Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 18

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 Ringes

Definition 18.1. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn jede Nichteinheit $f \neq 0$ sich als ein Produkt von Primelementen schreiben lässt.

Satz 18.2. *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 assoziiertes Element ergibt. Das gekürzte Element hat eine Faktorzerlegung mit $r-1$ 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 18.3. *Ein Hauptidelabereich ist ein faktorieller Ring.*

Beweis. Dies folgt sofort aus Satz 17.15, Lemma 17.16 und Satz 18.2. □

Korollar 18.4. *Sei R ein faktorieller Ring und seien a und b zwei Elemente $\neq 0$ mit Primfaktorzerlegungen*

$$a = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k} \text{ und } b = v \cdot p_1^{s_1} \cdot p_2^{s_2} \cdots p_k^{s_k}$$

(wobei die u, v Einheiten sind und die Exponenten auch null sein können). Dann gilt $a|b$ genau dann, wenn $r_i \leq s_i$ ist für alle Exponenten $i = 1, \ldots, k$.

Beweis. Wenn die Exponentenbedingung erfüllt ist, so ist $s_i - r_i \geq 0$ und man kann schreiben

$$b = vu^{-1} p_1^{s_1 - r_1} \cdots p_k^{s_k - r_k}\,,$$

was die Teilbarkeit bedeutet. Die Umkehrung folgt aus der Eindeutigkeit der Primfaktorzerlegung in einem faktoriellen Ring. □

Restklassenringe von Hauptidealbereichen

Satz 18.5. *Sei R ein Hauptidealbereich und $p \neq 0$ ein Element. Dann sind folgende Bedingungen äquivalent.*

(1) *p ist ein Primelement.*
(2) *$R/(p)$ ist ein Integritätsbereich.*
(3) *$R/(p)$ ist ein Körper.*

Beweis. Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt in jedem kommutativen Ring (auch für $p = 0$), und (3) impliziert natürlich (2). Sei also (1) erfüllt und sei $a \in R/(p)$ von null verschieden. Wir bezeichnen einen Repräsentanten davon in R ebenfalls mit a. Es ist dann $a \notin (p)$ und es ergibt sich eine echte Idealinklusion $(p) \subset (a, p)$. Ferner können wir $(a, p) = (b)$ schreiben , da wir in einem Hauptidealring sind. Es folgt $p = cb$. Da c keine Einheit ist und p prim (also irreduzibel) ist, muss b eine Einheit sein. Es ist also $(a, p) = (1)$, und das

bedeutet modulo p, also in $R/(p)$, dass a eine Einheit ist. Also ist $R/(p)$ ein Körper. □

Für die Restklassenringe von Hauptidealbereichen gilt wieder der chinesische Restsatz (für beliebige faktorielle Bereiche gilt er nicht, da das Lemma von Bezout dafür im Allgemeinen nicht gilt).

Satz 18.6. *(Chinesischer Restsatz)*

Es sei R ein Hauptidealbereich und $f \in R$, $f \neq 0$, ein Element mit kanonischer Primfaktorzerlegung

$$f = p_1^{r_1} \cdots p_k^{r_k} .$$

Dann gilt für den Restklassenring $R/(f)$ die kanonische Isomorphie

$$R/(f) \cong R/(p_1^{r_1}) \times \cdots \times R/(p_k^{r_k})$$

Beweis. Wegen $p_i^{r_i} | f$ gelten die Idealinklusionen $(f) \subseteq (p_i^{r_i})$ und daher gibt es kanonische Ringhomomorphismen

$$R/(f) \longrightarrow R/(p_i^{r_i}).$$

Diese setzen sich zu einem Ringhomomorphismus in den Produktring zusammen, nämlich

$$R/(f) \longrightarrow R/(p_1^{r_1}) \times \cdots \times R/(p_k^{r_k}),\ a \longmapsto (a \mod p_1^{r_1}, \ldots, a \mod p_1^{r_1}).$$

Wir müssen zeigen, dass dieser bijektiv ist. Zur Injektivität sei $a \in R$ derart, dass es in jeder Komponente auf null abgebildet wird. Das bedeutet $a \in (p_i^{r_i})$ für alle i. D.h. a ist ein Vielfaches dieser $p_i^{r_i}$ und aufgrund der Primfaktorzerlegung folgt, dass a ein Vielfaches von f sein muss. Also ist $\overline{a} = 0$ in $R/(f)$. Zur Surjektivität genügt es zu zeigen, dass alle Elemente, die in einer Komponente den Wert 1 und in allen anderen Komponenten den Wert 0 haben, im Bild liegen. Sei also $(1, 0, \ldots, 0)$ vorgegeben. Wegen der Eindeutigkeit der Primfaktorzerlegung sind $p_1^{r_1}$ und $p_2^{r_2} \cdots p_k^{r_k}$ teilerfremd. Daher gibt es nach Satz 17.12 eine Darstellung der Eins, sagen wir

$$s p_1^{r_1} + t p_2^{r_2} \cdots p_k^{r_k} = 1 .$$

Betrachten wir $t p_2^{r_2} \cdots p_k^{r_k} = 1 - s p_1^{r_1} \in R$. Das wird unter der Restklassenabbildung in der ersten Komponente auf 1 und in den übrigen Komponenten auf 0 abgebildet, wie gewünscht. □

