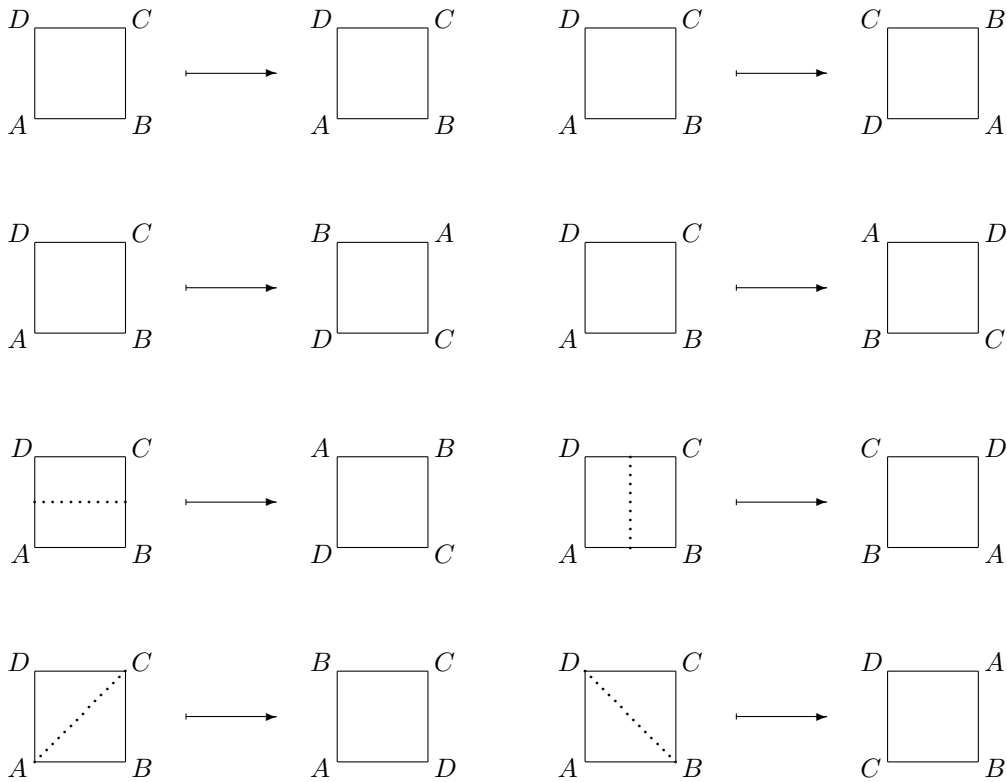


# 1 Kurze Einführung in die Gruppentheorie

## 1.1 Gruppen. Homomorphismen. Untergruppen

**Motivation:** Der Gruppenbegriff ist eine Mathematisierung des Phänomens der Symmetrie.

**Beispiel:** Die Gruppe der winkel- und längenerhaltenden Abbildungen des Quadrates auf sich. Die ersten vier Bilder beschreiben Drehungen, die letzten vier Spiegelungen an den gestrichelten Achsen:



**Historisches:** Die Anfänge der expliziten Theorie der abstrakten Gruppen gehen auf CAYLEY, GALOIS und ABEL zurück.

**Definition 1** (die schwache Variante):

Eine Gruppe ist eine nicht leere Menge  $G$  zusammen mit einer Abbildung  $\mu : G \times G \rightarrow G, (x, y) \mapsto \mu(x, y) =: x \cdot y =: xy$ , so daß folgende Eigenschaften erfüllt sind:

- (Ass) Für alle  $x, y, z \in G$  ist  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$   
(Assoziativgesetz)
- (Lneut) Es gibt ein  $e \in G$ , so daß  $e \cdot x = x$  für alle  $x \in G$ .  
(Existenz eines linksneutralen Elementes)
- (Linv) Zu jedem  $x \in G$  gibt es ein  $x' \in G$  mit  $x' \cdot x = e$ .  
(Existenz eines Linksinversen)

Eine Gruppe heißt *kommutativ* oder *abelsch*, wenn noch gilt:

- (Komm)  $xy = yx$  für alle  $x, y \in G$ .

**Bemerkung 1** (verallgemeinertes Assoziativ- und Kommutativgesetz):

Aus (Ass) folgt, daß der Wert eines Produktes von mehreren Faktoren nicht von der Klammerung abhängt.

**Übung:** Formulieren Sie diese Aussage präzise und geben Sie einen Beweis.

**Folgerung:** Für Tupel  $x_1, x_2, \dots, x_n$  von Elementen in  $G$  ist das Produkt  $x_1 \cdot x_2 \cdot \dots \cdot x_n$  wohldefiniert.

**Verallgemeinerung** von (Komm): Gilt (Komm), ist  $x_1, \dots, x_n$  ein Tupel von Elementen aus  $G$ , und ist  $\sigma \in S_n$  (s. Beispiel (6) unten) eine Permutation, so gilt

$$x_{\sigma(1)} \cdot x_{\sigma(2)} \cdot \dots \cdot x_{\sigma(n)} = x_1 \cdot x_2 \cdot \dots \cdot x_n.$$

**Tatsache 1.**

Sei  $G$  (mit Verknüpfung) eine Gruppe, und sei  $e \in G$  wie in (Lneut). In  $G$  gilt:

- (1)  $x' \cdot x = e \implies x \cdot x' = e$ .  
In Worten: Das zu  $x$  linksinverse Element  $x'$  ist auch rechtsinvers.
- (2)  $xe = x$  für alle  $x \in G$ .  
In Worten: Das linksneutrale Element  $e$  ist auch rechtsneutral.
- (3) Das  $e$  in (Lneut) ist eindeutig bestimmt.  
Zu  $x \in G$  ist das  $x'$  mit  $x' \cdot x = e (= x \cdot x'$  nach (1)) eindeutig bestimmt.

**Beweis:** (1) Sei  $x' \cdot x = e$  und sei  $x'' \in G$  mit  $x'' \cdot x' = e$  (gemäß (Lneut)).

Dann:  $x'' \cdot e = x$  (\*).

Denn:  $x'' \cdot e \underset{\text{Vor}}{=} x'' \cdot (x' \cdot x) \underset{(\text{Ass})}{=} (x'' \cdot x') \cdot x \underset{\text{Vor}}{=} e \cdot x \underset{(\text{Lneut})}{=} x$ .

(**Hinweis:** In dieser Gleichungskette haben wir das Assoziativgesetz explizit benutzt. In Zukunft werden wir das stillschweigend tun und Klammerungen meist weglassen.)

Daraus:  $e = x'' \cdot x' = x'' e x' \underset{(*)}{=} x x'$ .

(2)  $x e \underset{(\text{Linv})}{=} x \cdot x' \cdot x \underset{(1)}{=} e x \underset{(\text{Lneut})}{=} x$

(3) Auch  $e'$  möge (Lneut) erfüllen. Dann:  $e' \underset{(2)}{=} e' \cdot e \underset{(\text{Lneut})}{=} e$   
für  $e'$

Sei  $x' \cdot x = e = x'' \cdot x$ . Von rechts mit  $x'$  multipliziert:

$x' x \cdot x' = x'' x x'$ . Nach (1):  $x' e = x'' \cdot e$  und nach (2):  $x' = x''$ .

