7 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

Bisher haben wir zwei Hauptthemen untersucht: Wir haben einerseits diese Inklusionen Körper ⊆ Euklidische Bereiche ⊆ Hauptidealbereiche ⊆ Faktorielle Bereiche ⊆ Integritätsbereiche untersucht und andererseits haben wir Polynomringe über Integerringe untersucht. In diesem Skript werden wir diese zweite Untersuchung fortsetzen. Unser Ziel ist es, Satz 4.8 ähnlich für faktorielle Ringe zu zeigen.

§ 10 Polynomringe über faktorielle Ringe

Sei R stets integer.

Lemma 7.1.
$R[x]$ ist faktoriell $\Rightarrow R$ ist faktoriell.

Beweis:
Da R integer ist, wissen wir dass $\deg p(x)q(x) = \deg p(x) + \deg q(x)$ für alle $0 \neq p, q \in R[x]$ $(*)$ (und dass auch $R[x]$ integer ist; siehe Satz 4.8 und seinen Beweis). Aus $(*)$ folgt dass $(R[x])^\times = R^\times$ und $r \in R$ ist irreduzibel in $R[x]$ genau dann, wenn r irreduzibel in R ist. $(**)$ (ÜA).
Sei nun $0 \neq r \in R \setminus R^\times$, per Annahme ist r das Produkt vom Irreduziblen in $R[x]$ (und diese Darstellung ist eindeutig bis auf Reihenfolge und Assoziiertheit). Diese irreduzible Faktoren müssen wegen $(*)$ Grad 0 haben, d.h. die Faktoren sind Elemente aus R. Wegen $(**)$ sind diese Faktoren irreduzible auch in R. Wir haben eine Darstellung wie in Definition 6.4(1) (†) bekommen. Die Eindeutigkeit Bedingung in Definition 6.4(2) wird analog geprüft. □

Um die Umkehrung von Lemma 7.1 zu etablieren (siehe Skript 8) brauchen wir hier das Lemma von Gauß. Hierfür brauchen wir wiederum das Hilfslemma 7.2:

Lemma 7.2.
Sei $I \lhd R$. Dann gelten für das Ideal $< I > \lhd R[x]$:

1. $< I >= I[x] := \{f(x) \in R[x]\,;\ \ f(x) = \sum a_i x^i \text{ mit } a_i \in I\}$
2. $R[x]/I[x] \simeq (R/I)[x]$
3. I ist Primideal in $R \Rightarrow I[x]$ ist Primideal in $R[x]$.

Beweis:
Die 1. Aussage ist leicht zu prüfen. Betrachte nun $\begin{array}{rccc} \varphi: & R[x] & \to & (R/I)[x] \\ & \sum a_i x^i & \mapsto & \sum \overline{a_i} x^i \end{array}$

Es ist leicht zu prüfen dass φ ein Ringhomomorphismus ist; dass φ surjektiv ist; und dass $\ker \varphi = I[x]$. Die 2. und 3. folgen nun aus Isomorphiesatz sowie Proposition 3.5 und Satz 4.8. □

Lemma 7.3. (Lemma von Gauß)
Sei R faktoriell, $F := \text{Quot}(R)$ und $p(x) \in R[x]$. Wenn $p(x)$ reduzibel in $F[x]$ ist, so ist $p(x)$ reduzibel in $R[x]$. Genauer: Wenn

$$p(x) = A(x)B(x), A, B \in F[x], \deg A \geq 1, \deg B \geq 1\,,$$

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

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

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:

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

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

1. Fall: $d \in R^\times$ $\quad\checkmark$ (die Behauptung gilt in diesem Fall).

2. Fall: $d \in R \setminus R^\times$
So schreibe $d = p_1 \cdots p_n$, mit p_i irreduzibel in R für alle i.

- p_1 irreduzibel in $R \Rightarrow I :=< p_1 >$ ist Primideal in R und $d \in I$.
- $I[x] = p_1 R[x]$ Primideal in $R[x]$, $R[x]/I[x] \simeq (R/I)[x]$ und $(R/I)[x]$ ist integer (vgl. Lemma 7.2).

Wir reduzieren die Gleichung (*) mod I. Wir bekommen $0 = \overline{a'(x)b'(x)}$ in $(R/I)[x]$. Also ist ohne Einschränkung $\overline{a'(x)} = 0$, das heißt alle Koeffizienten von $a'(x)$ liegen in I 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 $p_2, \ldots, p_n$ (gleiche Argumente) ergibt eine Gleichung schließlich aus der Form

$$\begin{array}{lrcll} & p(x) & = & a(x)b(x) & a(x), b(x) \in R[x] \\ \text{mit} & a(x) & = & \alpha' a'(x) & \alpha', \beta' \neq 0 \\ & b(x) & = & \beta' b'(x) & \alpha', \beta' \in F \end{array}$$

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

Korollar 7.4.
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 $\{a_0, \ldots, a_n\} = 1$.
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 Koeffizient 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. □

Wie angekündigt werden wir im Skript 8 die Umkehrung von Lemma 7.1 zeigen; wir werden wir zeigen dass R faktoriell impliziert $R[x]$ faktoriell. Eigentlich werden wir das Resultat auch für $R[x_1, \ldots, x_n]$ erhalten. Wir beenden Skript 7 mit einem Exkurs. Hier führen wir diesen Ring ein, und fassen einige Begriffe zusammen.

Exkurs $R[x_1, \ldots, x_n] := R[x_1, x_2, \ldots, x_{n-1}][x_n]$.
Notation $= \{p(x_1, \ldots, x_n) | p \in R[x_1, \ldots, x_n]\}$.

Also: *Polynome* in den Variablen $x_1, \ldots, x_n$ werden folgendermaßen definiert:
Es ist eine endliche Sumem von *Monomen*.

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

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

- d_i ist der *Grad von* x_i in $m(\underline{x})$
- $|\underline{d}| := \sum_{i=1}^{n} d_i$ ist der *Grad von* $m(\underline{x})$ $\deg m(\underline{x}) := |\underline{d}|$
- $\deg p(x_1, \ldots, x_n)$ ist der größte Grad von seinen Monomen.
- Die Summe aller Monomen von $p(x_1, \ldots, x_n)$ 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).