Algebra B III

Kuhlmann

7. Vorlesung am 15.11.2012.

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

Konvention: deg vom Nullpolynom ist $= 0$

Proposition 1. Sei R integer, $p, q \in R[x]$.
(Zusammenfassung) Es gelten:

1. $\deg p(x)q(x) = \deg p(x) + \deg q(x)$.

2. $\left(R[x]\right)^\times = R^\times$

3. $R[x]$ ist integer

4. $R[x]$ ist E.R $\Leftrightarrow$ R ist Körper

5. $\mathrm{Quot}(R[x]) := R(x) := \left\{ \frac{p}{q} \;\middle/\; p, q \in R[x], q \neq 0 \right\}$

ist Körper.

Notation & Bem. $I \trianglelefteq R$

$$I[x] := \langle I \rangle \text{ in } R[x]$$
$$= \left\{ f(x) \in R[x] \;\middle/\; f(x) = \sum a_i x^i \text{ mit } a_i \in I \right\}.$$

Proposition 2. $R[x]/_{I[x]} \simeq \left(R/_I\right)[x]$.

Bew. $\varphi : R[x] \longrightarrow (R/I)[x]$
$\sum a_i x^i \mapsto \sum \bar{a}_i x^i$

ist Ringhom, surjektiv; $\ker\varphi = I[x]$. $\blacksquare$

Korollar. P Primideal in $R \Rightarrow$
$P[x]$ " " $R[x]$ $\blacksquare$

Exkurs. $R[x_1, .., x_n] := R[x_1, x_2, ..., x_{n-1}][x_n]$.
Also: Notation $:= \{ p(x_1, .., x_n) \mid p \in R[x_1, .., x_n] \}$.
Polynome in den Variablen $x_1, ..., x_n$ werden folgend definiert: es ist eine endliche Summe von monomen

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

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

- d_i ist der Grad von x_i in $m(\underline{x})$
- $|\underline{d}| := \sum_{i=1}^{n} d_i$ ist Grad von $m(\underline{x})$

$$\deg m(\underline{x}) := |\underline{d}|.$$

- $\deg p(x_1, .., x_n)$ ist der größte Grad von seinen monomen.

- die Summe aller Monomen von $p(x_1,\dots,x_n)$ vom Grad k heißt die <u>homogene Komponente von p vom grad k</u>.
- wenn $\deg p = d$ so läßt sich p eindeutig als Summe

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

Wobei p_k homogene komponente vom grad k ist für $0 \leq k \leq d$

(und $f_k = 0$ kann vorkommen). $\square$

<u>Lemma 1.</u> $R[x]$ Faktoriell $\Rightarrow$ R Faktoriell

<u>Bew.</u> (*) $(R[x])^\times = R^\times$

Sei $0 \neq r \in R \setminus R^\times$, r ist produkt vom irreduziblen in $R[x]$; und diese (deg. Bedingungen) müssen $\deg = 0$ haben; d. h sind Elemente aus R.

Beachte ferner daß: $r \in R$ irreduzible in $R[x]$

$\Rightarrow$ " " R

Sonst $r = ab$

$a, b \in R \setminus R^\times$ aber wegen (*) $r = ab$; $a, b \in R[x] \setminus (R[x])^\times$. ⚡ $\square$

Für die $\left\{\begin{array}{l}\text{Umkehrung} \\ \text{von Lemma 1}\end{array}\right\}$ brauchen wir ein Hilfslemma.

Lemma von Gauß.

Sei R faktoriell; $p(x) \in R[x]$.

Wenn $p(x)$ reduzible in $F[x]$ ist (wobei $F := \mathrm{Quot}(R)$) so ist $p(x)$ reduzible in $R[x]$.

D.h.: ist $p(x) = A(x)\, B(x)$; $A, B \in F[x]$, $\deg A \geq 1$, $\deg B \geq 1$

dann gibt es $0 \neq r$, $0 \neq s \in F$ mit

$$\left.\begin{array}{l} r\,A(x) := a(x) \\ s\,B(x) := b(x) \end{array}\right\} \in R[x] \quad ; \quad \begin{array}{l} \deg a(x) \geq 1 \\ \deg b(x) \geq 1 \end{array}$$

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

Bew.

$$\underset{R[x]}{\underset{\cap}{p(x)}} = \underset{F[x]}{\underset{\cap}{A(x)}}\ \underset{F[x]}{\underset{\cap}{B(x)}}$$

Die Koeff. 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 Nenner seine Koeff. und bekommen eine Gleichung der Form

$$(*) \quad \underset{R}{\overset{\cap}{d}}\, p(x) = \underset{R[x]}{\overset{\cap}{a'(x)}}\ \underset{R[x]}{\overset{\cap}{b'(x)}} \quad \left.\begin{array}{l} \text{mit } d \in R;\ d \neq 0 \\ \deg a'(x) \geq 1 \\ \deg b'(x) \geq 1 \\ a', b' \in R[x]. \end{array}\right.$$

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

1. Fall: $d \in R^\times$ ✓

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

So schreibe $d = p_1 \cdots p_m$ p_i irred. in R

- p_1 irred $\Rightarrow$ $I = \langle p_1 \rangle$ ist Primideal in R und $\boxed{d \in I.}$
(also auch $I[x] = p_1 R[x]$ " ").
- $\left(R/\langle p_1 \rangle\right)[x]$ ist integer

$\longrightarrow$ reduzieren mod $\langle p_1 \rangle$; wir bekommen

$$0 = \overline{a'(x)}\ \overline{b'(x)} \quad \text{in} \quad \left(R/_{\langle p_1 \rangle}\right)[x]$$

also ist ~~OE~~ $\overline{a'(x)} = 0$, d.h

alle Koeffizienten von $a'(x)$ liegen in $\langle p_1 \rangle$

also sind durch p_1 teilbar in R; so hat man

$$a''(x) := \frac{1}{p_1} a'(x) \quad \in R[x], \ \deg a''(x) \geq 1$$
$$\text{mit } \frac{1}{p_1} \in F$$

d.h wir können die Gleichung (*) um p_1 kürzen und bekommen eine neue Gleichung

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

aber nun hat d' ein irreduzibles 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

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

mit
$$a(x) = \alpha' a'(x) \qquad \alpha', \beta' \neq 0$$
$$b(x) = \beta' b'(x) \qquad \alpha', \beta' \in F$$

d.h
$$a(x) = \alpha\alpha' A(x)$$
$$b(x) = \beta\beta' B(x)$$
mit $\alpha\alpha' \in F$ und $\beta\beta' \in F$.

$\boxtimes$

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

Dann ist $p(x)$ in $R[x]$ irreduzible gdw $p(x)$ in $F[x]$

irreduzible. Insbesondere, ist $p(x) \in R[x]$ normiert und in $R[x]$ irreduzible, so ist $p(x)$ in $F[x]$ irreduzible.

<u>Beweis</u>: "$\Rightarrow$" GL ergibt: ist $p(x)$ in $F[x]$ reduzible, so ist $p(x)$ in $R[x]$ reduzible.

Umgekehrt ist $p(x)$ in $R[x]$ reduzible, dann ist

$$p(x) = a(x)\, b(x)$$

wobei $a(x), b(x) \in R[x] \setminus R$

(sonst wäre der ggT der Koeff. von $p(x)$ in R ungleich 1).

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

$\deg a(x) \geq 1$

$\deg b(x) \geq 1$.

insbesondere

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

$\deg a(x) \geq 1$

$\deg b(x) \geq 1$

d.h. $p(x)$ ist in $F[x]$ reduzible. ∎