Prof. Dr. H. Brenner **Osnabrück WS 2018/2019**

Körper- und Galoistheorie

Vorlesung 5

In dieser Vorlesung diskutieren wir Normalteiler, das sind Untergruppen, für die Links- und Rechtsnebenklassen übereinstimmen. Für Normalteiler kann man Restklassengruppen konstruieren.

Innere Automorphismen

Definition 5.1. Sei G eine Gruppe und $g \in G$ fixiert. Die durch g definierte Abbildung
$$\kappa_g \colon G \longrightarrow G,\, x \longmapsto gxg^{-1},$$
heißt *innerer Automorphismus*.

Eine solche Abbildung nennt man auch *Konjugation* (mit g). Wenn G eine kommutative Gruppe ist, so ist wegen $gxg^{-1} = xgg^{-1} = x$ die Identität der einzige innere Automorphismus. Der Begriff ist also nur bei nicht kommutativen Gruppen von Interesse. Ein wichtiges Beispiel für eine Konjugation tritt auf, wenn lineare Abbildungen durch Matrizen bezüglich verschiedener Basen beschrieben werden sollen, siehe Lemma 11.11 (Lineare Algebra (Osnabrück 2017-2018)). Man spricht auch von ähnlichen Matrizen (wobei der Ähnlichkeitsbegriff auch für nicht invertierbare Matrizen definiert ist).

Lemma 5.2. *Ein innerer Automorphismus ist in der Tat ein Automorphismus. Die Zuordnung*
$$G \longrightarrow \operatorname{Aut} G,\, g \longmapsto \kappa_g,$$
ist ein Gruppenhomomorphismus.

Beweis. Es ist
$$\kappa_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \kappa_g(x)\kappa_g(y),$$
so dass ein Gruppenhomomorphismus vorliegt. Wegen
$$\kappa_g(\kappa_h(x)) = \kappa_g(hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = \kappa_{gh}$$
ist einerseits
$$\kappa_{g^{-1}} \circ \kappa_g = \kappa_{g^{-1}g} = \mathrm{id}_G,$$
so dass κ_g bijektiv, also ein Automorphismus, ist. Andererseits ist deshalb die Gesamtabbildung κ ein Gruppenhomomorphismus. □

Normalteiler

Definition 5.3. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Man nennt H einen *Normalteiler*, wenn

$$xH = Hx$$

für alle $x \in G$ ist, wenn also die Linksnebenklasse zu x mit der Rechtsnebenklasse zu x übereinstimmt.

Bei einem Normalteiler braucht man nicht zwischen Links- und Rechtsnebenklassen zu unterscheiden und spricht einfach von *Nebenklassen*. Statt xH oder Hx schreiben wir meistens $[x]$. Die Gleichheit $xH = Hx$ bedeutet *nicht*, dass $xh = hx$ für alle $h \in H$ ist, sondern lediglich, dass es zu jedem $h \in H$ ein $\tilde{h} \in H$ mit $xh = \tilde{h}x$. gibt.

Lemma 5.4. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann sind folgende Aussagen äquivalent.*

(1) *H ist ein Normalteiler*
(2) *Es ist $xhx^{-1} \in H$ für alle $x \in G$ und $h \in H$.*
(3) *H ist invariant unter jedem inneren Automorphismus von G.*

Beweis. (1) bedeutet bei gegebenem $h \in H$, dass man $xh = \tilde{h}x$ mit einem $\tilde{h} \in H$ schreiben kann. Durch Multiplikation mit x^{-1} von rechts ergibt sich $xhx^{-1} = \tilde{h} \in H$, also (2). Dieses Argument rückwärts ergibt die Implikation (2) $\Rightarrow$ (1). Ferner ist (2) eine explizite Umformulierung von (3). $\square$

