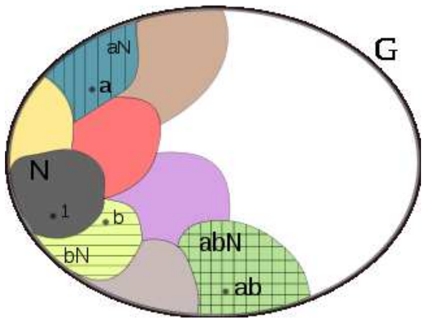
Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 12

Restklassenbildung

In der letzten Vorlesung haben wir in Lemma 11.12 gesehen, dass der Kern eines Gruppenhomomorphismus ein Normalteiler ist. Wir zeigen nun umgekehrt, dass sich jeder Normalteiler als Kern eines geeigneten, surjektiven Gruppenhomomorphismus realisieren lässt.



Die Multiplikation der Nebenklassen zu einem Normalteiler $N \subseteq G$.

Satz 12.1. *Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Es sei G/H die Menge der Nebenklassen (die Quotientenmenge) und*

$$q\colon G \longrightarrow G/H,\, g \longmapsto [g],$$

die kanonische Projektion. Dann gibt es eine eindeutig bestimmte Gruppenstruktur auf G/H derart, dass q ein Gruppenhomomorphismus ist.

Beweis. Da die kanonische Projektion zu einem Gruppenhomomorphismus werden soll, muss die Verknüpfung durch

$$[x][y] = [xy]$$

gegeben sein. Wir müssen also zeigen, dass durch diese Vorschrift eine wohldefinierte Verknüpfung auf G/H definiert ist, die unabhängig von der Wahl der Repräsentanten ist. D.h. wir haben für $[x] = [x']$ und $[y] = [y']$ zu zeigen, dass $[xy] = [x'y']$ ist. Nach Voraussetzung können wir $x' = xh$ und $hy' = \tilde{h}y = yh'$ mit $h, \tilde{h}, h' \in H$ schreiben. Damit ist

$$x'y' = (xh)y' = x(hy') = x(yh') = xyh'.$$

Somit ist $[xy] = [x'y']$. Aus der Wohldefiniertheit der Verknüpfung auf G/H folgen die Gruppeneigenschaften, die Homomorphieeigenschaft der Projektion und die Eindeutigkeit. $\square$

Definition 12.2. Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Die Quotientenmenge

$$G/H$$

mit der aufgrund von Satz 12.1 eindeutig bestimmten Gruppenstruktur heißt *Restklassengruppe von G modulo H*. Die Elemente $[g] \in G/H$ heißen *Restklassen*. Für eine Restklasse $[g]$ heißt jedes Element $g' \in G$ mit $[g'] = [g]$ ein *Repräsentant* von $[g]$.

Beispiel 12.3. Die Untergruppen der ganzen Zahlen sind nach Satz 5.2 von der Form $\mathbb{Z}n$ mit $n \geq 0$. Die Restklassengruppen werden mit

$$\mathbb{Z}/(n)$$

bezeichnet (sprich „$\mathbb{Z}$ modulo n“). Bei $n = 0$ ist das einfach $\mathbb{Z}$ selbst, bei $n = 1$ ist das die triviale Gruppe. Im Allgemeinen ist die durch die Untergruppe $\mathbb{Z}n$ definierte Äquivalenzrelation auf $\mathbb{Z}$ dadurch gegeben, dass zwei ganze Zahlen a und b genau dann äquivalent sind, wenn ihre Differenz $a - b$ zu $\mathbb{Z}n$ gehört, also ein Vielfaches von n ist. Daher ist (bei $n \geq 1$) jede ganze Zahl zu genau einer der n Zahlen

$$0, 1, 2, \ldots, n - 1$$

äquivalent (oder, wie man auch sagt, *kongruent modulo n*), nämlich zum Rest, der sich bei Division durch n ergibt. Diese Reste bilden also ein Repräsentantensystem für die Restklassengruppe, und diese besitzt n Elemente. Die Tatsache, dass die Restklassenabbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n),\ a \longmapsto [a] = a \mod n,$$

ein Homomorphismus ist, kann man auch so ausdrücken, dass der Rest einer Summe von zwei ganzen Zahlen nur von den beiden Resten, nicht aber von den Zahlen selbst, abhängt. Als Bild der zyklischen Gruppe $\mathbb{Z}$ ist auch $\mathbb{Z}/(n)$ zyklisch, und zwar ist 1 (aber auch -1) stets ein Erzeuger.

