

Teil II: RINGE (und Moduln)A14: Polynomringe

Stichworte: der von $x_1, \dots, x_n$ über A erzeugte Ring $A[x_1, \dots, x_n]$, Polynomring in $X_1, \dots, X_n$ über A , universelle Eigenschaft von Polynomringen, Einsetzhomomorphismus, Existenz und Eindeutigkeit des Polynomrings, Faktorringe von Polynomringen, Nullstellen und Grad, CRS für $K[T]$

14.1. Einleitung: Polynomringe können über beliebigen kommutativen Ringen erklärt werden, indem man erst den von $x_1, \dots, x_n$ über A (durch Ringadjunktion) erzeugten Ring betrachtet und die A -Lineare Unabhängigkeit der Monome fordert. Die universelle Eigenschaft von Polynomringen liefert die Existenz und Eindeutigkeit von Polynomringen. Im Polynomring $K[T]$ gilt weiter der CRS.

14.2. Vereinbarung: In diesem Kapitel: Alle Ringe kommutativ.

14.3. Def.: A UR von B , $x_1, \dots, x_n \in B$. Dann:

$$A[x_1, \dots, x_n] := \bigcap \{A' \text{ UR von } B; A \subseteq A' \wedge x_1, \dots, x_n \in A'\}$$

heißt der von $x_1, \dots, x_n$ über A erzeugte Ring.

Sprechweise: " $A[x]$ entsteht aus A durch (Ring-) Adjunktion von $x_1, \dots, x_n$."

14.4. Bem.: $A[x_1, \dots, x_n][y_1, \dots, y_m] = A[x_1, \dots, x_n, y_1, \dots, y_m]$.

14.5. Bem.: $A[x] = \left\{ \sum_{i=0}^{\infty} a_i x^i; m \in \mathbb{N}_0, \text{ die } a_i \in A \right\}$

Bew.: " $\supseteq$ ": klar nach Def. von $A[x]$.

" $\subseteq$ ": r. g. ist Ring, der A umfasst und x enthält. $\square$

14.6. Bem.: $A[x_1, \dots, x_n] = \left\{ \sum_{(i_1, \dots, i_n) \in E} a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}; E \subseteq \mathbb{N}_0^n \text{ endlich} \right\}, m \in \mathbb{N}$.

14.7. Def.: Seien $A \subseteq P$ Ringe, $X_1, \dots, X_n \in P$. P heißt ein Polynomring in "den Unbestimmten" $X_1, \dots, X_n$ über A

$$: (\Leftrightarrow) (1) \quad P = A[X_1, \dots, X_n]$$

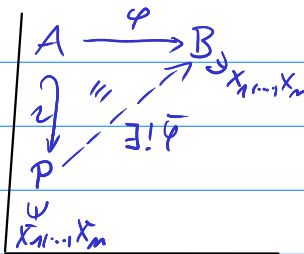
$$\wedge (2) \text{ Aus } \sum_{i \in E} a_i X_1^{i_1} \dots X_n^{i_n} = 0, E \subseteq \mathbb{N}_0^n \text{ endlich, folgt stets } a_i = 0 \quad \forall i \in E.$$

14.8. Satz: Universelle Eigenschaft von Polynomringen:

Sei P Polynomring in $X_1, \dots, X_n$ über A . Dann gilt:

$\forall$ Ringhom. $\varphi: A \rightarrow B$, B (Komm.) Ring $\forall$ Folgen $x_1, \dots, x_n \in B$

$\exists!$ Ringhom. $\bar{\varphi}: P \rightarrow B: \bar{\varphi}|_A = \varphi$ und $\bar{\varphi}(X_i) = x_i, 1 \leq i \leq n$.



Bew.: Setze $\bar{\varphi}(\sum_{i \in E} a_i X_1^{i_1} \dots X_n^{i_n}) := \sum_{i \in E} (\varphi a_i) x_1^{i_1} \dots x_n^{i_n}$,
ist wohldef.,

ein Ringhom. $P \rightarrow B$, $\bar{\varphi}|_A = \varphi$, $\bar{\varphi}(X_i) = x_i$ ($1 \leq i \leq n$), und eindeutig. $\square$

14.9. Bem.: Sei $A \subseteq B$ UR, d.h. φ Einbettung, $f = \sum_{i \in E} a_i X_1^{i_1} \dots X_n^{i_n}$.

Dann: $\bar{\varphi}(f) = \sum_{i \in E} a_i x_1^{i_1} \dots x_n^{i_n} =: f(x_1, \dots, x_n)$, Einsetzungshom.

$\bar{\varphi}: P = A[X_1, \dots, X_n] \rightarrow B$, Hom.satz ergibt:

$$\text{im } \bar{\varphi} = A[x_1, \dots, x_n] \cong A[X_1, \dots, X_n] / \ker \bar{\varphi}$$

$$\text{mit } \ker \bar{\varphi} = \{ f \in P; f(x_1, \dots, x_n) = 0 \}.$$

14.10. Satz: Für $n \geq 1$ gibt es bis auf Isomorphie genau einen Polynomring in n Unbestimmten über A .

Bew.: Eind.: Seien P, P' Polynomringe über A . Universelle Eigenschaft:

$$\begin{array}{ccc} A \hookrightarrow P' & & A \hookrightarrow P \\ \downarrow \text{inj.} & \text{und} & \downarrow \text{inj.} \\ P' & & P \end{array}$$

Somit: Ex. zwei inj. Ringhom.

$$\varphi_1: P \hookrightarrow P' \text{ und } \varphi_2: P' \hookrightarrow P.$$

Dies ist nur möglich, wenn φ_1 und φ_2 zueinander inverse Isomorphismen sind. Also: $P \cong P'$.