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 18.7. *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 16.11, aus Satz 18.3 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*. Diese Eigenschaft hängt wesentlich vom gewählten Körper ab, und nicht für jeden Körper lassen sich die irreduziblen Polynome übersichtlich beschreiben. Bei Irreduzibilitätsfragen kann man stets mit Einheiten multiplizieren, daher muss man nur normierte Polynome untersuchen.

Als echte Faktoren für ein Polynom kommen nur Polynome von kleinerem Grad in Frage. Insbesondere sind daher *lineare Polynome*, also Polynome von Typ $aX + b$, $a \neq 0$, stets irreduzibel. Ob ein lineares Polynom ein Faktor eines anderen Polynoms (und damit ein Primfaktor davon) ist, hängt direkt mit den Nullstellen des Polynoms zusammen.

Nullstellen von Polynomen

Lemma 18.8. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom und $a \in K$. Dann ist a genau dann eine Nullstelle von P, wenn P ein Vielfaches des linearen Polynoms $X - a$ ist.*

Beweis. Wenn P ein Vielfaches von $X - a$ ist, so kann man

$$P = (X - a)Q$$

mit einem weiteren Polynom Q schreiben. Einsetzen ergibt

$$P(a) = (a - a)Q(a) = 0 .$$

Im Allgemeinen gibt es aufgrund der Division mit Rest eine Darstellung

$$P = (X - a)Q + R ,$$

wobei $R = 0$ oder aber den Grad null besitzt, also eine Konstante ist. Einsetzen ergibt

$$P(a) = R .$$

Wenn also $P(a) = 0$ ist, so muss der Rest $R = 0$ sein, und das bedeutet, dass $P = (X - a)Q$ ist. Also ist $X - a$ ein Linearfaktor von P. □

Korollar 18.9. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dann ist ein Polynom vom Grad zwei oder drei genau dann irreduzibel, wenn es keine Nullstelle in K besitzt.*

Beweis. In einer echten Primfaktorzerlegung von P, $\operatorname{grad}(P) \leq 3$, muss ein Polynom vom Grad eins vorkommen, also ein lineares Polynom. Ein lineares Polynom $X - a$ teilt aber nach Lemma 18.8 das Polynom P genau dann, wenn $P(a) = 0$ ist. □

Korollar 18.10. *Es sei K ein Körper und $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom (ungleich null) vom Grad d. Dann besitzt P maximal d Nullstellen.*

Beweis. Wir beweisen die Aussage durch Induktion über d. Für $d = 0, 1$ ist die Aussage offensichtlich richtig. Sei also $d \geq 2$ und die Aussage sei für kleinere Grade bereits bewiesen. Sei a eine Nullstelle von P. Dann ist $P = Q(X - a)$ nach Lemma 18.8 und Q hat den Grad $d - 1$, so dass wir auf Q die Induktionsvoraussetzung anwenden können. Das Polynom Q hat also maximal $d - 1$ Nullstellen. Für $b \in K$ gilt $P(b) = Q(b)(b - a)$. Dies kann nur dann null sein, wenn einer der Faktoren null ist, so dass eine Nullstelle von P gleich a ist oder aber eine Nullstelle von Q ist. Es gibt also maximal d Nullstellen von P. □

Beispiel 18.11. Die Irreduzibilität eines Polynoms hängt wesentlich vom Grundkörper ab. Zum Beispiel ist das reelle Polynom $X^2 + 1 \in \mathbb{R}[X]$ irreduzibel, dagegen zerfällt es als Polynom in $\mathbb{C}[X]$ als

$$X^2 + 1 = (X + i)(X - i)\,.$$

Ebenso ist das Polynom $X^2 - 5 \in \mathbb{Q}[X]$ irreduzibel, aber über $\mathbb{R}$ hat es die Zerlegung

$$X^2 - 5 = (X - \sqrt{5})(X + \sqrt{5})\,.$$

Übrigens kann die Zerlegung über einem größeren Körper manchmal dazu benutzt werden um zu zeigen, dass ein Polynom über dem gegebenen Körper irreduzibel ist.