12. Polynomringe

Auch in diesem Kapitel sei R stets ein nicht-trivialer kommutativer Ring.

Für Mengen A, B sei ${}^AB$ die Menge aller Funktionen $f: A \to B$. Sei R ein Ring und sei

$$\mathcal{F}_R := \{ f \in {}^{\mathbb{N}}R : \exists n_f \in \mathbb{N} \, \forall k > n_f \, (f(k) = 0_R) \}.$$

Für $f, g \in \mathcal{F}_R$ definieren wir $f+g, f \cdot g \in \mathcal{F}_R$ wie folgt:

$$(f+g)(k) := f(k) +_R g(k)$$

$$(f \cdot g)(k) := \sum_{i=0}^{k} f(i) \cdot_R g(k-i)$$

Beachte: Für $m := \max\{n_f, n_g\}$ gilt für alle $k \geq 2m$:

$$(f \cdot g)(k) = 0_R, \text{ d.h. } f \cdot g \in \mathcal{F}_R.$$

- Die Funktionen "+" & "$\cdot$" sind assoz., komm., und es gelten die Distributivgesetze.
- $0_{\mathcal{F}_R}(k) := 0_R$ (für alle k) ist Neutralelem. bzgl. "+".
- $1_{\mathcal{F}_R}(k) := \begin{cases} 1_R & \text{für } k=0, \\ 0_R & \text{sonst,} \end{cases}$ ist Neutralelement bzgl. "$\cdot$".

Somit ist $(\mathcal{F}_R, 0_{\mathcal{F}_R}, 1_{\mathcal{F}_R}, +, \cdot)$ ein komm. Ring.

Sei nun X ein Symbol, das in R nicht vorkommt. Wir identifizieren nun $f \in \mathcal{F}_R$ mit $\sum_{i=0}^{\infty} f(i) \cdot X^i$, wobei wir üblicherweise nur die endlich vielen Terme $f(i) \cdot X^i$ aufschreiben, für die $f(i) \neq 0_R$ ist; ausser für $0_{\mathcal{F}_R}$, dafür schreiben wir 0_R. Weiter schreiben wir a_i für $f(i)$ und identifizieren X^0 mit 1_R und X^1 mit X.

↝ Damit wird $\mathcal{F}_R$ zum <u>Polynomring</u> $R[X]$ in der <u>Unbestimmten</u> X.

$X^k \hat{=} \langle 0, \ldots, 0, \overset{k}{1}, 0, \ldots \rangle$

Elemente von $R[X]$ sind somit von der Form

$$a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \quad (\text{für ein } n \in \mathbb{N}).$$

Bem. Elemente in $R[X]$ werden addiert und multipliziert wie Polynome, denn es sind Polynome! [aber keine Polynomfunktionen!]

Faktum 12.1 Die natürliche Inklusion $\iota : R \hookrightarrow R[X]$, $a \mapsto a + 0\cdot X + 0\cdot X^2 + \dots$ ist ein Ringhomom. und wir können R auffassen als Unterring von $R[X]$.

Bew: $\iota(a+b) = a+b+0\cdot X+\dots = (a+0\cdot X+\dots)+(b+0\cdot X+\dots)$
$= \iota(a) + \iota(b)$

und $\iota(a\cdot b) = a\cdot b + 0\cdot X+\dots = (a+0\cdot X+\dots)\cdot(b+0\cdot X+\dots)$,

und es gilt $\iota(1_R) = 1_R + 0\cdot X+\dots = 1_{R[X]}$ ⊣

Def. Ist S komm. Ring, $R \subseteq S$ ein Unterring von S, und $s_0 \in S$, so sei $R[s_0]$ der kleinste Unterring von S der R und s_0 enthält. [Beachte: $R[s_0]$ ist kein Polynomring]

Proposition 12.2 $R[s_0] = \{\tilde{s} \in S : \tilde{s} = a_0 + a_1 s + \dots + a_n s^n$ mit $n \in \mathbb{N}$ und $a_i \in R\}$.