Existenz: Rekursiv: $n=1: P = A[X_1]$, s. lineare Algebra.

$n \rightsquigarrow n+1$: Sei $P_n = A[X_1, \dots, X_n]$ Polynomring in n Unbest. über A .

Nach „ $n=1$ “: $\exists P := P_n[X_{n+1}]$ Polynomring in 1 Unbest. über P_n .

Dann: P Polynomring in $X_1, \dots, X_{n+1}$ über A , denn:

$$P = P_n[X_{n+1}] = A[X_1, \dots, X_n][X_{n+1}] \stackrel{14.4}{=} A[X_1, \dots, X_n, X_{n+1}],$$

$$\text{ferner: } \sum_{i \in E} a_i X_1^{i_1} \dots X_{n+1}^{i_{n+1}} = 0 \quad (E \subseteq \mathbb{N}^{n+1} \text{ endl.})$$

$$\Rightarrow \sum_{j=0}^m \left(\sum_{\substack{(i_1, \dots, i_n) \in E \\ \text{mit } i_{n+1}=j}} a_i X_1^{i_1} \dots X_n^{i_n} \right) X_{n+1}^j = 0 \Rightarrow \forall 0 \leq j \leq m: b_j = 0$$

$$\stackrel{IV}{\Rightarrow} \forall i \in E: a_i = 0. \quad \square$$

14.11. Bsp.: Sei K Körper, betr. Faktoringe von $K[T]$: $K[T]$ ist Hauptidealbereich.

Sei $f = a_m T^m + \dots + a_1 T + a_0 \in K[T]$, $a_m \neq 0$.

$\Rightarrow A := K[T]/(f)$ ist K -Algebra.

14.12. Lemma: In $K[T]$, K Körper, bilden die Restklassen von $1, T, T^2, \dots, T^{m-1}$ modulo (f) eine K -Basis von $A := K[T]/(f)$, wobei $f = a_m T^m + \dots + a_1 T + a_0$, $a_m \neq 0$.

Insb.: $\dim_K A = m = \deg f$.

Bew.: Erzeugen: Sei $\bar{g} \in A$, Div. mit Rest: $g = f \cdot h + r$, $h, r \in K[T]$ mit $\deg r < m$.

Sei $r = b_{m-1} T^{m-1} + \dots + b_1 T + b_0$, $b_i \in K$ ($0 \leq i \leq m-1$).

Dann: $\bar{g} = \bar{h} \cdot \bar{f} + \bar{r} = \bar{r} = b_{m-1} \bar{T}^{m-1} + \dots + b_1 \bar{T} + b_0$.

K -lineare Unabh.: $0 = \sum_{i=0}^{m-1} b_i \bar{T}^i = \sum_{i=0}^{m-1} b_i T^i \Rightarrow \sum_{i=0}^{m-1} b_i T^i \in (f)$

$\Rightarrow \sum_{i=0}^{m-1} b_i T^i = 0 \Rightarrow \forall 0 \leq i \leq m-1: b_i = 0$. $\square$

14.13. Satz: Ist $f \in K[T] \setminus \{0\}$, K Körper, und $a \in K$ eine Nullstelle von f , so ist $(T-a) \mid f$.

Daher hat $f \neq 0$ höchstens $\deg(f)$ viele Nullstellen in K .

Bew.: Da $K[T]$ euklidisch, existiert die Div. mit Rest $f(T) = (T-a) \cdot q(T) + r$ mit $\deg(r) = 0$, also $r \in K$. Mit $0 = f(a) = 0 + r$ folgt $(T-a) \mid f$. Sind $a_1, \dots, a_m$ verschiedene Nullstellen von f , folgt $(T-a_1) \dots (T-a_m) \mid f$, also $m = \deg((T-a_1) \dots (T-a_m)) \leq \deg(f)$. $\square$

14.14. Bem.: R Ring. Dann: $R[T]$ euklidisch $\Leftrightarrow R$ Körper.

14.15. Lemma: Chinesischer Restsatz in $K[T]$:

Sei $f = p_1^{e_1} \dots p_m^{e_m}$, die $p_i \in K[T]$ irred. und paarw. nicht assoz., $e_i \geq 1$.

Dann: $K[T]/(f) \cong K[T]/(p_1^{e_1}) \times \dots \times K[T]/(p_m^{e_m})$.

Bew.: Es sind $(p_i^{e_i})$ und $(p_j^{e_j})$ für $i \neq j$ coprime,

d.h. $K[T] = (p_i^{e_i}) + (p_j^{e_j})$, dann A12.4 (CRS). $\square$