Prof. Dr. H. Brenner **Osnabrück SS 2018**

Lineare Algebra und analytische Geometrie II

Vorlesung 47

Homomorphie- und Isomorphiesatz

Satz 47.1. *Seien G, Q und H Gruppen, es sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus und $\psi\colon G \to Q$ ein surjektiver Gruppenhomomorphismus. Es sei vorausgesetzt, dass*

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

ist. Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi}\colon Q \longrightarrow H$$

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

$$\begin{array}{ccc} G & \stackrel{\varphi}{\longrightarrow} & H \\ \psi\downarrow & \nearrow \tilde{\varphi} & \\ Q & & \end{array}$$

ist kommutativ.

Beweis. Wir zeigen zuerst die Eindeutigkeit. Für jedes Element $u \in Q$ gibt es mindestens ein $g \in G$ mit $\psi(g) = u$. Wegen der Kommutativität des Diagramms muss

$$\tilde{\varphi}(u) = \varphi(g)$$

gelten. Das bedeutet, dass es maximal ein $\tilde{\varphi}$ geben kann. Wir haben zu zeigen, dass durch diese Bedingung eine wohldefinierte Abbildung gegeben ist. Seien also $g, g' \in G$ zwei Urbilder von u. Dann ist

$$\psi\left(g'g^{-1}\right) = uu^{-1} = e_Q$$

und somit ist $g'g^{-1} \in \operatorname{kern}\psi \subseteq \operatorname{kern}\varphi$. Daher ist $\varphi(g) = \varphi(g')$. Die Abbildung ist also wohldefiniert. Seien $u, v \in Q$ und seien $g, h \in G$ Urbilder davon. Dann ist gh ein Urbild von uv und daher ist

$$\tilde{\varphi}(uv) = \varphi(gh) = \varphi(g)\varphi(h) = \tilde{\varphi}(u)\tilde{\varphi}(v).$$

D.h. $\tilde{\varphi}$ ist ein Gruppenhomomorphismus. □

Beispiel 47.2. Wir betrachten die beiden surjektiven Gruppenhomomorphismen

$$\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/(4)$$

und

$$\psi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/(12).$$

Es ist

$$\operatorname{kern}\psi \;=\; \mathbb{Z}\cdot 12 \;\subseteq\; \mathbb{Z}\cdot 4 \;=\; \operatorname{kern}\varphi.$$

Daher gibt es nach dem Homomorphiesatz einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi}\colon\; \mathbb{Z}/(12) \longrightarrow \mathbb{Z}/(4),$$

der mit den Restabbildungen verträglich ist. Dieser bildet den Rest der Zahl bei Division durch 12 auf den Rest bei Division durch 4 ab. Der Satz beinhaltet insbesondere die Aussage, dass dieser letztere Rest allein vom ersten Rest abhängt, nicht von der Zahl selbst.

Wenn man hingegen

$$\varphi\colon\; \mathbb{Z} \longrightarrow \mathbb{Z}/(5)$$

und

$$\psi\colon\; \mathbb{Z} \longrightarrow \mathbb{Z}/(12)$$

betrachtet, so ist

$$\operatorname{kern}\psi \;=\; \mathbb{Z}\cdot 12 \;\not\subseteq\; \mathbb{Z}\cdot 5 \;=\; \operatorname{kern}\varphi$$

und es gibt keine natürliche Abbildung

$$\mathbb{Z}/(12) \longrightarrow \mathbb{Z}/(5).$$

Beispielsweise haben $1, 13, 25, 37, 49$, die alle modulo 12 den Rest 1 haben, modulo 5 die Reste $1, 3, 0, 2, 4$.

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

Korollar 47.3. *Seien G und H Gruppen und sei*

$$\varphi\colon\; G \longrightarrow H$$

ein surjektiver Gruppenhomomorphismus. Dann gibt es eine kanonische Isomorphie

$$\tilde{\varphi}\colon\; G/\operatorname{kern}\varphi \longrightarrow H.$$

Beweis. Wir wenden Satz 47.1 auf $Q = G/\operatorname{kern}\varphi$ und die kanonische Projektion $q\colon\; G \to G/\operatorname{kern}\varphi$ an. Dies induziert einen Gruppenhomomorphismus

$$\tilde{\varphi}\colon\; G/\operatorname{kern}\varphi \longrightarrow H$$

mit $\varphi = \tilde{\varphi}\circ q$, der surjektiv ist. Sei $[x] \in G/\operatorname{kern}\varphi$ und $[x] \in \operatorname{kern}\tilde{\varphi}$. Dann ist

$$\tilde{\varphi}([x]) \;=\; \varphi(x) \;=\; e_H,$$

also $x \in \operatorname{kern}\varphi$. Damit ist $[x] = e_Q$, d.h. der Kern von $\tilde{\varphi}$ ist trivial und nach Lemma 44.21 ist $\tilde{\varphi}$ auch injektiv. □

Beispiel 47.4. Es sei G eine zyklische Gruppe mit einem Erzeuger g. Wir betrachten den im Sinne von Lemma 44.12 zugehörigen Gruppenhomomorphismus

$$\varphi\colon\ \mathbb{Z} \longrightarrow G,\ n \longmapsto g^n.$$

Da ein Erzeuger vorliegt, ist diese Abbildung surjektiv. Der Kern dieser Abbildung ist durch die Ordnung von g gegeben, die wir k nennen (oder 0, wenn die Ordnung ∞ ist). Aufgrund von Korollar 47.3 gibt es eine kanonische Isomorphie

$$\tilde{\varphi}\colon\ \mathbb{Z}/(k) \longrightarrow G.$$

Insbesondere gibt es bis auf Isomorphie für jedes k genau eine zyklische Gruppe, nämlich $\mathbb{Z}/(k)$.