Insbesondere ist $R[s_0]$ eindeutig bestimmt.

[Im Wesentlichen ersetzen wir im Polynomring $R[X]$ die Unbestimmte X durch s_0 und werten die Ausdrücke in S aus.]

Beweis:
- $R[s_0] \subseteq S$ ist ein Unterring von S der R und s_0 enthält. Beachte: $1_R \in R$ und damit auch $1_R s_0 = s_0 \in R[s_0]$.
- Ist $\tilde{S} \subseteq S$ ein Unterring mit $R \subseteq \tilde{S}$ und $s_0 \in \tilde{S}$, so muss gelten $R[s_0] \subseteq \tilde{S}$. ⊣

Bsp. $\mathbb{Z}[i]$; $\mathbb{Z}[e]$; $\mathbb{Z}[-\frac{1}{2} + i\cdot\frac{\sqrt{3}}{2}]$ $\omega^3 = 1$, Minimalpolynom ist X^2+X+1

Theorem 12.3 (universelle Eigenschaft)

Seien R, S komm. Ringe, $\varphi: R \to S$ ein Ringhomom., und $s_0 \in S$. Dann ex. ein eindeutig bestimmter Ringhomom. $\varphi_{s_0}: R[X] \to S$ mit $\varphi_{s_0} \circ \iota = \varphi$ und $\varphi_{s_0}(X) = s_0$. Anders ausgedrückt:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & \searrow^{\iota} \quad \nearrow_{\varphi_{s_0}} & \\ & R[X] & \end{array} \qquad \text{kommutiert}$$

Beweis: Wir definieren $\varphi_{s_0}: R[X] \to S$ durch

$$\varphi_{s_0}(a_0 + a_1 X + \dots + a_n X^n) := \varphi(a_0) + \varphi(a_1) s_0 + \dots + \varphi(a_n) s_0^n.$$

Damit gilt $\varphi_{s_0} \circ \iota = \varphi$, insbesondere gilt $\varphi_{s_0}(1_{R[X]}) = 1_S$, und es gilt $\varphi_{s_0}(X) = \varphi_{s_0}(1_R \cdot X) = \varphi(1_R) s_0 = 1_S \cdot s_0 = s_0$.

Bem: Sei $R' := \varphi[R]$, dann ist $R' \subseteq S$ ein Unterring von S und mit Prp. 12.2 ist $R'[s_0]$ eindeutig.

Wir müssen zeigen, dass φ_{s_0} ein Ringhomom. ist:

Seien $a = a_0 + \dots + a_n X^n$, $b = b_0 + \dots + b_m X^m \in R[X]$.

- $\varphi_{s_0}((a+b)_i) = \varphi(a_i + b_i) s_0^i = (\varphi(a_i) + \varphi(b_i)) s_0^i$
  $= \varphi(a_i) s_0^i + \varphi(b_i) s_0^i$

  also gilt $\varphi_{s_0}(a+b) = \varphi_{s_0}(a) + \varphi_{s_0}(b)$.

- $\varphi_{s_0}((a \cdot b)) = \varphi_{s_0}\left(\sum_{k=0}^{n+m} \left(\sum_{j+l=k} a_j b_l\right) X^k\right) = \sum_{k=0}^{n+m} \varphi\left(\sum_{j+l=k} a_j b_l\right) s_0^k$

Eindeutigkeit von φ_{s_0}:
Sei $\psi_{s_0}: R[X] \to S$ ein Ringhom. mit den gewünschten Eigenschaften.
Dann gilt: $\psi_{s_0}(aX^k) = \psi_{s_0}(a) \cdot \psi_{s_0}(X)^k$
$= \varphi(a) \cdot s_0^k = \varphi_{s_0}(aX^k)$.

$$= \sum_{k=0}^{n+m} \left(\sum_{j+l=k} \varphi(a_j)\varphi(b_l)\right) s_0^k$$

$$= \left(\sum_{j=0}^{n} \varphi(a_j) s_0^j\right) \cdot \left(\sum_{l=0}^{m} \varphi(b_l) s_0^l\right)$$

$$= \varphi_{s_0}(a) \cdot \varphi_{s_0}(b)$$

∎

[Beachte, dass $\ker(\varphi_{s_0}) \subseteq R[X]$ ein Ideal ist.]

