Prof. Dr. H. Brenner **Osnabrück SoSe 2025**

Lineare Algebra II

Vorlesung 46

Eine Äquivalenzrelation $\sim$ auf einer Menge M definiert die Quotientenmenge $M/\sim$ und die kanonische Projektion $M \to M/\sim$. Wenn es auf M zusätzliche Strukturen gibt und die Äquivalenzrelation diese respektiert, so kann man häufig auf $M/\sim$ wieder die gleiche Struktur erhalten. Als Hauptbeispiel für diesen Prozess betrachten wir Äquivalenzrelationen auf Gruppen, die durch eine Untergruppe definiert werden.

Nebenklassen

Definition 46.1. Es 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 $x^{-1}z \in H$.

Zwei Gruppenelemente x und y sind genau dann äquivalent, wenn es ein Element $h \in H$ der Untergruppe mit $y = xh$ gibt. In Anschluss an Beispiel 45.12 kann man die Situation so interpretieren, dass die Untergruppe H eine Menge an Bewegungsmöglichkeiten festlegt, und zwei Elemente genau dann äquivalent sind, wenn sie durch eine solche durch H gegebene Bewegung ineinander überführt werden können.

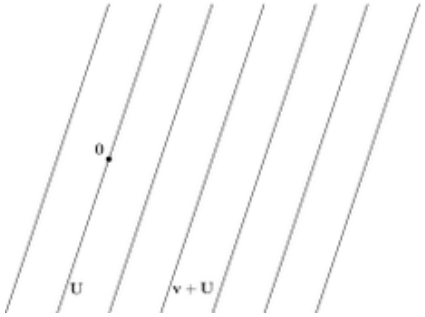
Beispiel 46.2. In einer (additiv geschriebenen) kommutativen Gruppe wie $\mathbb{Z}$ oder einem Vektorraum V und einer Untergruppe H bedeutet $x \sim_H y$, dass $y - x \in H$ ist bzw. dass es ein $h \in H$ mit

$$y = x + h$$

gibt. Die Äquivalenzklassen sind von der Form $x + H = \{x + h \mid h \in H\}$. Bei $H = \mathbb{Z}d \subseteq \mathbb{Z}$ mit einem festen d besitzen die Äquivalenzklassen die Form

$$H = \mathbb{Z}d,\ 1{+}H = \{\ldots, 1{-}d, 1, 1{+}d, 1{+}2d, \ldots\},\ 2{+}H = \{\ldots, 2{-}d, 2, 2{+}d, 2{+}2d, \ldots\}, \ldots .$$

Die Klassen vereinigen diejenigen ganzen Zahlen, die bei Division durch d den Rest 0 oder 1 oder 2 u.s.w. haben. Diese Klassen bilden eine vollständige Zerlegung von $\mathbb{Z}$.



Die Äquivalenzklassen zu einem Untervektorraum.

Wenn $H = U \subseteq V$ ein Untervektorraum ist, so haben die Äquivalenzklassen die Form $v+U = \{v+u \mid u \in U\}$ für einen Vektor $v \in V$. Dies ist der affine Raum mit dem Aufpunkt v und dem Verschiebungsraum U (im Sinne von Definition 29.1). Die Äquivalenzklassen bilden eine Familie von zueinander parallelen affinen Unterräumen.

Definition 46.3. Es sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann heißt zu jedem $x \in G$ die Teilmenge

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

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

$$Hx = \{hx \mid h \in H\}$$

Rechtsnebenklasse (zu x).

Die Äquivalenzklassen zu der oben definierten Äquivalenzrelation sind wegen

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

genau die Linksnebenklassen. Die Nebenklasse zum neutralen Element ist die Untergruppe H selbst. 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.

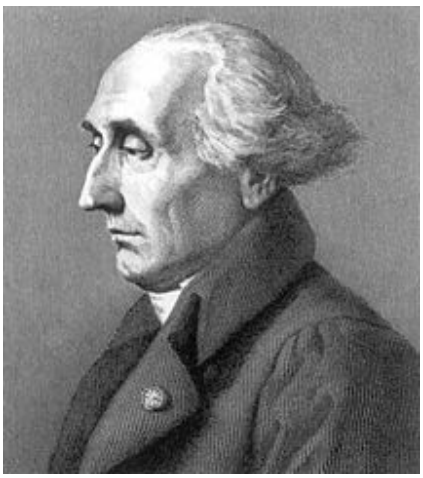
Lemma 46.4. *Es sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Es seien $x, y \in G$ Elemente. Dann sind folgende Aussagen äquivalent.*

(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) $x \sim_H y$.
(7) $xH = yH$.

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 gewissen $h_1, h_2 \in H$. Damit ist $x = yh_2h_1^{-1}$ und (1) ist erfüllt. (4) und (6) sind nach Definition 46.1 äquivalent. Da die Linksnebenklassen die Äquivalenzklassen sind, ergibt sich die Äquivalenz von (5) und (7). □

Der Satz von Lagrange



Joseph-Louis Lagrange (1736 Turin - 1813 Paris)

Definition 46.5. Zu einer endlichen Gruppe G bezeichnet man die Anzahl ihrer Elemente als *Gruppenordnung* oder als die *Ordnung der Gruppe*, geschrieben

$$\operatorname{ord}(G) = \#(G).$$

Mit diesem Begriff kann man sagen, dass die Ordnung einer Untergruppe die Ordnung der Gruppe teilt.