Beispiel 5.5. Wir betrachten die Permutationsgruppe $G = S_3$ zu einer dreielementigen Menge, d.h. S_3 besteht aus den bijektiven Abbildungen der Menge $\{1, 2, 3\}$ in sich. Die triviale Gruppe $\{\mathrm{id}\}$ und die ganze Gruppe sind Normalteiler. Die Teilmenge $H = \{\mathrm{id}, \varphi\}$, wobei φ die Elemente 1 und 2 vertauscht und 3 unverändert lässt, ist eine Untergruppe. Sie ist aber kein Normalteiler. Um dies zu zeigen, sei ψ die Bijektion, die 1 fest lässt und 2 und 3 vertauscht. Dieses ψ ist zu sich selbst invers. Die Konjugation $\psi\varphi\psi^{-1} = \psi\varphi\psi$ ist dann die Abbildung, die 1 auf 3, 2 auf 2 und 3 auf 1 schickt, und diese Bijektion gehört nicht zu H.

Lemma 5.6. *Seien G und H Gruppen und sei*

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

ein Gruppenhomomorphismus. Dann ist der Kern $\ker \varphi$ *ein Normalteiler in G.*

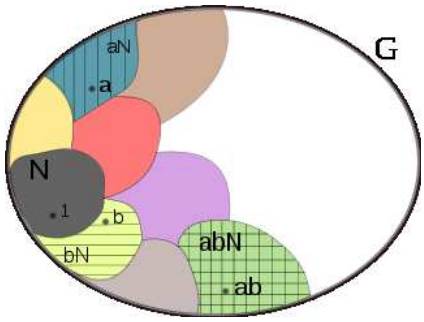
Beweis. Wir verwenden Lemma 5.4. Sei also $x \in G$ beliebig und $h \in \ker \varphi$. Dann ist

$$\varphi\left(xhx^{-1}\right) = \varphi(x)\varphi(h)\varphi\left(x^{-1}\right) = \varphi(x)e_H\varphi\left(x^{-1}\right) = \varphi(x)\varphi(x)^{-1} = e_H,$$

also gehört xhx^{-1} ebenfalls zum Kern. $\square$

Restklassenbildung

Wir zeigen nun umgekehrt, dass jeder Normalteiler sich als Kern eines geeigneten, surjektiven Gruppenhomomorphismus realisieren lässt.



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

Satz 5.7. *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 5.8. Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Die Quotientenmenge

$$G/H$$

mit der aufgrund von Satz 5.7 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 5.9. Die Untergruppen der ganzen Zahlen sind nach Satz 44.3 (Lineare Algebra (Osnabrück 2017-2018)) von der Form (diese Aussage ist analog zu der in Vorlesung 3 bewiesenen Aussage, dass $K[X]$ ein Hauptidealbereich ist) $\mathbb{Z}n$ 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.[1] Als Bild der zyklischen Gruppe[2] $\mathbb{Z}$ ist auch $\mathbb{Z}/(n)$ zyklisch, und zwar ist 1 (aber auch -1) stets ein Erzeuger.

Die Homomorphiesätze für Gruppen

Satz 5.10. *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

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

ist kommutativ.

[1] Dies gilt auch für das Produkt von zwei Zahlen, was bedeutet, dass diese Abbildung ein Ringhomomorphismus ist.

[2] Eine Gruppe G heißt *zyklisch*, wenn sie von einem Element erzeugt wird.

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. $\square$

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

Korollar 5.11. *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 5.10 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 4.9 ist $\tilde{\varphi}$ auch injektiv. $\square$

Satz 5.12. *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 5.11, angewandt auf die Bildgruppe $U = \operatorname{bild}\varphi \subseteq H$. □

Diese Aussage wird häufig kurz und prägnant so formuliert:

Bild = Urbild modulo Kern.

Satz 5.13. *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 5.25. Damit ist die Restklassengruppe $Q/\overline{H}$ wohldefiniert. Wir betrachten die Komposition

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

Wegen

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

ist $\operatorname{kern}(p \circ q) = H$. Daher ergibt Korollar 5.11 die kanonische Isomorphie

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

□

Kurz gesagt ist also

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

Abbildungsverzeichnis