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

Einführung in die Algebra

Vorlesung 14

Restklassenbildung

Nach Satz 13.6 ist der Kern eines Ringhomomorphismus ein Ideal. Man kann umgekehrt zu jedem Ideal $I \subseteq R$ in einem (kommutativen) Ring einen Ring R/I konstruieren, und zwar zusammen mit einem surjektiven Ringhomomorphismus

$$R \longrightarrow R/I,$$

dessen Kern gerade das vorgegebene Ideal I ist. Ideale und Kerne von Ringhomomorphismen sind also im Wesentlichen äquivalente Objekte, so wie das bei Gruppen für Kerne von Gruppenhomomorphismen und Normalteilern gilt. In der Tat gelten die entsprechenden Homomorphiesätze hier wieder, und können weitgehend auf die Gruppensituation zurückgeführt werden. Wir werden uns bei den Beweisen also kurz fassen können.

Definition 14.1. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Zu $a \in R$ heißt die Teilmenge

$$a + I = \{a + f | \, f \in I\}$$

die *Nebenklasse von* a zum Ideal I. Jede Teilmenge von dieser Form heißt *Nebenklasse* zu I.

Diese Nebenklassen sind gerade die Nebenklassen zur Untergruppe $I \subseteq R$, die wegen der Kommutativität ein Normalteiler ist. Zwei Elemente $a, b \in R$ definieren genau dann die gleiche Nebenklasse, also $a + I = b + I$, wenn ihre Differenz $a - b$ zum Ideal gehört. Man sagt dann auch, dass a und b dieselbe Nebenklasse *repräsentieren*.

Definition 14.2. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Dann ist der *Restklassenring* R/I (sprich „R modulo I“) ein kommutativer Ring, der durch folgende Daten festgelegt ist.

(1) Als Menge ist R/I die Menge der Nebenklassen zu I.
(2) Durch
$$(a + I) + (b + I) := (a + b + I)$$
wird eine Addition von Nebenklassen definiert.
(3) Durch
$$(a + I) \cdot (b + I) := (a \cdot b + I)$$
wird eine Multiplikation von Nebenklassen definiert.
(4) $\bar{0} = 0 + I = I$ definiert das neutrale Element für die Addition (die Nullklasse).

(5) $\bar{1} = 1 + I$ definiert das neutrale Element für die Multiplikation (die Einsklasse).

Man muss dabei zeigen, dass diese Abbildungen (also Addition und Multiplikation) wohldefiniert sind, d.h. unabhängig vom Repräsentanten, und dass die Ringaxiome erfüllt sind. Da I insbesondere eine Untergruppe der kommutativen Gruppe $(R, +, 0)$ ist, liegt ein Normalteiler vor, so dass R/I eine Gruppe ist und die Restklassenabbildung

$$R \longrightarrow R/I,\ a \longmapsto a + I =: \bar{a},$$

ein Gruppenhomomorphismus ist. Das einzig Neue gegenüber der Gruppensituation ist also die Anwesenheit einer Multiplikation. Die Wohldefiniertheit der Multiplikation ergibt sich so: Seien zwei Restklassen gegeben mit unterschiedlichen Repräsentanten, also $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$. Dann ist $a - a' \in I$ und $b - b' \in I$ bzw. $a' = a + x$ und $b' = b + y$ mit $x, y \in I$. Daraus ergibt sich

$$a'b' = (a + x)(b + y) = ab + ay + xb + xy.$$

Die drei hinteren Summanden gehören zum Ideal, so dass die Differenz $a'b' - ab \in I$ ist.

Aus der Wohldefiniertheit folgen die anderen Eigenschaften und insbesondere, dass ein Ringhomomorphismus in den Restklassenring vorliegt. Diesen nennt man wieder die *Restklassenabbildung* oder den *Restklassenhomomorphismus*. Das Bild von $a \in R$ in R/I wird häufig mit $[a]$, $\bar{a}$ oder einfach mit a selbst bezeichnet und heißt die *Restklasse* von a. Bei dieser Abbildung gehen genau die Elemente aus dem Ideal auf null, d.h. der Kern dieser Restklassenabbildung ist das vorgegebene Ideal.

Das einfachste Beispiel für diesen Prozess ist die Abbildung, die einer ganzen Zahl a den Rest bei Division durch eine fixierte Zahl n zuordnet. Jeder Rest wird dann repräsentiert durch eine der Zahlen $0, 1, 2, \ldots, n-1$. Im Allgemeinen gibt es nicht immer ein solch übersichtliches Repräsentantensystem.

Die Homomorphiesätze für Ringe

Für Ringe, ihre Ideale und Ringhomomorphismen gelten die analogen Homomorphiesätze wie für Gruppen, ihre Normalteiler und Gruppenhomomorphismen, siehe die achte Vorlesung. Wir beschränken uns auf kommutative Ringe.