Lemma 46.6. *Es sei G eine endliche Gruppe. Dann besitzt jedes Element $g \in G$ eine endliche Ordnung. Die Potenzen*

$$g^0 = e_G,\ g^1 = g,\ g^2, \ldots, g^{\operatorname{ord}(g)-1}$$

sind alle verschieden.

Beweis. Siehe Aufgabe 46.7. □

Satz 46.7. *Es 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 $gH := \{gh \mid h \in H\}$ für sämtliche $g \in G$. Es ist

$$H \longrightarrow gH,\, h \longmapsto gh,$$

eine Bijektion zwischen H und gH, sodass alle Nebenklassen gleich groß sind (und zwar $\#(H)$ Elemente haben). Die Nebenklassen bilden (als Äquivalenzklassen) zusammen eine Zerlegung von G, sodass $\#(G)$ ein Vielfaches von $\#(H)$ sein muss. □

Korollar 46.8. *Es sei G eine endliche Gruppe und sei $g \in G$ ein Element. Dann teilt die Ordnung von g die Gruppenordnung.*

Beweis. Es sei H die von g erzeugte Untergruppe. Nach Lemma 46.6 ist

$$\operatorname{ord}(g) = \operatorname{ord}(H).$$

Daher teilt diese Zahl nach Satz 46.7 die Gruppenordnung von G. □

Definition 46.9. 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 $H \subseteq G$ eine Untergruppe, so gilt aufgrund des Satzes von Lagrange die einfache *Indexformel*

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

Auch wenn G nicht endlich ist, so sind die verschiedenen Äquivalenzklassen untereinander insofern „ähnlich“, dass es stets eine natürliche bijektive Abbildung

$$H \longrightarrow gH,\, h \longmapsto gh,$$

gibt. Damit gibt es auch eine natürliche bijektive Abbildung zwischen je zwei Äquivalenzklassen.

Normalteiler

Definition 46.10. Es 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 46.11. *Es sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann sind folgende Aussagen äquivalent.*

(1) *H ist ein Normalteiler von G.*
(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). □

Beispiel 46.12. 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 46.13. *Es seien G und H Gruppen und sei*

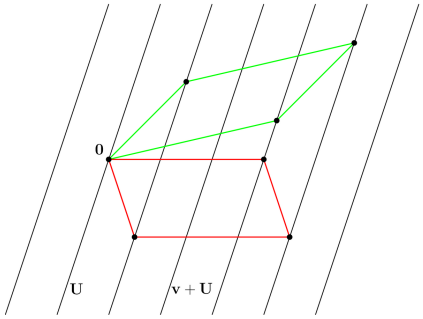
$$\varphi\colon G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann ist der Kern $\operatorname{kern}\varphi$ *ein Normalteiler in G.*

Beweis. Eine Untergruppe liegt aufgrund von Lemma 44.21 vor. Wir verwenden Lemma 46.11. Es sei also $x \in G$ beliebig und $h \in \operatorname{kern}\varphi$. Dann ist

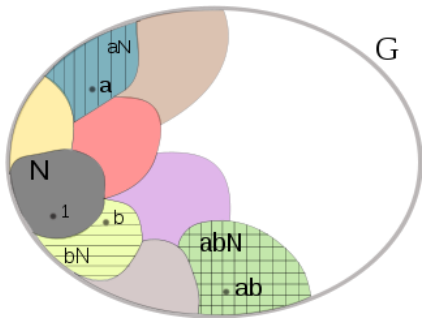
$$\varphi\big(xhx^{-1}\big) = \varphi(x)\varphi(h)\varphi\big(x^{-1}\big) = \varphi(x)e_H\varphi\big(x^{-1}\big) = \varphi(x)\varphi(x)^{-1} = e_H,$$

also gehört xhx^{-1} ebenfalls zum Kern. □



Das Bild zeigt die Äquivalenzklassen zu einem Untervektorraum mit der wohldefinierten Addition auf den Klassen.

Wir zeigen nun umgekehrt, dass jeder Normalteiler sich als Kern eines geeigneten, surjektiven Gruppenhomomorphismus realisieren lässt. Statt $G/\sim_H$ schreibt man einfach G/H.



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

Satz 46.14. *Es 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. □

Definition 46.15. Es sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Die Quotientenmenge

$$G/H$$

mit der aufgrund von Satz 46.14 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 46.16. Die Untergruppen der ganzen Zahlen sind nach Satz 44.3 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.

Abbildungsverzeichnis

Quelle = ParalleleGeradenEbene.png , Autor = Benutzer Mgausmann auf Commons, Lizenz = CC-by-sa 4.0 2

Quelle = Joseph-Louis Lagrange.jpeg , Autor = unbekannt (hochgeladen von Benutzer Katpatuka auf Commons), Lizenz = PD 3

Quelle = ParalleleGeradenEbeneAdditionWohlefiniert.png , Autor = Benutzer Mgausmann auf Commons, Lizenz = CC-by-sa 4.0 6

Quelle = Coset multiplication.svg , Autor = Benutzer Cronholm 144 auf Commons, Lizenz = CC-by-sa 2.5 6

Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von http://commons.wikimedia.org) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren Dateinamen auf Commons angeführt zusammen mit ihrem Autor bzw. Hochlader und der Lizenz. 9

Lizenzerklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 9