1. Elementare Gruppentheorie

Vorbemerkungen

Der Gruppenbegriff ist im Rahmen dieses Buches in zweierlei Hinsicht von Bedeutung. Einerseits beinhaltet er eine grundlegende mathematische Struktur, die man insbesondere bei Ringen, Körpern, Vektorräumen und Moduln findet, wenn man die dort gegebene Addition als Verknüpfung betrachtet. Gruppen dieses Typs sind stets kommutativ oder, wie man auch sagt, abelsch, benannt nach dem Mathematiker N. H. Abel. Daneben sind für uns aber auch die auf E. Galois zurückgehenden Galois-Gruppen von zentralem Interesse, da diese für die Theorie algebraischer Gleichungen benötigt werden. Galois-Gruppen sind aus einfachster Sicht Permutationsgruppen, also Gruppen, deren Elemente als bijektive Selbstabbildungen einer gegebenen endlichen Menge, etwa $\{1, \ldots, n\}$, aufgefasst werden.

Ein wesentliches Charakteristikum einer Gruppe G ist die Verknüpfungsvorschrift, welche je zwei Elementen $g, h \in G$ ein drittes Element $g \circ h \in G$ zuordnet, als Produkt oder im kommutativen Fall auch als Summe von g und h bezeichnet. Solche Verknüpfungen hatte man beim Rechnen in Zahlbereichen schon immer benutzt, ohne dass man zunächst eine Notwendigkeit sah, die Eigenschaften einer Verknüpfung genauer zu präzisieren. Diese wurden sozusagen als "evident" angesehen. So ist es auch zu verstehen, dass das Auftreten negativer Zahlen als Ergebnis einer Rechnung, etwa bei einer Differenzbildung, noch bis zum Beginn des 17. Jahrhunderts bei manchen Mathematikern als "suspekt" galt, da negative Zahlen eben keine reale Bedeutung zu haben schienen. Mit Beginn des 19. Jahrhunderts jedoch begann der eigentliche Gruppenbegriff Gestalt anzunehmen, und zwar in dem Maße, wie Verknüpfungsvorschriften auch auf Objekte angewendet wurden, die nicht in natürlicher Weise als Zahlbereichen zugehörig interpretiert werden konnten. Bei der Auflösung algebraischer Gleichungen spielten beispielsweise Permutationsgruppen eine wichtige Rolle. Da es sich hierbei um endliche Gruppen handelt, also um Gruppen mit endlich vielen Elementen, konnte man die Gruppenaxiome noch ohne explizite Erwähnung "inverser Elemente" formulieren, was bei unendlichen Gruppen nicht mehr möglich ist; man vergleiche hierzu etwa Aufgabe 3 aus Abschnitt 1.1. Eine explizite Forderung "inverser Elemente" und damit eine axiomatische Charakterisierung von Gruppen im heutigen Sinne taucht erstmalig im ausgehenden 19. Jahrhundert bei S. Lie und H. Weber auf. Zuvor hatte Lie noch vergeblich versucht, für die

von ihm betrachteten "Transformationsgruppen" die Existenz inverser Elemente aus den übrigen Axiomen abzuleiten.

In diesem Kapitel wollen wir in knapper Form einige elementare Grundlagen über Gruppen zusammenstellen, Dinge, die den meisten Lesern sicherlich schon geläufig sein dürften. Neben der Definition einer Gruppe handelt es sich um die Einführung von Normalteilern, der zugehörigen Faktorgruppen sowie um die Diskussion zyklischer Gruppen. Bereits hier spürt man etwas von dem prägenden Einfluss, den die Untersuchungen zur Auflösung algebraischer Gleichungen und insbesondere die Galois-Theorie auf die Gruppentheorie ausgeübt haben. Der Begriff des Normalteilers ist beispielsweise im Zusammenhang mit dem Hauptsatz der Galois-Theorie 4.1/6 entstanden. Denn dieser Satz besagt unter anderem, dass ein Zwischenkörper E zu einer endlichen Galois-Erweiterung L/K genau dann normal über K im Sinne von 3.5/5 ist, wenn die zu E gehörige Untergruppe der Galois-Gruppe $\mathrm{Gal}(L/K)$ die Normalteilereigenschaft besitzt. Auch die Benennung von 1.2/3 als Satz von Lagrange bezieht sich auf gruppentheoretische Argumente, die Lagrange bei seinen Untersuchungen zur Auflösung algebraischer Gleichungen entwickelte.

Weiter gehende Resultate über Gruppen und insbesondere Permutationsgruppen, die speziell für Anwendungen in der Galois-Theorie von Interesse sind, werden wir aber erst in Kapitel 5 bringen. Im Übrigen sei hier noch auf den Hauptsatz über endlich erzeugte abelsche Gruppen hingewiesen, der eine Klassifikation dieser Gruppen liefert und dessen Beweis wir in 2.9/9 im Rahmen der Elementarteilertheorie führen werden.

1.1 Gruppen

Es sei M eine Menge und $M \times M$ ihr kartesisches Produkt. Unter einer (*inneren*) *Verknüpfung* auf M versteht man eine Abbildung $M \times M \longrightarrow M$. Dabei schreibt man das Bild eines Paares $(a, b) \in M \times M$ meist als "Produkt" $a \cdot b$ oder ab, so dass die Verknüpfung auf M elementweise durch $(a, b) \longmapsto a \cdot b$ charakterisiert werden kann. Die Verknüpfung heißt

assoziativ, falls $(ab)c = a(bc)$ für alle $a, b, c \in M$.

kommutativ, falls $ab = ba$ für alle $a, b \in M$ gilt.

Man nennt ein Element $e \in M$ ein *Einselement* oder *neutrales Element* bezüglich der Verknüpfung auf M, wenn $ea = a = ae$ für alle $a \in M$ gilt. Ein solches Einselement e ist durch diese Eigenschaft eindeutig bestimmt; wir schreiben häufig auch 1 anstelle von e. Eine Menge M mit Verknüpfung $\sigma\colon M \times M \longrightarrow M$ heißt ein *Monoid*, wenn σ assoziativ ist und M ein Einselement bezüglich σ besitzt.