Satz 14.3. *Seien R, S und T kommutative Ringe, es sei $\varphi : R \to S$ ein Ringhomomorphismus und $\psi : R \to T$ ein surjektiver Ringhomomorphismus. Es sei vorausgesetzt, dass*

$$\operatorname{kern} \psi \subseteq \operatorname{kern} \varphi$$

ist. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi} : T \longrightarrow S$$

derart, dass $\varphi = \tilde{\varphi} \circ \psi$ ist. Mit anderen Worten: das Diagramm

$$\begin{array}{ccc} R & \longrightarrow & T \\ & \searrow & \downarrow \\ & & S \end{array}$$

ist kommutativ.

Beweis. Aufgrund von Satz 8.1 gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi} : T \longrightarrow S,$$

der die Eigenschaften erfüllt. Es ist also lediglich noch zu zeigen, dass $\tilde{\varphi}$ auch die Multiplikation respektiert. Seien dazu $t, t' \in T$, und diese seien repräsentiert durch r bzw. r' aus R. Dann wird tt' durch rr' repräsentiert und daher ist

$$\tilde{\varphi}(tt') = \psi(rr') = \psi(r)\psi(r') = \tilde{\varphi}(t)\tilde{\varphi}(t').$$

□

Die im vorstehenden Satz konstruierte Abbildung heißt wieder *induzierte Abbildung* oder *induzierter Homomorphismus* und entsprechend heißt der Satz auch *Satz vom induzierten Homomorphismus.*

Korollar 14.4. *Es seien R und S kommutative Ringe und es sei*

$$\varphi : R \longrightarrow S$$

ein surjektiver Ringhomomorphismus. Dann gibt es eine kanonische Isomorphie von Ringen

$$\tilde{\varphi} : R/\operatorname{kern} \varphi \longrightarrow S.$$

Beweis. Aufgrund von Korollar 8.2 liegt ein natürlicher Gruppenisomorphismus vor, der wegen Satz 14.3 auch die Multiplikation respektiert, also ein Ringhomomorphismus ist. □

Satz 14.5. *Es seien R und S kommutative Ringe und es sei*

$$\varphi : R \longrightarrow S$$

ein Ringhomomorphismus. Dann gibt es eine kanonische Faktorisierung

$$R \xrightarrow{q} R/\operatorname{kern} \varphi \xrightarrow{\theta} \operatorname{bild} \varphi \xhookrightarrow{\iota} S\,,$$

wobei q die kanonische Projektion, θ ein Ringisomorphismus und ι die kanonische Inklusion des Bildes ist.

Beweis. Dies beruht auf Korollar 8.2 und Satz 14.3. □

Es gilt also wieder:

Bild = Urbild modulo Kern.

Satz 14.6. *Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R mit dem Restklassenring $S = R/I$. Es sei J ein weiteres Ideal in R, das I umfasst. Dann ist das Bild $\overline{J}$ von J in S ein Ideal und es gilt die kanonische Isomorphie*

$$R/J \cong S/\overline{J}\,.$$

Beweis. Auch dies ergibt sich aus der Gruppensituation und Satz 14.3. □

Lemma 14.7. *Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R.*

Dann ist ein Element $a \in R$ genau dann eine Einheit modulo I, wenn a und I zusammen das Einheitsideal in R erzeugen.

Beweis. Es sei $\overline{a}$ eine Einheit im Restklassenring R/I. Dies ist genau dann der Fall, wenn es ein $r \in R$ gibt mit

$$\overline{a}\,\overline{r} = \overline{1}\ .$$

Dies bedeutet zurückübersetzt nach R, dass

$$ar - 1 \in I$$

ist, was wiederum äquivalent dazu ist, dass I und (a) zusammen das Einheitsideal erzeugen. □

$\mathbb{Z}$ ist ein Hauptidealbereich

Wir wollen nun die Restklassenringe der ganzen Zahlen verstehen. Bei den ganzen Zahlen muss man nicht zwischen Untergruppen und Idealen unterscheiden, da jede Untergruppe von $\mathbb{Z}$ die Gestalt $n\mathbb{Z}$ mit $n \geq 0$ besitzt und daher ein (Haupt-)Ideal ist. Insbesondere hat überhaupt jedes Ideal in $\mathbb{Z}$ diese einfache Gestalt. Dass jede Untergruppe von $\mathbb{Z}$ eine besonders einfache Gestalt hat ist eine Besonderheit der ganzen Zahlen, dagegen ist die Eigenschaft, dass jedes Ideal ein Hauptideal ist, weiter verbreitet und verdient einen eigenen Namen.

Definition 14.8. Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealbereich*.

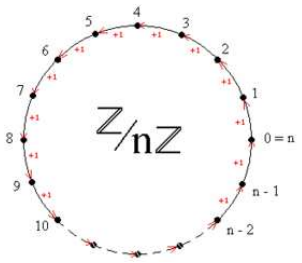
Ein kommutativer Ring, in dem jedes Ideal ein Hauptideal ist, der aber kein Integritätsbereich sein muss, heißt *Hauptidealring*.

Wir halten fest.