Bsp. $R = \mathbb{Z}$, $S = \mathbb{Z}\left[\frac{-1+i\sqrt{3}}{2}\right]$, $\ker(\varphi_{s_0}) = (X^2 + X + 1) = a_{s_0} \subseteq \mathbb{Z}[X]$

Korollar 12.4 Sei S ein komm. Ring, $R \subseteq S$ ein Unterring und sei $s_0 \in S$. Dann ex. ein Ideal $\sigma_{s_0} \subseteq R[X]$ mit $\sigma_{s_0} \cap R = \{0\}$ und $R[X]/\sigma_{s_0} \cong R[s_0]$.

Beweis: Sei $\varphi: R \hookrightarrow S$, $a \mapsto a$ und φ_{s_0} wie in Thm. 12.3.

Dann ist $\varphi_{s_0}[R[X]] = R[s_0]$ (mit Prp. 12.2), also ist $R[X]/\ker(\varphi_{s_0}) \cong R[s_0]$. Mit $\sigma_{s_0} := \ker(\varphi_{s_0})$ ist $R[X]/\sigma_{s_0} \cong R[s_0]$ und

$$\sigma_{s_0} \cap R = \{a \in R : \varphi_{s_0}(a) = 0\} = \{a \in R : a = 0\} = \{0\}.$$

⊣

Def. Sei S ein komm. Ring, $R \subseteq S$ ein Unterring und $s_0 \in S$. Weiter sei σ_{s_0} wie im Beweis von Kor. 12.4.

- Ist $\sigma_{s_0} = \{0\}$, so heisst s_0 transzendent über R.
- Ist $\sigma_{s_0} \neq \{0\}$, so heisst s_0 algebraisch über R.

Bem. Ist S ein komm. Ring, $R \subseteq S$, $s_0 \in S$, dann ist das "Einsetzen" $R[X] \longrightarrow S$, $p \longmapsto p(s_0)$ ein Ringhomomorphismus.

$s_0 \in S$ ist genau dann alg. über R, falls ein Polynom $p \in R[X]$ existiert mit $p \neq 0$ und $p(s_0) = 0$. Insbesondere sind alle $a \in R$ alg. über R: $p = -a + X \in R[X]$, $p \neq 0$, $p(a) = -a + a = 0$.

- $a \in R$, $R[X]/(X-a) \cong R$

[**Bsp.**
- $\mathbb{Q} \subseteq \mathbb{R}$: $\sqrt{2}$ alg., $-2 + X^2$; e & π sind transzendent über $\mathbb{Q}$.
- $\mathbb{Q} \subseteq \mathbb{C}$: i alg., $1 + X^2$; $\omega = e^{2\pi i/n}$, $n \in \mathbb{N}^+$, alg. über $\mathbb{Q}$, $X^n - 1$]

Def. Sei $p \in R[X]$, $p = a_0 + a_1 X + \ldots + a_n X^n$ mit $a_n \neq 0$. $\operatorname{grad}(p) := n$ heisst der Grad von p, a_n ist der Leitkoeffizient. Ist $a_n = 1$, so heisst p normiert; für $p = 0$ (also $a_0 = 0$) sei $\operatorname{grad}(p) := -\infty$.

Gradformeln: Seien $p, q \in R[X]$. $\left[-\infty + n = -\infty \,;\, -\infty < n\right]$

- $\operatorname{grad}(p+q) \leq \max\{\operatorname{grad}(p), \operatorname{grad}(q)\}$
- $\operatorname{grad}(p \cdot q) \leq \operatorname{grad}(p) + \operatorname{grad}(q)$ [< möglich falls R nicht Int.-Ring]
- Ist $\operatorname{grad}(p) = n$ und $\operatorname{grad}(q) = m$ mit $a_n \cdot b_m \neq 0$, (Leitkoeff. von p q)
  so ist $\operatorname{grad}(p \cdot q) = \operatorname{grad}(p) + \operatorname{grad}(q)$.

