Grundlagen der Gruppentheorie: Lagrange-Satz, drei Homomorphismussätze, Cayley-Satz, Poincare-Satz, direkte Produkte. Semidirekte Produkte

Seminarausarbeitung

Ivaylo Dobrikov

Mathematisches Institut
der
Heinrich-Heine-Universität Düsseldorf

Mai 2010

Betreuung: Prof. Dr. Oleg Bogopolski

Inhaltsverzeichnis

1 Grundbegriffe

In diesem Kapitel werden wir uns mit den Grundbegriffen der Gruppentheorie befassen. Bevor wir die erste Definition einführen, möchte ich hiermit folgende Konvention einführen: Für den Begriff einer Gruppe gilt folgende Notation $(G, \circ)$, wobei G eine nichtleere Menge ist und G ist hinsichtlich der Verknüpfung $\circ$ eine Gruppe. Dementsprechend ist man gewöhnt die Operation zwischen zwei Elementen dieser Gruppe $a, b \in G$ mit $a \circ b$ zu bezeichnen. Da wir in der vorliegenden Ausarbeitung ganz oft den Begriff der Gruppe benutzen werden und wir die zugehörige Verknüpfung dieser öfters als Komposition von Elementen aus dieser Gruppe behandeln werden, werde ich auf die Standardnotation verzichten und die Komposition $a \circ b$ zweier Elemente wie folgt schreiben: ab. Ebenfalls eine Gruppe $(G, \circ)$ werde ich hier nur mit G bezeichnen.

Definition 1 (Monoid/Halbgruppe)
Eine nichtleere Menge M heißt *Monoid* oder *Halbgruppe*, wenn gilt:

(M1) $a(bc) = (ab)c$ für alle $a, b, c \in G$, (Assoziativität)

(M2) Es gibt ein Element $e \in M$, so dass $ea = ae = a$ für alle $a \in M$ gilt. (neutrales Element)

Definition 2 (Gruppe)
Eine nichtleere Menge G heißt *Gruppe*, wenn gilt:

(G1) $a(bc) = (ab)c$ für alle $a, b, c \in G$, (Assoziativität)

(G2) Es gibt ein Element $e \in G$, so dass $ea = ae = a$ für alle $a \in G$ gilt, (neutrales Element)

(G3) Zu jedem $g \in G$ gibt es ein $h \in G$, so dass $gh = hg = e$ gilt. (inverses Element)

Bemerkung 3
Insbesondere ist jede Halbgruppe, in der zu jedem Element einen Inversen gibt, eine Gruppe.

Bemerkung 4
In jeder Gruppe gibt es genau ein neutrales Element. Der Inverse eines Elementes g einer Gruppe G ist **eindeutig bestimmt** und wir werden dieses meistens mit g^{-1} bezeichnen.

`Beweis:`
Sei die Gruppe G gegeben und es gebe zwei neutrale Elemente e und e' dieser Gruppe. Dann gilt:

$$\begin{aligned} e &= ee', \text{ nach Eigenschaft des neutralen Elementes } e' \text{ (G3)} \\ &= e'e = e', \text{ nach Eigenschaft des neutralen Elementes } e \end{aligned} \tag{1}$$

Also gibt es nach (1) nur ein neutrales Element in G.
Analog zeigt man die Behauptung, dass es genau ein inverses Element eines Elementes $g \in G$ existiert: Sei e das neutrale Element in G und seien h und h' invers zu g(, d.h. $gh = hg = e$ und $gh' = h'g = e$). Es folgt also:

$$\begin{aligned} h &= he, \text{ nach (G2)} \\ &= h(gh'), \ gh' = e \\ &= (hg)h', \text{ nach (G1)} \\ &= eh', \ hg = e \\ &= h', \text{ nach (G2)} \end{aligned} \tag{2}$$

Aus (2) folgern wir, dass es nur ein inverses Element zu g existiert.

Definition 5 (abelsche Gruppe)
Eine Gruppe G heißt *abelsch*, wenn für alle $g, h \in G$ gilt $gh = hg$.

Definition 6 (Untergruppe)
Eine nichtleere Teilmenge H einer Gruppe G, die das neutrale Element der Gruppe G enthält, heißt *Untergruppe* von G, wenn gilt:

(U1) $gh \in H$ für alle $g, h \in H$, (abgeschlossen unter Gruppenverknüpfung)

(U2) zu jedem $g \in H$ gibt es ein $h \in H$, so dass $gh = hg = e$ gilt. (inverses Element)

Bemerkung 7
Insbesondere ist der Schnitt $\bigcap_{i \in I} H_i$ einer Familie $(H_i)_{i \in I}$ von Untergruppen von einer Gruppe G wieder eine Untergruppe.

Definition 8 (Ordnung einer Gruppe)
Die Kardinalität $\mid G \mid$ einer Halbgruppe bzw. Gruppe G bezechnet man als die *Ordnung* dieser.

$$\text{ord}(G) =\mid G \mid= \begin{cases} n, & \text{wenn } G \text{ } n \text{ Elemente hat.} \\ \infty, & \text{wenn } G \text{ unendlich viele Elemente hat.} \end{cases}$$

Wenn die Ordnung einer Gruppe endlich ist, dann werden wir meistens diese Gruppe als endliche Gruppe bezeichnen.

Definition 9 (Erzeugendensystem)
Sei G eine Gruppe und $S \subset G$ mit $S = \{g_1, ..., g_n\}$. Die Gruppe

$$\langle S \rangle = \{\prod_{i=1}^{n} g_i^{k_i} | k_i \in \mathbb{Z}\}$$

heißt die von S erzeugte Untergruppe von S. Ist $G = \langle S \rangle$, dann heißt G von S erzeugt und S ein *Erzeugendensystem* von G. Die Gruppe G heißt *endlich erzeugt*, wenn es ein endliches Erzeundensystem $\{g_1, ..., g_n\} \subset G$ gibt. In diesem Fall bezeichnen wir diese wie folgt

$$G = \langle g_1, ..., g_n \rangle.$$

Definition 10 (zyklische Gruppe)
Eine Gruppe G heißt *zyklisch*, wenn sie von einem ihrer Elemente erzeugt wird, d.h. wenn es ein $g \in G$ existiert mit $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Bemerkung 11
(1) Jede zyklische Gruppe $G = \langle g \rangle$ ist abelsch, da für alle $m, n \in \mathbb{Z}$ gilt $g^m g^n = g^{m+n} = g^{n+m} = g^n g^m$.
(2) Wenn eine zyklische Gruppe $G = \langle g \rangle$ eine Gruppe bzgl. Addition ist, dann ist $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$.

Beispiel 12
(1) Die additive Gruppe $\mathbb{Z} = \{n \cdot 1 | n \in \mathbb{Z}\}$ wird von dem Element $1 \in \mathbb{Z}$ erzeugt und somit zyklisch.
(2) Für $n \in \mathbb{Z}$ ist die Untergruppe $n\mathbb{Z} \subseteq \mathbb{Z}$ aller ganzzahligen Vielfachen von n zyklisch, da diese von $n \cdot 1$ erzeugt wird.

Definition 13 (Ordnung eines Elementes)
Die Ordnung der von einem Element g einer Gruppe G erzeugten zyklischen Untergruppe $\langle g \rangle$ heißt *Ordnung von* g und wird wie folgt bezeichnet: $\text{ord}(g) =\mid \langle g \rangle \mid$ bzw. $\mid g \mid=\mid \langle g \rangle \mid$.

Satz 14
Sei G eine Gruppe und e das neutrale Element in G.
(i) Die Ordnung von $g \in G$ ist unendlich oder gleich der kleinsten Zahl n mit $g^n = e$.
(ii) Hat $g \in G$ die Ordnung n, dann ist

$$\langle g \rangle = \{e, g, g^2, ..., g^{n-1}\}.$$

`Beweis:`
(1) Die Behauptung zeigen wir erstens für $n \geq 0$. Sei n die kleinste positive ganze Zahl, so dass $g^n = e$. Dann für jedes $m > n$ gilt nach Division mit Rest folgende Gleichung $m = qn + r$, für $q, r \in \mathbb{Z}$ und $0 \leq r < m$. Daraus folgt $q^m = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r$ mit $r < n$. Insbesondere liegt g^r in $\langle g \rangle$ und $g^0 = e$. Daher behaupten wir, dass $\mid \langle g \rangle \mid = n$. Für den Fall, dass $n < 0$ nehmen wir das Element $g^{-n} = (g^n)^{-1}$. Gebe es keine solche Zahl $n \in \mathbb{Z}$, so dass $g^n = e$ ist die Ordnung von $\langle g \rangle$ unendlich, da diese in diesem Fall unendlich viele Elemente besitzt.
(2) Diese Behauptung ist Folgerung der ersten für den endlichen Fall.

