A15: Primitive und irreduzible/prime Polynome

15.1. Einleitung: primitive Pol., Lemma/Satz von Gauß, Eisensteinsches Irreduzibilitätskriterium

15.2. Vereinbarung: Hier: Alle Ringe kommutativ, sogar faktoriell! ↳ Eind. & Ex. der PFZ

15.3 Def.: A faktorieller Ring. (IB)

$f = \sum_{i=0}^{m} b_i X^i \in A[X]$ heißt primitiv $:\Leftrightarrow \deg(f) \geq 1$ und $\underbrace{ggT(b_0, b_1, \dots, b_m)}_{= \dots ggT(ggT(ggT(b_0,b_1),b_2),b_3)\dots)} = 1$

Grad eines Polynoms $f \neq 0$:

$\deg(f) := \max\{i;\ b_i \neq 0\}$ (nur für IB)

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

"Herausziehen des ggTs der Koeff."

↳ Zusammenfassen gemeinsamer Primfaktor (A faktoriell)

Bsp.: $4X^2 + 6 = \underline{2} \cdot \underbrace{(2X^2+3)}_{\text{primitives}} \in \mathbb{Z}[X]$

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 $f \cdot g = \sum_{k=0}^{m+n} c_k X^k$, $c_k = \underbrace{\sum_{i+j=k}}_{\hookrightarrow j = k-i} a_i b_j = \sum_i \underbrace{\sum_{j=k-i}} a_i b_j = \sum_i a_i b_{k-i}$

Ann.: $\exists p \in A$ prim: $p \mid c_k$ 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 $\underbrace{c_{k_0}}_{p \mid c_{k_0}} = \sum_{i+j=k_0} a_i b_j = a_{i_0} b_{j_0} + \underbrace{\sum_{\substack{i+j=k_0 \\ i \neq i_0, j \neq j_0}} a_i b_j}_{p \mid \text{''}}$

$\Rightarrow p \mid a_{i_0} b_{j_0} \overset{\text{d.v. Euklid}}{\Rightarrow} p \mid a_{i_0} \vee p \mid b_{j_0}$ ↯. □

$\widetilde{\mathbb{Z}[X]} \hookrightarrow \widetilde{\mathbb{Q}[X]}$ Bsp.: $\mathbb{Q} = \underline{\mathrm{Quot}(\mathbb{Z})}$

15.6. Lemma: Sei A <u>faktorieller IB</u>, $K = \mathrm{Quot}(A) = \{\frac{a}{b} ; a, b \in A, b \neq 0\}$, $A[X] \ni f$ primitiv.

Dann: f irred. in $A[X] \Leftrightarrow f$ irred. in $K[X]$

[Bsp.: f " $\mathbb{Z}[X] \Leftrightarrow f$ " $\mathbb{Q}[X]$, da $\mathbb{Z}$ faktoriell.]

<u>Bew.:</u> „$\Leftarrow$": Sei $f \in K[X]$ irred., d.h. $f = g \cdot h$ mit $g, h \in K[X]$

$\Rightarrow g \in K[X]^\times = \underline{\underline{K^\times}}$ oder $h \in K[X]^\times = \underline{\underline{K^\times}}$.

Sei also z.B. $g \in A$ mit $f = g \cdot h$ (Zerl. in $A[X]$).

Dann: $g \in \underline{\underline{A^\times}}$, 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 $a_1, b_1, a_2, b_2 \in A$:

$g = \frac{a_1}{b_1} \cdot \tilde{g}$, $h = \frac{a_2}{b_2} \cdot \tilde{h}$

$\hookrightarrow \in A[X]$ primitiv [Bem. 15.4]

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

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

* <u>Gen. z.z.</u>, $b \overset{!}{\in} A^\times$ (Dann: $f = \overbrace{a b^{-1}}^{\in A} \tilde{g}\tilde{h}$ echte Zerl. in $\underline{A[X]}$ ↯).