[nachprüfen]

Proposition 12.5 Ist R ein Integritätsring, so ist

(a) $R[X]$ ein Integritätsring,

(b) $R[X]^* = R^*$.

Beweis: (a) Seien $p, q \in R[X]$ mit $p \neq 0 \neq q$ und seien a_n, b_m die Leitkoeff. von p bzw. q. Weil R ein Integritätsring ist, ist $a_n \cdot b_m \neq 0$ und somit ist $\operatorname{grad}(p \cdot q) = n+m \geq 0$, insbes. ist $n+m > -\infty$, also ist $p \cdot q \neq 0$.

(b) $R^* \subseteq R[X]^*$:

- $a_0 \in R^* \Rightarrow$ es ex. $b_0 \in R^*$ mit $a_0 b_0 = 1$.
- Weil $a_0, b_0 \in R[X]$, ist $R^* \subseteq R[X]$.

$R[X]^* \subseteq R^*$:

- Sei $p \in R[X]^* \Rightarrow$ es ex. $q \in R[X]^*$ mit $p \cdot q = 1$.
- Weil R ein Integritätsring ist, ist das Produkt $a_n \cdot b_m$ der Leitkoeffizienten von p und q nicht 0.
- Also gilt $\underbrace{\operatorname{grad}(p)}_{\geq 0} + \underbrace{\operatorname{grad}(q)}_{\geq 0} = \operatorname{grad}(\underbrace{p \cdot q}_{=1}) = 0$

  $\Rightarrow \operatorname{grad}(p) = \operatorname{grad}(q) = 0$, d.h. $n = m = 0$.
- Somit ist $p = a_0$, $q = b_0$ und $p \cdot q = a_0 \cdot b_0 = 1$, also $p = a_0 \in R^*$.

Theorem 12.6 (Euklidischer Algorithmus)

Seien $p, q \in R[X]$, wobei $q \neq 0$ mit Leitkoeffizient b_m.
Dann ex. $s, r \in R[X]$ mit $\operatorname{grad}(r) < \operatorname{grad}(q)$ und ein $k \in \mathbb{N}$, sodass

$$b_m^k \cdot p = s \cdot q + r.$$

Beweis: Mit Induktion über $\operatorname{grad}(p)$.

- $\operatorname{grad}(p) < \operatorname{grad}(q)$: ($\operatorname{grad}(p)$ beliebig!)

  $p = 0 \cdot q + p$ (hier ist $s=0$, $r=p$, und $k=0$)

- $\operatorname{grad}(p) \geq \operatorname{grad}(q) = m$:

  Seien $\left.\begin{aligned} p &= a_0 + a_1 X + \ldots + a_n X^n, \; a_n \neq 0 \\ q &= b_0 + b_1 X + \ldots + b_m X^m, \; b_m \neq 0 \end{aligned}\right\} n \geq m$

  Sei $p_1 := b_m \cdot p - a_n X^{n-m} \cdot q \qquad (*)$

  $= b_m a_0 + b_m a_1 X + \ldots + b_m a_n X^n$

  $- a_n b_0 X^{n-m} - a_n b_1 X^{n-m+1} - \ldots - a_n b_m X^{\underbrace{n-m+m}_{=n}}$

  d.h. $\operatorname{grad}(p_1) < \operatorname{grad}(p)$.