Definition 15 (Gruppenhomomorphismus)
Seien G und H zwei Gruppen. Eine Abbildung $\phi : G \to H$ heißt *Gruppenhomomorphismus*, wenn für alle $a, b \in G$ gilt:

$$\phi(ab) = \phi(a)\phi(b).$$

Satz 16
Es seien G und H zwei Gruppen und $\phi : G \to H$ ein Homomorphismus. Und sei $e \in G$ noch das neutrale Element von G. Dann gilt:

(i) $\phi(e)$ ist das neutrale Element von H,

(ii) $\phi(g^{-1}) = \phi(g)^{-1}$ für alle $g \in G$,

(iii) $\phi(g^n) = \phi(g)^n$ für alle $g \in G$ und $n \in \mathbb{Z}$,

(iv) $\text{ord}(\phi(g))$ teilt $\text{ord}(g)$, falls $g \in G$ endliche Ordnung hat.

`Beweis:`
(i) Es gilt $\phi(e) = \phi(ee) = \phi(e)\phi(e)$ und sei e' das neutrale Element in H. Wir ersetzen $\phi(e)$ mit h (nur als Notation, die zwei Bezeichnungen repräsentieren dasselbe Element). Nach der Gleichung gilt, dass $h^2 = h$. Es gilt:

$$\begin{aligned} h = he' = e'h &= (h^{-1}h)h, \ h^{-1} \text{ ist der Inverse zu } h \\ &= h^{-1}(hh), \text{ nach Assoziativgesetz in } H \\ &= h^{-1}h, \ h^2 = h \\ &= e' \end{aligned} \tag{3}$$

Da in jeder Gruppe genau ein neutrales Element (Bemerkung 4) gibt, folgt, dass h und somit $\phi(e)$ das neutrale Element in der Gruppe H ist.
(ii) Sei $g \in G$ und g^{-1} das zu g inverse Element. Es gelten die Gleichungen $\phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ und $\phi(e) = \phi(g^{-1}g) = \phi(g^{-1})\phi(g)$. Weil $\phi(e)$ das neutrale Element in H ist, folgt aus der Eindeutigkeit des Inversen $\phi(g^{-1}) = \phi(g)^{-1}$.
(iii) Die Behauptung zeigen wir durch Induktion für den Fall $n \geq 0$:
Induktionsanfang $(n = 0)$:
In diesem Fall handelt es sich um das neutrale Element, da $g^0 g^n = g^{0+n} = g^n = g^n g^0$, und nach (i) gilt $\phi(g^0) = \phi(g)^0$.
Induktionsschritt $(n \to n + 1)$:
Wenn $\phi(g^n) = \phi(g)^n$ gilt, dann folgt:

$$\begin{aligned} \phi(g^{n+1}) = \phi(g^n g) &= \phi(g^n)\phi(g), \text{ da } \phi \text{ Homomorphismus} \\ &= \phi(g)^n \phi(g), \text{ nach Induktionsannahme} \\ &= \phi(g)^{n+1} \end{aligned} \tag{4}$$

Sei weiterhin $n \geq 0$, dann folgt:

$$\begin{aligned} \phi(g^{-n}) = \phi((g^{-1})^n) &= \phi(g^{-1})^n, \text{ nach (4)} \\ &= (\phi(g)^{-1})^n = \phi(g)^{-n}, \text{ nach Aussage (ii)} \end{aligned} \tag{5}$$

(iv) Die Ordnung von g ist nach Definition die Ordnung der von g erzeugten zyklischen Gruppe $\langle g\rangle$. Da g von endlicher Ordnung n nach Voraussetzung ist, gilt nach Satz 14 (ii) $\langle g\rangle = \{e, g, g^2, ..., g^{n-1}\}$. Der Homomorphismus ϕ bildet jedes g^k mit $0 \leq k \leq n$ nach $\phi(g)^k$ bzw. e', falls $g^k \in \ker(\phi)$ (siehe Definition 18). Daraus folgt

$$|\langle\phi(g)\rangle| = |\langle g\rangle/\ker(\phi)| = \frac{|\langle g\rangle|}{|\ker(\phi)|} \Leftrightarrow |\langle g\rangle| = |\langle\phi(g)\rangle| \cdot |\ker(\phi)|.$$

Infolgedessen teilt die Ordnung von $\phi(g)$ die Ordnung von g.

Definition 17
Seien G und H zwei Gruppen, zwischen den einen Homomorphismus $\phi : G \to H$ gibt.

(i) ϕ heißt ein *Monomorphismus*, wenn ϕ injektiv ist.

(ii) ϕ heißt ein *Epimorphismus*, wenn ϕ surjektiv ist.

(iii) ϕ heißt ein *Isomorphismus*, wenn ϕ injektiv und surjektiv. In dem Fall heißen G und H *isomorph* zueinander.

(iv) Wenn $\phi : G \to G$ ein Homomorphismus ist, heißt ϕ *Endomorphismus*. Wenn ϕ zusätzlich bijektiv ist, heißt ϕ *Automorphismus*.

Definition 18 (Kern, Bild und Urbild eines Homomorphismus)
Seien G und H zwei Gruppen und $\phi : G \to H$ ein Gruppenhomomorphismus. Sei e' das neutrale Element in H. Den Homomorphismus ϕ werden zwei Mengen zugeordnet:

$$\ker(\phi) := \{g \in G \mid \phi(g) = e'\} \subset G,$$

$$\mathrm{im}(\phi) := \{\phi(g) \mid g \in G\} \subset H,$$

Diese heißen *Kern* und *Bild* des Homomorphismus ϕ. Sei zusätzlich K eine Untergruppe von H. Die Menge

$$\phi^{-1}(K) := \{g \in G \mid \phi(g) \in K\}$$

heißt das *Urbild von* K unter dem Homomorphismus ϕ.

Beispiel 19
Sei $K^\star$ die multiplikative Gruppe des Körpers K. Die Abbildung $\phi : GL_n(K) \to K^\star$, die zu jeder invertierbaren Matrix die Derminante zuteilt, ist ein Homomorphismus mit Kern $SL_n(K)$. Wobei $SL_n(K) \leq GL_n(K)$ die Untergruppe aller invertierbaren Matrizen ist, deren Determinante gleich 1 ist. Das Beispiel kann man ganz leicht nachweisen, indem man die multiplikative Eigenschaft der Determinante benutzt.

Lemma 20
Seien G und H zwei Gruppen und $\phi : G \to H$ ein Homomorphismus. Es gilt:

(i) $\ker(\phi)$ ist Untergruppe von G,

(ii) $\mathrm{im}(\phi)$ ist Untergruppe von H.

(iii) Sei K eine Untergruppe der Gruppe H, dann ist das Urbild $\phi^{-1}(K)$ eine Untergruppe von G, die $\ker(\phi)$ beinhaltet.

`Beweis:`
(i) Aus Satz 16 (i) wissen wir, dass $\phi(e) = e'$, und deshalb ist $e \in \ker(\phi)$. Weiterhin seien $g, g' \in \ker(\phi)$, dann gilt $\phi(gg') = \phi(g)\phi(g') = e'e' = e'$. Also ist das Element $gg' \in \ker(\phi)$ und somit ist die Bedingung

(U1) erfüllt. Der zu einem beliebigen Element g aus dem Kern $\ker(\phi)$ gehörige Inverse g^{-1} liegt auch im Kern von ϕ aufgrund der folgenden Gleichung:

$$\begin{aligned} e' &= \phi(e) = \phi(gg^{-1}) \\ &= \phi(g)\phi(g^{-1}), \text{ da } \phi \text{ Homomorphismus} \\ &= \phi(g)\phi(g)^{-1}, \text{ nach Satz 16 (ii)} \\ &= e'\phi(g^{-1}), \ g \in \ker(\phi) \\ &= \phi(g^{-1}) \end{aligned} \tag{6}$$

