Polynomringe

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

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 gleich sind.

$R[X] :=$ Menge aller Polynome über R

Für $A = \sum_{i=0}^{n} a_i X^i$, $B = \sum_{i=0}^{m} b_i X^i$ definieren wir

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

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

korrigiert

3.13 Satz & Def: $(R[X], +_p, \cdot_p)$ ist ein kommutativer Ring, der **Polynomring** über R.

Ferner
$$\begin{aligned} R &\longrightarrow R[X] \\ a &\longmapsto a \end{aligned}$$
Ringhomomorphismus.

Beweis:

Sei
$$A = \sum a_i X^i$$
$$B = \sum b_i X^i$$
$$C = \sum c_i X^i$$

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

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

Null: $0_p := 0$

Negative: $-A = \sum (-a_i) X^i$

(R2) $(A \cdot_p B) \cdot_p C$

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

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

$$= \sum_i \Big(\sum_{\substack{l,m,k:\\ l+m+k=i}} (a_l b_m) c_k \Big) X^i$$

$$= \sum_i \Big(\sum_{\substack{l,m,k:\\ l+m+k=i}} a_l (b_m c_k) \Big) X^i$$

$$= \dots$$

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

Eins: $1_p := 1$

(R3) Distributivität [...]

kommutativ:

$$A \cdot_p B = \sum_i \Big(\sum_{\substack{j,k:\\ j+k=i}} a_j \cdot b_k \Big) X^i$$

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

$$= B \cdot_p A$$

$\square$

Bem: $X^j \cdot_p X^k = X^{j+k}$

$a_n X^n +_p \dots +_p a_1 X +_p a_0 = a_n X^n + \dots + a_1 X + a_0$

Notation: Ab jetzt $+$, $\cdot$ für $+_p$, $\cdot_p$

3.14 Def:
Sei $A = a_n X^n + \ldots + a_1 X + a_0$ mit $a_n \neq 0$.

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

Leitkoeffizient: a_n

Leitterm: $a_n X^n$

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

3.15 Satz (Gradformel)
Seien $A, B \in R[X]$, $A, B \neq 0$, mit Leitkoeffizienten a_n, b_m.

Falls $a_n \cdot b_m \neq 0$, ist auch $A \cdot B \neq 0$, und

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

Beweis:
Für die Koeffizienten c_i von $A \cdot B$ gilt:

$$c_{n+m} = \sum_{\substack{j,k:\\ j+k=n+m}} a_j \cdot b_k = a_n \cdot b_m \neq 0$$

und für $i > n+m$ ist

$$c_i = 0$$

$\square$

über $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \mathbb{C}, \ldots$
gilt $a_n \cdot b_m \neq 0$ automatisch (siehe 3.6).
Aber z.B. über $\mathbb{Z}/6\mathbb{Z}$ nicht:

$$([2] \cdot X) \cdot ([3] \cdot X) = \underbrace{[2][3]}_{[0] \text{ in } \mathbb{Z}/6\mathbb{Z}} \cdot X^2 = 0$$

3.16 Satz (Division mit Rest)

Seien $A, B \in R[X]$. Falls $B \neq 0$ mit Leitkoeffizient $b_m \in R^\times$, so existieren eindeutig bestimmte

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

und $A = Q \cdot B + S$.

Beispiel:

$$\begin{array}{l}
\overbrace{(5x^4+1)}^{A} : \overbrace{(x^2+1)}^{B} = \underbrace{\overbrace{5x^2}^{Q_1} \overbrace{-\,5}^{Q_2}}_{Q} \\
\underline{-(5x^4+5x^2)} \\
\qquad -5x^2+1 \\
\qquad \underline{-(-5x^2-5)} \\
\qquad\qquad \underbrace{6}_{S}
\end{array}$$

Konstruktiver Beweis:

Eindeutigkeit:

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

Dann ist $\underbrace{(Q - \tilde{Q}) \cdot B}_{\geq \deg B} + \underbrace{(S - \tilde{S})}_{< \deg B} = 0$

falls $Q - \tilde{Q} \neq 0$
(nach Gradformel) $\lightning$

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

Existenz:

Konstruiere schrittweise endlich viele Polynome
$Q_0, Q_1, Q_2, \ldots$
$S_0, S_1, S_2, \ldots$
derart, dass jeweils gilt:

$$\boxed{\begin{array}{l} A = (Q_0 + \ldots + Q_i) \cdot B + S_i \\ \text{und } \deg(S_{i+1}) < \deg(S_i) \end{array}}$$

Schritt 0: $\quad Q_0 := 0$

$\qquad\qquad\quad S_0 := A$

Schritt $i+1$: Seien $Q_0, \ldots, Q_i$ und $S_0, \ldots, S_i$ bereits konstruiert.

Falls $\deg(S_i) < \deg(B)$ – FERTIG

$$Q := Q_0 + \ldots + Q_i$$
$$S := S_i$$

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

Definiere Q_{i+1} so, dass

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

$$B = \overset{R^*}{\overset{\in}{b_m}} \cdot X^m + \text{kleinere Terme}$$

$$S_i = \underset{\neq 0}{s_n} \cdot X^n + \text{kleinere Terme}, \ n \geq m$$

$$Q_{i+1} := s_n \cdot b_m^{-1} \cdot X^{n-m}$$

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

Das funktioniert [...] $\square$

3.17 Def: Die Auswertungsabbildung/ Evaluationsabb. eines Polynoms

$$A = \sum a_i X^i$$

ist die Abbildung

$$ev(A): \begin{array}{ccc} R & \longrightarrow & R \\ x & \longmapsto & \sum_{i=1}^{n} a_i \cdot x^i \end{array}$$

Verschiedene Polynome können dieselbe Abbildung definieren.

z.B. $A = X^2 + X$ über $\mathbb{F}_2$

$(= [1] \cdot X^2 + [1] \cdot X)$

$$ev(A): \begin{array}{ccc} \mathbb{F}_2 & \longrightarrow & \mathbb{F}_2 \\ [0] & \longmapsto & [0]^2 + [0] = [0] \\ [1] & \longmapsto & [1]^2 + [1] = [0] \end{array}$$

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

Trotzdem schreiben wir kurz

$A(x)$ statt $ev(A)(x)$

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 von $A \in R[X]$, so ist

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

für ein $Q \in R[X]$.

Beweis: Division mit Rest (3.16):

$$A = \underbrace{(X - x)}_{\deg 1} \cdot Q + S$$

für ein S mit $\deg(S) < 1$.
Also $S = s$ für ein $s \in R$.
Werte aus an $x \in R$:

$$\underbrace{A(x)}_{\overset{\parallel}{0}} = \underbrace{(x - x)}_{0} \cdot Q(x) + s$$

nach Voraussetzung, also $s = 0$.
Also $S = 0$. $\square$

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

Beweis:

Induktion über $\deg(A)$.

IA: $\deg A = 0$

$A = a, \quad a \in K^\times$

Also $\forall x \in K: \; A(x) = a \neq 0.$

IV: Aussage gilt für Polynome vom Grad $< n$.

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

Falls A keine Nullstelle hat: FERTIG.

Falls x Nullstelle von A:

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

$\deg Q = \deg(A) - 1 < n$
(nach Gradformel)

Jede Nullstelle $y \neq x$ von A ist auch Nullstelle von Q:

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

Also dieser Faktor $= 0$ nach Notiz 3.6

hier geht ein: K Körper

Daher: $|NS \text{ von } A| \leq |NS \text{ von } Q| + 1$

$$\underset{(IV)}{\leq} \deg Q + 1$$

$$= \deg(A) \qquad \square$$

Beispiele:

A	$\deg(A)$	$NS(A)$
$(X-1)(X+3) \in \mathbb{R}[X]$	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	$\{i, -i\}$

3.21 Fundamentalsatz der Algebra

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

(Beweis: z.B. Vorlesung Funktionentheorie)

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

$$A = (X - x_1) \cdot (X - x_2) \cdot \ldots \cdot (X - x_n) \cdot a$$

für gewisse NS $x_i \in \mathbb{C}$, $a \in \mathbb{C}^*$, $n = \deg(A)$.