Sonst: $p \in A$ Primfaktor von $b \underset{(a,b)=1}{\Rightarrow} p \nmid a \underset{bf = a\tilde{g}\tilde{h}}{\Rightarrow} p$ teilt alle Koeff von $\tilde{g}\tilde{h}$, im ↯ zum L.v. Gauß 15.5. □

15.7. <u>Bem/Bsp.:</u> * $\underbrace{X^2 - 2}_{\text{primitiv}} \in \underline{\mathbb{Z}[X] \text{ irred.}}$

$\Leftrightarrow$ <u>in $\mathbb{Q}[X]$ irred.</u>:

$\leftarrow X^2 - 2 = (X - \underbrace{\sqrt{2}}_{\notin \mathbb{Q}})(X + \underbrace{\sqrt{2}}_{\notin \mathbb{Q}})$

* $2 + 6X = 2 \cdot (1 + 3X)$

ist irred. in $\mathbb{Q}[X]$, da $2 \in \mathbb{Q}^\times$

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

15.8. Bem.: Primel. aus A sind prim in $A[X]$ (A faktoriell).

Bew.: sonst: $A \ni \underbrace{p}_{\deg(p)=0} = g \cdot h \Rightarrow \deg g = \deg h = 0$, d.h. $g, h \in A$

$p = g \cdot h \Rightarrow g \in \underbrace{A^\times}_{=A[X]^\times}$ oder $h \in \underbrace{A^\times}_{=A[X]^\times}$. $\square$

15.9. Bem.: $(A[X])^\times = A^\times$ (A faktoriell)

15.10. Bem.: $(K[X])^\times = K^\times$ (K Körper)

15.11. Satz (von Gauß): A faktoriell $\Rightarrow$ $A[X]$ faktoriell.

Bew.:

* Eind. der PFZ: Sei $K = \mathrm{Quot}(A)$.

Sei $\underbrace{p_1 \cdots p_m}_{=:a} \cdot f_1 \cdots f_r = \underbrace{q_1 \cdots q_m}_{=:b} \cdot g_1 \cdots g_s$ $\circledast$

die $p_i, q_j \in A[X]$ prim/irred. vom Grad 0, d.h. $\in A$,

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

Nach Lemma 15.6: $f_i, g_j \in K[X]$ irred.,

nach Bem. 15.10: $a, b \in K^\times = (K[X])^\times$.

Wegen Eind. der PFZ in $K[X]$

[$K[X]$ faktoriell, da $K[X]$ eukl. $\Rightarrow K[X]$ HIB $\Rightarrow K[X]$ faktoriell]

ist $r = s$ und $\exists\, a_i, b_i \in A$: $f_i = \frac{a_i}{b_i} \cdot g_i$ ($1 \le i \le r$, OE so numeriert)

Sei OE a_i, b_i teilerfremd.

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

$$\Rightarrow p_1 \cdots p_m \cdot f_1 \cdots f_r = \underbrace{(b_1 a_1^{-1}) \cdots (b_r a_r^{-1})}_{\in A^\times} \cdot q_1 \cdots q_m f_1 \cdots f_r,$$

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

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

$n = 0$: PFZ in A, Bem. 15.9: $A[X]^\times = A^\times$.

$n > 0$: Schreibe $f = a\hat{f}$, $\hat{f}$ primitiv. Falls $\hat{f} = g \cdot h$, $g, h \in A[X]$, $g, h \notin (A[X])^\times = A^\times$

$\Rightarrow 0 < \deg g, \deg h < n \Rightarrow$ IV auf g, h liefert $\Rightarrow$ PFZ von $\hat{f}$. $\square$

15.12. <u>Kor.:</u> A faktoriell, $n \geq 1$. Dann: $A[X_1, \dots, X_n]$ faktoriell.

Bew.: VI nach n: $n=1$: $A[X_1]$ faktoriell nach 15.11 (S. von Gauß)

$n \rightsquigarrow n+1$: $A[X_1, \dots, X_n, X_{n+1}] = (\underbrace{A[X_1, \dots, X_n]}_{\text{faktoriell nach IV}})[X_{n+1}]$

ist faktoriell nach 15.11. (S. von Gauß).

Wann ist ein Polynom irred.?