Infolgedessen ist die zweite Bedingung (U2) erfüllt und hiermit ist $\ker(\phi)$ eine Untergruppe von G.
(ii) Wieder nach Satz 16 (i) gilt $e' \in \text{im}(\phi)$. Da $g, g' \in G$ gilt $\phi(g)\phi(g') = \phi(gg')$ und weil $gg' \in G$, folgt $\phi(g)\phi(g') \in \text{im}(\phi)$. Weiter sei $g \in G$ und g^{-1} der Inverse zu g, dann gilt nach Satz 16 (ii) $\phi(g^{-1}) = \phi(g)^{-1}$ und somit $\phi(g)^{-1} \in \text{im}(\phi)$. Das Element $\phi(g)^{-1}$ ist insbesondere invers zu $\phi(g)$, weil $e' = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g)^{-1}$. Also ist $\text{im}(\phi)$ eine Untergruppe von H.
(iii) Das neutrale Element e liegt in $\phi^{-1}(K)$, da $\phi(e) = e'$ und $e' \in K$. Es gilt noch für alle $x \in \ker(\phi)$ die Gleichung $\phi(x) = e' \in K$. Aus diesem Grund ist $\ker(\phi) \subseteq \phi^{-1}(K)$. Für alle $g, h \in \phi^{-1}(K)$ gilt $\phi(gh) = \phi(g)\phi(h)$ und $\phi(g)\phi(h) \in K$, da K eine Untergruppe ist, deshalb liegt gh ebenfalls in $\phi^{-1}(K)$. Weiter existiert zu jedem $g \in \phi^{-1}(K)$ genau einen Inversen $g^{-1} \in G$. Aus Satz 16 (ii) folgt $\phi(g^{-1}) = \phi(g)^{-1}$ und insbesondere ist $\phi(g)^{-1}$ ein Element in K, da K Untergruppe ist. Also g^{-1} ist ein Inverse, der in $\phi^{-1}(K)$ liegt. Daher ist das Urbild $\phi^{-1}(K)$ eine Untergruppe von G, die $\ker(\phi)$ enthält.

Notation 21
Für einen Homomorphismus $\phi : G \to H$ zweier Gruppen G und H, werden wir das Bild $\text{im}(\phi)$ des Homomorphismus manchmal mit $\phi(G)$ bezeichnen.

2 Lagrange-Satz. Normale Untergruppen und Faktorgruppen

Definition 22 (Links- und Rechtsnebenklassen)
Sei H eine Untergruppe von G. Die Mengen $gH = \{gh \mid h \in H\}$, wobei $g \in G$, heißen *Linksnebenklassen* der Untergruppe H in G. Genauso definiert man die *Rechtsnebenklassen* $Hg = \{hg \mid h \in H\}$ von H in G, wobei $g \in G$.

Lemma 23
Seien g_1, $g_2 \in G$ zwei Elemente aus der Gruppe G und H eine Untergruppe von G. Die Gleichung $g_1H = g_2H$ ist genau dann erfüllt, wenn $g_1^{-1}g_2 \in H$ gilt.

`Beweis:`

($\Rightarrow$): Sei $g_1H = g_2H$ gegeben. Dann gilt für alle $h_1, h_2 \in H$ folgendes:

$$g_1h_1 = g_2h_2 \Leftrightarrow g_1^{-1}g_2h_2 = h_1 \tag{7}$$

Aus (7) folgt, dass $(g_1^{-1}g_2)h_2 \in H$ und da H eine Untergruppe ist (, d.h. abgeschlossen unter Gruppenverknüpfung), gilt nach Definition 6 (U1) $g_1^{-1}g_2 \in H$.

($\Leftarrow$): $g_1^{-1}g_2 \in H$ und es folgt, nach Definition der Nebenklassen, dass

$$g_1^{-1}g_2H = H \Leftrightarrow g_2H = g_1H. \tag{8}$$

Beispiel 24
Alle Linksnebenklassen der Untegruppe $\{e, (12)\}$ der Gruppe S_3 sind

$$\{e, (12)\},\ \{(13), (123)\}\ \{(23), (132)\}$$

und alle Rechtsnebenklassen derselben Untergruppe

$$\{e, (12)\},\ \{(23), (132)\},\ \{(13), (123)\}.$$

Bemerkung 25
(1) Aus dem oberen Beispiel ersehen wir, dass jede zwei verschiedene Nebenklassen disjunkte Mengen sind. Aus dieser Beobachtung kann man für eine Gruppe G folgern, dass jede zwei verschiedene Links- bzw. Rechtsnebenklassen einer Untergruppe H in G disjunkte Mengen sind. Die Behauptung beweist man wie folgt:
Sei H eine Untergruppe von G und $g_1, g_2 \in G$. Wir nehmen an, dass die Linksnebenklassen g_1H und g_2H ein gemeinsames Element enthalten. D.h., dass für $h_1, h_2 \in H$ gilt $g_1h_1 = g_2h_2$. Dann folgt $g_1 = g_2h_2h_1^{-1}$ und somit gilt $g_1H = g_2h_2h_1^{-1}H$ und da $h_2h_1^{-1} \in H$, gilt zusätzlich $g_2h_2h_1^{-1}H = g_2H$, also $g_1H = g_2H$. Analog zeigt man die Behauptung für Rechtsnebenklassen.
(2) Zu jedem Element $g \in G$ einer Gruppe G gibt es nach Definition 2 (G3) ein eindeutiges inverses Element $g^{-1} \in G$ und nach (1) in dieser Bemerkung sind zwei verschiedene Links- bzw. Rechtsnebenklassen disjunkt. Dann ist die Beziehung $gH \leftrightarrow Hg^{-1}$ eins zu eins. Die Behauptung zeigt man wie folgt:
Für $g_1H = g_2H$ ist die Gleichung $g_1h_1 = g_2h_2$ für alle $h_1, h_2 \in H$ erfüllt und es folgen die Äquivalenzen:

$$\begin{aligned} g_1h_1 = g_2h_2 &\Leftrightarrow (g_1h_1)^{-1} = (g_2h_2)^{-1}, \text{ aufgrund der Einduetigkeit der Inversen in } G \\ &\Leftrightarrow h_1^{-1}g_1^{-1} = h_2^{-1}g_2^{-1} \Leftrightarrow h_1^{-1}g_1^{-1}g_2 = h_2^{-1} \end{aligned} \tag{9}$$

Aus (9) folgern wir $Hh_1^{-1}g_1^{-1}g_2 = Hg_1^{-1}g_2 = Hh_2^{-1} = H$ und folglich die Gleichung $Hg_1^{-1} = Hg_2^{-1}$. Aso ist die Beziehung $gH \leftrightarrow Hg^{-1}$ eins zu eins und daraus folgern wir, dass die Anzahl der Linksnebenklassen mit der Anzahl der Rechtsnebenklassen einer Untergruppe H in G übereinstimmt.
(3)Anschließend schließen wir hiermit ab, dass jede Gruppe G die disjunkte Vereinigung der verschiedenen Links- bzw. Rechtsnebenklassen einer Untergruppe H in G ist, seitdem für jedes $g \in G$ gilt $g \in gH$.

Definition 26 (Index)
Die Anzahl der verschiedenen Links- bzw. Rechtsnebenklassen einer Untergruppe H in der Gruppe G heißt der *Index* von H in G und wird mit $\mid G : H \mid$ bezeichnet.

Beispiel 27
Für jede Gruppe G gilt $\mid G : G \mid = 1$ und $\mid G : \{e\} \mid = \mid G \mid$. Aus dem letzten Beispiel folgern wir, dass $\mid S_3 : \{e, (12)\} \mid = 3$.

Theorem 28 (Lagrange)
Sei H eine Untergruppe einer endlichen Gruppe G, dann gilt:

$$\mid G \mid = \mid H \mid \cdot \mid G : H \mid .$$

`Beweis:`
Für jedes $g \in G$ ist die Abbildung

$$H \to gH$$

$$h \mapsto gh, h \in H$$

offensichtlich surjektiv. Diese ist außerdem injektiv, da für alle $gh_1, gh_2 \in gH$ mit $gh_1 = gh_2$ gilt $h_1 = h_2$. Also die Abbildung $H \to gH$ ist eine Bijektion und somit folgt, dass die Kardinalität jeder Linksnebenklasse einer Untergruppe H in G mit der Kardinalität der Untergruppe H übereinstimmt. Daher haben jede zwei verschiedene Linksnebenklassen gleiche Anzahl an Elementen (nämlich $\mid H \mid$) und da die Gruppe G eine disjunkte Vereinigung der verschiedenen Linksnebenklassen der Untergruppe H in G ist (Bemerkung 25 (3)), folgt, dass der Index $\mid G : H \mid$ von H in G mal die Ordnung $\mid H \mid$ der Untergruppe H gleich der Ordnung der Gruppe G ist. Somit folgt die Gleichung $\mid G \mid = \mid H \mid \cdot \mid G : H \mid$.

Folgerung 29
Sei G eine endliche Gruppe. Aus dem Lagrange Theorem folgern wir, dass die Ordnung jeder Untergruppe $H \leq G$ die Ordnung von G teilt.