Als **Folgerung: Definition** einer Gruppe (scharfe Variante).

Eine Menge  $G$  mit Verknüpfung ist genau dann eine Gruppe, wenn gilt:

- (Ass) Assoziativgesetz
- (Neut) Es gibt  $e \in G$  mit  $ex = xe = x$  für alle  $x \in G$ .  
(Existenz eines neutralen Elementes)
- (Inv) Zu jedem  $x \in G$  gibt es ein  $x' \in G$  mit  $x'x = x \cdot x' = e$   
(Existenz eines Inversen)

**Beweis:** Aus Tatsache 1

**Bezeichnung 1:**

Für das Element  $e$ , das *neutrale Element*, dessen Existenz das Axiom (Neut) sichert, schreiben wir in Zukunft  $1_G$  oder auch nur  $1$ .

Für das zu  $x$  eindeutig definierte Element  $x'$  mit  $x'x = xx' = 1$  schreiben wir  $x^{-1}$ ;  $x^{-1}$  heißt das Inverse zu  $x$ .

**Tatsache 2.**

In einer Gruppe  $G$  gelten:

- (1) Die sogenannten (Links-, und Rechts-) *Kürzungsregeln*:  
 $xy = xy' \iff y = y'$   
 $yx = y'x \iff y = y'$
- (2)  $(xy)^{-1} = y^{-1}x^{-1}$  (beachte die Änderung der Reihenfolge)
- (3)  $(x^{-1})^{-1} = x$

**Beweis:** (1) Von links bzw. von rechts mit  $x^{-1}$  (in der anderen Richtung mit  $x$ ) multiplizieren.

(2) Nachrechnen.

(3)  $(x^{-1})^{-1}x^{-1} = e = x \cdot x^{-1}$ . Dann Rechtskürzungsregel.

**Bemerkung 2 und Bezeichnung 2** Aus den Kürzungsregeln folgt:

Für jedes  $x \in G$  sind die Abbildungen  $l_x : G \rightarrow G, g \mapsto xg$ , und  $r_g : G \rightarrow G, g \mapsto gx$ , Bijektionen mit  $l_{x^{-1}}$  bzw.  $r_{x^{-1}}$  als Umkehrabbildungen.

$l_x$  heißt Linkstranslation und  $r_x$  Rechtstranslation mit  $x$ .

**Beispiele** von Gruppen:

- 1)  $\{1\}$  mit dem einzig möglichen Produkt ist eine Gruppe.  
 $\{1, -1\}$  mit 1 als neutralem Element und der Vorschrift  $(-1) \cdot (-1) = 1$  ist eine Gruppe.
- 2) Die ganzen Zahlen und die reellen Zahlen, jeweils mit der Addition, sind Gruppen.
- 3) Die positiven reellen Zahlen mit der Multiplikation.
- 4) Die komplexen Zahlen vom Betrag 1 mit der Multiplikation.
- 5) Das Beispiel bei der Motivation. Das Produkt ist das Hintereinanderschalten von Abbildungen. ("Gruppe der Isometrien des Quadrates")
- 6) Die Menge der bijektiven Abbildungen einer Menge auf sich mit der Hintereinanderschaltung. Man nennt diese Gruppe die symmetrische Gruppe von  $X$ , bezeichnet mit  $S(X)$ . Ist  $X = \{1, 2, \dots, n\} =: \underline{n}$ , so schreibt man  $S_n := S(\underline{n})$  und nennt diese Gruppe die *symmetrische Gruppe* in  $n$  Elementen.

Von den Beispielen sind 1) - 4) abelsch, 5) nicht und 6) nicht, falls die Menge mehr als zwei Elemente hat.

Mit  $G$  ist in Zukunft immer eine Gruppe gemeint.

**Definition 2.**

Eine Abbildung  $f : G \rightarrow H$  zwischen Gruppen heißt *Homomorphismus*, wenn  $f(xy) = f(x) \cdot f(y)$  für alle  $x, y \in G$ . Der *Kern* von  $f$  ist definiert als

$$\text{Kern } f := f^{-1}(1_H)$$

Ein bijektiver Homomorphismus heißt *Isomorphismus*.

Ein Isomorphismus von  $G$  nach  $G$  heißt *Automorphismus*.

**Beispiele:**

7)  $\mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto nx$  für ein vorgegebenes  $n$  ist ein Homomorphismus.

8)  $\exp : (\mathbb{R}, +) \mapsto (\mathbb{R}^+, \cdot)$  ist ein Isomorphismus.

9) Seien  $X, Y$  Mengen und  $\alpha : X \rightarrow Y$  eine Bijektion. Dann ist

$$\Phi_\alpha : S(Y) \rightarrow S(X), \tau \mapsto \alpha^{-1} \circ \tau \circ \alpha,$$

ein Isomorphismus.

Zum Beweis:  $\Phi_\alpha$  ist Homomorphismus und  $\Phi_{\alpha^{-1}} : S(Y) \rightarrow S(X), \sigma \mapsto \alpha \circ \sigma \circ \alpha^{-1}$ , ist die Umkehrabbildung.

**Tatsache 3.**

Sei  $f : G \rightarrow H$  ein Homomorphismus zwischen zwei Gruppen, und  $1_G$  bzw.  $1_H$  seien die neutralen Elemente von  $G$  bzw.  $H$ . Dann gilt:

- (i)  $f(1_G) = 1_H$ .
- (ii)  $f(x^{-1}) = f(x)^{-1}$  für alle  $x \in G$ .
- (iii)  $f$  ist injektiv  $\iff f^{-1}(\{1_H\}) = \{1_G\}$ .
- (iv) Ist  $f : G \rightarrow H$  ein Isomorphismus, so ist auch  $f^{-1} : H \rightarrow G$  ein Homomorphismus und somit ein Isomorphismus.

**Beweis:** (i), (ii), (iv) als Übung.

(iii) Interessant ist nur die Richtung " $\Leftarrow$ ": Seien  $x, y \in G$  und sei  $f(x) = f(y)$ . Dann  $f(xy^{-1}) = f(x)f(y)^{-1} = 1_H$ . Also ist  $xy^{-1} = 1_G$ , folglich  $x = (y^{-1})^{-1} = y$ .

**Tatsache 4.** Sei  $y \in G$ . Dann ist die Abbildung  $f_y : G \rightarrow G, x \mapsto yxy^{-1}$  ein Automorphismus von  $G$ .

**Beweis:**  $y(x \cdot z)y^{-1} = (yxy^{-1})(yzy^{-1})$  und  $f_y$  ist eine Bijektion mit  $f_{y^{-1}}$  als Umkehrabbildung.

