Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 9

Faktorielle Ringe

In der letzten Vorlesung haben wir gesehen, dass in einem Hauptidealbereich einerseits jedes irreduzible Element prim ist und andererseits jedes Element ein Produkt von irreduziblen Elementen und damit auch von Primelementen ist. Wir werden gleich zeigen, dass unter diesen Voraussetzung die Zerlegung in Primelemente sogar im Wesentlichen eindeutig ist. Um dies prägnant fassen zu können, dient der Begriff des faktoriellen Bereiches.

Definition 9.1. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn jede Nichteinheit $f \neq 0$ sich als ein Produkt von Primelementen schreiben lässt.

Satz 9.2. *Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent.*

(1) *R ist faktoriell.*
(2) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und diese Zerlegung ist bis auf Umordnung und Assoziiertheit eindeutig.*
(3) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und jedes irreduzible Element ist ein Primelement.*

Beweis. (1) $\Rightarrow$ (2). Sei $f \neq 0$ eine Nichteinheit. Die Faktorisierung in Primelemente ist insbesondere eine Zerlegung in irreduzible Elemente, so dass also lediglich die Eindeutigkeit zu zeigen ist. Dies geschieht durch Induktion über die minimale Anzahl der Primelemente in einer Faktorzerlegung. Wenn es eine Darstellung $f = p$ mit einem Primelement gibt, und $f = q_1 \cdots q_r$ eine weitere Zerlegung in irreduzible Faktoren ist, so teilt p einen der Faktoren q_i und nach Kürzen durch p erhält man, dass das Produkt der übrigen Faktoren rechts eine Einheit sein muss. Das bedeutet aber, dass es keine weiteren Faktoren geben kann. Sei nun $f = p_1 \cdots p_s$ und diese Aussage sei für Elemente mit kleineren Faktorisierungen in Primelemente bereits bewiesen. Es sei

$$f = p_1 \cdots p_s = q_1 \cdots q_r$$

eine weitere Zerlegung mit irreduziblen Elementen. Dann teilt wieder p_1 einen der Faktoren rechts, sagen wir $p_1 u = q_1$. Dann muss u eine Einheit sein und wir können durch p_1 kürzen, wobei wir u^{-1} mit q_2 verarbeiten können, was ein zu q_2 assoziiertes Element ergibt. Das gekürzte Element $p_2 \cdots p_s$ hat eine

Faktorzerlegung mit $s-1$ Primelementen, so dass wir die Induktionsvoraussetzung anwenden können. (2) $\Rightarrow$ (3). Wir müssen zeigen, dass ein irreduzibles Element auch prim ist. Sei also q irreduzibel und es teile das Produkt fg, sagen wir

$$qh = fg.$$

Für h, f und g gibt es Faktorzerlegungen in irreduzible Elemente, so dass sich insgesamt die Gleichung

$$qh_1 \cdots h_r = f_1 \cdots f_s g_1 \cdots g_t$$

ergibt. Es liegen also zwei Zerlegungen in irreduzible Element vor, die nach Voraussetzung im Wesentlichen übereinstimmen müssen. D.h. insbesondere, dass es auf der rechten Seite einen Faktor gibt, sagen wir f_1, der assoziiert zu q ist. Dann teilt q auch den ursprünglichen Faktor f. (3) $\Rightarrow$ (1). Das ist trivial. □

Satz 9.3. *Ein Hauptidelabereich ist ein faktorieller Ring.*

Beweis. Dies folgt sofort aus Satz 8.8, Lemma 8.9 und Satz 9.2. □

Zerlegung in irreduzible Polynome

Wir möchten nun, abhängig von einem gewählten Grundkörper K, Aussagen über die irreduziblen Elemente in $K[X]$ und über die Primfaktorzerlegung von Polynomen treffen.

Korollar 9.4. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dann besitzt jedes Polynom $F \in K[X]$, $F \neq 0$, eine eindeutige Faktorzerlegung*

$$F = \lambda P_1^{r_1} \cdots P_k^{r_k},$$

wobei $\lambda \in K$ ist und die P_i verschiedene, normierte, irreduzible Polynome sind.

Beweis. Dies folgt aus Satz 8.3, aus Satz 9.2 und daraus, dass jedes Polynom $\neq 0$ zu einem normierten Polynom assoziiert ist. □

Die irreduziblen Elemente stimmen mit den Primelementen überein, man spricht meist von *irreduziblen Polynomen*.

Beispiel 9.5. Das Polynom X^6-1 besitzt in $\mathbb{Q}[X]$ die Primfaktorzerlegung

$$X^6 - 1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1),$$

die quadratischen Polynome sind nicht weiter zerlegbar, da sie in $\mathbb{Q}$ (ebenson in $\mathbb{R}$) keine Nullstelle besitzen.

Im Allgemeinen ist es schwierig, zu einem gegebenen Polynom die Primfaktorzerlegung zu finden.