  Mit Induktionsvoraussetzung ex. $s_1, r_1 \in R[X]$ mit $\operatorname{grad}(r_1) < \operatorname{grad}(q)$ und ein $k_1 \in \mathbb{N}$, sodass

  $$b_m^{k_1} \cdot p_1 = s_1 \cdot q + r_1. \qquad (**)$$

  $$b_m^{k_1} \cdot p_1 \overset{(*)}{=} b_m^{k_1+1} \cdot p - b_m^{k_1} \cdot a_n X^{n-m} \cdot q \overset{(**)}{=} s_1 q + r_1$$

  $$\overset{k := k_1+1}{\Longrightarrow} b_m^k \cdot p = \underbrace{(b_m^{k_1} \cdot a_n X^{n-m} + s_1)}_{=:s} \cdot q + \underbrace{r_1}_{=:r}$$

  also $b_m^k \cdot p = s \cdot q + r$ mit $\underbrace{\operatorname{grad}(r)}_{=\operatorname{grad}(r_1)} < \operatorname{grad}(q)$.

⊣

Def. Für $p, q \in R$ sagen wir p teilt q, geschrieben $p \mid q$, falls es ein $s \in R$ gibt, sodass $p \cdot s = q$.

Korollar 12.7 Sei $p \in R[X]$ und $a \in R$.

(a) Es ex. ein eindeutig bestimmtes Polynom $s \in R[X]$ mit $p = s \cdot (X-a) + p(a)$.

(b) $(X-a) \mid p \iff p(a) = 0$ (Abspalten einer Nullstelle)

Beweis: (a) Existenz von s:

- Sei $q = (X-a)$. Dann ist $\operatorname{grad}(q) = 1$ und Leitkoeff. von q ist $b_1 = 1$.
- Mit Thm. 12.6 ex. Polynome $s, r \in R[X]$ mit $\operatorname{grad}(r) < \operatorname{grad}(q) = 1$ und $p = s \cdot q + r$.
  Beachte: $b_1^k = 1$ und $\operatorname{grad}(r) = 0$ (d.h. $r \in R$, $r \neq 0$) oder $\operatorname{grad}(r) = -\infty$ (d.h. $r = 0$).
- Einsetzen von a: $p(a) = \underbrace{s(a) \cdot (a-a)}_{=0} + r(a) = r(a)$,

  und weil $r \in R$ gilt:

  $p(a) = 0$ für $\operatorname{grad}(r) = -\infty$, oder

  $p(a) = r \neq 0$ mit $r \in R$.

Eindeutigkeit von s:

- Sei $\tilde{s} \in R[X]$ mit $p = \tilde{s} \cdot (X-a) + p(a)$
  $= s \cdot (X-a) + p(a)$ ↓ −

  $\Rightarrow (X-a) \cdot (\tilde{s} - s) = 0$

  Wäre $\tilde{s} \neq s$, dann wäre $\tilde{s} - s = a_0 + a_1 X + \ldots + a_n X^n$ $(a_n \neq 0)$,

  somit wäre $(X-a) \cdot (\tilde{s} - s) = a_0 X + \ldots + \underbrace{a_n X^{n+1}}_{\neq 0} - a a_n X^n - \ldots - a \cdot a_n$

  also $(X-a) \cdot (\tilde{s} - s) \neq 0$.

(b) $(X-a) \mid p \iff \underbrace{r = 0}_{\text{wie oben}} \iff p(a) = 0$.

∎

Theorem 12.8 Ist K ein Körper, dann ist $K[X]$ ein Hauptidealring.

[allgemein gilt: Ist R ein Integritätsring, dann gilt
$R[X]$ ist Hauptidealring $\Leftrightarrow$ R ist ein Körper]

Beweis: Sei K ein Körper und $\alpha \subseteq K[X]$ ein Ideal mit $\alpha \neq (0)$.

zu zeigen: α wird von einem Element erzeugt.

