine Basis  $B$  von  $V$ , sodass  $\Phi_B^B(f)$  möglichst einfache Gestalt hat

vgl:  $\Phi_C^B(f) = \begin{bmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix}$

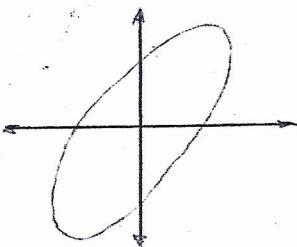
bzw zu einer gegebenen Matrix  $A$  finde Matrix  $T$  sodass  $TAT^{-1}$  möglichst einfache Gestalt hat

- "Einfache" Matrizen:



•  $A = I$

•  $A = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$   $Ae_1 = \lambda_1 e_1$   
 $Ae_2 = \lambda_2 e_2$



$$a_0 + \sum a_{ij}x^i y^j + bx + cy = 0$$

$$\sum a_{ij}x^i y^j + bx + cy = 0$$

$$Ax = \lambda x$$

#### 10.1 DEF

$V$  Vektorraum über  $\mathbb{K}$ ,  $f \in \text{End}(V)$

- $\lambda \in \mathbb{K}$  heißt Eigenwert von  $f$  wenn  $\exists v \in V \setminus \{0\}$  sodass  $f(v) = \lambda \cdot v$
- $v$  heißt Eigenvektor zum Eigenwert  $\lambda$
- engl: eigenvalue, eigenvector
- $\lambda := \{\lambda \mid \lambda \text{ Eigenwert von } f\}$  heißt von  $f$

(C.2 LEMMA

$\eta_\lambda = \{v \in V \mid f(v) = \lambda v\} = \ker(\lambda \text{id} - f)$  ist ein Unterraum  
und heißt Eigenraum von  $f$  zum Eigenwert  $\lambda$   
 $v \in \eta_\lambda \Leftrightarrow f(v) = \lambda v \Leftrightarrow \lambda v - f(v) = 0 \Leftrightarrow \lambda \text{id} - f(v) = 0$   
 $\Rightarrow v \in \ker(\lambda \text{id} - f)$

10.3 BSP

a)  $f = c \cdot \text{id}$   
 $\Rightarrow f(v) = c \cdot v \quad \forall v \in V$   
 $\Rightarrow \text{spec } f = \{c\}$   
 $\lambda = c, \eta_\lambda = V$

b) Sei  $B$  Basis,  $f: V \rightarrow V$   
 $b_i \mapsto \lambda_i b_i$

Fortsetzungssatz  $\Rightarrow f(\mathcal{I}_{\alpha; b_i}) = f(\mathcal{I}_{\alpha; b_i}) = \mathcal{I}_{\alpha; \lambda_i b_i}$   
 $\Rightarrow \text{spec } f = \{\lambda_1, \dots, \lambda_n\}$   
 $\eta = L(b_1), \lambda_i = \lambda$

Sei  $\lambda$  Eigenwert

$(\exists v = \mathcal{I}_{\alpha; b_i}) : f(\mathcal{I}_{\alpha; b_i}) = \lambda \cdot \mathcal{I}_{\alpha; b_i}$

$\mathcal{I}_{\alpha; \lambda b_i} = \mathcal{I}(\lambda - \lambda_i) \alpha; b_i = 0$

$b_i$  l.u.  $\Rightarrow (\lambda - \lambda_i) \alpha_i = 0 \quad \forall i$

$\Rightarrow \lambda = \lambda_i \quad \forall \alpha_i = 0$

$\Phi_B^B(f) = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$

c)  $V = C^\infty(\mathbb{R})$

$$\begin{array}{rccc} \frac{d}{dx} : & C^\infty & \rightarrow & C^\infty \\ & f & \mapsto & f' = \frac{df}{dx} \end{array}$$

Eigenvektoren?

$$y' = \lambda y$$

$$\frac{dy}{dx} = \lambda y \Rightarrow \frac{dy}{y} = \lambda dx$$

$$\int \frac{dy}{y} = \lambda \int dx \Rightarrow \log y = \lambda x + c$$

$$\Rightarrow y = c e^{\lambda x}$$

$$\Rightarrow \text{spec}(\frac{d}{dx}) = \mathbb{R}, \quad \eta_\lambda = \mathcal{L}(e^{\lambda x})$$

$V = C^\infty(\mathbb{R}, \mathbb{C}) \quad e^{i\omega x} \rightsquigarrow \text{Fouriertransformation}$

d)  $C^\infty[0, L]$

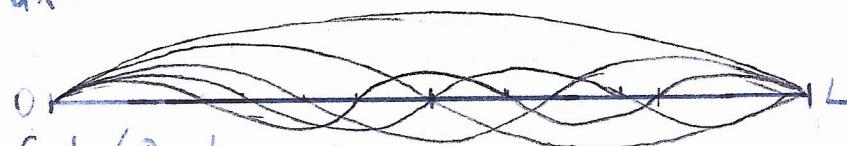
$$\frac{d^2}{dx^2} : C^\infty[0, L] \hookrightarrow \mathbb{C}$$