Ist M ein Monoid, so kann man für $a_1, \ldots, a_n \in M$ das Produkt

$$\prod_{i=1}^{n} a_i := a_1 \cdot \ldots \cdot a_n$$

definieren. Da die Verknüpfung assoziativ ist, erübrigt sich eine spezielle Klammerung auf der rechten Seite (was man am besten mit Hilfe eines geschickt angelegten induktiven Arguments beweist). Als Konvention vereinbaren wir noch

$$\prod_{i=1}^{0} a_i := e = \text{ Einselement.}$$

Wie üblich lässt sich zu einem Element $a \in M$ und einem Exponenten $n \in \mathbb{N}$ die n-te Potenz a^n bilden,[1] wobei man aufgrund vorstehender Konvention $a^0 = e$ hat. Ein Element $b \in M$ heißt *invers* zu einem gegebenen Element $a \in M$, wenn $ab = e = ba$ gilt. Es ist dann b eindeutig durch a bestimmt, denn wenn auch $ab' = e = b'a$ gilt, so folgt

$$b = eb = b'ab = b'e = b'.$$

Üblicherweise bezeichnet man das inverse Element zu a, falls es existiert, mit a^{-1}.

Definition 1. *Eine* Gruppe *ist ein Monoid G, so dass jedes Element von G ein inverses Element besitzt. Im Einzelnen bedeutet dies, man hat eine Menge G mit einer Verknüpfung $G \times G \longrightarrow G$, $(a, b) \longmapsto ab$, welche folgenden Eigenschaften genügt*:

(i) *Die Verknüpfung ist* assoziativ, *d. h. es gilt $(ab)c = a(bc)$ für $a, b, c \in G$.*

(ii) *Es existiert ein* Einselement, *d. h. ein Element $e \in G$ mit $ea = a = ae$ für alle $a \in G$.*

(iii) *Zu jedem $a \in G$ gibt es ein* inverses Element, *d. h. ein $b \in G$ mit $ab = e = ba$.*

Die Gruppe heißt kommutativ *oder* abelsch, *falls die Verknüpfung kommutativ ist, d. h. falls*

(iv) *$ab = ba$ für alle $a, b \in G$ gilt.*

Bemerkung 2. *Es genügt, in Definition* 1 *statt* (ii) *und* (iii) *die folgenden etwas schwächeren Bedingungen zu fordern*:

(ii′) *Es existiert ein* links-neutrales Element, *d. h. ein $e \in G$ mit $ea = a$ für alle $a \in G$.*

(iii′) *Zu jedem $a \in G$ existiert ein* links-inverses Element, *d. h. ein $b \in G$ mit $ba = e$.*

Bezüglich des Nachweises, dass die vorstehenden Bedingungen (ii′) und (iii′) in Verbindung mit (i) bereits zur Definition einer Gruppe ausreichen, verweisen wir auf Aufgabe 1 bzw. auf die im Anhang gegebene Lösung.

Bei einer abelschen Gruppe schreibt man die Verknüpfung oft auch in additiver Form, d. h. man schreibt $a + b$ statt $a \cdot b$ und $\sum a_i$ statt $\prod a_i$, bzw. $n \cdot a$ anstelle einer n-ten Potenz a^n. Entsprechend verwendet man die Bezeichnung

[1] $\mathbb{N}$ bezeichnet die natürlichen Zahlen *einschließlich* der 0.

$-a$ statt a^{-1} für das inverse Element zu a sowie 0 (*Nullelement*) statt e oder 1 für das neutrale Element. Wir wollen einige Beispiele für Monoide und Gruppen anführen:

(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, jeweils mit der gewöhnlichen Addition, sind abelsche Gruppen.

(2) $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, jeweils mit der gewöhnlichen Multiplikation, sind abelsche Gruppen; ebenso $\mathbb{Q}_{>0} = \{x \in \mathbb{Q}\,;\, x > 0\}$ und $\mathbb{R}_{>0} = \{x \in \mathbb{R}\,;\, x > 0\}$. Allgemeiner kann man die aus der Linearen Algebra bekannten Matrizengruppen Sl_n oder Gl_n mit Koeffizienten in $\mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$ betrachten. Diese sind für $n > 1$ nicht mehr kommutativ.

(3) $\mathbb{N}$ mit Addition, $\mathbb{N}$, $\mathbb{Z}$ mit Multiplikation sind kommutative Monoide, aber keine Gruppen.

(4) Es sei X eine Menge und $S(X)$ die Menge der bijektiven Abbildungen $X \longrightarrow X$. Dann ist $S(X)$ mit der Komposition von Abbildungen als Verknüpfung eine Gruppe; diese ist nicht abelsch, sofern X aus mindestens 3 Elementen besteht. Für $X = \{1, \ldots, n\}$ setzt man $\mathfrak{S}_n := S(X)$ und nennt dies die *symmetrische Gruppe* bzw. die *Gruppe der Permutationen* der Zahlen $1, \ldots, n$. Elemente $\pi \in \mathfrak{S}_n$ beschreibt man häufig unter expliziter Angabe aller Bilder $\pi(1), \ldots, \pi(n)$ in der Form

$$\begin{pmatrix} 1 & \ldots & n \\ \pi(1) & \ldots & \pi(n) \end{pmatrix}.$$

Indem man die Anzahl der möglichen Anordnungen von $1, \ldots, n$ abzählt, sieht man, dass $\mathfrak{S}_n$ aus genau $n!$ Elementen besteht.

