Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 7

Nebenklassen

DEFINITION 1. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wir setzen $x \sim_H y$ (und sagen, dass x und y äquivalent sind) wenn $x^{-1}y \in H$.

Dies ist in der Tat eine Äquivalenzrelation: aus $x^{-1}x = e_G \in H$ folgt, dass diese Relation reflexiv ist. Aus $x^{-1}y \in H$ folgt sofort $y^{-1}x = (x^{-1}y)^{-1} \in H$ und aus $x^{-1}y \in H$ und $y^{-1}z \in H$ folgt $x^{-1}z \in H$.

DEFINITION 2. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann heißt zu jedem $x \in G$ die Teilmenge

$$xH = \{xh : h \in H\}$$

die *Linksnebenklasse* von x in G bzgl. H. Jede Teilmenge von dieser Form heißt *Linksnebenklasse*. Entsprechend heißt eine Menge der Form

$$Hy = \{hy : h \in H\}$$

Rechtsnebenklasse (zu y).

Die Linksnebenklassen sind wegen

$$\begin{aligned}[x] &= \{y \in G : x \sim y\} \\ &= \{y \in G : x^{-1}y \in H\} \\ &= \{y \in G : \text{es gibt } h \in H \text{ mit } x^{-1}y = h\} \\ &= \{y \in G : \text{es gibt } h \in H \text{ mit } y = xh\} \\ &= xH\end{aligned}$$

die Äquivalenzklassen zu der oben definierten Äquivalenzrelation. Die Linksnebenklassen bilden somit eine disjunkte Zerlegung (eine *Partition*) von G. Dies gilt ebenso für die Rechtsnebenklassen. Im kommutativen Fall muss man nicht zwischen Links- und Rechtsnebenklassen unterscheiden.

LEMMA 3. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Es seien $x, y \in G$ zwei Elemente. Dann sind folgende Aussagen äquivalent.*

(1) $x \in yH$
(2) $y \in xH$
(3) $y^{-1}x \in H$
(4) $x^{-1}y \in H$
(5) $xH \cap yH \neq \emptyset$
(6) $x \sim_H y$.

Beweis. Die Äquivalenz von (1) und (3) (und die von (2) und (4)) folgt aus Multiplikation mit y^{-1} bzw. mit y. Die Äquivalenz von (3) und (4) folgt durch Übergang zum Inversen. Aus (1) folgt (5) wegen $1 \in H$. Wenn (5) erfüllt ist, so bedeutet das $xh_1 = yh_2$ mit $h_1, h_2 \in H$. Damit ist $x = yh_2h_1^{-1}$ und (1) ist erfüllt. Schließlich sind (4) und (6) äquivalent nach Definition. □

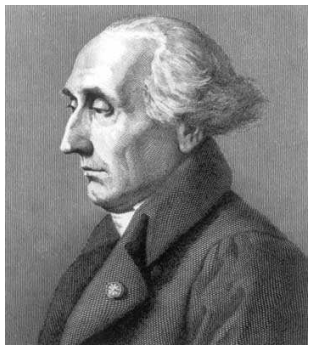
Der Satz von Lagrange

Satz 4. *(Satz von Lagrange) Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe von G. Dann ist ihre Kardinalität $\#(H)$ ein Teiler von $\#(G)$.*

Beweis. Betrachte die Linksnebenklassen $gH := \{gh : h \in H\}$ für sämtliche $g \in G$. Es ist $h \mapsto gh$ eine Bijektion zwischen H und gH, so dass alle Nebenklassen gleich groß sind (und zwar $\#(H)$ Elemente haben). Haben zwei Nebenklassen g_1H, g_2H ein Element g gemeinsam, etwa $g = g_1h_1 = g_2h_2$, so sind die Nebenklassen sogar gleich:

$$g_1H = g_1h_1H = g_2h_2H = g_2H\,.$$

Da schließlich die Nebenklassen ganz G überdecken, werden G in endlich viele $\#(H)$-elementige Teilmengen zerlegt, so dass $\#(G)$ ein Vielfaches von $\#(H)$ ist. □



Joseph-Louis Lagrange
(1736 Turin - 1813 Paris)

Korollar 5. *Sei G eine endliche Gruppe und sei $g \in G$ ein Element. Dann teilt die Ordnung von g die Gruppenordnung.*

Beweis. Sei H die von g erzeugte Untergruppe. Nach Lemma 2.3 ist $\operatorname{ord} g = \operatorname{ord} H$. Daher teilt diese Zahl nach Satz 7.4 die Gruppenordnung von G. □

Definition 6. Zu einer Untergruppe $H \subseteq G$ heißt die Anzahl der (Links- oder Rechts)Nebenklassen der *Index* von H in G, geschrieben

$$\operatorname{ind}_G H\,.$$

In der vorstehenden Definition ist Anzahl im allgemeinen als die *Mächtigkeit* einer Menge zu verstehen. Der Index wird aber hauptsächlich dann verwendet, wenn er endlich ist, wenn es also nur endlich viele Nebenklassen gibt. Das ist bei endlichem G automatisch der Fall, kann aber auch bei unendlichem G der Fall sein, wie schon die Beispiele $\mathbb{Z}n \subseteq \mathbb{Z}, n \geq 1$, zeigen. Wenn G eine endliche Gruppe ist und $G \subseteq H$ eine Untergruppe, so gilt aufgrund des Satzes von Lagrange die einfache *Indexformel*

$$\#(G) = \#(H) \cdot \operatorname{ind}_G H\,.$$

Normalteiler

Definition 7. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Man nennt H einen *Normalteiler*, wenn

$$xH = Hx$$

ist für alle $x \in G$, 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*. Die Gleichheit $xH = Hx$ bedeutet *nicht*, dass $xh = hx$ ist, sondern lediglich, dass es zu jedem $h \in H$ ein $\tilde{h} \in H$ gibt mit $xh = \tilde{h}x$. Statt xH oder Hx schreiben wir meistens $[x]$.

Lemma 8. *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.*

Beweis. (1) bedeutet bei gegebenem $h \in H$, dass man $xh = \tilde{h}x$ schreiben kann mit $\tilde{h} \in H$. 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). □

Beispiel 9. 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 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 2, 2 auf 2 und 3 auf 1 schickt, und diese Bijektion gehört nicht zu H.

Lemma 10. *Seien G und H Gruppen und sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist der Kern* $\ker \varphi$ *ein Normalteiler in G.*

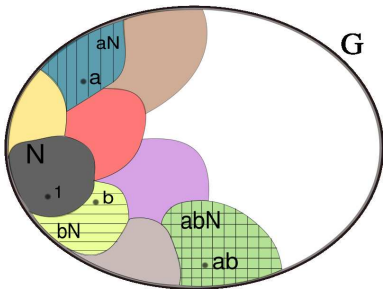
Beweis. Wir verwenden Lemma 7.8(2). Sei also $x \in G$ beliebig und $h \in \ker \varphi$. Dann ist

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

also gehört xhx^{-1} zum Kern. □

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

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

die kanonische Projektion. Dann gibt es eine eindeutig bestimmte Gruppenstruktur auf G/H derart, dass ψ 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 $hy' = \tilde{h}y = yh'$ schreiben mit $h, h' \in H$. 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. □

Definition 12. Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Die Quotientenmenge

$$G/H$$

mit der aufgrund von Satz 7.9 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 13. (Die zyklischen Gruppen) Die Untergruppen der ganzen Zahl sind nach Satz 3.2 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 der Restklassenhomomorphismus

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

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

Abbildungsverzeichnis