Lemma 30
Sei G eine endliche Gruppe mit $H_1 \leq H \leq G$. Es gilt $\mid G : H_1 \mid = \mid G : H \mid \cdot \mid H : H_1 \mid$.

Beweis:
Da H_1 Untegruppe von H ist, folgt automatisch, dass H_1 eine Untergruppe von G ist. Nach Lagranges Theorem gelten die Gleichungen $|G| = |H_1| \cdot |G : H_1|$ und $|H| = |H_1| \cdot |H : H_1|$. Es folgt also:

$$|H_1| \cdot |G : H_1| = |G| = |H| \cdot |G : H| = |H_1| \cdot |H : H_1| \cdot |G : H|. \tag{10}$$

Aus (10) folgern wir $|G : H_1| = |G : H| \cdot |H : H_1|$.

Korollar 31
(1) Die Ordnung jedes Elementes einer endlichen Gruppe teilt die Ordnung dieser Gruppe.
(2) Wenn die Ordnung einer Gruppe eine Primzahl p ist, dann ist diese Gruppe isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Beweis:
(1) Sei G eine endliche Gruppe und $g \in G$ ein beliebiges Element. Nach Definition 13 ist die Ordnung von g gleich der Ordnung der Gruppe $\langle g \rangle$, die eine Untergruppe von G nach Definition 9 ist. Nach Lagranges Theorem folgt, dass die Ordnung der Untergruppe $\langle g \rangle$ und somit die des Elementes g die Ordnung von G teilen.
(2) Sei G wieder eine endliche Gruppe. Falls $\text{ord}(G) = p$, wobei p eine Primzahl ist, und falls $g \in G$ mit $g \neq e$, folgt dass die Ordnung dieses nach (1) die Ordnung der Gruppe G teilt. Dies gilt nur dann, wenn $\text{ord}(g) = \text{ord}(\langle g \rangle) = p$, also $G = \langle g \rangle$. Nach Satz 14 (2) ist $\langle g \rangle = \{e, g^1, ..., g^{p-1}\}$ und diese ist insbesondere isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Definition 32
Das Produkt zweier Teilmengen A und B einer Gruppe G ist wie folgt definiert:

$$AB = \{ab \mid a \in A, b \in B\}.$$

Bemerkung 33
Sei G eine Gruppe und $H \leq G$ eine Untergruppe von G. Für ein $g \in G$ stimmt das Produkt $\{g\}H$ mit der Linksnebenklasse gH überein. Und es gilt noch $HH = H$.

Definition 34 (normale Untergruppe)
Sei G eine Gruppe und H eine Untergruppe von G. Die Gruppe H heißt *normal*, wenn für alle $g \in G$ gilt:

$$gH = Hg.$$

Diese bezeichnen wir mit $H \trianglelefteq G$.

Beispiel 35
(1) Das Zentrum $Z(G) = \{z \in G \mid zg = gz \text{ für alle } g \in G\}$ einer Gruppe G ist eine normale Untergruppe von G.
(2) Sei $\phi : G \to H$ ein Homomorphismus zwischen den Gruppen G und H. Dann ist $\ker(\phi)$ eine normale Untergruppe von G.
(3)Sei G eine Gruppe und H eine Untergruppe vom Index 2 von G. Dann ist H eine normale Untergruppe $H \trianglelefteq G$.

Beweis:
(1) Es ist offensichtlich, dass $e \in Z(G)$. Für $z_1, z_2 \in Z(G)$ und für jedes $g \in G$ gilt $(z_1z_2)g = z_1(z_2g) = z_1(gz_2) = (z_1g)z_2 = (gz_1)z_2 = g(z_1z_2)$, also ist $z_1z_2 \in G$ (hiermit ist (U1) erfüllt). Zu jedem $z \in Z(G)$ gibt es ein $z^{-1} \in G$, so dass $zz^{-1} = z^{-1}z = e$. Für alle $g \in G$ gilt $z(z^{-1}g) = (zz^{-1})g = eg = ge = g(zz^{-1}) = (gz)z^{-1} = (zg)z^{-1} = z(gz^{-1})$ und somit folgt, dass $z^{-1} \in Z(G)$. Infolgedessen ist $Z(G)$ eine Untergruppe von G. Weiterhin sei g ein beliebiges Element aus G. Es gilt $gZ(G) = \{gz \in G \mid zh = hz \text{ für alle } h \in G\} = \{zg \in G \mid zh = hz \text{ für alle } h \in G\} = Z(G)g$. Also ist $Z(G)$ eine normale Untergruppe.
(2)Sei e das neutrale Element in G und e' das neutrale Element in H. Dass der Kern von ϕ eine Untergruppe von G ist, haben wir in Lemma 20 (i) gezeigt. Für ein $g \in G$ ist $g^{-1}\ker(\phi)g = \{g^{-1}xg \mid x \in \ker(\phi)\}$. Es gilt für jedes $x \in \ker(\phi)$ die Gleichung $\phi(g^{-1}xg) = \phi(g)^{-1}\phi(x)\phi(g) = \phi(g)^{-1}e'\phi(g) = \phi(g)^{-1}\phi(g) = e'$.

Hiermit folgt, dass $g^{-1}xg \in \ker(\phi)$ und somit $g^{-1}\ker(\phi)g \subset \ker(\phi)$ für jedes $g \in G$. Aus der Gleichung $\ker(\phi) = (gg^{-1})\ker(\phi)(gg^{-1}) = g(g^{-1}\ker(\phi)g)g^{-1} \subset g\ker(\phi)g^{-1}$ folgern wir, dass $\ker(\phi) \subset g^{-1}\ker(\phi)g$ gilt. Infolgedessen gilt $g\ker(\phi)g^{-1} = \ker(\phi)$ und somit $g\ker(\phi) = \ker(\phi)g$ für alle $g \in G$. Daher ist $\ker(\phi)$ eine normale Untergruppe von G.
(3) Für alle $g \in H$ ist $gH = H = Hg$. Da H vom Index 2 von G ist, gibt es genau ein $g \in G \setminus H$, so dass gH bzw. Hg die zweite Links-bzw. Rechtsnebenklasse ist. Weil G die disjunkte Vereinigung der Linksnebenklassen H und gH und gleichzeitig die disjunkte Vereinigung der Rechtsnebenklassen H und Hg ist, folgt, dass $gH = Hg$ und für alle andere $h \in G \setminus \{g\}$ gilt $hH = H = Hh$ und somit ist H normal.

Lemma 36
Sei G eine Gruppe und $H_1, H_2 \leq G$ zwei Untergruppen. Es gilt:

(i) Falls eine der Untergruppen H_1 und H_2 normal ist, dann ist das Produkt H_1H_2 dieser eine Untergruppe von G.

(ii) Falls H_1 und H_2 normal sind, ist das Produkt H_1H_2 eine normale Untergruppe von G.

`Beweis:`
(1) O.B.d.A. nehmen wir an, dass H_1 die normale Untergruppe ist. Das Produkt ist wie folgt definiert $H_1H_2 = \{h_1h_2 \mid h_1 \in H_1, h_2 \in H_2\}$. Das neutrale Element $e \in G$ ist offensichtlich im Produkt H_1H_2 wegen $ee = e$. Für alle $h_1h_2, h_1'h_2' \in H_1H_2$ gilt nach Annahme, dass H_1 normal ist, folgendes:

$$(h_1h_2)(h_1'h_2') = (h_1h_2h_1')h_2' = (h_1h_1'h_2)h_2' = (h_1h_1')(h_2h_2') \in H_1H_2.$$

Somit ist (U1) erfüllt. Zu jedem $h_1h_2 \in H_1H_2$ gibt es genau ein $h_1^{-1}h_2^{-1} \in H_1H_2$ (aufgrund der Eindeutigkeit der Inversen von h_1 und h_2), so dass gilt

$$(h_1h_2)(h_1^{-1}h_2^{-1}) = (h_1h_2h_1^{-1})h_2^{-1} = (h_1h_1^{-1}h_2)h_2^{-1} = e(h_2h_2^{-1}) = ee = e.$$

Die Gleichung $(h_1^{-1}h_2^{-1})(h_1h_2) = e$ zeigt man analog und hiermit ist (U2) erfüllt. Also ist H_1H_2 eine Untergruppe von G.
(2) Weiter sei H_2 zusätzlich auch normale Untergruppe. In diesem Fall gilt für jedes $g \in G$:

$$g(H_1H_2) = (gH_1)H_2 = (H_1g)H_2 = H_1(gH_2) = H_1(H_2g) = (H_1H_2)g.$$

Also ist das Produkt H_1H_2 ebenfalls eine normale Untergruppe von G.

