

Polynomringe

R kommutativer Ring (z.B. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, ...)

3.12 Def.: Ein Polynom über R ist ein Symbol

$$\sum_{i=0}^n a_i x^i = a_n x^n + \dots + a_1 x + a_0$$

mit $n \in \mathbb{N}_0$, $a_i \in R$.

x : Unbestimmte

a_i : Koeffizienten

$a_i := 0$ für $i > n$.

Polynome sind gleich, wenn alle Koeffizienten übereinstimmen.

$R[x] :=$ Menge aller Polynome über R

Polynomring über R

Für $A = \sum_{i=0}^n a_i x^i$

$$B = \sum_{i=0}^m b_i x^i$$

definieren wir

$$A +_p B := \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$$

$$A \cdot_p B := \sum_{i=0}^{n+m} \left(\sum_{\substack{j,k: \\ j+k=i}} a_j \cdot b_k \right) x^i$$

3.13 Satz: $(R[x], +_p, \cdot_p)$ ist ein kommutativer Ring, und die Abb.

$$\begin{array}{ccc} R & \longrightarrow & R[x] \\ a & \longmapsto & a \end{array}$$

ist ein Ringhomomorphismus.

Beweis:

$$\begin{aligned}\text{Sei } A &= \sum_i a_i x^i \\ B &= \sum_i b_i x^i \\ C &= \sum_i c_i x^i\end{aligned}$$

R1: $(R[x], +_p)$ abelsche Gruppe

$$(A +_p B) +_p C = \sum_i ((a_i + b_i) + c_i) x^i$$

$$\stackrel{\substack{(R, +) \\ \text{ist Gruppe}}}{=} \sum_i (a_i + (b_i + c_i)) x^i$$

$$= A +_p (B +_p C)$$

$$\text{Null: } 0_p := 0 \quad (a_i = 0 \ \forall i)$$

$$\text{Negative } -A = \sum_i (-a_i) x^i$$

$+_p$ kommutativ, da $+$ in R kommutativ.

R2: $\cdot_p$ assoziativ

$$(A \cdot_p B) \cdot_p C = \sum_i \left(\sum_{\substack{j, k: \\ j+k=i}} a_j \cdot b_k \right) x^i \cdot_p C$$

$$= \sum_i \left(\sum_{\substack{l, m: \\ l+m=i}} a_l \cdot b_m \right) x^i \cdot_p C$$

$$= \sum_i \left(\sum_{\substack{j, k: \\ j+k=i}} \left(\sum_{\substack{l, m: \\ l+m=j}} a_l \cdot b_m \right) \cdot c_k \right) x^i$$

$$= \sum_i \left(\sum_{\substack{l, m, k: \\ l+m+k=i}} (a_l \cdot b_m) \cdot c_k \right) x^i$$

• assoziativ
in R

$$\stackrel{\text{assoziativ in } R}{=} \sum_i \left(\sum_{\substack{l, m, k: \\ l+m+k=i}} a_l \cdot (b_m \cdot c_k) \right) x^i$$

$$= \dots$$

$$= A \cdot_p (B \cdot_p C)$$

Eins:

$$1_P := 1$$

$$(a_0 = 1, a_i = 0 \quad \forall i \geq 1)$$

123: Distributivität [...]

$\cdot_P$ kommutativ:

$$A \cdot_P B = \sum_i \left(\sum_{\substack{j,k: \\ j+k=i}} a_j \cdot b_k \right) x^i$$

$\overset{R}{\text{kommutativ}} \Rightarrow \sum_i \left(\sum_{\substack{j,k: \\ j+k=i}} b_k \cdot a_j \right) x^i$

$$= \sum_i \left(\sum_{\substack{k,j: \\ k+j=i}} b_j \cdot a_k \right) x^i$$

$$= B \cdot_P A$$

□

Bemerkung: $x^j \cdot_P x^k = x^{j+k}$

$$a_n x^n +_P \dots +_P a_1 x +_P a_0 = a_n x^n + \dots + a_1 x + a_0$$

Notation: ab sofort $+$, $\cdot$

für $+_P$, $\cdot_P$.

