

7. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Gabriel Lehericy, Simon Müller

WS 2016/2017: 18. November 2016

Körper \subsetneq Euklidische Bereiche \subsetneq Hauptidealbereiche \subsetneq Faktorielle Bereiche \subsetneq Integritätsbereiche

Konvention

deg von Nullpolynom ist = 0.

Proposition 1 (Zusammenfassung)

Sei R integer und $p, q \in R[x]$. Es gelten:

1. $\deg p(x)q(x) = \deg p(x) + \deg q(x)$
2. $(R[x])^\times = R^\times$
3. $R[x]$ ist integer
4. $R[x]$ ist E.R. $\Leftrightarrow R$ ist Körper
5. $\text{Quot}(R[x]) := F(x) := \{\frac{p}{q} \mid p, q \in R[x], q \neq 0\}$ ist Körper, wobei $F := \text{Quot}(R)$.

Bemerkung

Sei $I \triangleleft R$. Dann ist $I[x] := \langle I \rangle \triangleleft R[x] = \{f(x) \in R[x] \mid f(x) = \sum a_i x^i \text{ mit } a_i \in I\}$

Proposition 2

$R[x]/I[x] \simeq (R/I)[x]$

Beweis

$$\begin{aligned} \varphi: R[x] &\rightarrow (R/I)[x] \\ \sum a_i x_i &\mapsto \sum \bar{a}_i x^i \end{aligned}$$

ist ein Ringhomomorphismus; surjektiv; $\ker \varphi = I[x]$. □

Korollar

P ist Primideal in $R \Rightarrow P[x]$ ist Primideal in $R[x]$. □

Exkurs $R[x_1, \dots, x_n] := R[x_1, x_2, \dots, x_{n-1}][x_n]$.

Notation = $\{p(x_1, \dots, x_n) | p \in R[x_1, \dots, x_n]\}$.

Also: *Polynome* in den Variablen x_1, \dots, x_n werden folgendermaßen definiert:

Es ist eine endliche Summe von *Monomen*.

$$m(x_1, \dots, x_n) := ax_1^{d_1} \cdots x_n^{d_n} \quad a \in R$$

$$\text{Notation} \quad \begin{cases} := a \underline{x}^{\underline{d}} & d_i \in \mathbb{N}_0 \\ (x_1, \dots, x_n) := \underline{x} \\ (d_1, \dots, d_n) := \underline{d} \in \mathbb{N}_0^n \end{cases}$$

- d_i ist der *Grad von x_i* in $m(\underline{x})$
- $|\underline{d}| := \sum_{i=1}^n d_i$ ist der *Grad von $m(\underline{x})$* $\deg m(\underline{x}) := |\underline{d}|$
- $\deg p(x_1, \dots, x_n)$ ist der größte Grad von seinen Monomen.
- Die Summe aller Monome von $p(x_1, \dots, x_n)$ vom Grad k heißt die *homogene Komponente von p vom Grad k* .
- Wenn $\deg p = d$, so läßt sich p eindeutig als Summe

$$p = p_0 + p_1 + \cdots + p_d$$

beschreiben, wobei p_k die homogene Komponente vom Grad k ist für $0 \leq k \leq d$ (und $p_k = 0$ vorkommen kann).

Lemma 1

$R[x]$ ist faktoriell $\Rightarrow R$ ist faktoriell.

Beweis

$$(R[x])^\times = R^\times \quad (*)$$

Sei $0 \neq r \in R \setminus R^\times$. r ist das Produkt von Irreduziblen in $R[x]$ und diese (deg Bedingungen) müssen $\deg = 0$ haben, d.h. sind Elemente aus R . Beachte ferner, dass $r \in R$ irreduzibel in $R[x] \Rightarrow$ irreduzibel in R , sonst $r = ab$; $a, b \in R \setminus R^\times$. Aber wegen $(*)$: $r = ab$; $a, b \in R[x] \setminus (R[x])^\times$ - Widerspruch. □

Für die Umkehrung von Lemma 1 brauchen wir ein Hilfslemma.

Lemma von Gauß

Sei R faktoriell und $p(x) \in R[x]$. Wenn $p(x)$ reduzibel in $F[x]$ ist, (wobei $F := \text{Quot}(R)$), so ist $p(x)$ reduzibel in $R[x]$.

Das heißt: Wenn $p(x) = A(x)B(x)$ mit $A, B \in F[x]$, $\deg A \geq 1, \deg B \geq 1$, dann gibt es $0 \neq r, 0 \neq s \in F$ mit

$$\left. \begin{array}{l} rA(x) := a(x) \\ sB(x) := b(x) \end{array} \right\} \in R[x] \quad \deg a(x) \geq 1, \deg b(x) \geq 1$$

und $p(x) = a(x)b(x) \in R[x]$.