Lemma 37 (Quotientgruppe/Faktorgruppe)
Sei G eine Gruppe und $H \trianglelefteq G$ eine normale Untergruppe von G. Die Menge aller Nebenklassen von H in G charakterisiert eine Gruppe mit der folgenden Verknüpfung:

$$g_1H \cdot g_2H = g_1(Hg_2)H = g_1(g_2H)H = g_1g_2H, \text{ wobei } g_1, g_2 \in G.$$

Diese Gruppe nennen wir die *Quotientgruppe* bzw. *Faktorgruppe* der Gruppe G über der normalen Untegruppe H und bezeichnen diese mit G/H.

`Beweis:`
Für $g_1, g_2, g_3 \in G$ gilt:

$$g_1H(g_2Hg_3H) = g_1H(g_2g_3)H = g_1(g_2g_3)H = (g_1g_2)g_3H = (g_1g_2)g_3HH = (g_1g_2)Hg_3H = (g_1Hg_2H)g_3H.$$

Somit ist (G1) erfüllt. Das neutrale Element ist H, weil $(gH)H = (gH)eH = (ge)HH = gH = Hg$ für alle $g \in G$ gilt. Und letztendlich gibt zu jedem gH ein Hg^{-1}, so dass $(gH)(Hg^{-1}) = gH(g^{-1}H) = g(Hg^{-1})H = g(g^{-1}H)H = (gg^{-1})HH = eH = H$. Also ist die Menge G/H eine Gruppe hinsichtlich der oben angegebenen Verknüpfung.

Beispiel 38
$\mathbb{Z}/n\mathbb{Z}$ ist Faktorgruppe. Insbesondere ist diese zyklisch der Ordnung n, sie wird von $1 + n\mathbb{Z}$ erzeugt.

Bemerkung 39
Sei G eine endliche Gruppe und $H \trianglelefteq G$ eine normale Untergruppe von G. Dann können wir das Lagrange Theorem zu der Gleichung $\mid G \mid = \mid H \mid \cdot \mid G/H \mid$ fortsetzen.

Beispiel 40
(1)Die Untergruppe $K = \{e, (12)(34), (13)(24), (14)(24)\}$ von S_4 ist normal und

$$S_4/K = \{K, (12)K, (13)K, (23)K, (123)K, (132)K\} \cong S_3.$$

(2) Sei H eine normale Untergruppe von der Gruppe G. Die Abbildung $\phi : G \to G/H$ charaktersiert mit $\phi(g) = gH$ ist ein Homomorphismus mit Kern H:
Für alle $g_1, g_2 \in G$ gilt

$$\phi(g_1g_2) = (g_1g_2)H = (g_1g_2)HH = g_1(g_2H)H = g_1(Hg_2)H = (g_1H)(g_2H) = \phi(g_1)\phi(g_2).$$

Falls $h \in H$ gilt: $\phi(h) = hH = H$ und somit $\ker(\phi) = H$.

3 Homomorphismussätze

Notation 41
Sei G eine Gruppe und H eine Untergruppe von G. Mit $L(G, H)$ werden wir die Menge aller Untergruppen von G, die H enthalten, bezeichnen. Insbesondere ist $L(G, \{e\})$ die Menge aller Untergruppen von G.

Lemma 42
Sei $\phi : G \to G_1$ ein Gruppenhomomorphismus. Für jede zwei Teilmengen A, B aus der Gruppe G gilt:

$$\phi(A) = \phi(B) \Leftrightarrow A \cdot \ker(\phi) = B \cdot \ker(\phi).$$

`Beweis:`
Sei e' das neutrale Element in der Grupppe G_1. Wir betrachten die Bilder der Produkte $A \cdot \ker(\phi)$ und $B \cdot \ker(\phi)$. Es gelten die Gleichungen:

$$\begin{aligned} \phi(A \cdot \ker(\phi)) &= \{\phi(ax) \mid a \in A, x \in \ker(\phi)\} \\ &= \{\phi(a)\phi(x) \mid a \in A, x \in \ker(\phi)\} \\ &= \{\phi(a)e' \mid a \in A\} = \{\phi(a) \mid a \in A\} \\ &= \phi(A) \end{aligned} \tag{11}$$

und

$$\begin{aligned} \phi(B \cdot \ker(\phi)) &= \{\phi(bx) \mid b \in B, x \in \ker(\phi)\} \\ &= \{\phi(b)\phi(x) \mid b \in B, x \in \ker(\phi)\} \\ &= \{\phi(b)e' \mid b \in B\} = \{\phi(b) \mid b \in B\} \\ &= \phi(B). \end{aligned} \tag{12}$$

Aus (11) und (12) folgern wir:

$$A \cdot \ker(\phi) = B \cdot \ker(\phi) \Leftrightarrow \phi(A \cdot \ker(\phi)) = \phi(B \cdot \ker(\phi)) \Leftrightarrow \phi(A) = \phi(B).$$

Satz 43
Sei $\phi : G \to G_1$ ein Homomorphismus zwischen den Gruppen G und G_1. Dann gilt:

(i) die Abbildung

$$\begin{aligned} \psi : L(G, \ker(\phi)) &\to L(G_1, \{e\}) \\ H &\mapsto \phi(H), \end{aligned}$$

die eine Untergruppe der ersten Menge nach ihrem Bild unter ϕ schickt, ist eine Bijektion,

(ii) die bijektive Abbildung ψ aus (i) behält die Indizen, d.h. falls $\ker(\phi) \leq H_1 \leq H_2$, dann gilt:

$$|H_2 : H_1| = |\phi(H_2) : \phi(H_1)|,$$

(iii) die bijektive Abbildung ψ aus (i) behält die Normalität, d.h. falls $\ker(\phi) \leq H_1 \leq H_2$, dann gilt:

$$H_1 \trianglelefteq H_2 \Leftrightarrow \phi(H_1) \trianglelefteq \phi(H_2).$$

`Beweis:`
(i) Sei $H_1 \leq G_1$ eine Untergruppe von G_1. Das Urbild $\phi^{-1}(H_1)$ ist nach Lemma 20 (iii) eine Untergruppe von G, die den Kern des Homomorphismus ϕ enthält. Da die Abbildung ψ tatsächlich die Untergruppen der Gruppe G, die $\ker(\phi)$ enthalten, in die Menge aller Untergruppen von G_1 abbildet, folgt, dass diese surjetkiv ist. Weiterhin seien $H, H' \leq G$ Untergruppen von G, die $\ker(\phi)$ beinhalten, dann gilt offensichtlich $H \cdot \ker(\phi) = H$ und $H' \cdot \ker(\phi) = H'$. Nach Lemma 42 gilt, dass $\phi(H) = \phi(H') \Leftrightarrow H \cdot \ker(\phi) = H' \cdot \ker(\phi)$ und nach der letzten Vorüberlegung gilt insbesondere $\phi(H) = \phi(H') \Leftrightarrow H = H'$. Daher ist ψ auch injektiv. ψ ist also bijektiv.
(ii) Wir definieren eine Abbildung mit Definitionsbereich die Menge aller Linksnebenklassen der Untergruppe H_1 in H_2 und Wertebereich die Menge aller Linksnebenklassen von $\phi(H_1)$ in $\phi(H_2)$, die durch die Abbildungsvorschrift $xH_1 \mapsto \phi(x)\psi(H_1)(= \phi(x)\phi(H_1))$ charakterisiert ist. Diese ist surjektiv aufgrund der Bijektivität der Abbildung ψ und injektiv, weil $\phi(xH_1) = \phi(yH_1)$ die Gleichung $xH_1 \cdot \ker(\phi) = yH_1 \cdot \ker(\phi)$ induziert und die letzte nach Lemma 42 die Gleichung $xH_1 = yH_1$ für alle $x, y \in G$. Da es eine Bijektion zwischen der Menge aller Linksnebenklassen der Untergruppe H_1 in H_2 und der Menge aller Linksnebenklassen von $\phi(H_1)$ in $\phi(H_2)$ gibt, folgt, dass diese gleichmächtig sind. Infolgedessen folgern wir $|H_1 : H_2| = |\phi(H_1) : \phi(H_2)|$.
(iii) Da $\ker(\phi)$ eine normale Untergruppe von G ist und diese in H_1 liegt, gelten $H_1 \cdot \ker(\phi) = H_1$ und $x \cdot \ker(\phi) = \ker(\phi) \cdot x$ für alle $x \in G$. Daher gilt für alle $x \in G$:

$$xH_1 = x(H_1 \cdot \ker(\phi)) = (xH_1) \cdot \ker(\phi) = (H_1x) \cdot \ker(\phi) = H_1(x \cdot \ker(\phi)) = H_1 \cdot \ker(\phi)x = H_1x,$$

wenn H_1 normal ist. In diesem Fall kehren wir auf Lemma 42 zurück, das besagt:

$$xH_1 \cdot \ker(\phi) = H_1x \cdot \ker(\phi) \Leftrightarrow \phi(xH_1) = \phi(H_1x).$$

Somit folgt die Äquivalenz $xH_1 = H_1x \Leftrightarrow \phi(x)\phi(H_1) = \phi(H_1)\phi(x)$ für alle $x \in G$ und damit die Behauptung.