(5) Es sei X eine Menge, G eine Gruppe. Dann ist $G^X := \mathrm{Abb}(X, G)$, die Menge der Abbildungen $X \longrightarrow G$, in natürlicher Weise eine Gruppe. Man definiere nämlich für $f, g \in G^X$ das Produkt $f \cdot g$ mittels $(f \cdot g)(x) := f(x) \cdot g(x)$, also durch Multiplikation der "Funktionswerte", indem man die Gruppenverknüpfung von G verwendet. Es heißt G^X auch *Gruppe der G-wertigen Funktionen auf X*. In gleicher Weise können wir die Gruppe $G^{(X)}$ derjenigen Abbildungen $f\colon X \longrightarrow G$ bilden, welche $f(x) = 1$ für fast alle $x \in X$ erfüllen (d. h. für alle $x \in X$, bis auf endlich viele Ausnahmen). Die Gruppen G^X und $G^{(X)}$ sind kommutativ, wenn G kommutativ ist. G^X und $G^{(X)}$ stimmen überein, wenn X endlich ist.

(6) Es sei X eine Indexmenge und $(G_x)_{x \in X}$ eine Familie von Gruppen. Dann wird das mengentheoretische Produkt $\prod_{x \in X} G_x$ zu einer Gruppe, wenn wir die Verknüpfung zweier Elemente $(g_x)_{x \in X}$, $(h_x)_{x \in X} \in \prod_{x \in X} G_x$ komponentenweise erklären durch

$$(g_x)_{x \in X} \cdot (h_x)_{x \in X} := (g_x \cdot h_x)_{x \in X}.$$

Man nennt $\prod_{x \in X} G_x$ das *Produkt* der Gruppen G_x, $x \in X$. Falls $X = \{1, \ldots, n\}$, so schreibt man hierfür üblicherweise auch $G_1 \times \ldots \times G_n$. Sind die Gruppen G_x Exemplare ein und derselben Gruppe G, so gilt $\prod_{x \in X} G_x = G^X$ in der

Notation des vorstehenden Beispiels. Ist zudem X endlich, etwa $X = \{1, \ldots, n\}$, so schreibt man auch G^n statt G^X oder $G^{(X)}$.

Definition 3. *Es sei G ein Monoid. Eine Teilmenge $H \subset G$ heißt* Untermonoid, *wenn H die Bedingungen*

(i) $e \in H$,

(ii) $a, b \in H \Longrightarrow ab \in H$,

erfüllt. Ist G sogar eine Gruppe, so nennt man H eine Untergruppe *von G, wenn zusätzlich gilt*:

(iii) $a \in H \Longrightarrow a^{-1} \in H$.

Eine Untergruppe einer Gruppe G ist also ein Untermonoid, welches abgeschlossen unter Inversenbildung ist.

Man kann die Bedingung (i) bei der Definition einer Untergruppe $H \subset G$ abschwächen zu $H \neq \emptyset$, denn mit (ii) und (iii) folgt dann bereits $e \in H$. Für Monoide ist ein entsprechendes Vorgehen natürlich nicht möglich. Jede Gruppe G besitzt $\{e\}$ und G als *triviale Untergruppen*. Ist $m \in \mathbb{Z}$, so ist $m\mathbb{Z}$, die Menge der ganzzahligen Vielfachen von m, eine Untergruppe der additiven Gruppe $\mathbb{Z}$. Wir werden in 1.3/4 sehen, dass alle Untergruppen in $\mathbb{Z}$ von diesem Typ sind. Allgemeiner kann man die von einem Element a einer Gruppe G erzeugte *zyklische Untergruppe* betrachten. Diese besteht aus allen Potenzen a^n, $n \in \mathbb{Z}$, wobei man $a^n = (a^{-1})^{-n}$ für $n < 0$ setze; man vergleiche hierzu auch Abschnitt 1.3.

Definition 4. *Es seien G, G' Monoide mit den Einselementen e und e'. Ein* Monoidhomomorphismus $\varphi\colon G \longrightarrow G'$ *ist eine Abbildung φ von G nach G' mit*

(i) $\varphi(e) = e'$,

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ *für alle $a, b \in G$.*

Sind G, G' Gruppen, so heißt φ auch Gruppenhomomorphismus.

Bemerkung 5. *Eine Abbildung $\varphi\colon G \longrightarrow G'$ zwischen Gruppen ist genau dann ein Gruppenhomomorphismus, wenn $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$ gilt.*

Beweis. Es folgt $\varphi(e) = e'$ aus $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$. □

Bemerkung 6. *Ist $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus, so folgt $\varphi(a^{-1}) = (\varphi(a))^{-1}$ für alle $a \in G$.*

Beweis. $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$. □

Ein Gruppenhomomorphismus $\varphi\colon G \longrightarrow G'$ heißt *Isomorphismus*, falls φ ein Inverses besitzt, d. h. falls es einen Gruppenhomomorphismus $\psi\colon G' \longrightarrow G$ mit $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_{G'}$ gibt. Äquivalent hierzu ist, dass der Homomorphismus φ bijektiv ist. Injektive (bzw. surjektive) Gruppenhomomorphismen $G \longrightarrow G'$ nennt man auch *Monomorphismen* (bzw. *Epimorphismen*). Ein *En-*

domorphismus von G ist ein Homomorphismus $G \longrightarrow G$, ein *Automorphismus* von G ein Isomorphismus $G \longrightarrow G$.

Seien $\varphi\colon G \longrightarrow G'$ und $\psi\colon G' \longrightarrow G''$ Gruppenhomomorphismen. Dann ist auch die Komposition $\psi \circ \varphi\colon G \longrightarrow G''$ ein Gruppenhomomorphismus. Weiter kann man zu $\varphi\colon G \longrightarrow G'$ die Untergruppen

$$\ker \varphi = \{g \in G\,;\, \varphi(g) = 1\} \subset G \qquad (\textit{Kern} \text{ von } \varphi)$$

sowie

$$\operatorname{im} \varphi = \varphi(G) \subset G' \qquad (\textit{Bild} \text{ von } \varphi)$$

bilden. Die Injektivität von φ ist äquivalent zu $\ker \varphi = \{1\}$. Im Folgenden seien noch einige Beispiele für Homomorphismen notiert.