Bsp.: $2X^{10} + 3X^2 + 9X + 12 \in \mathbb{Z}[X]$ bzw. $\in \mathbb{Q}[X]$? ja, irred. $(p=3)$

15.13. <u>Eisensteinsches Irreduzibilitätskriterium:</u>

Vor.: A faktoriell, $K = \mathrm{Quot}(A)$.

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

so dass $\exists p \in A$ prim: $p \nmid a_n$,

$p \mid a_i$ für $0 \leq i < n$, $p^2 \nmid a_0$.

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

15.14. <u>Bsp.:</u> Sei $A = \mathbb{Z} \subseteq \mathbb{Q} = K$, $\mathbb{Z} \ni p$ prim.

Dann ist $X^n - p \in \mathbb{Q}[X]$ irred. nach 15.13.

$\ulcorner \Rightarrow \sqrt[n]{p} \notin \mathbb{Q}$ $\ulcorner$sonst $X - \sqrt[n]{p}$ abspaltbar$\lrcorner$ $\lrcorner$

15.15. Bew. von 15.13: Sei OE f primitiv (sonst gst heraus).

Anderfalls $\exists\, 0 < n_1, n_2 < n$, $b_i, c_j \in A$:

$$f = \left(\sum_{i=0}^{n_1} b_i X^i\right)\left(\sum_{j=0}^{n_2} c_j X^j\right) = \sum_{a=0}^{n_1+n_2=n} \underbrace{\left(\sum_{i+j=a} b_i c_j\right)}_{=a_a} X^a$$

dabei ist $a_0 = b_0 c_0$.

Da $p \mid a_0$, $p^2 \nmid a_0$, gilt OE $p \mid b_0$, $p \nmid c_0$.

Setze $i_0 := \min\{i;\ p \nmid b_i\}$ $(\neq \emptyset)$, dann $0 < i_0 \leq n_1 < n$.

Nun $\underbrace{a_{i_0}}_{p \mid a_{i_0} \text{ wegen Krit.}} = \underbrace{b_{i_0} c_0}_{\text{und}} + \underbrace{b_{i_0-1} c_1 + \dots + b_0 c_{i_0}}_{p \mid \text{ da } p \mid b_i \text{ für alle } 0 \leq i < i_0}$

$\Rightarrow p \mid b_{i_0} c_0 \underset{p \nmid c_0}{\Rightarrow} p \mid b_{i_0}$ ↯ zur Def. von i_0.

$\square$

15.16. Bsp.: Sei $f(X,Y) = X^m + \underbrace{Y(Y+1)}_{=a_0} \in \mathbb{C}[X,Y] = (\underbrace{\mathbb{C}[Y]}_{=:A \text{ faktoriell}})[X]$

Die Vor. von Eisenstein sind mit $p := Y$ erfüllt

$\rightarrow p \nmid a_m = 1, \quad p \mid a_0, \quad p^2 \nmid a_0$

$\Rightarrow f$ irred.

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

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

Bew.: Sei $\varphi : \mathbb{Q}[X] \to \mathbb{Q}[X]$, $X \mapsto X+1$, ist Ring-Auto ✓

Also: irred. von $f(X)$ $\Leftrightarrow$ irred. von $f(X+1)$

Noch z.z.: $f(X+1)$ irred.

$$X^p - 1 = (X-1) f(X) \overset{\varphi}{\Rightarrow} \underbrace{(X+1)^p - 1}_{= \sum_{i=1}^{p} \binom{p}{i} X^i} = X \cdot \underbrace{f(X+1)}$$

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

$$= \frac{p(p-1)\cdots(p-i)}{1 \cdot 2 \cdots (i+1)} \in \mathbb{N}, \text{ Vielf. von } p$$

Also $p \mid \binom{p}{i+1}$ für $0 \le i < p-1$, $p^2 \nmid \binom{p}{1} = p$, $p \mid \binom{p}{p} = 1$.

$\underset{\text{Eisenstein}}{\Rightarrow}$ $f(X+1)$ irred. $\underset{\text{Auto-trick}}{\Rightarrow}$ $f(X)$ irred. $\square$

Bsp.: $X^2 + X + 1$ irred, $X^4 + X^3 + X^2 + X + 1$ irred.

Aber: $X^3 + X^2 + X + 1$ red., hat Nst. -1 ...