$$\frac{d^2}{dx^2} e^{\lambda x} = \lambda^2 e^{\lambda x}$$

$$\frac{d^2}{dx^2} e^{i\omega x} = -\omega^2 e^{i\omega x}$$

Re  $\frac{d^2}{dx^2} \cos(\omega x) = -\omega^2 \cos \omega x$

$$\frac{d^2}{dx^2} \sin(\omega x) = -\omega^2 \sin \omega x$$



Saite / Brücke

$$C_0^\infty[0, L] := \{ f \in C^\infty[0, L] \mid f(0) = f(L) = 0 \}$$

$$\frac{d^2}{dx^2} : C_0^\infty[0, L] \hookrightarrow \mathbb{C}$$

$$\sin \omega x \quad \omega L = \pi \cdot k$$

$$\sin \frac{\pi}{L} kx \quad \Rightarrow \omega = \frac{\pi}{L} \cdot k$$

... H-Atom

## 10.4 DEF

$$A \in \mathbb{K}^{n \times n}$$

•  $\lambda \in \mathbb{K}$  heißt LEW

wenn  $\exists v \in \mathbb{K}^n \setminus \{0\} : A \cdot v = \lambda \cdot v$

•  $\lambda \in \mathbb{K}$  heißt LEW

wenn  $\exists v \in \mathbb{K}^n : v^t A = \lambda v^t \Leftrightarrow A^t v = \lambda v \Leftrightarrow \lambda$  REW von  $A^t$

## 10.5 LEMMA

Linkseigenwerte sind automatisch Rechteigenwerte

BEWEIS

Sei  $\lambda$  Rechteigenwert

$$\Rightarrow \exists v: \lambda v - \lambda v = 0$$

$$\ker(\lambda I - A) \neq \{0\}$$

$$\Leftrightarrow \text{rank } (\lambda I - A) < n$$

$$\Leftrightarrow \text{rank } (\lambda I - A^t) < n \Leftrightarrow \lambda \text{ Linkseigenwert von } A$$

## 10.6 BEH

1) Eigenvektoren müssen nicht die gleichen sein

2) In  $\dim = \infty$  stimmt das nicht:

$$S: (\xi_1, \xi_2, \dots) \mapsto (0, \xi_1, \xi_2, \dots)$$

injektiv  $\Rightarrow 0$  ist kein Rechteigenwert

$$S^*: (\xi_1, \xi_2, \dots) \mapsto (\xi_2, \xi_3, \dots)$$

hat Eigenwert 0:  $S^*(1, 0, 0, \dots) = (0, 0, \dots)$

Daher allgemeine Definition des Spektrums:

$$\text{spec}(S) = \{\lambda \mid \lambda I + S \text{ nicht invertierbar}\}$$

## 10.7 · DEF

$$\text{Sei } A \in \mathbb{K}^{n \times n}$$

$$\text{spec}_{\mathbb{K}}(A) = \{\lambda \in \mathbb{K} \mid \lambda \text{ REW von } A\} = \{\lambda \in \mathbb{K} \mid \lambda \text{ LEW von } A\}$$

10.7 Lemma 4

$\dim V = n$ ,  $f \in \text{End } V$ ,  $B$  Basis von  $V$

Dann ist  $\text{spec } f = \text{spec} (\Phi_B^B(f))$

$$f(v) = \lambda v \Leftrightarrow \Phi_B^B(f) \Phi_B(v) = \lambda \Phi_B(v)$$

10.8 Folgerung

1) Das Spektrum hängt nicht von der Wahl der Basis ab

2)  $T$  regulär  $\Rightarrow \text{spec } T A T^{-1} = \text{spec } A$

Eigenvektor von  $T^{-1} A T$ ?

$$A x = \lambda x \Leftrightarrow A T T^{-1} x = \lambda x$$

$$\Leftrightarrow T^{-1} A T T^{-1} x = \lambda T^{-1} x$$

$x$  Eigenvektor von  $A \Leftrightarrow T^{-1} x$  Eigenvektor von  $T^{-1} A T$

$\lambda I - A$  nicht injektiv?

10.10 Satz + DEF

Sei  $A \in K^{n \times n}$

i)  $\chi_A(\lambda) = \det(\lambda I - A)$  ist ein Polynom vom Grad  $n$   
 $\chi_A(x)$  und heißt charakteristisches Polynom von  $A$

ii)  $\lambda$  Eigenwert von  $A \Leftrightarrow \lambda$  Nullstelle von  $\chi_A(x)$

bew

$$\therefore \det(\lambda I - A) = \begin{bmatrix} \lambda + a_{11} & -a_{12} & \cdots & \cdots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & & & -a_{2n} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \cdots & \lambda - a_{nn} \end{bmatrix}$$

$$= \prod_{i \in \Omega_n} (\lambda - a_{ii}) (\lambda - a_{22}) \cdots (\lambda - a_{nn}) + \text{Polynom vom Grad } \leq n-1$$

Polynom in  $\lambda = \lambda^n + \text{Polynom vom Grad } \leq n-1$

ii)  $\lambda I - A$  nicht injektiv  $\Leftrightarrow \det(\lambda I - A) = 0$