3.14 Def.: Sei $A = a_n x^n + \dots + a_1 x^1 + a_0$ mit $a_n \neq 0$.

Grad: $\deg(A) := n$

Leitkoeff. a_n

Leitterm: $a_n x^n$

Konvention: $\deg(0_P) := -1$

3.15 Satz (Gradformel)

Seien $A, B \in R[x]$, $A, B \neq 0$, mit Leitkoeffizienten a_n, b_m . Falls

$$(*) \quad a_n \cdot b_m \neq 0,$$

$$\text{ist auch} \quad A \cdot B \neq 0$$

und

$$\deg(A \cdot B) = \deg A + \deg B.$$

Beweis: Per Def. von $\cdot = \cdot_p$ sind die Koeff. von $A \cdot B$ gegeben durch

$$c_i = \sum_{\substack{j, k: \\ j+k=i}} a_j b_k$$

Für $i > n+m$ ergibt sich $c_i = 0$ (denn in der Summe ist entweder $j > n$ oder $k > m$, also $a_j = 0$ oder $b_k = 0$.)

Für $i = n+m$ ergibt sich

$$c_{n+m} = a_n \cdot b_m \neq 0 \text{ nach Annahme. } \square$$

Bemerkung:

Über $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \dots$ folgt $a_n \cdot b_m \neq 0$ automatisch aus $a_n \neq 0$ und $b_m \neq 0$ (siehe 3.6).

Aber z. B. über $\mathbb{Z}/6\mathbb{Z}$ nicht:

$$\underbrace{[2]}_{a_1} \cdot x \cdot \underbrace{[3]}_{b_1} \cdot x = \underbrace{([2] \cdot [3])}_{\substack{[6] \\ \parallel \\ [0] \\ a_1 b_1}} x^2 = 0$$

3.16 Satz (Division mit Rest)

Seien $A, B \in R[x]$.

Falls $B \neq 0$ mit Leitkoeffizient $b_m \in R^*$, so existieren eindeutig bestimmte

$$Q, S \in R[x] \quad \text{mit} \quad \deg S < \deg B$$

$$\text{und} \quad A = Q \cdot B + S.$$

Beispiel:

$$\begin{array}{r} \overbrace{(5x^4 + 1)}^A : \overbrace{(x^2 + 1)}^B = \overbrace{5x^2}^{Q_1} - \overbrace{5}^{Q_2} = Q \\ \hline \begin{array}{r} - (5x^4 + 5x^2) \\ \hline \end{array} \\ \begin{array}{r} -5x^2 + 1 \\ - (-5x^2 - 5) \\ \hline \end{array} \\ \begin{array}{r} 6 \\ \hline \end{array} \end{array} \quad \deg S = 0 < 2 = \deg B$$

$$5x^4 + 1 = (5x^2 - 5) \cdot (x^2 + 1) + 6$$

Beweis:

Eindeutigkeit: Angenommen

$$A = Q \cdot B + S \quad \text{mit} \quad \deg S < \deg B$$

$$\text{und} \quad A = \tilde{Q} \cdot B + \tilde{S} \quad \text{mit} \quad \deg \tilde{S} < \deg B.$$

$$\begin{array}{l} \text{Dann ist} \quad 0 = (Q - \tilde{Q}) \cdot B + (S - \tilde{S}) \\ \qquad \qquad \qquad \underbrace{\hspace{2cm}}_{\geq \deg B} \quad \underbrace{\hspace{2cm}}_{< \deg B} \\ \qquad \qquad \qquad \text{falls } Q - \tilde{Q} \neq 0 \end{array}$$

(nach Gradformel: Voraussetzung (*) erfüllt, da $b_m \in R^*$)

Also muss gelten $Q - \tilde{Q} = 0$, also $Q = \tilde{Q}$,
und es folgt $S = \tilde{S}$.

Existenz (konstruktiv):

Konstruiere schrittweise endlich viele Polynome

$$Q_0, Q_1, Q_2, Q_3, \dots$$

$$S_0, S_1, S_2, S_3, \dots$$

derart, dass jeweils gilt:

$$A = (Q_0 + \dots + Q_i) \cdot B + S_i$$

$$\text{und } \deg(S_{i+1}) < \deg(S_i).$$

Schritt 0: $Q_0 := 0$

$$S_0 := A.$$

Schritt $i+1$: Seien $Q_0, \dots, Q_i$,

und $S_0, \dots, S_i$ bereits konstruiert.

Falls $\deg S_i < \deg B$ — FERTIG.

$$Q := Q_0 + \dots + Q_i$$

$$S := S_i$$

Falls $\deg S_i \geq \deg B$:

Definiere Q_{i+1} so, dass gilt

$$\text{Leitterm}(Q_{i+1} \cdot B) = \text{Leitterm}(S_i),$$

nämlich

$$\text{für } B = \overset{\mathbb{R}^+}{\underset{0}{\overset{u}{b_m}}} \cdot x^m + \text{kleinere Terme}$$

$$\text{und } S_i = \underset{0}{\overset{u}{s_n}} \cdot x^n + \text{kleinere Terme}, \quad n \geq m$$

$$Q_{i+1} := s_i \cdot b_m^{-1} x^{n-m}.$$

Definiere

$$S_{i+1} := S_i - Q_{i+1} \cdot B$$

Das funktioniert [...].

