Ringe und Körper

Lineare Algebra individuell
Online-Fassung, Ver. 0.41
— — *internes Material* — —

W. Pohl, D.Popescu, R. Laza
28.4.2004

Das Homomorphieprinzip für Ringe

1/2/29

Wir beginnen mit einem Beispiel. $R = \mathbb{Z}/m\mathbb{Z}$ sei die Faktorgruppe von $\mathbb{Z}$ nach der Untergruppe $m\mathbb{Z}$, $m \in \mathbb{N}$. Für $m = 0$ ist der kanonische Homomorphismus $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ bijektiv, d.h. die Faktorgruppe R besitzt bereits eine Ringstruktur. Nun sei m beliebig. Wir definieren auf R eine Multiplikation durch

$$(*) \qquad \overline{a}\cdot\overline{b} := \overline{a\cdot b} \quad \text{für } a, b \in \mathbb{Z},$$

wobei $\overline{x} := x + m\mathbb{Z}$ die Klasse des Elements x bezeichnet.

Dieses Beispiel wird zur nachfolgenden Konstruktion einiger endlicher Körper verwendet.

Die Vereinbarung $(*)$ ist nicht a priori sinnvoll, denn wir haben zur Definition des Produkts Repräsentanten der Klassen $\overline{a}$, $\overline{b}$ verwendet.
Es sei also $\overline{a} = \overline{a_1}$ und $\overline{b} = \overline{b_1}$. Dann ist $a = a_1 + q\cdot m$, $b = b_1 + r\cdot m$ mit geeigneten Zahlen $q, r \in \mathbb{Z}$. Multiplizieren wir beide Gleichungen miteinander, so erhalten wir $ab = a_1b_1 + c$ mit $c = (a_1r + b_1q + qrm)m \in m\mathbb{Z}$; die Klassen von ab und a_1b_1 stimmen daher überein.

$R = \mathbb{Z}/m\mathbb{Z}$ erfüllt mit der Multiplikation $(*)$ alle Eigenschaften eines kommutativen Ringes und heißt *Ring der Restklassen* modulo m. Die Gleichheit $\overline{x} = \overline{y}$ zweier Klassen wird auch durch die Notation $a \equiv b \mod (m)$ ausgedrückt.
Wir bemerken, dass sich diese Konstruktion verallgemeinern lässt; in Analogie zur Faktorgruppe haben wir hier in einem Spezialfall den *Faktorring* konstruiert. Die Abbildung $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, die $n \in \mathbb{Z}$ auf die Klasse $\overline{n}$ abbildet, ist konstruktionsgemäß ein Ringhomomorphismus.

Die in der Zahlentheorie übliche Notation $a \equiv b \mod (m)$ wird hier selten verwendet.

Allgemein können wir so vorgehen: Der bereits unter 1/2/3 definierte *Kern eines Ringhomomorphismus* $f : R \to S$ ist der Kern des zugehörigen Homomorphismus der additiven Gruppen, d.h. $\ker(f) = f^{-1}(0)$. Er ist bis auf Ausnahmen kein Unterring, erfüllt jedoch stets die folgende

$\ker(f)$ ist zwar stets eine Untergruppe von $(R, +)$, enthält aber nur dann 1_R, wenn $R = \ker(f)$. Es folgt $f(1_R) = 1_S = 0$, d.h. S ist der Nullring.

1/2/30

Definition. (*Ideal*)

Eine Untergruppe $\boldsymbol{a}$ der additiven Gruppe des Ringes R heißt (*zweiseitiges*) *Ideal,* falls für beliebige $r \in R$ und $x \in \boldsymbol{a}$ gilt $r\cdot x \in \boldsymbol{a}$ und $x\cdot r \in \boldsymbol{a}$.

Bemerkung. (*Rechnen mit Idealen*)

1. In einem Ring R gibt es wenigstens die *trivialen* Ideale
   $\mathbf{0} := \{0\}$ (*Nullideal*) und R (*Einsideal*).
2. Ein Körper besitzt nur die trivialen Ideale.
3. Der Durchschnitt einer Menge von Idealen im Ring R ist stets wieder ein Ideal.
4. Ist $F \subseteq R$ Teilmenge des Ringes R, so ist der Durchschnitt aller Ideale $\boldsymbol{a}$ aus R mit $F \subseteq \boldsymbol{a}$ ein Ideal (F), es heißt das von F *erzeugte Ideal.* (F) ist das kleinste Ideal, das F enthält.

   Insbesondere ergibt sich $\mathbf{0} = (0) = (\emptyset)$.

   Für einen kommutativen Ring R gilt
   $$(F) = \sum_{f\in F} fR := \Big\{ \sum_{f\in F} a_f f \mid a_f \in R, \text{ fast alle } a_f = 0 \Big\}.$$
   Im Fall einer endlichen Menge $F = \{f_1, \ldots, f_s\}$ wird meist die Notation $(F) =: (f_1, \ldots, f_s)$ verwendet.

Die angegebenen Eigenschaften sind mehr oder weniger offensichtlich.
3. folgt z.B. aus 1/1/8 und daraus, dass die Multiplikation mit Ringelementen nicht aus einem Ideal herausführt.