**Definiton 3.**

Sei  $\alpha : G \rightarrow G$  ein Automorphismus. Gibt es  $y \in G$ , so daß  $\alpha = f_y$ ,  $f_y$  wie in Tatsache 4, so heißt  $\alpha$  ein *innerer Automorphismus* von  $G$ . Man nennt  $f_y = \alpha$  dann auch die *Konjugation mit  $y$* .

**Übungen und Bezeichnungen:**

- 1) Gib eine Gruppe  $G$  und einen Automorphismus  $\alpha : G \rightarrow G$  an, der kein innerer Automorphismus ist.

- 2) Sind  $f : G \rightarrow H$  und  $y : H \rightarrow K$  Homomorphismen, so ist auch  $g \circ f$  ein Homomorphismus. Die Menge der Automorphismen von  $G$  bilden eine Gruppe.
- 3) Sei  $M$  eine Menge von Gruppen. Die Relation auf  $M$

$$"G \cong H \iff \text{es gibt einen Isomorphismus von } G \text{ nach } H"$$

ist eine Äquivalenzrelation auf  $M$ . Zwei Gruppen  $G, H$  mit  $G \cong H$  heißen *isomorph!*

**Bezeichnung 2** (die sogenannte "Komplex-Schreibweise"):

Seien  $A_1, \dots, A_k$  Untermengen der Gruppe  $G$ . Dann bezeichnen wir mit  $A_1 \cdot A_2 \cdots A_k$  oder auch  $A_1 A_2 \cdots A_k$  die Untermenge

$$\{a_1 a_2 \cdots a_k \mid a_i \in A_i \text{ für } i = 1, \dots, k\}$$

von  $G$ . Für einpunktige Mengen  $A_i = \{a_i\}$  schreiben wir in  $A_1 A_2 \cdots A_k$  auch  $a_i$  anstelle von  $A_i$ , z.B. schreiben wir  $x A$  anstelle von  $\{x\} \cdot A$ .

Bemerke: Ist  $A_i = \emptyset$  für ein  $i$ , so ist  $A_1 A_2 \cdots A_k = \emptyset$

**Definition 4.**

$H \subset G$  heißt *Untergruppe* von  $G$ , wenn  $H \cdot H \subset H$  ist und wenn die Einschränkung  $H \times H \rightarrow H$ ,  $(h_1, h_2) \mapsto h_1 \cdot h_2$ , der Multiplikation von  $G$  eine Gruppenstruktur auf  $H$  definiert.

Schreibweise für Untergruppen:  $H < G$ .

**Tatsache 5** ("Untergruppenkriterium"):

Für  $H \subset G$  sind folgende Aussagen äquivalent:

- (i)  $H$  ist Untergruppe.
- (ii)  $1_G \in H$  und für alle  $x, y \in H$  sind  $x \cdot y \in H$  und  $x^{-1} \in H$ .
- (iii)  $H \neq \emptyset$  und für alle  $x, y \in H$  ist  $x \cdot y^{-1} \in H$ .

**Beweis:** Übung

**Beispiele:**

10)  $n \cdot \mathbb{Z} \subset \mathbb{Z}$ .

$\mathbb{Q} \subset \mathbb{R}$  und  $\{1, -1\}$  im Beispiel 4) sind jeweils Untergruppen.

- 11) Die vier Drehungen in der oberen Reihe des Motivationsbeispiels bilden eine Untergruppe der Gruppe der Isometrien des Quadrats.

**Tatsache 6.**

Sei  $(H_i)_{i \in I}$  eine Familie von Untergruppen von  $G$ . Dann ist  $\bigcap_{i \in I} H_i = H$  eine Untergruppe von  $G$ .

**Beweis:**  $1_G \in \bigcap_{i \in I} H_i$  und mit  $x, y \in H_i$  für alle  $i$  ist auch  $xy^{-1} \in H_i$  für alle  $i$ .

**Definition 5.**

Sei  $H$  Untergruppe von  $G$ . Die Untermengen von  $G$  der Gestalt  $xH$ ,  $x \in G$ , heißen die *Linksnebenklassen* oder *Linksrestklassen* von  $H$  in  $G$ .

Die Untermengen der Gestalt  $Hx$ ,  $x \in G$ , heißen *Rechtsnebenklassen*.

Die Untermengen der Gestalt  $HxH$ ,  $x \in G$ , heißen *Doppelnebenklassen* von  $H$  in  $G$ .  
(Im Englischen: Nebenklasse  $\equiv$  coset.)

**Bezeichnung 3:** Mit  $G/H$  wird die Menge der Linksnebenklassen, mit  $H \backslash G$  die Menge der Rechtsnebenklassen und mit  $H \backslash G/H$  die Menge der Doppelnebenklassen von  $H$  in  $G$  bezeichnet.

**Tatsache 7.**

Für eine Untergruppe  $H$  von  $G$  gilt:

- (i)  $xH = yH \iff y^{-1}x \in H$
- (ii) Die Menge  $\{xH \mid x \in G\}$  der Linksnebenklassen bildet eine Zerlegung von  $G$  in paarweise disjunkte Teilmengen.

Entsprechendes gilt für die Rechtsnebenklassen.

Offenbar: Tatsache 7 ist äquivalent zu **Tatsache 7'**:

Die Relation " $x \sim y \iff y^{-1}x \in H$ " ist eine Äquivalenzrelation auf  $G$ , und die Äquivalenzklassen sind die Linksnebenklassen von  $H$  in  $G$ .

**Beweis** von Tatsache 7: (i) " $\Rightarrow$ "  $xH = yH \implies y^{-1}xH = H \implies y^{-1}x \in H$ .

" $\Leftarrow$ " Sei  $y^{-1}x = h' \in H$ , also  $x = y \cdot h'$ . Dann ist  $xH = y \cdot h' \cdot H = yH$ , da  $h' \cdot H = H$ .

(ii) Zu zeigen:  $xH \cap yH \neq \emptyset \implies xH = yH$ . Sei also  $z \in xH \cap yH$ . Dann  $z = xh_1 = yh_2$ . Also  $y^{-1}x = h_2h_1^{-1} \in H$  und somit nach (i):  $xH = yH$ .

## 1.2 Normalteiler. Faktorgruppen.

**Tatsache 1.**

Sei  $H \subset G$  eine Untergruppe. Dann sind folgende Aussagen äquivalent:

- (i)  $xHx^{-1} \subset H$  für alle  $x \in G$ .
- (ii)  $xHx^{-1} = H$  für alle  $x \in G$ .
- (iii)  $xH = Hx$  für alle  $x \in G$ .

**Beweis:** Übung.

**Definition 1.**

Eine Untergruppe  $H \subset G$ , welche die Bedingung (i), (ii) oder (iii) erfüllt, heißt *Normalteiler* von  $G$ .

Wir schreiben " $H \triangleleft G$ " für " $H$  ist (bzw. sei) Normalteiler in  $G$ ".