□

3.17 Def.: Die Auswertungsabb./Evaluationsabb. eines Polynoms $A = \sum_{i=0}^n a_i x^i$ ist die Abb.

$$\begin{aligned} \text{ev}(A): \quad \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \sum_{i=0}^n a_i \cdot x^i = a_n x^n + \dots + a_1 x + a_0 \\ &\quad + a_0 \in \mathbb{R} \end{aligned}$$



Verschiedene Polynome können dieselbe Abb. definieren.

$$\text{z.B.: } A = X^2 + X \in \mathbb{F}_2[X] \\ (= [1]X^2 + [1]X)$$

$$\begin{aligned} \text{ev}(A): \quad \mathbb{F}_2 &\longrightarrow \mathbb{F}_2 \\ [0] &\mapsto [0]^2 + [0] = [0] \\ [1] &\mapsto [1]^2 + [1] = [0] \end{aligned}$$

Hier ist $ev(A) = ev(0)$
obwohl $A \neq 0$.

Notation: Für $A \in \mathcal{R}[X]$, $x \in \mathcal{R}$ schreiben wir
kurz $A(x) := (ev(A))(x)$.

3.18 Def.: $x \in R$ ist Nullstelle von $A \in R[X]$
falls $A(x) = 0$.

3.19 Satz: Ist $x \in R$ Nullstelle von $A \in R[X]$,
so ist $\frac{1 \cdot X + (-x)}{A} = \overbrace{(X - x) \cdot Q}$
für ein $Q \in R[X]$.

Beweis: Division mit Rest (3.16) liefert

$$A = (X - x) \cdot Q + S$$

für ein S mit $\deg S < 1$.

Also $S = s$ für ein $s \in R$.

Werte aus an $x \in R$:

$$\underbrace{A(x)}_0 = \underbrace{(x - x)}_0 \cdot Q(x) + s$$

Also folgt $s = 0$, also $A = (X - x) \cdot Q$. □

3.20 Korollar: Ein Polynom $A \neq 0$ über einem
Körper hat höchstens $\deg(A)$
Nullstellen.

Beweis:

Sei $A \in K[X]$, K Körper.

Induktion über $\deg(A) \in \mathbb{N}_0$.

IA: $\deg(A) = 0$.

In diesem Fall ist $A = a$ für ein $a \in K$,
also $\forall x \in K: A(x) = a$.

Da $A \neq 0$, ist $a \neq 0$.

Also hat A keine Nullstelle.

IS: $\deg(A) = n$.

(IV: Korollar gilt für Polynome vom Grad $< n$.)

Falls A keine Nullstellen hat: FERTIG.

Andernfalls wähle Nullstelle x . Nach 3.19

gilt dann: $A = (X - x) \cdot Q$.

Hier ist $\deg(Q) = \deg(A) - 1$ (Gradsatz)
 $< n$.

Nach IV hat Q höchstens $n-1$
Nullstellen.

Andererseits ist jede Nullstelle $y \neq x$ von A
auch eine Nullstelle von Q :

$$\text{Aus } \underbrace{A(y)}_0 = \underbrace{(y-x)}_{\neq 0} \cdot Q(y)$$

folgt $Q(y) = 0$, da K Körper ist
(siehe Notiz 3.6).

Also hat A höchstens $1 + (n-1) = n$
Nullstellen.

x $\nearrow$ Nullstellen
von Q

□

Beispiele:

A	$\deg(A)$	Nullst. von A
$(x-1) \cdot (x+3) \in \mathbb{R}[x]$	2	$\{1, -3\}$
$(x-1)^2 \in \mathbb{R}[x]$	2	$\{1\}$
$x^2+1 \in \mathbb{R}[x]$	2	$\emptyset$
$x^2+1 \in \mathbb{C}[x]$	2	$\{i, -i\}$

3.2.1 Fundamentalsatz der Algebra

Jedes Polynom $A \in \mathbb{C}[x]$ von Grad ≥ 1 besitzt eine Nullstelle.

(Beweis: z.B. Vorlesung über Funktionentheorie)

Es folgt: ein Polynom $A \neq 0$ über $\mathbb{C}$ lässt sich schreiben als

$$A = (x-x_1) \cdot (x-x_2) \cdot \dots \cdot (x-x_n) \cdot a$$

für gewisse Nullstellen $x_i \in \mathbb{C}$, $a \in \mathbb{C}^*$;

$$n = \deg(A).$$