Beweis

$$\begin{array}{ccccc} p(x) & = & A(x) & B(x) & \\ \uparrow & & \uparrow & \uparrow & \\ R[X] & & F[x] & F[x] & \end{array}$$

Die Koeffizienten von A, B sind aus der Form $\frac{r_i}{s_i}$ mit $r_i, 0 \neq s_i \in R$. Wir multiplizieren A, B jeweils mit den gemeinsamen Nennern seiner Koeffizienten und bekommen eine Gleichung der Form

$$\left. \begin{array}{ccc} dp(x) & = & a'(x) \quad b'(x) \\ \uparrow & & \uparrow \quad \uparrow \\ d \in R & & \in R[x] \quad \in R[x] \end{array} \right\} \text{ mit } d \in R, d \neq 0; \deg a'(x) \geq 1, \deg b'(x) \geq 1; a', b' \in R[x]. \quad (*)$$

und $a'(x) = \alpha A(x), b'(x) = \beta B(x); \alpha, \beta \in F$.

1. Fall: $d \in R^\times \quad \checkmark$

2. Fall: $d \in R \setminus R^\times$

So schreibe $d = p_1 \cdots p_n$, p_i ist irreduzibel in R .

- p_1 irreduzibel $\Rightarrow I = \langle p_1 \rangle$ ist Primideal in R und $d \in I$
(also ist auch $I[x] = p_1 R[x]$ Primideal).
- $(R / \langle p_1 \rangle)[x]$ ist integer.

(*) reduziere $\text{mod } \langle p_1 \rangle$. Wir bekommen $0 = \overline{a'(x)b'(x)}$ in $(R / \langle p_1 \rangle)[x]$. Also ist ohne Einschränkung $\overline{a'(x)} = 0$, das heißt alle Koeffizienten von $a'(x)$ liegen in $\langle p_1 \rangle$ sind also durch p_1 teilbar in R . So hat man $a''(x) := \frac{1}{p_1} a'(x) \in R[x]$, $\deg a''(x) \geq 1$ mit $\frac{1}{p_1} \in F$, das heißt wir können die Gleichung (*) um p_1 kürzen und bekommen eine neue Gleichung

$$d'p(x) = a''(x)b''(x) \text{ in } R[x].$$

Aber nun hat d' einen irreduziblen Faktor weniger, i.e. $d' = p_2 \cdots p_n$.

Wiederholung mit p_2, \dots , mit p_n (gleiche Argumente) ergibt eine Gleichung schließlich aus der Form

$$p(x) = a(x)b(x) \quad a(x), b(x) \in R[x]$$

$$\text{mit } a(x) = \alpha'a'(x) \quad \alpha', \beta' \neq 0$$

$$b(x) = \beta'b'(x) \quad \alpha', \beta' \in F$$

$$\text{d.h. } \begin{aligned} a(x) &= \alpha\alpha'A(x) \\ b(x) &= \beta\beta'B(x) \end{aligned} \quad \text{mit } \alpha\alpha' \in F \text{ und } \beta\beta' \in F. \quad \square$$

Korollar

Sei R faktoriell, $F := \text{Quot}(R)$; $\deg p \geq 1$, wobei $\sum_{i=0}^n a_i x_i =: p(x) \in R[x]$ mit ggT von $\{a_0, \dots, a_n\} = 1$.

Dann ist $p(x)$ in $R[x]$ irreduzibel genau dann, wenn $p(x)$ in $F[x]$ irreduzibel. Insbesondere ist $p(x) \in R[x]$ normiert und in $R[x]$ irreduzibel, so ist $p(x)$ in $F[x]$ irreduzibel.

Beweis

GL ergibt: Ist $p(x)$ in $F[x]$ reduzibel, so ist $p(x)$ in $R[x]$ reduzibel. Umgekehrt ist $p(x)$ in $R[x]$ reduzibel, dann ist $p(x) = a(x)b(x)$, wobei $a(x), b(x) \in R[x] \setminus R$ (sonst wäre der ggT der Koeffizienten von $p(x)$ in R ungleich 1).

Das heißt $p(x) = a(x)b(x)$ für $a(x), b(x) \in R[x]$, $\deg a(x) \geq 1, \deg b(x) \geq 1$. Insbesondere $p(x) = a(x)b(x)$ für $a(x), b(x) \in F[x]$, $\deg a(x) \geq 1, \deg b(x) \geq 1$, das heißt $p(x)$ ist in $F[x]$ reduzibel. \square