**Bemerkung 1 und Bezeichnung 1:** Die Aussage (i) in Tatsache 1 kann man auch so interpretieren: Die Normalteiler in  $G$  sind genau diejenigen Untergruppen von  $G$ , die invariant unter allen inneren Automorphismen (1.1 Def. 3) von  $G$  sind.

Ist eine Untergruppe  $H < G$  sogar invariant unter allen Automorphismen von  $G$ , so heißt  $H$  eine *charakteristische Untergruppe* von  $G$ .

**Beispiele:**

- 1) In einer kommutativen Gruppe ist jede Untergruppe Normalteiler.

- 2) In jeder Gruppe sind  $\{1_G\}$  und  $G$  Normalteiler.
- 3) In der Gruppe  $S_3$  der Gruppe aller Permutationen von  $\{1, 2, 3\}$  ist die Untergruppe  $\left\{ \text{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$  kein Normalteiler und  $\left\{ \text{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$  ist ein Normalteiler.

**Tatsache 2.** Sei  $f : G \rightarrow G'$  ein Homomorphismus. Dann:

- (1) Sind  $H \subset G$  und  $H' \subset G'$  Untergruppen, so sind  $f(H) \subset G'$  und  $f^{-1}(H') \subset G$  ebenfalls Untergruppen.
- (2) Ist  $H' \triangleleft G'$  ein Normalteiler, so auch  $f^{-1}(H') \triangleleft G$ .
- (3) Ist  $f$  surjektiv, so ist auch  $f(H) \triangleleft G'$ , falls  $H \triangleleft G$ .

**Beweis:** Verifizieren.

**Warnung:** Generell (d.h. bei nicht surjektiven Homomorphismen) sind Bilder von Normalteilern bei Homomorphismen i.a. keine Normalteiler. (Gib ein Gegenbeispiel an!)

**Tatsache 3.** Sei  $H \subset G$  eine Untergruppe. Dann sind äquivalent:

- (i)  $H$  ist Normalteiler.
- (ii) Für je zwei Linksrestklassen  $xH$  und  $yH$  ist  $xH \cdot yH$  die Linksnebenklasse  $xyH$ .

**Beweis:** (i)  $\Rightarrow$  (ii)  $xHx^{-1} \subset xx^{-1}H = H$ .

(ii)  $\Rightarrow$  (i)  $Hx = yH \implies xHyH = xyHH = xyH$ .

**Bemerkung 2:** Die vorausgehende Tatsache sagt insbesondere Folgendes:

Für  $H \triangleleft G$  ist die Komplex-Multiplikation  $(xH, yH) \mapsto (xH) \cdot (yH)$  die wohldefinierte Abbildung  $G/H \times G/H \rightarrow G/H$ ,  $(xH, yH) \mapsto xyH$ .

**Tatsache 4.**

Sei  $H \triangleleft G$ . Die Abbildung  $G/H \times G/H \rightarrow G/H$ ,  $(xH, yH) \mapsto xyH$ , definiert eine Gruppenstruktur auf  $G/H$ .

**Beweis:** Verifizieren, und zwar:  $H$  ist das neutrale Element und  $x^{-1}H$  das Inverse zu  $xH$ . Alle Verifikationen "repräsentantenweise".

**Definition 2:** Ist  $H \triangleleft G$ , so heißt  $G/H$  zusammen mit der eben definierten Gruppenstruktur die *Faktorgruppe* (oder *Quotientengruppe*) von  $G$  nach  $H$ .

**Tatsache 5.**

Die Abbildung  $\pi : G \rightarrow G/H$ ,  $x \mapsto xH$ , ist ein surjektiver Homomorphismus von  $G$  auf  $G/H$ . Es ist Kern  $\pi = H$ .

**Beweis:** klar.

**Bezeichnung 2:** Diese Abbildung  $\pi : G \rightarrow G/H$  heißt die *natürliche Projektion*.

**Anmerkung:** Sei  $H$  der triviale Normalteiler  $H = \{1_G\}$ . Dann gilt  $xH = \{x\}$ ,  $G/H = \{\{x\} \mid x \in G\}$  und  $\pi : G \rightarrow G/H$ ,  $x \mapsto \{x\}$  ist die natürliche Bijektion. Wir

identifizieren in diesem Fall  $G/H$  mit  $G$  via  $\{x\} \equiv x$ , d.h. wir schreiben einfach  $G$  für  $G/H$  und  $x$  für  $\{x\}$ .

**Satz 4** (Eine Charakterisierung der Normalteiler):

Sei  $G$  eine Gruppe. Es gilt:

$$H \triangleleft G \iff \text{Es gibt eine Gruppe } G' \text{ und einen Homomorphismus } f : G \longrightarrow G' \\ \text{mit Kern } f = H.$$

**Beweis:** “ $\Leftarrow$ ” 3. Satz 5,(ii)

“ $\Rightarrow$ ” Nehme für  $f$  die natürliche Projektion  $\pi : G \longrightarrow G/H$ .

### 1.3 Homomorphiesatz und Isomorphiesätze

**Faktorisierungslemma:**

Sei  $f : G \longrightarrow G'$  ein Gruppenhomomorphismus,  $H \triangleleft G$  und  $H' \triangleleft G'$  seien Normalteiler und  $\pi : G \longrightarrow G/H$ ,  $\pi' : G' \longrightarrow G'/H'$ , die entsprechenden natürlichen Projektionen. Dann:

$$\left. \begin{array}{l} \text{Es gibt einen Homomorphismus} \\ \bar{f} : G/H \longrightarrow G'/H' \text{ mit} \\ (*) \quad \bar{f} \circ \pi = \pi' \circ f \end{array} \right\} \iff f(H) \subset H'$$

In diesem Fall (d.h. wenn  $f(H) \subset H'$  bzw. wenn solch ein  $\bar{f}$  existiert) ist  $\bar{f}$  eindeutig bestimmt und wird definiert durch

$$(**) \quad \bar{f}(x \cdot H) = f(x) \cdot H'.$$

Der Kern von  $\bar{f}$  ist  $f^{-1}(H') \cdot H := \{xH \mid f(x) \in H'\}$ .

Zur Orientierung:

$$\text{Diagramm zu } \bar{f} : \begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & & \downarrow \pi' \\ G/H & \xrightarrow{\bar{f}} & G'/H' \end{array}$$

**Beweis:** Bemerkung im voraus: Offenbar:  $(*) \iff (**)$ .

Nun zum Beweis des Satzes:

“ $\Rightarrow$ ” Sei  $x \in H$ . Es ist  $\pi(x) = xH = H = 1_{G/H}$ .

$$\text{Also: } f(x) \cdot H' = \pi' \circ f(x) \underset{(*)}{=} \bar{f} \circ \pi(x) = \bar{f}(1_{G/H}) = 1_{G'/H'} = H'$$

Daraus:  $f(x) \in H'$ .

“ $\Leftarrow$ ” Definiere  $\bar{f}$  durch (\*\*), d.h. durch  $\bar{f}(xH) := f(x)H'$ .

