Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Vorlesung 7

Restklassenringe

Nach Satz 6.7 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 7.1. 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 7.2. 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 fünfte Vorlesung. Wir beschränken uns auf kommutative Ringe.

Satz 7.3. *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*

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

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 5.10 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 7.4. *Es seien R und S kommutative Ring 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 5.10 liegt ein natürlicher Gruppenisomorphismus vor, der wegen Satz 7.3 auch die Multiplikation respektiert, also ein Ringhomomorphismus ist. □

Satz 7.5. *Es seien R und S kommutative Ring und es sei*

$$\varphi : R \longrightarrow S$$

ein Ringhomomorphismus. Dann gibt es eine kanonische Faktorisierung

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

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

Beweis. Dies beruht auf Satz 5.12 und Satz 7.3. □

Es gilt also wieder:

Bild = Urbild modulo Kern.

Restklassenringe von Hauptidealbereichen

Da wir nun die Restklassenbildung für kommutative Ringe zur Verfügung haben, kehren wir zu Hauptidealbereichen, insbesondere zu Polynomringen über einem Körper zurück.

Satz 7.6. *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. □

Korollar 7.7. *Es sei K ein Körper und $P \in K[X]$, $P \neq 0$, ein Polynom. Dann ist P genau dann irreduzibel, wenn der Restklassenring $K[X]/(P)$ ein Körper ist.*

Beweis. Dies folgt direkt aus Satz 3.15 und Satz 7.6. □

Jedes irreduzible Polynom $F \in K[X]$ definiert also eine (endliche) Körpererweiterung $K \subseteq K[X]/(F)$, und dies wird unsere Hauptkonstruktionsweise für endliche Körpererweiterungen sein.

Für die ganzen Zahlen hat man das entsprechende Resultat.

Korollar 7.8. *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 folgt direkt aus Satz 7.6. □

Rechnen in $K[X]/(P)$

Körper werden häufig ausgehend von einem schon bekannten Körper als Restklassenkörper des Polynomrings konstruiert. Die Arithmetik in einem solchen Erweiterungskörper wird in der folgenden Aussage beschrieben.

PROPOSITION 7.9. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $P = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom vom Grad n und $R = K[X]/(P)$ der zugehörige Restklassenring. Dann gelten folgende Rechenregeln (wir bezeichnen die Restklasse von X in R mit x).*

(1) *Man kann stets P als normiert annehmen (also $a_n = 1$; das werden wir im Folgenden tun).*
(2) *In R ist*
$$x^n = -\sum_{i=0}^{n-1} a_i x^i \, .$$
(3) *Höhere Potenzen x^k, $k \geq n$, kann man mit den Potenzen x^i, $i \leq n-1$, ausdrücken, indem man mittels Vielfachen von (2) sukzessive den Grad um eins reduziert.*
(4) *Die Potenzen $x^0 = 1$, x^1, $, \ldots, x^{n-1}$ bilden eine K-Basis von R.*
(5) *R ist ein K-Vektorraum der Dimension n.*
(6) *In R werden zwei Elemente $P = \sum_{i=0}^{n-1} b_i x^i$ und $Q = \sum_{i=0}^{n-1} c_i x^i$ komponentenweise addiert, und multipliziert, indem sie als Polynome multipliziert werden und dann die Restklasse berechnet wird.*

Beweis. (1) Es ist $(P) = (\frac{P}{a_n})$, da es bei einem Hauptideal nicht auf eine Einheit ankommt.
(2) Dies folgt direkt durch Umstellung der definierenden Gleichung.
(3) Dies folgt durch Multiplikation der Gleichung in (2) mit Potenzen von x.
(4) Dass die Potenzen x^i, $i = 0, \ldots, n-1$, ein Erzeugendensystem bildet, folgt aus Teil (2) und (3). Zum Beweis der linearen Unabhängigkeit sei angenommen, es gebe eine lineare Abhängigkeit, sagen wir $\sum_{i=0}^{n-1} c_i x^i = 0$. D.h., dass das Polynom $Q = \sum_{i=0}^{n-1} c_i X^i$ unter der Restklassenabbildung auf null geht, also zum Kern gehört. Dann muss es aber ein Vielfaches von P sein, was aber aus Gradgründen erzwingt, dass Q das Nullpolynom sein muss. Also sind alle $c_i = 0$.
(5) Dies folgt direkt aus (4).
(6) Dies ist klar.

