

A15: Primitive und irreduzible Polynome

Stichworte: primitive Polynome, Grad eines Polynoms, Lemma von Gauß über primitive Polynome,  $A$  faktoriell und  $f$  primitiv  $\Rightarrow (f \text{ in } A[X] \text{ irred.} \Leftrightarrow f \text{ in } \text{Quot}(A)[X] \text{ irred.})$ , Satz von Gauß:  $A$  faktoriell  $\Rightarrow A[X]$  faktoriell,  $A[X]^* = A^*$ , Eisensteinsches Irreduzibilitätskriterium

15.1. Einkleitung: In Polynomring  $A[X]$  über einem faktoriellen Ring  $A$  können primitive Polynome definiert werden. Nach einem Lemma von Gauß sind Produkte primitiver Polynome wieder primitiv. Die Irreduzibilität primitiver Polynome in  $A[X]$  kann dann in  $\text{Quot}(A)[X]$  überprüft werden. Nach dem Satz von Gauß ist  $A[X]$  faktoriell, wenn  $A$  es ist, und dies folgt aus dem Lemma von Gauß. Zuletzt zeigen wir das Eisensteinsche Irreduzibilitätskriterium für Polynome.

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

15.3. Def.:  $A$  faktorieller Ring.

$f = \sum_{i=0}^m b_i X^i \in A[X]$  heißt primitiv  $\Leftrightarrow \deg(f) \geq 1$  und  $\text{ggT}(b_0, \dots, b_m) = 1$ .

Grad eines Polynoms  $\neq 0$ :  $\deg(f) = \max\{i; b_i \neq 0\}$  (nur für  $\mathbb{F}[B]$ ).

15.4. Bem.:  $f = \sum_{i=0}^m b_i X^i \in A[X]$ ,  $d \in A$  ein  $\text{ggT}(b_0, \dots, b_m)$ ,  $b_i = da_i$ .

Dann:  $\bar{f} = \sum_{i=0}^m a_i X^i$  primitiv.

15.5. Lemma von Gauß: Sei  $A$  faktoriell. Dann:

$A[X] \ni f, g$  primitiv  $\Rightarrow f \cdot g$  primitiv

Bew.: Sei  $f = \sum_{i=0}^m a_i X^i$ ,  $g = \sum_{j=0}^n b_j X^j \in A[X]$ . Dann ist  $f \cdot g = \sum_{k=0}^{m+n} c_k X^k$  mit  $c_k = \sum_{i+j=k} a_i b_j$ .

Ann.:  $\exists p \in A$  prim:  $p | c_k$  für alle  $k$ .

Sei  $i_0 := \min\{i; p \nmid a_i\} (\neq \emptyset)$  (da  $a_i$  teilerfremd),

und  $j_0 := \min\{j; p \nmid b_j\} (\neq \emptyset)$  (da  $b_j$  teilerfremd).

Setze  $k_0 = i_0 + j_0$ . Dann ist  $c_{k_0} = \sum_{i+j=k_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i+j=k_0 \\ i \neq i_0, j \neq j_0}} a_i b_j$ .

$\Rightarrow p$  teilt jeden Summanden der 2. Summe,  $p | c_{k_0} \Rightarrow p | a_{i_0} b_{j_0} \Rightarrow p | a_{i_0} \vee p | b_{j_0} \quad \downarrow \quad \square$

156. Lemma: Sei  $A$  faktorieller IB,  $K$  Quotientenkörper von  $A$ ,  $A[X] \ni f$  primitiv.

Dann:  $f$  irreduzibel in  $A[X] \Leftrightarrow f$  irreduzibel in  $K[X]$ . Bem. 15.10

Bew.: " $\Leftarrow$ ": Sei  $f \in K[X]$  irred., d.h.  $f = g \cdot h$  mit  $g, h \in K[X] \Rightarrow g \in K[X]^{\times} = K^{\times}$  oder  $h \in K[X]^{\times} = K^{\times}$ . Sei also z.B.  $g \in A$ .

Dann:  $g \in A^{\times}$ , da  $f$  primitiv  $\Rightarrow f$  irred. in  $A[X]$ .

" $\Rightarrow$ ": \* Sei  $f \in K[X]$  reduzibel, etwa  $f = g \cdot h$ ,  $g, h \in K[X]: 0 < \deg(g) < \deg(f)$ .

Seien  $a_1, b_1, a_2, b_2 \in A: g = \frac{a_1}{b_1} \tilde{g}, h = \frac{a_2}{b_2} \tilde{h}$  mit  $\tilde{g}, \tilde{h} \in A[X]$  primitiv

(vgl. Bem. 15.4).

Schreiben:  $f = g \cdot h = \frac{a_1 a_2}{b_1 b_2} \tilde{g} \tilde{h} = \frac{a}{b} \tilde{g} \tilde{h}$  mit  $a, b$  teilerfremd.