- Sei $q \in \alpha$, $q \neq 0$ mit minimalem Grad.
  $q = b_0 + b_1 X + \dots + b_m X^m$ mit $b_m \neq 0$, $\operatorname{grad}(q) \geq 0$.
- Wir zeigen $\alpha = (q)$.
  - Sei $p \in \alpha$. Dann ex. mit Thm. 12.6 $s, r \in K[X]$ mit $\operatorname{grad}(r) < \operatorname{grad}(q)$ und ein $k \in \mathbb{N}$, sodass
    $$b_m^k \cdot p = s \cdot q + r.$$
  - Weil K ein Körper ist und $b_m \neq 0$, ist b_m (und damit auch b_m^k) invertierbar. Somit ist
    $$\underbrace{p}_{\in \alpha} = \underbrace{(b_m^{-k} \cdot s) \cdot q}_{\in \alpha} + (b_m^{-k} \cdot r)$$
    und damit $p - (b_m^{-k} \cdot s) \cdot q = b_m^{-k} \cdot r \in \alpha$
    mit $\operatorname{grad}(r) = \operatorname{grad}(b_m^{-k} \cdot r) < \operatorname{grad}(q)$.
  - Weil $\operatorname{grad}(q) \geq 0$ minimal war, muss $\operatorname{grad}(r) = -\infty$ sein, also $r = 0$ und somit ist $p = (b_m^{-k} \cdot s) \cdot q$, also $p \in (q)$, und weil p beliebig war ist $\alpha = (q)$. ⊣

Korollar 12.9 Sei K ein Körper und $p \in K[X]$ ein Polynom vom Grad $n > 0$. Dann hat p höchstens n verschiedene Nullstellen in K. (siehe Übungen für K kein Körper)

Beweis: Seien $a_1, \dots, a_k$ die versch. Nullstellen von p in K.

- Weil $p(a_1) = 0$ folgt aus Kor. 12.7 (b)
$$p = (X - a_1) \cdot s_1 \qquad (\text{mit } -\infty < \operatorname{grad}(s_1) < n)$$
- Weil $p(a_2) = 0$ und $a_1 \neq a_2$ gilt
$$0 = p(a_2) = \underbrace{(a_2 - a_1)}_{\neq 0} \cdot s_1(a_2) \underset{K \text{ nullteilerfrei}}{\Longrightarrow} s_1(a_2) = 0.$$
- Wieder mit Kor. 12.7 (b) folgt
$$s_1 = (X - a_2) \cdot s_2 \Longrightarrow p = (X - a_1) \cdot (X - a_2) \cdot s_2$$
$$(\text{mit } -\infty < \operatorname{grad}(s_2) < \operatorname{grad}(s_1) < n)$$
- $$p(a_3) = \underbrace{(a_3 - a_1)}_{\neq 0} \cdot \underbrace{(a_3 - a_2)}_{\neq 0} \cdot s_2(a_3) \Longrightarrow s_2(a_3) = 0$$
$$\Longrightarrow s_2 = (X - a_3) \cdot s_3$$
und somit ist $p = (X - a_1) \cdot (X - a_2) \cdot (X - a_3) \cdot s_3$, etc.
- Schliesslich ist
$$p = \underbrace{(X - a_1) \cdot (X - a_2) \cdot \dots \cdot (X - a_k)}_{=: q} \cdot s_k$$
mit $\operatorname{grad}(q) = k \leq n = \operatorname{grad}(p)$.

⊣

Bsp.
- $X^3 - 1$ hat 3 Nullstellen in $\mathbb{C}$ aber nur eine Nullstelle in $\mathbb{R}$ (bzw. $\mathbb{Q}$).
- $X^3 - 2$ hat 3 Nullstellen in $\mathbb{C}$, eine in $\mathbb{R}$, keine in $\mathbb{Q}$.

[**Bem.** $X^3 - X$ hat 6 Nullstellen in $\mathbb{Z}/6\mathbb{Z}$ (Übung)

[**Bem.** Kombination von Kor. 12.4 ($R[X]/a_{s_0} \cong R[s_0]$) mit Thm. 12.8 ($K[X]$ ist Hauptidealring) führt zum Begriff der **Minimalpolynome**: $\mathbb{Q}[X]/(X^2-2) \cong \mathbb{Q}[\sqrt{2}]$]