Beispiel 47.5. Der Gruppenhomomorphismus

$$\mathbb{R} \longrightarrow S^1,\ t \longmapsto \begin{pmatrix} \cos\, t \\ \sin\, t \end{pmatrix},$$

ist surjektiv und aufgrund der Periodizität der trigonometrischen Funktionen ist der Kern gleich $\mathbb{Z}2\pi$. Nach dem Isomorphiesatz gibt es eine kanonische Isomorphie

$$\mathbb{R}/\mathbb{Z}2\pi\ \cong\ S^1.$$

Beispiel 47.6. Die komplexe Exponentialfunktion

$$(\mathbb{C}, 0, +) \longrightarrow (\mathbb{C}^\times, 1, \cdot),\ z \longmapsto \exp\, z,$$

ist ein surjektiver Gruppenhomomorphismus. Der Kern ist $\mathbb{Z}2\pi\mathrm{i}$. Nach dem Isomorphiesatz gibt es eine kanonische Isomorphie

$$\mathbb{C}/\mathbb{Z}2\pi\mathrm{i}\ \cong\ \mathbb{C}^\times.$$

Beispiel 47.7. Die Determinante

$$\det:\ \mathrm{GL}_n(K) \longrightarrow K^\times,\ M \longmapsto \det\, M,$$

ist ein surjektiver Gruppenhomomorphismus, der Kern ist nach Definition die spezielle lineare Gruppe $\mathrm{SL}_n(K)$. Nach dem Isomorphiesatz gibt es eine kanonische Isomorphie

$$\mathrm{GL}_n(K)\,/\,\mathrm{SL}_n(K)\ \cong\ K^\times.$$

Satz 47.8. *Seien G und H Gruppen und sei*

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann gibt es eine kanonische Faktorisierung

$$G \xrightarrow{q} G/\operatorname{kern}\varphi \xrightarrow{\theta} \operatorname{bild}\varphi \xhookrightarrow{\iota} H\,,$$

wobei q die kanonische Projektion, θ ein Gruppenisomorphismus und ι die kanonische Inklusion der Bildgruppe ist.

Beweis. Dies folgt aus Korollar 47.3, angewandt auf die Bildgruppe $U = \operatorname{bild}\varphi \subseteq H$. □

Diese Aussage wird häufig kurz und prägnant so formuliert:

Bild = Urbild modulo Kern.

Satz 47.9. *Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler mit der Restklassengruppe $Q = G/N$. Es sei $H \subseteq G$ ein weiterer Normalteiler in G, der N umfasst. Dann ist das Bild $\overline{H}$ von H in Q ein Normalteiler und es gilt die kanonische Isomorphie*

$$G/H \cong Q/\overline{H}.$$

Beweis. Für die erste Aussage siehe Aufgabe 46.18. Damit ist die Restklassengruppe $Q/\overline{H}$ wohldefiniert. Wir betrachten die Komposition

$$p \circ q : G \longrightarrow Q \longrightarrow Q/\overline{H}\,.$$

Wegen

$$\begin{array}{rcl} \operatorname{kern}(p \circ q) & = & \{x \in G |\, (p \circ q)(x) = e\} \\ & = & \{x \in G |\, q(x) \in \operatorname{kern} p\} \\ & = & \left\{x \in G |\, q(x) \in \overline{H}\right\} \\ & = & H \end{array}$$

ist $\operatorname{kern}(p \circ q) = H$. Daher ergibt Korollar 47.3 die kanonische Isomorphie

$$G/H \longrightarrow Q/\overline{H}.$$

□

Kurz gesagt ist also

$$G/H = (G/N)/(H/N).$$

Restklassenringe

Auf einer Restklassengruppe zu einem Normalteiler in einer Gruppe gibt es häufig zusätzliche Strukturen, wenn die Ausgangsgruppe und der Normalteiler zusätzliche Eigenschaften besitzen. In der nächsten Vorlesung werden wir Restklassenräume zu Untervektorräumen besprechen. Hier besprechen wir kurz Restklassenringe zu einem Ideal in einem kommutativen Ring. Gelegentlich sind uns schon Ringhomomorphismen begegnet, wir erinnern an die Definition.

Definition 47.10. Seien R und S Ringe. Eine Abbildung

$$\varphi\colon\ R \longrightarrow S$$

heißt *Ringhomomorphismus*, wenn folgende Eigenschaften gelten:

(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$.
(2) $\varphi(1) = 1$.
(3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Nach Aufgabe 47.14 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 Normalteiler 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 47.11. 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 47.12. 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

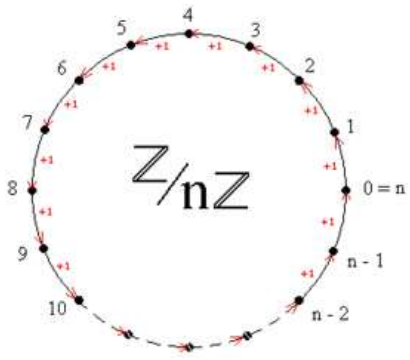
$$a'b' = (a+x)(b+y) = ab + ay + xb + xy.$$

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 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 $0, 1, 2, \ldots, d-1$. 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 47.13. *Sei $d \geq 0$ eine natürliche Zahl. Dann gibt es eine eindeutig bestimmte Ringstruktur auf $\mathbb{Z}/(d)$ derart, dass die Restklassenabbildung*

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

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. □

Satz 47.14. *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. Siehe Aufgabe 48.15. □

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.

Abbildungsverzeichnis