Warnung: Im Polynomring $K[X_1, X_2]$ ist dagegen $(X_1, X_2) = \{a_1X_1 + a_2X_2 \mid a_i \in K[X_1, X_2]\}$ kein Hauptideal, d.h. es existiert kein Polynom f mit der Eigenschaft $(X_1, X_2) = (f)$.

5. Ist $\boldsymbol{a} = (f)$ für ein geeignetes Element $f \in R$, so wird $\boldsymbol{a}$ ein *Hauptideal* genannt. Das Nullideal und das Einsideal $(1) = R$ sind spezielle Hauptideale.
   Nach Satz 1/1/10 ist jedes Ideal im Ring $\mathbb{Z}$ ein Hauptideal, genauer: eines der Ideale $(m) = m\mathbb{Z}$, $m \in \mathbb{N}$.
   Mit der unter 4. eingeführten Bezeichnung gilt z.B. $(6, 4) = (2)$.
6. Die *Summe der Ideale* $\boldsymbol{a}$ *und* $\boldsymbol{b}$ des Ringes R ist
   $$\boldsymbol{a} + \boldsymbol{b} := (\boldsymbol{a} \cup \boldsymbol{b}) = \{a + b \mid a \in \boldsymbol{a}, b \in \boldsymbol{b}\};$$
   diese Operation ist kommutativ und assoziativ.
   Unter Verwendung der Bezeichnung aus 4. gilt beispielsweise
   $$(f_1, \ldots, f_s) = (f_1) + \ldots + (f_s).$$

Satz – Definition. (*Faktorring*) 1/2/31

Ist $\boldsymbol{a}$ ein Ideal in dem Ring R, so besitzt die Faktorgruppe $R/\boldsymbol{a}$ eine eindeutig bestimmte Multiplikation, für die der kanonische Gruppenhomomorphismus $p : R \to R/\boldsymbol{a}$, $r \mapsto \overline{r}$ ein Ringhomomorphismus ist.

$R/\boldsymbol{a}$ heißt *Faktorring* von R nach $\boldsymbol{a}$ und p der *kanonische* (*Ring-*)*Homomorphismus* von R auf $R/\boldsymbol{a}$.

Dieser Satz und der nachfolgende Homomorphiesatz für Ringe sind nahezu identisch mit den entsprechenden Aussagen für Gruppen.

Beweis. Der Gruppenhomomorphismus p ist nur dann ein Ringhomomorphismus, wenn für $a, b \in R$ stets $p(a \cdot b) = p(a) \cdot p(b)$ gilt. Folglich ist

$$(*) \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b} \quad \text{für } a, b \in R$$

(in diesem Fall) die einzig mögliche Definition einer Multiplikation auf $R/\boldsymbol{a}$. Wie im zuvor ausgeführten Beispiel 1/2/29 kann verifiziert werden, dass die Vorschrift $(*)$ nicht von der Wahl der Repräsentanten in den Klassen $\overline{a}$, $\overline{b}$ abhängt und daher auch sinnvoll ist. Die Ringeigenschaften sind unter Verwendung von $(*)$ leicht nachzurechnen. ❏

Wie im anfangs erläuterten Spezialfall heißt $R/\boldsymbol{a}$ auch Restklassenring von R modulo $\boldsymbol{a}$. Für $a, b \in R$ mit $\overline{a} = \overline{b}$ wird gelegentlich die Schreibweise $a \equiv b \mod \boldsymbol{a}$ verwendet.

Satz. (*Homomorphiesatz für Ringe*) 1/2/32

$f : R \to R'$ sei ein Ringhomomorphismus, so existiert ein eindeutig bestimmter injektiver Ringhomomorphismus $j : R/\ker(f) \to R'$ mit $f = j \cdot p$, wobei p den kanonischen Homomorphismus $p : R \to R/\ker(f)$ bezeichnet.

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "p"'] & & R' \\ & R/\ker(f) \arrow[ur, "j"'] & \end{tikzcd}$$

Hier steht wieder das vertraute kommutative Diagramm, das wir im Zusammenhang mit dem Homomorphieprinzip für Gruppen kennengelernt haben.

Es gilt insbesondere $\operatorname{im}(f) \cong R/\ker(f)$.

Beweis. Nach dem Homomorphiesatz für Gruppen (vgl. 1/2/26) existiert ein eindeutig bestimmter Gruppenhomomorphismus j, für den das angegebene Diagramm kommutiert. Aus 1/2/31 folgt unmittelbar, dass j mit der Multiplikation verträglich ist. ❏

Die Faktorisierung eines beliebigen Homomorphismus über den kanonischen Homomorphismus lässt sich ebenso für Algebren ausführen, d.h. wenn die 1/2/33

Ringe R und R' mit Strukturmorphismen versehen sind, die mit f kommutieren. Das bereitet keinerlei Schwierigkeiten, hätte allerdings die Bezeichnungen unnötig kompliziert. Der Begriff des Faktorringes ist dann durch den der *Faktoralgebra* zu ersetzen, deren Strukturmorphismus durch Komposition des Strukturmorphismus von R mit dem kanonischen Homomorphismus entsteht.

Schwerpunkte zum gewählten Stoff

- Ideale, durch Teilmengen eines Ringes erzeugte Ideale, Hauptideale [1/2/30]
- Konstruktion von Faktorringen [1/2/29 – 1/2/31]
- Homomorphiesatz für Ringe [1/2/32]

Sachverzeichnis