(1) Sei G ein Monoid. Für festes $x \in G$ definiert

$$\varphi\colon \mathbb{N} \longrightarrow G, \qquad n \longmapsto x^n,$$

einen Monoidhomomorphismus, wenn man $\mathbb{N}$ als Monoid unter der Addition auffasst. Ist G eine Gruppe, so erhält man in gleicher Weise einen Gruppenhomomorphismus

$$\varphi\colon \mathbb{Z} \longrightarrow G, \qquad n \longmapsto x^n,$$

wobei $x^n := (x^{-1})^{-n}$ für $n < 0$ gesetzt sei. Umgekehrt ist klar, dass jeder Monoidhomomorphismus $\varphi\colon \mathbb{N} \longrightarrow G$ bzw. jeder Gruppenhomomorphismus $\varphi\colon \mathbb{Z} \longrightarrow G$ von dieser Gestalt ist; man setze $x = \varphi(1)$.

(2) Sei G eine Gruppe, $S(G)$ die Gruppe der bijektiven Selbstabbildungen von G. Für $a \in G$ definiere man $\tau_a \in S(G)$ als *Linkstranslation* mit a auf G, d. h.

$$\tau_a\colon G \longrightarrow G, \qquad g \longmapsto ag.$$

Dann ist

$$G \longrightarrow S(G), \qquad a \longmapsto \tau_a,$$

ein injektiver Gruppenhomomorphismus. Man kann daher G mit seinem Bild in $S(G)$ identifizieren, so dass G zu einer Untergruppe von $S(G)$ Anlass gibt. Insbesondere lässt sich eine Gruppe von n Elementen stets als Untergruppe der Permutationsgruppe $\mathfrak{S}_n$ interpretieren, ein Resultat, welches man auch als Satz von Cayley bezeichnet.

Analog zu den Linkstranslationen kann man auch *Rechtstranslationen* auf G erklären. Diese eignen sich ebenfalls dazu, einen injektiven Gruppenhomomorphismus $G \longrightarrow S(G)$ zu konstruieren; vgl. Aufgabe 4.

(3) Sei G eine abelsche Gruppe, $n \in \mathbb{N}$. Dann ist

$$G \longrightarrow G, \qquad g \longmapsto g^n,$$

ein Gruppenhomomorphismus.

(4) Sei G eine Gruppe, $a \in G$. Dann ist

$$\varphi_a \colon G \longrightarrow G, \qquad g \longmapsto aga^{-1},$$

ein so genannter *innerer Automorphismus* von G. Die Menge $\mathrm{Aut}(G)$ der Automorphismen von G ist unter der Komposition als Verknüpfung eine Gruppe, und die Abbildung $G \longrightarrow \mathrm{Aut}(G)$, $a \longmapsto \varphi_a$, ist ein Gruppenhomomorphismus.

(5) Die reelle Exponentialfunktion definiert einen Gruppenisomorphismus $\mathbb{R} \xrightarrow{\sim} \mathbb{R}_{>0}$. Um dies zu verifizieren, müssen wir natürlich die aus der Analysis bekannten Eigenschaften der Exponentialfunktion benutzen, insbesondere die Funktionalgleichung $\exp(x+y) = \exp(x) \cdot \exp(y)$.

Aufgaben

1. *Man führe den Beweis zu Bemerkung* 2.
2. *Die Exponentialfunktion liefert einen Isomorphismus zwischen der additiven Gruppe* $\mathbb{R}$ *und der multiplikativen Gruppe* $\mathbb{R}_{>0}$. *Man überlege, ob es auch einen Isomorphismus zwischen der additiven Gruppe* $\mathbb{Q}$ *und der multiplikativen Gruppe* $\mathbb{Q}_{>0}$ *geben kann.*
3. Für ein Monoid G betrachte man die folgenden Bedingungen:
   (i) G ist eine Gruppe.
   (ii) Für $a, x, y \in G$ mit $ax = ay$ oder $xa = ya$ folgt stets $x = y$.

   Es gilt stets (i) $\Longrightarrow$ (ii). Man zeige, dass die Umkehrung für endliche Monoide G richtig ist, nicht aber für beliebige Monoide G.
4. Es sei G eine Gruppe. In Analogie zur Notation der Linkstranslation erkläre man Rechtstranslationen auf G und konstruiere mit deren Hilfe einen injektiven Gruppenhomomorphismus $G \longrightarrow S(G)$.
5. Es sei X eine Menge mit einer Teilmenge $Y \subset X$. Man zeige, dass man die Gruppe $S(Y)$ in kanonischer Weise als Untergruppe von $S(X)$ auffassen kann.
6. Es sei G eine endliche abelsche Gruppe. Dann gilt $\displaystyle\prod_{g \in G} g^2 = 1$.
7. Es sei G eine Gruppe. Für alle $a \in G$ gelte $a^2 = 1$. Man zeige, dass G abelsch ist.
8. Es sei G eine Gruppe mit Untergruppen $H_1, H_2 \subset G$. Man zeige, dass $H_1 \cup H_2$ genau dann eine Untergruppe von G ist, wenn $H_1 \subset H_2$ oder $H_2 \subset H_1$ gilt.

1.2 Nebenklassen, Normalteiler, Faktorgruppen

Es sei G eine Gruppe, $H \subset G$ eine Untergruppe. Eine *Linksnebenklasse* von H in G ist eine Teilmenge von G der Gestalt

$$aH := \{ah \,;\, h \in H\},$$

wobei $a \in G$.

