

Elemente der Algebra

Vorlesung 14

Restklassenringe

Nach Satz 13.10 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

$$a + I = \{a + f \mid f \in I\}$$

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 $\bar{a} = \bar{a}'$ und $\bar{b} = \bar{b}'$. 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

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

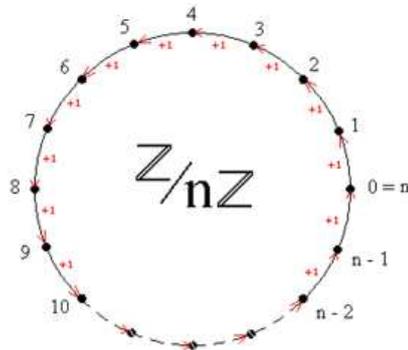
Die drei hinteren Summanden gehören zum Ideal, so dass die Differenz $a'b' - ab \in I$ ist.

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 0, 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 d zuordnet. Jeder Rest wird dann repräsentiert durch eine der Zahlen $0, 1, 2, \dots, d-1$. Im Allgemeinen gibt es nicht immer ein solch übersichtliches Repräsentantensystem.

Die Restklassenringe von \mathbb{Z}

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



KOROLLAR 14.3. Sei $d \geq 0$ eine natürliche Zahl. Dann gibt es eine eindeutig bestimmte Ringstruktur auf $\mathbb{Z}/(d)$ derart, dass die Restklassenabbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(d), a \longmapsto \bar{a},$$

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

Beweis. Dies ist ein Spezialfall der obigen Überlegungen. □

Die Restklassenringe $S = K[X]/(P)$ sind ebenfalls gut überschaubar. Wenn P den Grad d besitzt, so wird jede Restklasse in S durch ein eindeutiges Polynom von einem Grad $< d$ repräsentiert. Dieses ist der Rest, den man erhält, wenn man durch P durchdividiert.

Die Homomorphiesätze für Ringe

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

SATZ 14.4. Seien R, S und T kommutative Ringe, es sei $\varphi: R \rightarrow S$ ein Ringhomomorphismus und $\psi: R \rightarrow T$ ein surjektiver Ringhomomorphismus. Es sei vorausgesetzt, dass

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

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 12.5 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

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

□

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

KOROLLAR 14.5. *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

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

Beweis. Aufgrund von Korollar 12.6 liegt ein natürlicher Gruppenisomorphismus vor, der wegen Satz 14.4 auch die Multiplikation respektiert, also ein Ringhomomorphismus ist. □

SATZ 14.6. *Es seien R und S kommutative Ringe und es sei*

$$\varphi: R \longrightarrow S$$

ein Ringhomomorphismus. Dann gibt es eine kanonische Faktorisierung

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

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

Beweis. Dies beruht auf Satz 12.7 und Satz 14.4. □

Es gilt also wieder:

$$\text{Bild} = \text{Urbild modulo Kern}.$$

SATZ 14.7. *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 \bar{J} von J in S ein Ideal und es gilt die kanonische Isomorphie*

$$R/J \cong S/\bar{J}.$$

Beweis. Auch dies ergibt sich aus der Gruppensituation und Satz 14.4. □

Anwendung auf $\mathbb{Z}/(d)$

Die Charakteristik von $\mathbb{Z}/(d)$ ist d . Dies zeigt insbesondere, dass es zu jeder Zahl n Ringe gibt mit dieser Charakteristik. Zu einem beliebigen Ring R der Charakteristik d faktorisiert der charakteristische Ringhomomorphismus $\mathbb{Z} \rightarrow R$ nach Satz 14.6 durch Ringhomomorphismen

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

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

KOROLLAR 14.8. *Seien n und k positive natürliche Zahlen, und k teile n . Dann gibt es einen kanonischen Ringhomomorphismus*

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

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

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

Aufgrund des Homomorphiesatzes hat man daher einen kanonischen Ringhomomorphismus von links unten nach rechts oben. \square

Einheiten im Restklassenring

LEMMA 14.9. *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 \bar{a} eine Einheit im Restklassenring R/I . Dies ist genau dann der Fall, wenn es ein $r \in R$ gibt mit

$$\bar{a}\bar{r} = \bar{1}.$$

Dies bedeutet zurückübersetzt nach R , dass

$$ar - 1 \in I$$

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

Abbildungsverzeichnis

Quelle = Anillo cíclico.png , Autor = Romero Schmidtke (= Benutzer FrancoGG auf es.wikipedia.org), Lizenz = CC-BY-SA-3.0 3