Satz 44 (erster Homomorphismussatz)
Sei $\phi : G \to G_1$ ein Homomorphismus zwischen den Gruppen G und G_1, dann gilt:

$$G/\ker(\phi) \cong \mathrm{im}(\phi).$$

`Beweis:`
Sei e' das neutrale Element in G_1. In Beispiel 35 (ii) haben wir nachgewiesen, dass $\ker(\phi)$ eine normale Untergruppe von G ist. Aus diesem Grund ist $G/\ker(\phi)$ die Faktorgruppe mit der Verknüpfung, die in Lemma 37 angegeben ist. Wir definieren die Abbildung $\Phi : G/\ker(\phi) \to \phi(G)$ mit der Abbildungsvorschrift $g \cdot \ker(\phi) \mapsto \phi(g)$. Nach Definition der Abbildung Φ können wir sofort folgern, dass diese surjektiv ist. Für alle $g, h \in G$ gilt:

$$g \cdot \ker(\phi) = h \cdot \ker(\phi) \Leftrightarrow gh^{-1} \in \ker(\phi) \Leftrightarrow \phi(gh^{-1}) = e' \Leftrightarrow \phi(g) = \phi(h) \Leftrightarrow \Phi(g \cdot \ker(\phi)) = \Phi(h \cdot \ker(\phi))$$

und somit folgt, dass die Abbildung Φ injektiv und wohldefiniert ist und dementsprechend bijektiv. Φ ist sogar ein Isomorhpismus, weil für alle $g, h \in G$ gilt:

$$\Phi((g \cdot \ker(\phi))(h \cdot \ker(\phi))) = \Phi(gh \cdot \ker(\phi)) = \phi(gh) = \phi(g)\phi(h) = \Phi(g \cdot \ker(\phi))\Phi(h \cdot \ker(\phi)).$$

Die Gruppen $G/\ker(\phi)$ und $\mathrm{im}(\phi)$ sind also isomorph zueinander.

Satz 45 (zweiter Homomorphismussatz)
Seien A und B zwei normale Untergruppen einer Gruppe G mit $A \leq B$. Es gelten:

$$B/A \trianglelefteq G/A \text{ und } (G/A)/(B/A) \cong G/B.$$

`Beweis:`
Wir definieren die Abbildung $\phi : G/A \to G/B$ mit der Abbildungsvorschrift $gA \mapsto gB$. Insbesondere sind G/A und G/B nach Lemma 37 die Faktorgruppen und die neutrale Elemente dieser sind $eA = A$ und $eB = B$. Die Abbildung ist wohldefiniert und ist ein Homomorphismus, da für alle $g, h \in G$ gilt:

$$\phi((gA)(hA)) = \phi(ghA) = ghB = g(hB)B = g(Bh)B = (gB)(hB) = \phi(gA)\phi(hA).$$

ϕ ist surjektiv und deshalb gilt $\text{im}(\phi) = G/B$. Leicht folgern wir die äquivalente Aussage $gA \in B/A \Leftrightarrow \phi(gA) = gB = B$ und hiermit ist $\ker(\phi) = B/A$. Weil $\ker(\phi)$ nach Beispiel 35 (2) normale Untergruppe von G/A und dieser gleich B/A ist, folgt $B/A \trianglelefteq G/A$. Jetzt wenden wir den ersten Homomorphismussatz auf den Homomorphismus $\phi : G/A \to G/B$ aufgrund der oberen Vorüberlegungen an und folgern wir, dass $(G/A)/(B/A) \cong G/B$.

Satz 46 (dritter Homomorphismussatz)
Es seien H eine normale Untergruppe und B eine Untergruppe einer Gruppe G. Dann gilt:

$$BH/H \cong B/B \cap H.$$

`Beweis:`
Nach Lemma 36 (i) folgern wir sofort, dass BH eine Untergruppe von G ist. Insbesondere ist $B/B\cap H$ auch eine Gruppe. Wir definieren folgende Abbildung $\phi : BH \to B/B\cap H$, die wir mit der Abbildungsvorschrift $bh \mapsto b(B \cap H)$ charakterisieren. Da BH Untergruppe von G ist, folgt, dass $H \trianglelefteq BH$ und trivialerweise $B \cap H \trianglelefteq BH$. Die folgende Gleichung zeigt, dass ϕ ein Homomorphismus für alle $b_1h_1, b_2h_2 \in BH$ ist, indem wir die Normalität der Untergruppen H und $B \cap H$ benutzen:

$$\begin{aligned}\phi((b_1h_1)(b_2h_2)) &= \phi(b_1(h_1b_2)h_2) = \phi(b_1(b_2h_1)h_2) = \phi((b_1b_2)(h_1h_2)) \\ &= (b_1b_2)(h_1h_2)(B \cap H) = b_1(b_2h_1)h_2(B \cap H) = b_1(h_1b_2)h_2(B \cap H) \\ &= (b_1h_1)(b_2h_2)(B \cap H)(B \cap H) = (b_1h_1)(B \cap H)(b_2h_2)(B \cap H) = \phi(b_1h_1)\phi(b_2h_2)\end{aligned} \tag{13}$$

Weiterhin gilt

$$\ker(\phi) = \{bh \in BH \mid b(B\cap H) = (B\cap H)\} = \{bh \in BH \mid b \in B\cap H\} = \{bh \in H \mid b \in B \text{ und } b \in H\} = H$$

und $\text{im}(\phi) = B/B \cap H$, da ϕ offensichtlich surjektiv ist. Wenn wir den ersten Homomorphismussatz auf ϕ anwenden, bekommen wir, dass BH/H isomorph zu $B/(B \cap H)$ ist.

Beispiel 47
(1) Ist B eine Untergruppe und H eine normale Untergruppe einer Gruppe G, so dass BH endlich ist, folgt nach Lemma 36 (i), Bemerkung 39 und dem dritten Homomorphismussatz die Gleichung:

$$\frac{\mid BH \mid}{\mid H \mid} = \mid BH/H \mid = \mid B/B \cap H \mid = \frac{\mid B \mid}{\mid B \cap H \mid}$$

und daraus ergibt sich die Gleichung:

$$\mid BH \mid = \frac{\mid B \mid \cdot \mid H \mid}{\mid B \cap H \mid}.$$

(2) Mithilfe des ersten Homomorphismussatzes kann man nachweisen, dass die Gruppen $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ bis auf Isomorphie die einzigen zyklischen Gruppen sind:

Satz 48
(i) Jede unendliche zyklische Gruppe ist zu der zyklischen Gruppe $\mathbb{Z}$ isomorph.
(ii) Jede endliche zyklische Gruppe der Ordnung n ist zu der zyklischen Gruppe $\mathbb{Z}/n\mathbb{Z}$ isomorph.

Beweis:
(i) Da G eine unendliche zyklische Gruppe, die von $g \in G$ erzeugt wird, gibt es eine surjektive Abbildung $\phi : \mathbb{Z} \to G$ mit der Abbildungsvorschrift $n \mapsto g^n$. Dass ϕ ein Homomorphismus ist, folgt aus $g^m g^n = g^{m+n}$. Weil jedes Element g^n eindeutiges Element in der Gruppe G ist, folgt, dass ϕ sogar wohldefiniert ist und somit ist ϕ ein Isomorphismus.
(ii) Sei G endliche zyklische Gruppe von der Ordnung n. Es existiert wiederum einen surjektiven Homomorphismus $\phi : \mathbb{Z} \to G$. Es gilt $\ker(\phi) = n\mathbb{Z}$ und $\mathrm{im}(\phi) = G$. Daher folgt nach Satz 44 $G \cong \mathbb{Z}/n\mathbb{Z}$.

