

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

- $a * (b + c) = a * b + a * c$ Distributivität
- $(a + b) * c = a * c + b * c$
- $\lambda(a * b) = (\lambda a) * b = a * (\lambda b)$ Assoziativität

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

$f * g := f \circ g$ nichtkommutativ, assoziativ, Algebra

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

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 $a \times b = -b \times a$

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

→ nicht assoziativ, nichtkommutativ - Quaternionen

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

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

Die - Produkt

Kommutatorprodukt

nichtkommutativ, nicht assoziativ

→ Jacobi - Identität

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

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

assoziativ, kommutativ

9.6 DEFINITION

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

$$P_{IK} = \{(a_0, a_1, \dots, a_n, 0, a_{n+1}) \mid a_i \in K\}$$

Unterraum der endlichen Folgen

Basis von $P_{\mathbb{N}}$, $(e_i)_{i \geq 0}$

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

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

9. 5 SATURDAY

i) $(P_K, *)$ ist eine assoziative, kommutative
 $\forall K \in \mathbb{S}$ K -Algebra

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

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

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

$\mathbb{K}[Ex]$ bilden kommutative, assoziative Algebra

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

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

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

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

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

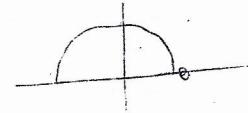
$$e^{i\varphi} = \cos \varphi + i \sin \varphi$$

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

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

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

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



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

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

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

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

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

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

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

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

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

$$k > m+n$$

$$i < m$$

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

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

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

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

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

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

→ 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}_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

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

$i)$ $\mathbb{K}[x]$ 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?

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

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

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

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

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

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

surjektiv? $\rightarrow \textcircled{u}$

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 Algebrehomomorphismus, wenn ψ 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 $x \in \mathbb{K}$

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

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

Einbettung, Algebrehomomorphismus

$x \mapsto x \cdot 1$

9.12 Einsetzungssatz

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

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

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 Algebrehomomorphismus

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

- Multiplikativität

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

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

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

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

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

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

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

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

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

9.13 BEISPIEL

a) $A = \mathbb{K}$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9.18 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

ζ 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:

$$\gamma_n = a_n \quad \text{für } k$$

$$\text{für } k = n-1, \dots, 0 \quad \gamma_n = 2\gamma_{n+1} + a_n$$

$$\Rightarrow p(\lambda) = \gamma_0$$

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

$$\gamma_5 = 3$$

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

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

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

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

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

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 ≥ 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 α 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

$GF(2^2) = GF(4)$... 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

$p(x) = p_1(x) \dots p_k(x)$ 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 $g(x)$ 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 $\Rightarrow g(x) = s(x) \cdot d(x) + r(x)$, $\deg r(x) < \deg d(x)$

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

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

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

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

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

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

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

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 ≥ 2 sind die

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

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