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

Elemente der Algebra

Vorlesung 15

In dieser Vorlesung wollen wir die Restklassenringe von Hauptidealbereichen verstehen.

Restklassenringe von Hauptidealbereichen

SATZ 15.1. *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 0 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. □

SATZ 15.2. *Es sei $n \geq 1$ eine natürliche Zahl und $\mathbb{Z}/(n)$ der zugehörige Restklassenring. Dann sind folgende Aussagen äquivalent.*

(1) *$\mathbb{Z}/(n)$ ist ein Körper.*
(2) *$\mathbb{Z}/(n)$ ist ein Integritätsbereich.*
(3) *n ist eine Primzahl.*

Beweis. Dies ist ein Spezialfall von Satz 15.1. □

Wenn also p eine Primzahl ist, so ist der Restklassenring $\mathbb{Z}/(p)$ ein Körper mit p Elementen, den man auch den *Restklassenkörper* nennt. Die Einheitengruppe

$$\mathbb{Z}/(p)^\times = \{1, \ldots, p-1\}$$

ist eine Gruppe mit $p-1$ Elementen (bezüglich der Multiplikation). Bei $p = 5$ hat man beispielsweise

$$\overline{2}^{\,0} = \overline{1}\,,\ \overline{2}^{\,1} = \overline{2}\,,\ \overline{2}^{\,2} = \overline{4} = \overline{-1}\,,\ \overline{2}^{\,3} = \overline{8} = \overline{3}\,,$$

d.h. die Potenzen von $\overline{2}$ durchlaufen sämtliche vier Elemente dieser Gruppe, die sich damit als zyklisch erweist. Es gilt generell, ws wir aber nicht beweisen werden, dass für jede Primzahl p die Einheitengruppe des Restklassenkörpers $\mathbb{Z}/(p)$ zyklisch ist! Diese Gruppen nennt man auch die *primen Restklassengruppen*.

Pierre de Fermat (1607/08-1665)

Die folgende Aussage heißt *kleiner Fermat*.

SATZ 15.3. *Für eine Primzahl p und eine beliebige ganze Zahl a gilt*

$$a^p \equiv a \mod p\,.$$

Anders ausgedrückt: $a^p - a$ ist durch p teilbar.

Beweis. Ist a nicht durch p teilbar, so definiert a ein Element $\bar{a}$ in der Einheitengruppe $(\mathbb{Z}/p)^\times$; diese Gruppe hat die Ordnung $p-1$, und nach dem Satz von Lagrange gilt $\bar{a}^{p-1} = 1$. Durch Multiplikation mit a ergibt sich die Behauptung. Für Vielfache von p gilt die Aussage ebenso, da dann beidseitig null steht. □

Für $p = 5$ gilt beispielsweise in $\mathbb{Z}/(5)$

$$1^p = 1,\ 2^5 = 32 = 2,\ 3^5 = 243 = 3,\ 4^5 = 1024 = 4\,,$$

Für Zahlen, die keine Primzahlen sind, gilt die entsprechende Aussage nicht. So ist etwa in $\mathbb{Z}/(5)$

$$3^4 = 81 = 1 \neq 3.$$

Produktringe

Um die Restklassenringe von $\mathbb{Z}$ besser verstehen zu können, insbesondere dann, wenn man n als Produkt von kleineren Zahlen schreiben kann - z.B., wenn die Primfaktorzerlegung bekannt ist - braucht man den Begriff des Produktringes.

DEFINITION 15.4. Seien $R_1, \ldots, R_n$ kommutative Ringe. Dann heißt das Produkt

$$R_1 \times \cdots \times R_n \,,$$

versehen mit komponentenweiser Addition und Multiplikation, der *Produktring* der R_i, $i = 1, \ldots, n$.

Eng verwandt mit dem Begriff des Produktringes ist das Konzept der idempotenten Elemente.

DEFINITION 15.5. Ein Element e eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Die Elemente 0 und 1 sind trivialerweise idempotent, man nennt sie die trivialen idempotenten Elemente. In einem Produktring sind auch diejenigen Elemente, die in allen Komponenten nur den Wert 0 oder 1 besitzen, idempotent, also beispielsweise $(1, 0)$. In einem Integritätsbereich gibt es nur die beiden trivialen idempotenten Elemente: Ein idempotentes Element e besitzt die Eigenschaft

$$e(1 - e) \;=\; e - e^2 \;=\; e - e \;=\; 0.$$

Im nullteilerfreien Fall folgt daraus $e = 1$ oder $e = 0$.

LEMMA 15.6. *Es sei $R = R_1 \times \cdots \times R_n$ ein Produkt aus kommutativen Ringen. Dann gilt für die Einheitengruppe von R die Beziehung*

$$R^\times = R_1^\times \times \cdots \times R_n^\times$$

Beweis. Dies ist klar, da ein Element genau dann eine Einheit ist, wenn es in jeder Komponente eine Einheit ist. □

Der chinesische Restsatz

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

SATZ 15.7. *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

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

Wir müssen zeigen, dass dieser bijektiv ist. Zur Injektivität sei $a \in R$ derart, dass es in jeder Komponente auf 0 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 dem Lemma von Bezout eine Darstellung der Eins, sagen wir

$$sp_1^{r_1} + tp_2^{r_2} + \cdots + p_k^{r_k} = 1.$$

Betrachten wir $tp_2^{r_2} \cdots p_k^{r_k} = 1 - sp_1^{r_1} \in R$. Das wird unter der Restklassenabbildung in der ersten Komponente auf 1 und in den übrigen Komponenten auf 0 abgebildet, wie gewünscht. □

Abbildungsverzeichnis