(i)  $\bar{f}$  ist wohldefiniert. Denn:

Sei  $x'H = xH$ , also  $x^{-1}x' \in H$ . Dann  $H' \underset{\text{Vor}}{\ni} f(x^{-1}x') = f(x)^{-1}f(x')$  und

somit  $f(x)H' = f(x')H'$ .

(ii)  $\bar{f}$  ist ein Homomorphismus. Denn:

$$\bar{f}(xH \cdot yH) = \bar{f}(xyH) = f(xy)H' = f(x)f(y)H' = f(x)H' \cdot f(y)H' = \bar{f}(x)H \cdot \bar{f}(y)H$$

(iii)  $\bar{f}$  erfüllt (\*), da es (\*\*) per definitionem erfüllt.

(iv)  $\bar{f}$  hat den angegebenen Kern. Denn:

Sei  $\bar{f}(xH) = 1_{G'/H'} = H'$ . Dann ist  $f(x) \cdot H' = H'$ , also  $f(x) \in H'$ .

Folgerungen und Spezialfälle:

**Satz 1** (Homomorphiesatz):

$$\begin{array}{ccc}
 G & \xrightarrow{f} & G' \\
 \pi \searrow & & \nearrow \bar{f} \\
 & G/\text{Kern } f &
 \end{array}$$

Sei  $f : G \rightarrow G'$  ein Homomorphismus. Dann:

Durch  $x \cdot \text{Kern } f \mapsto f(x)$  wird ein injektiver Homomorphismus  $\bar{f} : G/\text{Kern } f \rightarrow G'$  wohldefiniert. Insbesondere induziert  $\bar{f}$  einen Isomorphismus von  $G/\text{Kern } f$  auf  $\text{Bild } f$ . Es ist also insbesondere

$$G/\text{Kern } f \underset{\text{(isomorph zu)}}{\cong} \text{Bild } f$$

**Beweis:** Wähle  $H := \text{Kern } f$ ,  $H' = \{1_{G'}\}$ . Insbesondere ist dann  $f(H) = H'$ . Identifiziere noch  $G'/H'$  gemäß der Anmerkung nach Tatsache 5 mit  $G'$ . Dann:

Das  $\bar{f}$  aus dem Faktorisierungslemma ist – wie gesucht – ein Homomorphismus  $\bar{f} : G/\text{Kern } f \rightarrow G'$ . Der Kern von  $\bar{f}$  ist  $f^{-1}(H') \cdot H = \text{Kern } f \cdot \text{Kern } f = \text{Kern } f = \{1_{G/\text{Kern } f}\}$ , d.h.  $\bar{f}$  ist injektiv. Die restlichen Behauptungen folgen unmittelbar.

**Tatsache** Seien  $H, F \subset G$  Untergruppen und  $H \triangleleft G$ .

Dann ist  $H \cdot F = F \cdot H$ , und  $F \cdot H$  ist eine Untergruppe.

**Beweis:** Daß  $HF = FH$  ist klar, da  $H \triangleleft G$ . Offenbar ist  $1 \in FH$ .

Seien  $x \in FH$ ,  $y \in FH \implies xy^{-1} \in FH \cdot H^{-1} \cdot F^{-1} = FH \cdot F = F \cdot FH = FH$ .

**Satz 2** (Erster Isomorphiesatz):

Seien  $H, F \subset G$  Untergruppen und  $H \triangleleft G$ . Dann ist  $H \cap F \triangleleft F$ , und es ist  $F/H \cap F \cong FH/H$ .

**Beweis:**  $\pi : G \rightarrow G/H$  sei die natürliche Projektion. Sei  $\pi_0$  die Einschränkung von  $\pi$  auf  $F$ . Dann ist  $\pi_0$  ein Homomorphismus mit Kern  $H \cap F$ . Also ist  $H \cap F$  Normalteiler in  $F$ .

Nach Satz 1 ist  $F/H \cap F$  isomorph zum Bild von  $\pi_0$ . Das Bild von  $\pi_0$  besteht aber genau aus den Linksnebenklassen von  $H$ , die mit  $F$  nicht leeren Durchschnitt haben. Das sind aber gerade die Elemente von  $FH/H$ .

**Satz 3** (Zweiter Isomorphiesatz):

Seien  $F, H$  Normalteiler in  $G$ , und sei  $F \subset H$ . Dann ist  $H/F$  ein Normalteiler in  $G/F$ , und es gilt

$$(G/F)/(H/F) \cong G/H.$$

**Beweis:** Sei  $f : G/F \rightarrow G/H$  definiert durch  $x \cdot F \mapsto x \cdot H$ . Man zeigt ohne Schwierigkeiten der Reihe nach:

- (i)  $f$  ist wohldefiniert,
- (ii) Kern  $f = H/F$ ,
- (iii) Bild  $f = G/H$  und
- (iv)  $f$  ist ein Homomorphismus.

Nach Satz 1 folgt dann die Behauptung.

**Satz 3** (“Korrespondenzsatz”):

Sei  $N_0 \triangleleft G$  ein Normalteiler und  $\pi : G \rightarrow G/N_0$  die natürliche Projektion. Dann:

Durch  $N \mapsto \pi(N)$  wird eine Bijektion von der Menge aller solchen Normalteiler von  $G$ , die  $N_0$  enthalten, auf die Menge aller Normalteiler von  $G/N_0$  definiert.

Die Umkehrabbildung ist  $N' \mapsto \pi^{-1}(N')$ .

**Beweis:** Als Übung.

## 1.4 Spezielle Untergruppen

Sei  $X \subset G$  eine Untermenge.

### Definition 1.

Die von  $X$  erzeugte Untergruppe, mit  $\langle X \rangle$  bezeichnet, ist der Durchschnitt aller Untergruppen  $H$  von  $G$  mit  $X \subset H$ .

**Bemerkung 1:** Nach Satz 2 in 3 ist  $\langle X \rangle$  eine Untergruppe, und sie ist nach Definition minimal unter allen Untergruppen  $H$  mit  $X \subset H$ .

Man kann  $\langle X \rangle$  auch so beschreiben: Sei  $Y = X \cup X^{-1}$ ,  $Y^k = \underbrace{Y \cdot Y \cdot \dots \cdot Y}_{k\text{-mal}}$ . Dann ist

$$\langle X \rangle = \{1\} \cup \bigcup_{k=1}^{\infty} Y^k.$$

### Definition 2.

Eine Gruppe  $G$  heißt *zyklisch*, wenn es  $x \in G$  gibt mit  $G = \langle x \rangle$  (dabei  $\langle x \rangle := \langle \{x\} \rangle$ ).  
 $G$  heißt *endlich erzeugt*, wenn es eine endliche Untermenge  $\{x_1, \dots, x_n\} \in G$  gibt mit  $G = \langle \{x_1, \dots, x_n\} \rangle$ .