$\Rightarrow b f = a \tilde{g} \tilde{h}$ .

\* Somit genügt es, zu zeigen:  $b \in A^{\times}$ . (Dann:  $f = \frac{a}{b} \tilde{g} \tilde{h}$  echte Zerl. in  $A[X]$   $\Downarrow$ )

Sonst:  $p \in A$  Primfaktor von  $b \Rightarrow p \mid a \Rightarrow p$  teilt alle Koeff. von  $\tilde{g} \tilde{h}$

im  $\Downarrow$  zum Lemma von Gauß 15.5.  $\square$

157. Bem.:  $2 + 6X = 2 \cdot (1 + 3X)$  ist irreduzibel in  $\mathbb{Q}[X]$  (da  $2 \in \mathbb{Q}^{\times}$ ),

ist reduzibel in  $\mathbb{Z}[X]$  ( $2, 1+3X$  "echte" Polynome in  $\mathbb{Z}[X]$ ).

158. Bem.: Primelemente aus  $A$  sind prim in  $A[X]$ . ( $A$  faktoriell)

Bew.: Sonst:  $p = g \cdot h \Rightarrow \deg g = \deg h = 0$ , d.h.  $g, h \in A \Rightarrow g \in A^{\times}$  oder  $h \in A^{\times}$ .  $\square$

159. Bem.:  $(A[X])^{\times} = A^{\times}$  ( $A$  faktoriell).

1510. Bem.:  $(K[X])^{\times} = K^{\times}$  ( $K$  Körper).

1511. Satz:  $A$  faktoriell  $\Rightarrow$  Polynomring  $A[X]$  faktoriell. (auch: "Satz von Gauß".)

Bew.: \* Eind. der PFZ: Sei  $K$  der Quotientenkörper von  $A$ ,

sei  $\underbrace{p_1 \cdots p_m}_a \cdot \underbrace{f_1 \cdots f_r}_b = \underbrace{q_1 \cdots q_m}_c \cdot \underbrace{g_1 \cdots g_s}_d$ ,  $\otimes$

die  $p_i, q_j \in A[X]$  prim vom Grad 0,

die  $f_i, g_j \in A[X]$  prim vom Grad  $> 0$ , und primitiv.

Nach Lemma 15.6:  $f_i, g_j \in K[X]$  prim, nach Bem. 15.10:  $a, b \in K^{\times} = (K[X])^{\times}$ .

Wegen der Eind. der PFZ in  $K[X]$  ist  $r=s$ ,  
und  $\exists a_i, b_i \in A: f_i = \frac{a_i}{b_i} \cdot g_i$  ( $1 \leq i \leq r$ ),  $\subseteq$  so numeriert.

Seien  $\subseteq a_i, b_i$  teilerfremd.

Nun:  $b_i f_i = a_i g_i \Rightarrow b_i, a_i \in A^*$ , da  $f_i, g_i$  primitiv, vgl. Lemma 15.6.

$$\Rightarrow p_1 \dots p_m \cdot \underline{f_1 \dots f_r} = \underbrace{(b_1 a_1^{-1}) \dots (b_r a_r^{-1})}_{\in A^*} \cdot g_1 \dots g_m \cdot \underline{f_1 \dots f_r}$$

jetzt Eind. der PFZ in  $A$   $\Rightarrow$  Eind. der PFZ  $\otimes$  in  $A[X]$ .

\* Ex. der PFZ: Sei  $f \in A[X]$ , VI nach  $\deg(f) =: m$ :

$m=0$ : PFZ in  $A$ , Bem. 15.9.  $\checkmark$

$m>0$ : Schreiben  $f = a \tilde{f}$ ,  $\tilde{f}$  primitiv.

1. Fall:  $\tilde{f}$  irreduzibel: ist PFZ  $\checkmark$

2. Fall:  $\tilde{f}$  reduzibel:  $\tilde{f} = g \cdot h$  für  $g, h \in A[X]$ ,  $g, h \notin (A[X])^* = A^*$ .

$$\Rightarrow 0 < \deg(g), \deg(h) < m.$$

IV auf  $g, h$   $\Rightarrow$  PFZ von  $\tilde{f}$ .  $\checkmark$  □

15.12. Kor.:  $K$  Körper,  $m \geq 1$ . Dann: Polynomring  $K[X_1, \dots, X_m]$  faktoriell.

Bew.: VI nach  $m$ :  $m=1$ :  $K[X_1]$  ist HIB, also faktoriell nach A13.17.

$m \rightarrow m+1$ :  $K[X_1, \dots, X_m, X_{m+1}] = \underbrace{(K[X_1, \dots, X_m])}_{\text{faktoriell nach IV}} [X_{m+1}]$  ist faktoriell nach Satz 15.11. □

15.13. Eisensteinsches Irreduzibilitätskriterium:

Vor.:  $A$  faktorieller Ring,  $K$  Quotientenkörper von  $A$ .