Satz 1. *Je zwei Linksnebenklassen von H in G sind gleichmächtig*[2]*; verschiedene Linksnebenklassen von H in G sind disjunkt. Insbesondere ist G disjunkte Vereinigung der Linksnebenklassen von H.*

Beweis. Für $a \in G$ ist die Linkstranslation $H \longrightarrow aH$, $h \longmapsto ah$, bijektiv. Folglich sind alle Linksnebenklassen gleichmächtig. Die zweite Behauptung ergibt sich aus folgendem Lemma:

Lemma 2. *Seien aH und bH Linksnebenklassen von H in G. Dann ist äquivalent*:

(i) $aH = bH$.
(ii) $aH \cap bH \neq \emptyset$.
(iii) $a \in bH$.
(iv) $b^{-1}a \in H$.

Beweis. Aus (i) folgt wegen $H \neq \emptyset$ trivialerweise (ii). Ist (ii) gegeben, so existiert ein $c \in aH \cap bH$, etwa $c = ah_1 = bh_2$ mit $h_1, h_2 \in H$. Es folgt $a = bh_2h_1^{-1} \in bH$ und somit (iii) bzw. die hierzu äquivalente Bedingung (iv). Gilt schließlich (iv), so erhält man $a \in bH$ und folglich $aH \subset bH$. Da mit $b^{-1}a$ aber auch das hierzu inverse Element $a^{-1}b$ zu H gehört, folgt entsprechend $bH \subset aH$ und somit $aH = bH$. □

Die Elemente einer Linksnebenklasse aH werden auch als *Repräsentanten* dieser Nebenklasse bezeichnet. Insbesondere ist also a ein Repräsentant der Nebenklasse aH. Für jeden Repräsentanten $a' \in aH$ gilt aufgrund des Lemmas $a'H = aH$. Die Menge der Linksnebenklassen von H in G wird mit G/H bezeichnet. Man definiert in analoger Weise die Menge $H\backslash G$ der *Rechtsnebenklassen* von H in G, d. h. der Teilmengen der Gestalt

$$Ha = \{ha\,;\, h \in H\},$$

wobei $a \in G$. Man prüft leicht nach, dass die bijektive Abbildung

$$G \longrightarrow G, \qquad g \longmapsto g^{-1},$$

eine Linksnebenklasse aH auf die Rechtsnebenklasse Ha^{-1} abbildet und somit eine Bijektion

$$G/H \longrightarrow H\backslash G, \qquad aH \longmapsto Ha^{-1},$$

definiert. Insbesondere gelten daher Satz 1 und Lemma 2 (mit den offensichtlichen Modifikationen in Lemma 2) auch für Rechtsnebenklassen. Man bezeichnet die Anzahl der Elemente von G/H bzw. $H\backslash G$ auch als *Index* $(G : H)$ von H in G. Schreiben wir noch $\operatorname{ord} G$ für die Anzahl der Elemente einer Gruppe G, man nennt dies die *Ordnung* von G, so ergibt sich als Folgerung zu Satz 1:

[2] Zwei Mengen X, Y heißen *gleichmächtig*, wenn es eine bijektive Abbildung $X \longrightarrow Y$ gibt.

Korollar 3 (Satz von Lagrange). *Sei G eine endliche Gruppe, H eine Untergruppe von G. Dann gilt*

$$\operatorname{ord} G = \operatorname{ord} H \cdot (G : H).$$

Definition 4. *Eine Untergruppe $H \subset G$ heißt* Normalteiler *oder* normale Untergruppe *von G, wenn $aH = Ha$ für alle $a \in G$ gilt, d. h. wenn für jedes $a \in G$ die zugehörigen Links- und Rechtsnebenklassen von H in G übereinstimmen. Man bezeichnet die zu a gehörige Nebenklasse aH bzw. Ha dann auch als die* Restklasse *von a modulo H.*

Die Bedingung $aH = Ha$ lässt sich umschreiben zu $aHa^{-1} = H$. Eine Untergruppe $H \subset G$ ist jedoch bereits dann Normalteiler in G, wenn $aHa^{-1} \subset H$ für alle $a \in G$ gilt (alternativ: $H \subset aHa^{-1}$ für alle $a \in G$). Denn $aHa^{-1} \subset H$ ist gleichbedeutend mit $aH \subset Ha$, ebenso $a^{-1}Ha \subset H$ mit $Ha \subset aH$. Im Übrigen ist jede Untergruppe einer kommutativen Gruppe bereits Normalteiler.

Bemerkung 5. *Der Kern eines Gruppenhomomorphismus $\varphi\colon G \longrightarrow G'$ ist stets ein Normalteiler in G.*

Beweis. $\ker\varphi$ ist Untergruppe von G, und man hat $a \cdot (\ker\varphi) \cdot a^{-1} \subset \ker\varphi$ für alle $a \in G$ aufgrund von 1.1/6. □

Wir wollen nun das umgekehrte Problem behandeln und zeigen, dass es zu jedem Normalteiler $N \subset G$ einen Gruppenhomomorphismus $\varphi\colon G \longrightarrow G'$ mit $\ker\varphi = N$ gibt. Die Idee hierzu ist, auf der Menge der Restklassen G/N eine geeignete Gruppenstruktur zu definieren und für φ die kanonische Projektion $\pi\colon G \longrightarrow G/N$ zu nehmen, welche ein Element $a \in G$ auf die zugehörige Restklasse aN abbildet. Sei also $N \subset G$ ein Normalteiler. Definiert man das Produkt von Teilmengen $X, Y \subset G$ durch

$$X \cdot Y : = \{x \cdot y \in G\,;\, x \in X, y \in Y\},$$

so kann man für $a, b \in G$ unter Benutzung der Normalteilereigenschaft von N schreiben:

$$(aN) \cdot (bN) = \{a\} \cdot (Nb) \cdot N = \{a\} \cdot (bN) \cdot N = \{ab\} \cdot (NN) = (ab)N.$$