(3) Für zwei $m, n \in \mathbb{Z}$ sind $m\mathbb{Z}$ und $n\mathbb{Z}$ normale Untergruppen der Gruppe $\mathbb{Z}$. Sei $m > n$, dann existiert ein $r \in \mathbb{Z}$, so dass $m = nr$. Daher gilt $m\mathbb{Z} \leq n\mathbb{Z}$ und nach zweitem Homomorphismussatz gilt, dass $n\mathbb{Z}/m\mathbb{Z} \trianglelefteq \mathbb{Z}/m\mathbb{Z}$ und $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

4 Cayley's Satz und Poincare's Satz

Für jede Menge M werden wir in diesem Kapitel mit $S(M)$ die Gruppe aller Bijektionen von M auf sich selbst bezeichnen. Falls die Kardinalität m der Menge M endlich ist, dann werden wir die Gruppe $S(M)$ mit S_m kennzeichnen.

Satz 49 (Satz von Cayley)
Sei H eine Untergruppe einer Gruppe G und M sei die Menge aller Linksnebenklassen von H in G. Die Abbildung

$$\phi : G \to S(M)$$
$$g \mapsto (xH \mapsto gxH), \text{ für } g, x \in G$$

ist ein Homomorphsmus mit Kern:

$$\ker(\phi) = \bigcap_{x \in G} xHx^{-1}.$$

Beweis:
Nach Assoziativität in G gilt $g_1 g_2 (xH) = g_1(g_2 xH)$ für alle $g_1, g_2, x \in G$. Insbesondere gilt noch

$$\phi(g_1 g_2)(xH) = g_1 g_2 xH = g_1(g_2 xH) = \phi(g_1) \circ \phi(g_2)(xH) \text{ für alle } x \in G$$

und somit $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$. Also ist ϕ ein Homomorphismus mit Kern:

$$\ker(\phi) = \{g \in G \mid xH = gxH \text{ für alle } xH\} = \{g \in G \mid g \in xHx^{-1} \text{ für alle } x \in G\} = \bigcap_{x \in G} xHx^{-1}.$$

Definition 50 (reguläre Darstellung)
Falls $H = \{1\}$ in dem oben angegebenen Satz ist, nennt man den Homomorphismus $\phi : G \to S(M)$ die *reguläre Darstellung* der Gruppe G.

Korollar 51
(i) Die reguläre Darstellung einer Gruppe G ist Einbettung dieser Gruppe G in der Gruppe $S(G)$. Das Bild jedes nichttrivialen Elementes von G unter dieser Einbettung ist eine Permutation, die jedes Element von G nach einem verschiedenen Element von G schickt.
(ii) Daher jede endliche Gruppe G kann in die Gruppe S_m eingebettet werden, wobei $m = \mathrm{ord}(G)$.
(iii) Jede endliche Gruppe G kann in die Gruppe $GL_m(F)$ eingebettet werden, wobei F ein Körper ist und $m = \mathrm{ord}(G)$.

Beweis:
(i) und (ii) gelten aufgrund dem Cayley's Satz.
(iii) Aus der Linearen Algebra wissen wir, dass wir S_m in die Gruppe $GL_m(F)$ einbetten können. Die Abbildungsvorschrift dieser Einbettung ist $\sigma \to A_\sigma$. Dann sind die Matrizen A_σ der Form $(A_\sigma)_{ij} = 1$, falls $\sigma(j) = i$ und $(A_\sigma)_{ij} = 0$, anderenfalls.

Korollar 52 (*Satz von Poincaré*)
Jede Untergruppe H mit endlichem Index m in der Gruppe G enthält eine Untergruppe N, die normal in G ist und endlichen Index k hat, so dass $m \mid k$ und $k \mid (m!)$.

`Beweis:`
Wir ziehen wierder den Homomorphismus ϕ aus dem Cayley's Satz in Betracht. $\ker(\phi)$ ist eine Teilmenge der Untergruppe H, da

$$\ker(\phi) = \bigcap_{x \in G} xHx^{-1} = H \cap (\bigcap_{x \in G \setminus \{e\}} xHx^{-1}) \subseteq H.$$

Nach Beispiel 35 (2) ist $\ker(\phi)$ eine normale Untergruppe von G und somit beinhaltet H eine normale Untergruppe von G. Sei $k =\mid G : \ker(\phi) \mid$. Nach dem ersten Homomorphismussatz gilt $k =\mid \mathrm{im}(\phi) \mid$ und weil $\mathrm{im}(\phi)$ Untergruppe von S_m ist, gilt $k \mid (m!)$. Also k ist endlicher Index, der die Ordnung von der symmetrischen Gruppe S_m teilt. Aus den Relationen $\ker(\phi) \leq H \leq G$ gilt nach Lemma 30

$$\mid G : \ker(\phi) \mid =\mid G : H \mid \cdot \mid H : \ker(\phi) \mid \Leftrightarrow k = m \cdot t.$$

Also gilt noch $m \mid k$.

5 Direkte Produkte von Gruppen

Definition 53 (direkte Produkte von Gruppen)
Seien $G_1, ..., G_n$ Gruppen. Die Menge $G = G_1 \times ... \times G_n$ der Sequenzen $(g_1, ..., g_n)$ für $g_i \in G_i$ ist eine Gruppe bezüglich der Multiplikation

$$(g_1, ..., g_n) \cdot (g'_1, ..., g'_n) = (g_1 g'_1, ..., g_n g'_n).$$

Diese Gruppe G heißt das *direkte Produkt* der Gruppen $G_1, ..., G_n$ mit neutralem Element $(e_1, ..., e_n)$, wobei e_i das neutrale Element in G_i für $1 \leq i \leq n$.

Lemma 54
Sei die Gruppe $G = G_1 \times ... \times G_n$ das direkte Produkt der Gruppen $G_1, ..., G_n$. Die Mengen $U_i = \{e_1, ..., e_{i-1}, g, e_{i+1}, ..., e_n \mid g \in G_i\}$ sind Untergruppen von G isomorph zu G_i. Es gelten:

$$G = \langle \bigcup_{j=1}^{n} U_j \rangle, \tag{14}$$

$$U_i \trianglelefteq G, \tag{15}$$

$$U_i \cap \langle \bigcup_{j \neq i} U_j \rangle = \{e\} \text{für alle } i. \tag{16}$$

Satz 55
Sei G eine Gruppe und seien $U_1, ..., U_n$ Untergruppen von G, so dass die Bedingungen (14), (15) und (16) erfüllt sind. Dann gilt $G \cong U_1 \times ... \times U_n$ und wir sagen, dass G das direkte Produkt der Untergruppen $U_1, ..., U_n$ ist.

`Beweis:`
Seien $a \in U_i$, $b \in U_j$ mit $i \neq j$. Nach (15) und (16) gilt $a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in U_i \cap U_j = \{e\}$ und hiermit folgt $ab = ba$. Nach (14) kann jedes Element $g \in G$ als Produkt $g = u_1...u_n$ von $u_i \in U_i$ repräsentiert werden. Die Darstellung von g mit den $u_i \in U_i$ ist wohldefiniert:
Sei $g = u'_1...u'_n$ weitere Darstellung mit $u'_i \in U_i$. Aufgrund der schon gezeigten Kommutativität gilt $(u'_1)^{-1}u_1 = u_2^{-1}u'_2...u_n^{-1}u'_n$ und nach (16) folgt die Äquivalenz $(u'_1)^{-1}u_1 = e \Leftrightarrow u_1 = u'_1$. Analog zeigt man mithilfe der Kommutaitvität zwichen u_i und u_j mit $i \neq j$, dass $u_i = u'_i$ für alle $i = 2...n$.
Anhand der Wohldefiniertheit und (14) kann man einen Isomorphismus $\phi : G \to U_1 \times ... \times U_n$ mit der Abbildungsvorschrift $g \mapsto (u_1, ..., u_n)$ angeben, wobei $g = u_1...u_n$ mit $u_i \in U_i$.

Beispiel 56
Jede Gruppe der Ordnung 6 ist isomorph zu $\mathbb{Z}/6\mathbb{Z}$ oder zu der symmetrischen Gruppe S_3.

`Beweis:`
Sei G eine Gruppe der Ordnung 6. Die Gruppe G hat die Ordnung $\mid G \mid = 3^1 2$. Seien H die 2-Sylowgruppe und F die 3-Sylowgruppe von G. Offensichtlich ist F die einzige 3-Sylowgruppe, deshalb gilt $F \trianglelefteq G$. In dem Fall, dass die 2-Sylowgruppe H normal ist, gilt nach Konstruktion des direkten Produktes $G \cong H \times F \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. Anderenfalls, wenn $H \ntrianglelefteq G$, folgt $\bigcap_{x \in G} xHx^{-1} = \{1\}$ und hiermit nach Cayley's Satz die Isomorphie $G \cong S_3$.