### Definition 3.

Der *Normalisator*  $N_G(X)$  einer Teilmenge  $X \in G$  ist definiert durch

$$N_G(X) = \{g \in G \mid g^{-1}Xg = X\}.$$

Der *Zentralisator*  $Z_G(X)$  von  $X$  in  $G$  ist definiert durch

$$Z_G(X) = \{g \in G \mid gx = xg \text{ (d.h. } xgx^{-1} = x) \text{ für alle } x \in X\}.$$

(Gebräuchlich ist auch  $C_G(X)$  für  $Z_G(X)$  ( $C$  von *centralizer*).)

$$Z(G) := Z_G(G) \text{ heißt das Zentrum von } G.$$

**Bemerkung 2:** Ist  $X \triangleleft G$ , so ist  $N_G(X) = G$ . Ist  $G$  abelsch, so ist  $Z_G(G) = G$ .

### Satz 1.

$N_G(X)$  und  $Z_G(X)$  sind Untergruppen.

Ist  $H < G$ , so ist  $H$  Normalteiler von  $N_G(H)$ .

$Z(G)$  ist charakteristische Untergruppe von  $G$ .

**Beweis:** Kleine Übung.

### Definition 4.

Seien  $x, y \in G$ . Dann heißt  $[x, y] := xyx^{-1}y^{-1}$  ein *Kommutator* in  $G$ .

Sei  $K = \{xyx^{-1}y^{-1} \mid x, y \in G\}$  die Menge aller Kommutatoren in  $G$ . Die Gruppe  $G' = [G, G] := \langle K \rangle$  heißt die *Kommutatoruntergruppe* von  $G$ .

### Satz 2.

(i)  $[G, G]$  ist eine charakteristische Untergruppe.

(ii) Sei  $H \triangleleft G$ . Dann ist  $G/H$  abelsch genau dann, wenn  $[G, G] \subset H$ .

**Beweis:** (i) Für jeden Automorphismus  $\alpha$  von  $G$  und jeden Kommutator  $[x, y] \in K$  gilt  $\alpha([x, y]) = [\alpha(x), \alpha(y)]$ , also ist  $\alpha(K) \subset K$ . Nach Konstruktion von  $\langle K \rangle$  gilt dann auch  $\alpha(\langle K \rangle) \subset \langle K \rangle$ , d.h. es ist  $\alpha([G, G]) \subset [G, G]$ .

(ii) Es gilt:  $[G, G] \subset H \iff K \subset H \iff x^{-1}y^{-1}xy \in H$  für alle  $x, y \in G \iff xyH = yxH$ , alle  $x, y \in G \iff G/H$  abelsch.

## 1.5 Ordnungen

### Definition 1.

Die Anzahl der Elemente in  $G$  heißt die *Ordnung* von  $G$ , geschrieben  $|G|$  (dabei ist  $|G| = n \in \mathbb{N}$  oder  $|G| = \infty$ ).

Die Ordnung eines Elementes  $x \in G$  ist die Ordnung von  $\langle x \rangle$ . Ist  $|G|$  endlich, so heißt  $G$  eine endliche Gruppe.

**Lemma:** Sei  $H$  eine Untergruppe von  $G$ ,  $x, y \in G$ . Dann gibt es eine Bijektion von  $xH$  auf  $yH$ . ( $yH$  ist das Bild von  $xH$  unter der Bijektion  $l_y \circ l_{x^{-1}}$ )

### Definition 2.

In einer endlichen Gruppe wird die Anzahl der Linksnebenklassen von  $H$  in  $G$  mit  $[G : H]$  bezeichnet und der *Index* von  $H$  in  $G$  genannt

**Bemerkung:** Der Index von  $H$  in  $G$  ist auch die Anzahl der Rechtsnebenklassen von  $H$ .

**Satz:** (Lagrange) In einer endlichen Gruppe gilt für Untergruppen  $H < G$ :

$$|G| = |H| \cdot [G : H].$$

Insbesondere sind also sowohl die Ordnung als auch der Index einer Untergruppe Teiler der Gruppenordnung.

**Beweis:** Es gibt  $[G : H]$  Linksnebenklassen von  $H$  in  $G$ . Jede hat nach dem Lemma  $|H|$  Elemente. Da die Linksnebenklassen  $G$  disjunkt zerlegen (s.1.1 Tats. 7), gilt  $|G| = |H| \cdot [G : H]$ .

**Korollar:** Die Ordnung eines Elementes teilt die Gruppenordnung.

### Übungen:

- 1) Sei  $x \in G$ . Die Ordnung von  $x$  ist entweder  $\infty$  oder gleich der kleinsten positiven ganzen Zahl  $n$  mit  $x^n = 1$ .
- 2) Sei  $H$  eine endliche Untermenge der Gruppe  $G$ , und sei  $H \cdot H = H$ . Dann ist  $H$  Untergruppe.

## 1.6 Konstruktionen mit Gruppen

Sei  $I$  eine Menge und  $G^I = \{f \mid f : I \rightarrow G\}$  die Menge aller Abbildungen von  $I$  nach  $G$ . Für  $f, g \in G^I$  sei  $f \cdot g$  definiert durch  $(f \cdot g)(x) = f(x) \cdot g(x)$  für alle  $x \in I$ .

**Satz 1.**

$G^I$  zusammen mit  $G^I \times G^I \rightarrow G^I, (f, g) \mapsto f \cdot g$  ist eine Gruppe.

**Beweis:** Übung

Sei  $(G_i)_{i \in I}$  eine Familie von Gruppen. Im kartesischen Produkt  $\prod_{i \in I} G_i$  sei eine Multiplikation folgendermaßen definiert:

$$(x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i \cdot y_i)_{i \in I},$$

wo  $x_i, y_i \in G_i$  für alle  $(x_i)_{i \in I}$  und  $(y_i)_{i \in I}$  aus  $\prod_{i \in I} G_i$ .

**Satz 2.**

$\prod_{i \in I} G_i$  mit diesem Produkt ist eine Gruppe.

**Definition 1.**

$\prod_{i \in I} G_i$  heißt das *direkte Produkt* der Gruppe  $G_i$ .

$\prod_{i \in I} G_i$  sei die Untermenge derjenigen  $(x_i)_{i \in I} \in \prod_{i \in I} G_i$ , für die nur endlich viele der  $x_i \neq 1_{G_i}$  sind. Dann ist  $\prod_{i \in I} G_i$  eine Untergruppe von  $\prod_{i \in I} G_i$ .  $\prod_{i \in I} G_i$  heißt das *schwache Produkt* der  $G_i$ .

Seien  $H, G, G'$  Gruppen.

**Definition 2.**

Die Folge  $\{1\} \xrightarrow{f} N \xrightarrow{f} G \xrightarrow{f} G' \xrightarrow{f} \{1\}$  von Homomorphismen heißt *exakt*, wenn  $f$  injektiv,  $g$  surjektiv und  $\text{Bild } f = \text{Kern } g$  ist. In diesem Fall heißt  $G$  *Erweiterung* von  $G'$  durch  $N$ . Seien  $N, H$  Untergruppen von  $G$  und sei  $N \triangleleft G$ .