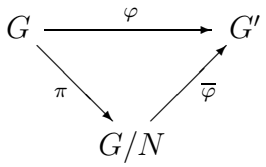
Es ist also das Produkt zweier Nebenklassen mit Repräsentanten a bzw. b wieder eine Nebenklasse, und zwar mit Repräsentant ab. Wir können daher dieses Produkt als Verknüpfung "$\cdot$" in G/N auffassen, und es folgt unmittelbar aus den Gruppeneigenschaften von G, dass G/N mit dieser Verknüpfung eine Gruppe ist; $N = 1N$ ist das Einselement in G/N, und $a^{-1}N$ ist das inverse Element zu $aN \in G/N$. Des Weiteren ist klar, dass die kanonische Projektion

$$\pi\colon G \longrightarrow G/N, \qquad a \longmapsto aN,$$

ein surjektiver Gruppenhomomorphismus mit $\ker\pi = N$ ist. Wir nennen G/N die *Faktor-* oder *Restklassengruppe* von G modulo N.

Für viele Anwendungen ist es wichtig, zu wissen, dass der Gruppenhomomorphismus $\pi\colon G \longrightarrow G/N$ eine so genannte universelle Eigenschaft erfüllt, welche G/N bis auf kanonische Isomorphie eindeutig charakterisiert:

Satz 6 (Homomorphiesatz). *Es sei $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus und $N \subset G$ ein Normalteiler mit $N \subset \ker\varphi$. Dann existiert eindeutig ein Gruppenhomomorphismus $\overline{\varphi}\colon G/N \longrightarrow G'$ mit $\varphi = \overline{\varphi} \circ \pi$, so dass also das Diagramm*



kommutiert. Es gilt

$$\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi, \qquad \ker\overline{\varphi} = \pi(\ker\varphi), \qquad \ker\varphi = \pi^{-1}(\ker\overline{\varphi}).$$

Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $N = \ker\varphi$ gilt.

Beweis. Wenn $\overline{\varphi}$ existiert, so folgt

$$\overline{\varphi}(aN) = \overline{\varphi}(\pi(a)) = \varphi(a)$$

für $a \in G$, also ist $\overline{\varphi}$ eindeutig. Umgekehrt können wir natürlich $\overline{\varphi}$ durch die Gleichung $\overline{\varphi}(aN) = \varphi(a)$ erklären, wenn wir zeigen, dass $\varphi(a)$ unabhängig von der Auswahl des Repräsentanten $a \in aN$ ist. Gelte also $aN = bN$ für zwei Elemente $a, b \in G$. Dann folgt $b^{-1}a \in N \subset \ker\varphi$ und somit $\varphi(b^{-1}a) = 1$, also $\varphi(a) = \varphi(b)$. Dass $\overline{\varphi}$ ein Gruppenhomomorphismus ist, ergibt sich aus der Definition der Gruppenstruktur auf G/N oder, anders ausgedrückt, aus der Tatsache, dass π ein Epimorphismus ist. Existenz und Eindeutigkeit von $\overline{\varphi}$ sind damit geklärt.

Die Gleichung $\ker\varphi = \pi^{-1}(\ker\overline{\varphi})$ folgt aus der Tatsache, dass φ die Komposition von $\overline{\varphi}$ mit π ist. Weiter gelten $\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi$ und $\ker\overline{\varphi} = \pi(\ker\varphi)$ aufgrund der Surjektivität von π. □

Korollar 7. *Ist $\varphi\colon G \longrightarrow G'$ ein surjektiver Gruppenhomomorphismus, so ist G' kanonisch isomorph zu $G/\ker\varphi$.*

Wir wollen als Anwendung von Satz 6 die so genannten Isomorphiesätze für Gruppen beweisen.

Satz 8 (1. Isomorphiesatz). *Es sei G eine Gruppe, $H \subset G$ eine Untergruppe und $N \subset G$ ein Normalteiler. Dann ist HN Untergruppe von G mit Normalteiler N, und $H \cap N$ ist Normalteiler von H. Der kanonische Homomorphismus*

$$H/H \cap N \longrightarrow HN/N$$

ist ein Isomorphismus.

Beweis. Unter Benutzung der Normalteilereigenschaft von N zeigt man unmittelbar, dass HN Untergruppe von G mit Normalteiler N ist. Man betrachte dann den Homomorphismus

$$H \hookrightarrow HN \xrightarrow{\pi} HN/N,$$

wobei π die kanonische Projektion bezeichne. Dieser ist surjektiv und besitzt $H \cap N$ als Kern. Somit ist $H \cap N$ Normalteiler in H, und der induzierte Homomorphismus

$$H/H \cap N \longrightarrow HN/N$$

ist nach Satz 6 oder Korollar 7 ein Isomorphismus. □

Satz 9 (2. Isomorphiesatz). *Sei G eine Gruppe, und seien N, H Normalteiler in G mit $N \subset H \subset G$. Dann ist N auch Normalteiler in H, und man kann H/N als Normalteiler von G/N auffassen. Der kanonische Gruppenhomomorphismus*

$$(G/N)/(H/N) \longrightarrow G/H$$

ist ein Isomorphismus.

Beweis. Wir wollen zunächst überlegen, dass man H/N als Untergruppe von G/N auffassen kann. Man betrachte hierzu den Gruppenhomomorphismus

$$H \hookrightarrow G \xrightarrow{\pi} G/N,$$

wobei π wieder die kanonische Projektion bezeichne. Da dieser Homomorphismus N als Kern besitzt, liefert er mit Satz 6 einen Monomorphismus $H/N \hookrightarrow G/N$, so dass wir H/N mit seinem Bild in G/N identifizieren können.