Satz 14.9. *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Hauptidealbereich.*

Beweis. Zunächst ist $\mathbb{Z}$ ein Integritätsbereich. Es sei $I \subseteq \mathbb{Z}$ ein Ideal. Damit ist I insbesondere eine (additive) Untergruppe von $\mathbb{Z}$ und hat nach Satz 3.2 die Gestalt $I = \mathbb{Z}d$. Damit handelt es sich um ein Hauptideal. □

Die Restklassenringe von $\mathbb{Z}$



Die Restklassengruppen $\mathbb{Z}/(n)$ haben wir bereits kennengelernt, es handelt sich um zyklische Gruppen der Ordnung n. Diese Gruppen bekommen jetzt aber noch zusätzlich eine Ringstruktur.

KOROLLAR 14.10. *Sei $n \geq 0$ eine natürliche Zahl. Dann gibt es eine eindeutig bestimmte Ringstruktur auf $\mathbb{Z}/(n)$ derart, dass die Restklassenabbildung*

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n),\, a \longmapsto \overline{a}\,,$$

ein Ringhomomorphismus ist. $\mathbb{Z}/(n)$ ist ein kommutativer Ring mit n Elementen (bei $n \geq 1$).

Beweis. Dies ist ein Spezialfall von Definition 14.2 und den sich daran anschließenden Überlegungen. □

Die Charakteristik von $\mathbb{Z}/(n)$ ist n. Dies zeigt insbesondere, dass es zu jeder Zahl n Ringe gibt mit dieser Charakteristik. Zu einem beliebigen Ring R der Charakteristik n faktorisiert der charakteristische Ringhomomorphismus $\mathbb{Z} \to R$ durch

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n) \longrightarrow R\,,$$

wobei die hintere Abbildung injektiv ist. Der Ring $\mathbb{Z}/(n)$, $n = \operatorname{char}(R)$, ist der kleinste Unterring von R, und wird der *Primring* von R genannt.

KOROLLAR 14.11. *Seien n und k positive natürliche Zahlen, und k teile n. Dann gibt es einen kanonischen Ringhomomorphismus*

$$\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k),\, (a \mod n) \longmapsto (a \mod k).$$

Beweis. Wir betrachten die Ringhomomorphismen

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/(k) \\ \phi\downarrow & & \\ \mathbb{Z}/(n) & & \end{array}$$

Aufgrund der Teilerbeziehung haben wir die Beziehung

$$\operatorname{kern}\, \phi = (n) \subseteq (k) = \operatorname{kern}\, \varphi\,.$$

Aufgrund des Homomorphisatzes hat man daher eine kanonische Abbildung von links unten nach rechts oben. □

Vor dem nächsten Satz erinnern wir der Vollständigkeit halber an die Definition einer Primzahl.

DEFINITION 14.12. Eine natürliche Zahl $n \geq 2$ heißt eine *Primzahl*, wenn die einzigen natürlichen Teiler von ihr 1 und n sind.

Wir werden uns bald mit ähnlichen Begriffen in einem allgemeineren Kontext auseinandersetzen.

SATZ 14.13. *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. (1) $\Rightarrow$ (2). Da jede Einheit ein Nichtnullteiler ist, ist jeder Körper insbesondere ein Integritätsbereich. (2) $\Rightarrow$ (3). Es ist $n = \operatorname{char}(\mathbb{Z}/(n))$ und dies ist im integren Fall eine Primzahl, wie in Lemma 13.9 gezeigt wurde. (3) $\Rightarrow$ (1). Sei also $n = p$ eine Primzahl und $\overline{a} \in \mathbb{Z}/(p)$ eine von null verschiedene Restklasse. Diese wird durch eine ganze Zahl a zwischen 1 und $p-1$ repräsentiert. Da p prim ist, ist $a = 1$ oder aber kein Teiler von p. In jedem Fall sind a und p teilerfremd und nach Satz 4.1 gibt es eine Darstellung der 1. D.h. es gibt ganze Zahlen $r, s \in \mathbb{Z}$ mit

$$ra + sp = 1\,.$$

Diese Gleichung gilt auch, wenn man die Restklassenbildung modulo p darauf los lässt. Es gilt also

$$\overline{r}\,\overline{a} + \overline{s}\,\overline{p} = \overline{1}$$

in $\mathbb{Z}/(p)$. Dort ist aber $\overline{p} = \overline{0} = 0$, so dass man den zweiten Summanden ignorieren kann und lediglich

$$\overline{r}\,\overline{a} = \overline{1} = 1$$

übrig bleibt. Diese Gleichung zeigt, dass $\overline{a}$ eine Einheit ist (mit $\overline{r}$ als Inversem). □

Die vorstehende Aussage folgt auch aus Lemma 14.7. 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 (bzgl. der Multiplikation). Bei $p = 5$ hat man bspw.

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

d.h. die Potenzen von $\overline{2}$ durchlaufen sämtliche vier Elemente dieser Gruppe, die sich damit als zyklisch erweist. Wir werden in ein paar Wochen zeigen,

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)

SATZ 14.14. *(Kleiner Fermat)*

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 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. □

Abbildungsverzeichnis