6 Semidirekte Produkte von Gruppen

Wir bezeichnen mit $Aut(K)$ die Menge aller Automorphismen einer Gruppe K auf sich selbst. Diese ist insbesondere eine Gruppe. Für ein $x \in H$ in der Gruppe H sagen wir, dass x auf der Gruppe K operiert, wenn diesem einen Automorphismus aus der Gruppe $Aut(K)$ zugeordnet wird. Und wir sagen, eine Gruppe H operiert auf einer Gruppe K, wenn die Operation jedes Elementes $x \in H$ auf der Gruppe K ein Automorphismus ist. Sei $\tau : H \to Aut(K)$ der Gruppenhomomorphismus, der den Elementen der Gruppe H Automorphismen aus $Aut(K)$ zuordnet. Mit τ_x werden wir den dem x zugeordneten Automorphismus mit der Abbildungsvorschrift $u \mapsto u^x$ bezeichnen, wobei u^x das Element $\tau_x(u) \in K$ bezeichnet.

Definition 57 (semidirektes Produkt)
Seien H und K zwei Gruppen. Die Gruppe

$$G := \{(u, x) \mid u \in K, x \in H\}$$

mit der Verknüpfung

$$(u, x)(v, y) := (uv^{x^{-1}}, xy)$$

für alle $(u, x), (v, y) \in G$ heißt das *semidirekte Produkt* der Gruppen H und G. Wir werden dieses wie folgt bezeichnen: $G = K \rtimes H$.

`Beweis:`
Hier werden wir kurz nachweisen, dass G eine Gruppe bezüglich der oben definierten Verknüpfung ist. Es gilt die Gleichung

$$(vw^{y^{-1}})^{x^{-1}} = v^{x^{-1}} w^{y^{-1}x^{-1}} \tag{17}$$

und daher die Assoziativität der Gruppe G für alle $(u, x), (v, y), (w, z) \in G$:

$$\begin{aligned}(u, x)((v, y)(w, z)) &= (u, x)(vw^{y^{-1}}, yz) = (u(vw^{y^{-1}})^{x^{-1}}, xyz) \\ &= (uv^{x^{-1}} w^{y^{-1}x^{-1}}, xyz) = (uv^{x^{-1}}, xy)(w, z) \\ &= ((u, x)(v, y))(w, z).\end{aligned} \tag{18}$$

Das neutrale Element ist $(1, 1)$:

$$\begin{aligned}(u, x)(1, 1) &= (u1^{x^{-1}}, x) = (u, x) \\ (1, 1)(u, x) &= (1u^1, v) = (u, x).\end{aligned} \tag{19}$$

Und zu jedem $(u, x) \in G$ gibt es eindeutigen Inversen $(u, x)^{-1} = ((u^x)^{-1}, x^{-1})$ mit:

$$\begin{aligned}(u, x)((u^x)^{-1}, x^{-1}) &= (u((u^x)^{-1})^{x^{-1}}, xx^{-1}) \\ &= (u(u^{-xx^{-1}}), xx^{-1}) = (uu^{-1}, 1) = (1, 1)\end{aligned} \tag{20}$$

$$((u^x)^{-1}, x^{-1})(u, x) = ((u^x)^{-1}u^{x^1}, x^{-1}x) = (1, 1).$$

Bemerkung 58
Für zwei Gruppen H und K enthält das semidirekte Produkt $G = K \rtimes H$ Untergruppen $H^* = \{(1,x)|x \in H\}$ und $K^* = \{(u,1)|u \in K\}$, die zu H und K isomorph sind. Die Isomorphismen zwischen H^* und H, sowie K^* und K sind durch die Abbildungsvorschriften $(1,x) \mapsto x$ und $(u,1) \mapsto u$ gegeben. Dementsprechend gilt $G = K^*H^*$ und $K^* \cap H^* = \{1\}$. Insbesondere ist K^* normal in G, weil für alle $(u,1) \in K^*$ und $(v,y) \in G$ gilt:

$$\begin{aligned}(v,y)(u,1)(v,y)^{-1} &= (vu^{y^{-1}},y)((v^y)^{-1},y^{-1}) \\ &= (vu^{y^{-1}},y)((v^{-y}),y^{-1}) \\ &= (vu^{y^{-1}}(v^{-y})^{y^{-1}},yy^{-1}) = (vu^{y^{-1}}v^{-1},1) \in K.\end{aligned} \tag{21}$$

Die Operation der Untergruppe H^* auf K^* mit Konjugation ist identisch mit der ursprünglichen Operation der Gruppe H auf K:

$$(1,x)(u,1)(1,x)^{-1} = (u^x,x)(1,x^{-1}) = (u^x,xx^{-1}) = (u^x,1) \text{ für alle } x \in H \text{ und } u \in K. \tag{22}$$

Lemma 59
Seien K und H zwei Gruppen. Das direkte Produkt $K \times H$ dieser ist ein besonderer Fall des semidirekten Produktes.

`Beweis:`
Die Verknüpfung des semidirekten Produktes $K \rtimes H$ ist wie folgt definiert:

$$(u,x)(v,y) = (uv^{x^{-1}},xy) \tag{23}$$

für alle $(u,x),(v,y) \in K \rtimes H$. Falls die Gruppe der Automorphismen $Aut(K)$ auf K die triviale Gruppe ist, d.h. $Aut(K)$ besteht nur aus dem identischen Automorphismus, folgt, dass für alle $v \in K$ und $x \in H$ gilt $v^{x^{-1}} = v$ und somit ist die Verknüpfung (23) des semidirekten Produktes $K \rtimes H$ die Verknüpfung des direkten Produktes $K \times H$, nämlich:

$$(u,x)(v,y) = (uv,xy).$$

Satz 60
Sei G eine Gruppe und K und H Untergruppen von G mit $K \trianglelefteq G$, $G = KH$ und $K \cap H = \{1\}$. Dann gilt $G \cong K \rtimes H$, wobei die Operation von H auf K die Konjugation in G ist.

`Beweis:`
Nach Bemerkung 58 ist die Operation der Gruppe H^* auf K^* mit Konjugation identisch mit der üblichen Operation der Gruppe H auf K(siehe Gleichung (22)), deshalb gilt hier, dass die Konjugation in G die Operation von H auf G ist, d.h. $u^x = x^{-1}ux$. Sei g ein beliebiges Element in G. Nach Voraussetzung ist $G = KH$ und somit kann g als Produkt zweier Elemente $u \in K$ und $x \in H$ geschrieben werden. Dieses ist wohldefiniert: Gebe es weitere $v \in K$ und $y \in H$ mit $g = vy$, gilt die Äquivalenz $ux = vy \Leftrightarrow v^{-1}u = yx^{-1}$. Da $K \cap H = \{1\}$ folgt, dass die Gleichungen $v^{-1}u = 1$ und $yx^{-1} = 1$ gelten und somit folgt $v = u$ und $y = x$. Daher ist das Produkt ux des Elementes g eindeutig und folglich jedes Elementes $g \in G$. Aufgrund der Wohldefiniertheit kann man eine bijektive Abbildung $\phi : G \to K \rtimes H$ mit der Abbildungsvorschrift $g \mapsto (u,x)$ angeben, wobei $g = ux$ für $u \in K$ und $x \in H$. Die Abbildung ϕ ist zusätzlich ein Homomorphismus, da für alle $g_1, g_2 \in G$ mit $g_1 = ux$ und $g_2 = vy$ gilt:

$$\begin{aligned}\phi(g_1g_2) &= \phi((ux)(vy)) = \phi(uxv(x^{-1}x)y) \\ &= \phi((uxvx^{-1})(xy)) = (u(xvx^{-1}),xy) \\ &= (uv^{x^{-1}},xy) = (u,x)(v,y) = \phi(g_1)\phi(g_2),\end{aligned} \tag{24}$$

wobei $u,v \in K$ und $x,y \in H$. Infolgedessen ist ϕ ein Isomorphismus und somit $G \cong K \rtimes H$.

Literatur

[Bog08] Oleg Bogopolski. *Introduction to group theory.* European Math. Society Publishing House, 2008.

[Lan02] Serge Lang. *Algebra.* Springer Science+Business Media Inc., 2002.

[Mey80] Kurt Meyberg. *Algebra 1.* Carl Hanser Verlag, 1980.

[uBM96] John D. Dixon und Brian Mortimer. *Permutation Groups.* Springer, 1996.