Der Hauptsatz der elementaren Zahlentheorie

Wir beweisen nun, dass sich jede natürliche Zahl in eindeutiger Weise als Produkt von Primzahlen darstellen lässt.

Satz 9.6. *Jede natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$, besitzt eine eindeutige Zerlegung in Primfaktoren.*

D.h. es gibt eine Darstellung

$$n = p_1 \cdots p_r$$

mit Primzahlen p_i, und dabei sind die Primfaktoren bis auf ihre Reihenfolge eindeutig bestimmt.

Beweis. Dies folgt aus Satz 8.4 und aus Satz 9.2. □

Exponententest

Definition 9.7. Es sei R ein faktorieller Bereich und $p \in R$ ein Primelement. Dann heißt zu jedem $f \in R$, $f \neq 0$, die natürliche Zahl $n \in \mathbb{N}$ mit $p^n | f$ aber $p^{n+1} \nmid f$, der *Exponent* (oder die *Ordnung*) von f zu p. Er wird mit $\exp_p(f)$ bezeichnet.

Wenn von f die kanonische Primfaktorzerlegung

$$f = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$$

und p zu p_i assoziiert ist, so ist

$$\exp_p(f) = r_i.$$

Denn offenbar wird f von $p_i^{r_i}$ geteilt, aber nicht von $p_i^{r_i+1}$, da nach kürzen mit $p_i^{r_i}$ folgen würde, dass p_i einen der übrigen Faktoren $p_2, \ldots, p_k$ teilt. Insbeondere ist also der Exponent wohldefiniert.

Lemma 9.8. *Es sei R ein faktorieller Integritätsbereich und $p \in R$ ein Primelement. Dann besitzt der Exponent die Eigenschaft*

$$\exp_p(fg) = \exp_p(f) + \exp_p(g).$$

Beweis. Dies folgt aus Satz 9.2. □

Der Exponent übersetzt also die Multiplikation in die Addition.

Mit diesen Bezeichnungen kann man die Primfaktorzerlegung in einem faktoriellen Bereich als

$$f = u \prod_p p^{\nu_p(n)}$$

mit einer Einheit u schreiben, wobei das Produkt rechts endlich in dem Sinne ist, dass nur endlich viele Exponenten von 0 verschieden sind, und wobei für zueinander assoziierte Primelemente jeweils ein Vertreter genommen wird

(das Produkt erstreckt sich also beispielsweise über alle positiven Primzahlen oder über alle irreduziblen normierten Polynome). Die Teilbarkeit und einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches kann man aus den Exponenten ablesen.

LEMMA 9.9. *Es sei R ein faktorieller Integritätsbereich und $a, b \in R$. Dann ist a ein Teiler von b genau dann, wenn für die Exponenten zu jedem Primelement die Abschätzung*

$$\exp_p(a) \leq \exp_p(b)$$

gelten.

Beweis. (1) $\Rightarrow$ (2). Aus der Beziehung $b = ac$ folgt mit Lemma 9.8 direkt

$$\exp_p(b) = \exp_p(ac) = \exp_p(a) + \exp_p(c) \geq \exp_p(a).$$

(2) $\Rightarrow$ (1). Wir schreiben

$$a = u \prod_p p^{\exp_p(a)}$$

und

$$b = v \prod_p p^{\exp_p(b)}$$

mit Einheiten u, v. Wenn die Exponentenbedingung erfüllt ist, so ist $t = u^{-1}v \prod_p p^{\nu_p(b)-\nu_p(a)}$ ein Ringelement, das mit a multipliziert gerade b ergibt. □

KOROLLAR 9.10. *Es sei R ein faktorieller Bereich und $a_1, \ldots, a_n \in R$ Elemente mit Primfaktorzerlegungen*

$$a_i = u_i \prod_p p^{\exp_p(a_i)}.$$

Dann ist

$$\mathrm{kgV}(a_1, \ldots, a_n) = \prod_p p^{\max\left(\exp_p(a_1), \ldots, \exp_p(a_n)\right)}$$

und

$$\mathrm{ggT}(a_1, \ldots, a_n) = \prod_p p^{\min\left(\exp_p(a_1), \ldots, \exp_p(a_n)\right)}.$$

Beweis. Dies folgt direkt aus Lemma 9.9. □

Insbesondere kann man den größten gemeinsamen Teiler primelementweise bestimmen, indem man schaut, mit welcher Potenz p in a_1, a_2 etc. aufgeht.

In einem faktoriellen Bereich muss ein größter gemeinsamer Teiler nicht als Linearkombination der Elemente darstellbar sein. Beispielsweise ist $K[X, Y]$ faktoriell, aber kein Hauptidealbereich, die beiden Variablen X und Y sind prim und teilerfremd, erzeugen aber nicht das Einheitsideal.