Wie bei jeder Äquivalenzrelation $\sim$ auf G nennt man eine Teilmenge $R \subseteq G$ ein Repräsentantensystem für die Äquivalenzrelation, wenn jede Äquivalenzklasse genau ein Element aus R enthält. Dies bedeutet, dass die Abbildung $R \to G/\sim$ bijektiv ist. Solche Repräsentantensysteme gibt es immer. In unserem gruppentheoretischen Kontext gibt es manchmal eine Untergruppe $F \subseteq G$ mit der Eigenschaft, dass die Gesamtabbildung

$$F \longrightarrow G/H,\ f \longmapsto [f],$$

bijektiv und damit ein Isomorphismus ist. Dies liefert dann eine einfache Beschreibung der Restklassengruppe, wie im folgenden Beispiel.

Beispiel 12.4. Wir betrachten die Einheitengruppe von $\mathbb{C}$, also $(\mathbb{C}^\times, 1, \cdot)$. Zur Untergruppe $\mathbb{R}_+ \subseteq \mathbb{C}^\times$ ist die Abbildung

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} \longrightarrow \mathbb{C}^\times \longrightarrow \mathbb{C}/\mathbb{R}_+$$

ein Isomorphismus, die Restklassengruppe ist also isomorph zur Kreisgruppe. Der Kern der Gesamtabbildung besteht aus dem Durchschnitt

$$S^1 \cap \mathbb{R}_+ = \{1\},$$

daher ist die Abbildung nach Lemma 10.13 injektiv. Zum Beweis der Surjektivität müssen wir zeigen, dass die Äquivalenzklasse zu jedem $x \in \mathbb{C}^\times$ durch ein Element des Einheitskreises repräsentiert werden kann. Hierzu kann man $\frac{x}{|x|}$ nehmen.

Zur Untergruppe $S^1 \subseteq \mathbb{C}^\times$ ist die Abbildung

$$\mathbb{R}_+ \longrightarrow \mathbb{C}^\times \longrightarrow \mathbb{C}/S^1$$

bijektiv, die Restklassengruppe ist also isomorph zur Gruppe der positiven reellen Zahlen. Die Injektivität ergibt sich wie eben. Die Surjektivität ergibt sich daraus, dass $x \in \mathbb{C}^\times$ zu $|x|$ (bezüglich der Untergruppe S^1) äquivalent ist.

Homomorphie- und Isomorphiesatz

Satz 12.5. *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

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

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

$$\begin{array}{ccc} G & \longrightarrow & Q \\ & \searrow & \downarrow \\ & & H \end{array}$$

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

$$g'g^{-1} \in \operatorname{kern} \psi \subseteq \operatorname{kern} \varphi$$

und 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. $\square$

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

Korollar 12.6. *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 12.5 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 10.13 ist $\tilde{\varphi}$ auch injektiv. $\square$

Satz 12.7. *Seien G und H Gruppen und sei*

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

ein Gruppenhomomorphismus. Dann gibt es eine kanonische Faktorisierung

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

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

Beweis. Dies folgt aus Korollar 12.6 angewandt auf die Bildgruppe $U = \operatorname{bild}\varphi \subseteq H$. $\square$

Diese Aussage wird häufig kurz und prägnant so formuliert:

Bild = Urbild modulo Kern.

Satz 12.8. *Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler mit der Restklassengruppe $Q = G/N$. Es sei $H \subseteq G$ eine 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 11.6. Damit ist die Restklassengruppe $Q/\overline{H}$ wohldefiniert. Wir betrachten die Komposition

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

Wegen

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

ist $\operatorname{kern} p \circ q = H$. Daher ergibt Korollar 12.6 die kanonische Isomorphie

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

□

Kurz gesagt ist also

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

Abbildungsverzeichnis