**Definition 3.**

Seien  $N, H$  Untergruppen von  $G$  und sei  $N \triangleleft G$ . Dann:

$G$  heißt *semidirektes Produkt* von  $N$  mit  $H$ , geschrieben  $G = N \rtimes H$ , falls gilt:

- (i)  $N \cdot H = G$     und    (ii)  $N \cap H = \{1\}$ .

Sei nun  $G = N \rtimes H$  ein semidirektes Produkt. Wir betrachten die Abbildung

$$\sigma : H \rightarrow \text{Aut}(N), h \mapsto f_h, \text{ wo } f_h(n) = hnh^{-1}.$$

Dabei bezeichnet  $\text{Aut}(N)$  die Gruppe der Automorphismen von  $N$  (vgl. 2. Übung 1).

**Lemma:**  $\sigma$  ist ein Homomorphismus.

Es ist nach Definition des semidirekten Produktes  $G = H \cdot N$ . Seien  $g_1, g_2 \in G$  und  $g_1 = n_1 \cdot h_1, g_2 = n_2 \cdot h_2$  (aus (ii) der Definition 3 folgt, daß diese Darstellungen der

$g_1, g_2$  eindeutig sind).

Was ist  $(n_1 \cdot h_1) \cdot (n_2 \cdot h_2) = n \cdot h$  dargestellt als  $n \cdot h$  mit  $h \in H, n \in N$ .

**Satz 3.**

$(n_1 \cdot h_1) \cdot (n_2 \cdot h_2) = n \cdot h$ , wo  $h = h_1 h_2$  und  $n = n_1 \cdot f_{h_1}(n_2)$ .

**Beweis:** Nachrechnen.

Wir kehren nun das bisher Beschriebene in gewissem Sinne um und konstruieren nur semidirekte Produkte.

Seien  $N, H$  Gruppen, und  $\sigma : H \rightarrow \text{Aut}(N)$  sei ein Homomorphismus. Auf der Menge  $N \times H$  definieren wir folgende Multiplikation “\*“:

$$(n_1, h_1) \times (n_2, h_2) := (n_1 \cdot \sigma(h_1)(n_2), h_1 h_2)$$

**Satz 4.**

$N \times H$  zusammen mit dem Produkt “\*” ist eine Gruppe. Identifizieren wir  $N$  durch  $n \mapsto (n, 1_H)$  und  $H$  durch  $h \mapsto (1_N, h)$  mit den Untergruppen  $\{(n, 1_H) \mid n \in N\}$  bzw.  $\{(1_N, h) \mid h \in H\}$  von  $(N \times H, *)$ , so ist  $(N \times H, *)$  das semidirekte Produkt von  $N$  mit  $H$ .

**Beweis:** Leicht.

## 1.7 Spezielle Typen von Gruppen

**Definition 1.**

Eine Gruppe  $G$  heißt *einfach* genau dann, wenn  $G$  und  $\{1\}$  die einzigen Normalteiler von  $G$  sind.

**Satz 1:** Eine abelsche Gruppe  $\neq \{1\}$  ist einfach  $\iff G$  ist endlich und zyklisch von Primzahlordnung.

**Beweis:** “ $\Leftarrow$ ” folgt aus dem Satz in 7 (zusammen mit Beispiel 2) in 3.)

“ $\Rightarrow$ ” Sei  $x \neq 1$  aus  $G$ . Es ist  $\langle x \rangle = G$ .

**1. Fall:**  $\langle x \rangle$  ist endlich. Dann ist  $|\langle x \rangle|$  eine Primzahl. Denn wäre  $d > 1, d \neq |\langle x \rangle|$  ein Teiler von  $|\langle x \rangle|$ , so wäre  $\langle x^d \rangle$  eine echte Untergruppe von  $G$ .

**2. Fall:**  $\langle x \rangle$  ist nicht endlich. Dann ist  $\langle x^2 \rangle$  eine echte Untergruppe von  $G$ . Das widerspricht der Einfachheit.

**Anmerkung:** In den 80er Jahren ist es gelungen, alle endlichen einfachen Gruppen zu klassifizieren. Dies gilt als eine der größten Leistungen der Mathematik in der letzten Zeit.

**Definition 2.**

Eine Gruppe  $G$  heißt *auflösbar*, wenn es Untergruppen

$$G = G_0, G_1, G_2, \dots, G_k = \{1\}$$

in  $G$  gibt mit  $G_{i+1} \triangleleft G_i$  für  $i = 0, \dots, k-1$  und  $G_i/G_{i+1}$  ist abelsch für alle  $i = 0, 1, \dots, k-1$ .

### Bezeichnungen

Sei  $G$  eine Gruppe. Sind  $A, B \subset G$  zwei Untermengen, so bezeichnen wir mit  $[A, B]$  die Untergruppe von  $G$ , die von der Menge  $\{aba^{-1}b^{-1} \mid a \in A, b \in B\}$  von Kommutatoren erzeugt wird.

Setze  $G =: G^{(0)} = Z_0G$  Man definiert induktiv:

$$G^{(i+1)} := [G^{(i)}, G^{(i)}]$$

$$\text{und } Z_{i+1}G := [G, Z_iG] \text{ f\"ur } i = 0, 1, \dots$$

### Satz 2:

$G$  ist auflösbar, wenn es  $n \in \mathbb{N}$  gibt  $G^{(n)} = \{1\}$ .

**Bew.:** Als Übung mit Hilfe von Satz 2 in 1.4. (Es ist  $G^{(i+1)} = (G^{(i)})'$ ,  $i = 1, 2, \dots$ , im Sinne der Definition 4 in 1.4.)

### Definition 3.

Die Gruppe  $G$  heißt *nilpotent*, falls es ein  $r \in \mathbb{N}$  gibt mit  $Z_r(G) = \{1\}$ .

## 1.8 Hauptsatz für abelsche Gruppen

**Satz:** Sei  $G$  eine endlich erzeugte abelsche Gruppe. Dann ist  $G$  die direkte Summe  $F \oplus G_0$ , wo  $F = \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$  eine endliche direkte Summe von Exemplaren von  $\mathbb{Z}$  ist und wo  $G_0 = \bigoplus_{n_1, \dots} \mathbb{Z}_{n_i}$  die direkte Summe von zyklischen Gruppen  $\mathbb{Z}_{n_i}$  der Ordnung  $n_i$ ,  $i = 1, \dots, s$  ist, mit der Eigenschaft, daß  $n_i$  Teiler von  $n_{i+1}$  ist für  $i = 1, \dots, s-1$ .

**Bemerkung:** Wir haben in der Formulierung die Gruppe additiv geschrieben. Deshalb auch die Zeichen  $\bigoplus, \oplus$  für die Produktzeichen  $\prod, \times$ . Die additive Schreibweise behalten wir im Beweis bei.