Als Nächstes beachte man, dass der Kern H der kanonischen Projektion $G \longrightarrow G/H$ den Normalteiler N enthält. Also induziert dieser Epimorphismus gemäß Satz 6 einen Epimorphismus $G/N \longrightarrow G/H$, dessen Kern ein Normalteiler ist und mit dem Bild von H unter der Projektion $G \longrightarrow G/N$ übereinstimmt. Dieses Bild hatten wir gerade mit H/N identifiziert. Wenden wir dann Satz 6 bzw. Korollar 7 nochmals an, so folgt, dass $G/N \longrightarrow G/H$ einen Isomorphismus

$$(G/N)/(H/N) \xrightarrow{\simeq} G/H$$

induziert. □

Aufgaben

1. *Sei G eine Gruppe und H eine Untergruppe vom Index 2. Man zeige, dass H Normalteiler in G ist. Gilt die gleiche Aussage auch für den Fall, dass H vom Index 3 ist?*

2. *Sei G eine Gruppe und $N \subset G$ ein Normalteiler. Man gebe eine alternative Konstruktion der Faktorgruppe G/N an, indem man die* Menge $X = G/N$ *der Linksnebenklassen von N in G betrachtet und die Existenz eines Gruppenhomomorphismus $\varphi\colon G \longrightarrow S(X)$ mit $\ker\varphi = N$ zeigt.*

3. Sei X eine Menge, $Y \subset X$ eine Teilmenge, G eine Gruppe und G^X die Gruppe der G-wertigen Funktionen auf X. Sei $N := \{f \in G^X\,;\, f(y) = 1 \text{ für alle } y \in Y\}$. Man zeige, dass N ein Normalteiler in G^X mit $G^X/N \simeq G^Y$ ist.

4. Sei $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Man zeige:
   (i) Ist $H \subset G$ Untergruppe, so ist $\varphi(H)$ Untergruppe in G'. Die entsprechende Aussage für Normalteiler ist allgemein nur dann richtig, wenn φ surjektiv ist.
   (ii) Ist $H' \subset G'$ Untergruppe (bzw. Normalteiler) in G', so gilt dasselbe für $\varphi^{-1}(H') \subset G$.

5. Sei G eine endliche Gruppe, $H_1, H_2 \subset G$ seien Untergruppen mit $H_1 \subset H_2$. Dann gilt $(G : H_1) = (G : H_2) \cdot (H_2 : H_1)$.

6. Eine Gruppe G enthalte einen Normalteiler N mit der folgenden Maximalitätseigenschaft: Ist $H \subset G$ Untergruppe mit $H \supset N$, so gilt bereits $H = G$ oder $H = N$. Man zeige, dass je zwei Untergruppen $H_1, H_2 \subset G$ mit $H_1 \neq \{1\} \neq H_2$ und $H_1 \cap N = H_2 \cap N = \{1\}$ zueinander isomorph sind.

1.3 Zyklische Gruppen

Sei G eine Gruppe und $X \subset G$ eine Teilmenge. Definiert man H als Durchschnitt aller Untergruppen von G, welche X enthalten, so ist H wieder eine Untergruppe von G, und zwar die (eindeutig bestimmte) kleinste Untergruppe von G, welche X enthält. Man sagt, H werde von X erzeugt oder, wenn H schon gleich G ist, G werde von X erzeugt. Die von X in G erzeugte Untergruppe H kann auch in konkreter Weise angegeben werden. Sie besteht aus allen Elementen der Form

$$x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n}$$

mit $x_1, \ldots, x_n \in X$ und $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$, wobei n in $\mathbb{N}$ variieren darf. (Die so beschriebenen Elemente bilden offenbar die kleinste Untergruppe von G, die X enthält, und dies ist nach Definition die Gruppe H.)

Im Folgenden interessieren wir uns nur für den Fall, dass X aus genau einem Element x besteht. Die Beschreibung der von einem Element $x \in G$ erzeugten Untergruppe, für die wir auch die Notation $\langle x \rangle$ verwenden, vereinfacht sich dann:

Bemerkung 1. *Sei x ein Element einer Gruppe G. Dann besteht die von x erzeugte Untergruppe $\langle x\rangle \subset G$ aus allen Potenzen x^n, $n \in \mathbb{Z}$. Mit anderen Worten, $\langle x\rangle$ ist gleich dem Bild des Gruppenhomomorphismus*

$$\mathbb{Z} \longrightarrow G, \qquad n \longmapsto x^n,$$

wobei mit $\mathbb{Z}$ die additive Gruppe der ganzen Zahlen gemeint sei. Insbesondere ist $\langle x\rangle$ kommutativ.

Definition 2. *Eine Gruppe G heißt* zyklisch, *wenn sie von einem Element erzeugt wird. Äquivalent hierzu ist, dass es einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \longrightarrow G$ gibt.*

Man beachte, dass für eine kommutative Gruppe G mit additiv geschriebener Verknüpfung die Abbildung $\mathbb{Z} \longrightarrow G$ aus Bemerkung 1 durch die Vorschrift $n \longmapsto n \cdot x$ gegeben wird. Dabei ist $n \cdot x$ für $n \geq 0$ als n-fache Summe von x aufzufassen und für $n < 0$ als $(-n)$-fache Summe von $-x$. Insbesondere ist damit klar, dass die additive Gruppe $\mathbb{Z}$ von dem Element $1 \in \mathbb{Z}$ erzeugt wird und somit zyklisch ist. Man nennt $\mathbb{Z}$ die *freie zyklische Gruppe*; die Ordnung dieser Gruppe ist unendlich. Für $m \in \mathbb{Z}$ ist aber auch die Untergruppe $m\mathbb{Z}$ aller ganzzahligen Vielfachen von m zyklisch, ebenso wie die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$. Ist $m \neq 0$, etwa $m > 0$, so bezeichnet man $\mathbb{Z}/m\mathbb{Z}$ als *zyklische Gruppe der Ordnung* m. In der Tat besteht $\mathbb{Z}/m\mathbb{Z}$ für $m > 0$ aus genau m Elementen, nämlich aus den Restklassen $0+m\mathbb{Z}, \ldots, (m-1)+m\mathbb{Z}$. Wir wollen im Folgenden zeigen, dass $\mathbb{Z}$ und die Gruppen des Typs $\mathbb{Z}/m\mathbb{Z}$ bis auf Isomorphie die einzigen zyklischen Gruppen sind. Mit Hilfe des Homomorphiesatzes (in der Version 1.2/7) sieht man, dass eine Gruppe G genau dann zyklisch ist, wenn es einen Isomorphismus $\mathbb{Z}/H \xrightarrow{\sim} G$ gibt, wobei H eine Untergruppe und damit ein Normalteiler von $\mathbb{Z}$ ist. Damit reduziert sich die Bestimmung aller zyklischen Gruppen auf die Bestimmung aller Untergruppen von $\mathbb{Z}$.