□

BEISPIEL 7.10. Wir betrachten den Restklassenring
$$L = \mathbb{Q}[X]/(X^3 + 2X^2 - 5)$$
und bezeichnen die Restklasse von X mit x. Aufgrund von Proposition 7.9 besitzt jedes Element f aus L eine eindeutige Darstellung $f = ax^2 + bx + c$

mit $a, b, c \in \mathbb{Q}$, so dass also ein dreidimensionaler $\mathbb{Q}$-Vektorraum vorliegt. Da $X^3 + 2X^2 - 5$ in L zu null gemacht wird, gilt

$$x^3 = -2x^2 + 5\,.$$

Daraus ergeben sich die Gleichungen

$$x^4 \;=\; -2x^3 + 5x \;=\; -2(-2x^2 + 5) + 5x \;=\; 4x^2 + 5x - 10,$$

$$x^5 \;=\; -2x^4 + 5x^2 \;=\; -2(4x^2 + 5x - 10) + 5x^2 \;=\; -3x^2 - 10x + 20,$$

etc. Man kann hierbei auf verschiedene Arten zu dem eindeutig bestimmten kanonischen Repräsentanten reduzieren.

Berechen wir nun das Produkt

$$(3x^2 - 2x + 4)(2x^2 + x - 1)\,.$$

Dabei wird distributiv ausmultipliziert und anschließend werden die Potenzen reduziert. Es ist

$$\begin{aligned}(3x^2 - 2x + 4)(2x^2 + x - 1) &= 6x^4 + 3x^3 - 3x^2 - 4x^3 - 2x^2 + 2x + 8x^2 + 4x - 4\\ &= 6x^4 - x^3 + 3x^2 + 6x - 4\\ &= 6(4x^2 + 5x - 10) + 2x^2 - 5 + 3x^2 + 6x - 4\\ &= 29x^2 + 36x - 69.\end{aligned}$$

Restklassendarstellung von Unteralgebren

Satz 7.11. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Es sei P das Minimalpolynom von f. Dann gibt es eine kanonische K-Algebra-Isomorphie*

$$K[X]/(P) \longrightarrow K[f],\, X \longmapsto f.$$

Beweis. Die Einsetzung $X \mapsto f$ ergibt nach Satz 6.4 den kanonischen K-Algebra-Homomorphismus

$$K[X] \longrightarrow L,\, X \longmapsto f.$$

Das Bild davon ist genau $K[f]$, so dass ein surjektiver K-Algebra-Homomorphismus

$$K[X] \longrightarrow K[f]$$

vorliegt. Daher gibt es nach Korollar 7.4 eine Isomorphie zwischen $K[f]$ und dem Restklassenring von $K[X]$ modulo dem Kern der Abbildung. Der Kern ist aber nach Lemma 6.12 das vom Minimalpolynom erzeugte Hauptideal. □

Lemma 7.12. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann gelten folgende Aussagen.*

(1) *Das Minimalpolynom P von f über K ist irreduzibel.*

(2) *Wenn $Q \in K[X]$ ein normiertes, irreduzibles Polynom mit $Q(f) = 0$ ist, so handelt es sich um das Minimalpolynom.*

Beweis. (1) Es sei $P = P_1P_2$ eine Faktorzerlegung des Minimalpolynoms. Dann gilt in L die Beziehung

$$0 = P(f) = P_1(f)P_2(f).$$

Da L ein Körper ist, muss ein Faktor null sein, sagen wir $P_1(f) = 0$. Da aber P unter allen Polynomen $\neq 0$, die f annullieren, den minimalen Grad besitzt, müssen P und P_1 den gleichen Grad besitzen und folglich muss P_2 konstant ($\neq 0$), also eine Einheit sein.

(2) Wegen $Q(f) = 0$ ist Q aufgrund von Lemma 6.12 ein Vielfaches des Minimalpolynoms P, sagen wir $Q = GP$. Da Q nach Voraussetzung irreduzibel ist, und da P zumindest den Grad eins besitzt, muss G konstant sein. Da schließlich sowohl P als auch Q normiert sind, ist $P = Q$.

□