**Beweis:** Induktion über die Anzahl  $k$  der Elemente eines minimalen Erzeugendensystems, d.h. hier eines Erzeugendensystems mit minimaler Anzahl von Erzeugenden.

(i)  $k = 1$  klar

(ii)  $k > 1$

**1. Fall:** Kein minimales Erzeugendensystem erfüllt eine nicht triviale Relation.

(Eine Relation zwischen einer Menge  $x_1, \dots, x_m$  von Elementen ist eine Gleichung  $n_1x_1 + \dots + n_mx_m = 0$ . Die Relation heißt *nicht trivial*, falls mindestens eines der  $n_j \neq 0$  ist.)

Sei dann  $\{g_1, \dots, g_k\}$  ein minimales Erzeugendensystem.

Es ist  $G = \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \dots \oplus \langle g_k \rangle$  und  $\langle g_i \rangle \cong \mathbb{Z}$  für alle  $i$ .

**2. Fall:** Es gebe nicht triviale Relationen für gewisse minimale Erzeugendensysteme.

Sei  $g_1, \dots, g_k$  ein minimales Erzeugendensystem, so daß

$$(1) \quad m_1g_1 + m_2g_2 + \dots + m_kg_k = 0, \quad m_i \in \mathbb{Z},$$

und  $m_1$  der kleinste positive Koeffizient ist, der in einer Relation bei minimalen Erzeugendensystemen auftritt.

**Beh. 1:** Ist (2):  $n_1g_1 + n_2g_2 + \dots + n_kg_k = 0$ , so ist  $m_1$  Teiler von  $n_1$ .

**Bew.:** Sei  $n_1 = qm_1 + r, 0 \leq r < m_1$ . Subtrahiert man die Gleichung (1)  $q$ -fach von der Gleichung (2), so erhält man eine Relation mit  $r$  als Koeffizient (bei  $g_1$ ). Nach Wahl von  $m_1$  ist  $r = 0$ .

**Beh. 2:** In (1) gilt:  $m_1$  ist Teiler von  $m_i, i > 1$ .

**Bew.:** Sei  $m_i = q_i m_1 + r_i, i = 2, \dots, k, 0 \leq r_i < m_1$ . Im Erzeugendensystem  $g_1 + q_i g_i, g_2, \dots, g_k$  wäre  $m_1(g_1 + qg_2) + \dots + r_i g_i + \dots = 0$ , also ist  $r_i = 0$ . Somit ist  $m_i = q_i m_1, i = 2, \dots, k$ .

Sei das System  $\bar{g}_1, g_2, \dots, g_k$  betrachtet mit  $\bar{g}_1 = g_1 + q_2 g_2 + q_3 g_3 + \dots + q_k g_k$ . Es ist ein minimales Erzeugendensystem. Aus (1) wird:  $m_1 \bar{g}_1 = 0$ .

Wir betrachten nun die Gleichung  $n_1 \bar{g}_1 + n_2 g_2 + \dots + n_k g_k$  als Gleichung (2) und die Gleichung  $m_1 \bar{g}_1 = 0$  als Gleichung (1). Beh. 1 besagt dann, daß  $m_1$  Teiler von  $n_1$  ist. Also gilt  $n_1 \bar{g}_1 = 0$ .

Sei  $G_0$  die von  $g_2, \dots, g_k$  erzeugte Untergruppe und  $G_1 = \langle \bar{g}_1 \rangle$ . Jedes  $g \in G$  ist eindeutig darstellbar als  $g = n_1 \bar{g}_1 + n_2 g_2 + \dots + n_k g_k = n_1 \bar{g}_1 + g_0$  mit  $g_0 \in G_0$ . Denn aus

$$\begin{aligned} n_1 \bar{g}_1 + g'_0 = n_2 \bar{g}_1 + g''_0 &\Rightarrow (n_1 - n_2) \bar{g}_1 + (g'_0 - g''_0) = 0 \\ &\Rightarrow (n_1 - n_2) \bar{g}_1 = 0, \end{aligned}$$

wie davor gezeigt. Also ist  $n_1 \bar{g}_1 = n_2 \bar{g}_1$  und damit auch  $g'_0 = g''_0$ .

Es ist also  $G = G_1 \oplus G_0$ . Schließlich: Auf  $G_0$  kann die Induktionsvoraussetzung angewandt werden. q.e.d.

## 1.9 Operationen von Gruppen auf Mengen

Sei  $X$  eine Menge und  $G$  sei eine Gruppe.

### Definition 1.

Eine *Operation* (oder *Aktion*) von  $G$  auf  $X$  ist eine Abbildung

$$\Phi : G \times X \longrightarrow X, (g, x) \longmapsto g \cdot x = gx$$

mit den Eigenschaften:

- (i)  $1 \cdot x = x$  für alle  $x \in X$ .
- (ii)  $(g_1 \cdot g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$  für alle  $g_1, g_2 \in G, x \in X$ .

Sei eine Operation von  $G$  auf  $X$  gegeben. Für alle  $g \in G$  ist dann die Abbildung  $\varphi(g) : X \longrightarrow X, x \longmapsto gx$ , eine Bijektion. Denn  $\varphi(g^{-1})$  ist die inverse Abbildung.

### Satz 1.

- (i) Die Abbildung  $\varphi : G \longrightarrow S_x, g \longmapsto \varphi(g)$ , ist ein Homomorphismus.
- (ii) Sei umgekehrt  $\psi : G \longrightarrow S_x$  ein Homomorphismus. Dann ist  $G \times X \longrightarrow X, (g, x) \longmapsto (\psi(g))(x)$  eine Operation von  $G$  auf  $X$ .

( $S_x$  ist die Gruppe der Permutationen von  $X$ , d.i. die Gruppe der bijektiven Abbildungen von  $X$  auf sich.)

**Beweis:** Übung.

In Zukunft sei eine Operation  $G \times X \longrightarrow X$  fest vorgegeben.

**Definition 2.**

Die Untermengen von  $X$  der Gestalt  $G \cdot x = \{gx \mid g \in G\}$ ,  $x \in X$ , heißen die *Bahnen* (oder *Orbiten* der Aktion;  $G_x$  ist *die Bahn durch  $x$* ).

Zu  $x \in X$  sei  $G_x = \{g \in G \mid gx = x\}$ .  $G_x$  ist Untergruppe von  $G$  und heißt der *Stabilisator* (oder die *Isotropiegruppe* oder die *Standuntergruppe*) von  $x$ .

**Satz 2.**

- (i) Die Menge  $\{G \cdot x \mid x \in X\}$  der Orbiten bilden eine Zerlegung von  $X$  in disjunkte Teilmengen. Anders ausgedrückt: Die Relation " $x \sim y \iff y \in Gx$ " ist eine Äquivalenzrelation auf  $X$ .
- (ii) Ist  $y = gx$ , so ist  $G_y = gG_xg^{-1}$ .

**Beispiel** einer Operation von  $G$  auf  $G : G \times G \longrightarrow G, (g, x) \longmapsto gxg^{-1}$ .

**Beweis:** Übung.