Sei  $f(X) = a_m X^m + \dots + a_1 X + a_0 \in A[X]$  mit  $\deg(f) = m \geq 1$ ,

so dass  $\exists p \in A$  prim:

$$\begin{aligned} p &\nmid a_m, \\ p &\mid a_i \text{ für } 0 \leq i < m, \\ p^2 &\nmid a_0. \end{aligned}$$

Beh.:  $f$  irreduzibel in  $K[X]$ .

15.14 Bsp.: Sei  $A = \mathbb{Z} \subseteq \mathbb{Q} = K$ ,  $\mathbb{Z} \ni p$  prim. Dann ist  $X^m - p \in \mathbb{Q}[X]$

irreduzibel nach Eisenstein 15.13.

15.15. Bew. von 15.13: Sei  $\mathcal{O} \nmid f$  primitiv (sonst ggT herausziehen).

Andernfalls  $\exists 0 < m_1, m_2 < m, b_i, c_j \in A$ :

$$f = \left( \sum_{i=0}^{m_1} b_i X^i \right) \cdot \left( \sum_{j=0}^{m_2} c_j X^j \right) = \sum_{k=0}^{m_1+m_2} \left( \sum_{i+j=k} b_i c_j \right) X^k,$$

dabei ist  $a_0 = b_0 c_0$ .

Da  $p \mid a_0, p^2 \nmid a_0$ , gilt  $\mathcal{O} \nmid b_0, p \nmid c_0$ .

Setze  $i_0 := \min \{ i_j \mid p \nmid b_{i_j} \} (\neq \emptyset)$ , dann  $0 < i_0 \leq m_1 < m$ .

Nun  $a_{i_0} = b_{i_0} c_0 + b_{i_0-1} c_1 + \dots + b_0 c_{i_0}$ .

Dabei:  $p \mid a_{i_0}$  und  $p \nmid b_i$  für alle  $0 \leq i < i_0$ ,

d.h.  $p \mid b_{i_0} c_0 \Rightarrow p \mid b_{i_0} \nabla$ . □

15.16. Bsp.: Sei  $f(X, Y) = X^m + Y(Y+1) \in \mathbb{C}[X, Y] = (\mathbb{C}[Y])[X]$ . Die Vor. von Eisenstein ( $A = \mathbb{C}[Y]$ ) sind mit  $p := Y$  erfüllt  $\Rightarrow f$  irreduzibel.

15.17. Bsp.: Sei  $A = \mathbb{Z} \subseteq \mathbb{Q} = K, p \in \mathbb{N}$  prim.

Dann:  $f(X) := X^{p-1} + X^{p-2} + \dots + X + 1$  irreduzibel über  $\mathbb{Q}$ .

Bew.: Sei  $\varphi: \mathbb{Q}[X] \rightarrow \mathbb{Q}[X]$  der eind. best. Endomorphismus mit  $X \mapsto X+1$ , also  $\varphi(g(X)) = g(X+1)$ .

Dieser ist Automorphismus: Betr. den eind. best. Endo

$\psi: \mathbb{Q}[X] \rightarrow \mathbb{Q}[X]$  mit  $X \mapsto X-1$ , dann gilt

$$\varphi \circ \psi(X) = \varphi(X-1) = (X-1)+1 = X, \text{ sowie}$$

$$\psi \circ \varphi(X) = \psi(X+1) = (X+1)-1 = X.$$

Nun ex. genau ein Endo mit  $X \mapsto X$ , nämlich  $\text{id}_{\mathbb{Q}[X]}$ ,

also:  $\varphi \circ \psi = \text{id}_{\mathbb{Q}[X]} = \psi \circ \varphi \Rightarrow \varphi$  Automorphismus.

Zeige also nur:  $\varphi(f) = f(X+1)$  ist irreduzibel:

$$\text{Es gilt } \underline{X^p - 1 = (X-1)f(X)} \Rightarrow \underline{(X+1)^p - 1 = X \cdot f(X+1)} \quad (\varphi \text{ anwenden})$$

$$= \sum_{i=1}^p \binom{p}{i} X^i \Rightarrow \underline{f(X+1) = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i}.$$

Für  $0 \leq i < p-1$

mit  $\binom{p}{i+1} = \frac{p(p-1)\dots(p-i)}{1 \cdot 2 \dots (i+1)}$  gilt also:  $p \mid \binom{p}{i+1}$  für  $0 \leq i < p-1$ ,  
 $p^2 \nmid \binom{p}{p} = p, p \nmid \binom{p}{p} = 1$ .

Nach Eisenstein 15.13 ist daher  $f(X+1)$  irreduzibel. □

15.18. Bsp.: Beachte:  $X^3 + X^2 + X + 1$  hat Nst. -1, also reduzibel.