Satz 3. *Es sei G eine zyklische Gruppe. Dann gilt*

$$G \simeq \begin{cases} \mathbb{Z}, & \text{falls } \operatorname{ord} G = \infty, \\ \mathbb{Z}/m\mathbb{Z}, & \text{falls } \operatorname{ord} G = m < \infty. \end{cases}$$

Die Gruppen $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ sind bis auf Isomorphie die einzigen zyklischen Gruppen.

Zum Beweis des Satzes genügt es, wie wir gesehen haben, folgendes Lemma bereitzustellen:

Lemma 4. *Sei $H \subset \mathbb{Z}$ Untergruppe. Dann existiert ein $m \in \mathbb{Z}$ mit $H = m\mathbb{Z}$. Insbesondere ist jede Untergruppe von $\mathbb{Z}$ zyklisch.*

Beweis. Wir dürfen $H \neq 0$ annehmen, wobei 0 die nur aus dem Nullelement bestehende Untergruppe von $\mathbb{Z}$ bezeichne. Dann gibt es in H positive Elemente; es

sei m das kleinste positive Element von H. Wir behaupten $H = m\mathbb{Z}$. Natürlich gilt $m\mathbb{Z} \subset H$. Sei umgekehrt $a \in H$. Indem wir a durch m mit Rest dividieren, erhalten wir $q, r \in \mathbb{Z}$, $0 \leq r < m$, mit $a = qm + r$. Dabei ist $r = a - qm$ Element von H und, da alle positiven Elemente von H größer oder gleich m sind, folgt notwendig $r = 0$. Also gilt $a = qm \in m\mathbb{Z}$ und damit $H \subset m\mathbb{Z}$. Insgesamt ergibt sich $H = m\mathbb{Z}$. □

Satz 5. (i) *Ist G eine zyklische Gruppe, so ist jede Untergruppe $H \subset G$ zyklisch.*

(ii) *Ist $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus und ist G zyklisch, so sind auch* $\ker\varphi$ *und* $\operatorname{im}\varphi$ *zyklisch.*

Beweis. Es ergibt sich unmittelbar aus der Definition zyklischer Gruppen, dass das Bild einer zyklischen Gruppe unter einem Gruppenhomomorphismus $\varphi\colon G \longrightarrow G'$ wieder zyklisch ist. Da $\ker\varphi$ eine Untergruppe von G ist, bleibt somit lediglich Aussage (i) zu verifizieren. Sei also G zyklisch und $H \subset G$ eine Untergruppe. Weiter sei $\pi\colon \mathbb{Z} \longrightarrow G$ ein Epimorphismus. Dann ist $\pi^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$ und somit gemäß Lemma 4 zyklisch. Es folgt, dass H als Bild von $\pi^{-1}(H)$ unter π wieder zyklisch ist, d. h. Aussage (i) ist bewiesen. □

Sei G eine Gruppe. Für ein Element $a \in G$ definiert man dessen *Ordnung* $\operatorname{ord} a$ als die Ordnung der von a erzeugten zyklischen Untergruppe in G. Wir wissen bereits, dass $\varphi\colon \mathbb{Z} \longrightarrow G$, $n \longmapsto a^n$, einen Epimorphismus von $\mathbb{Z}$ auf die von a erzeugte zyklische Untergruppe $H \subset G$ definiert. Gilt $\ker\varphi = m\mathbb{Z}$ und ist die Gruppe G endlich, so folgt notwendig $m \neq 0$, etwa $m > 0$, und es ist H isomorph zu $\mathbb{Z}/m\mathbb{Z}$. Also ist m die kleinste positive Zahl mit der Eigenschaft $a^m = 1$, und man sieht, dass H aus genau den (paarweise verschiedenen) Elementen $1 = a^0, a^1, \ldots, a^{m-1}$ besteht. Insbesondere folgt $\operatorname{ord} a = m$.

Satz 6 (Kleiner Fermatscher Satz). *Sei G eine endliche Gruppe, $a \in G$. Dann ist* $\operatorname{ord} a$ *ein Teiler von* $\operatorname{ord} G$, *und es gilt* $a^{\operatorname{ord} G} = 1$.

Zum *Beweis* wendet man den Satz von Lagrange 1.2/3 auf die von a erzeugte zyklische Untergruppe von G an.

Korollar 7. *Für eine Gruppe G sei $p := \operatorname{ord} G$ eine Primzahl. Dann ist G zyklisch, $G \simeq \mathbb{Z}/p\mathbb{Z}$, und für jedes $a \in G$, $a \neq 1$, folgt* $\operatorname{ord} a = p$. *Insbesondere erzeugt jedes solche a die zyklische Gruppe G.*

Beweis. Sei $a \in G$, $a \neq 1$, und sei $H \subset G$ die von a erzeugte zyklische Gruppe. Da $\operatorname{ord} a = \operatorname{ord} H$ größer als 1 ist, nach Satz 6 aber auch ein Teiler von $p = \operatorname{ord} G$ sein muss, folgt $\operatorname{ord} a = \operatorname{ord} H = p$. Also hat man $H = G$, d. h. G wird von a erzeugt und ist somit zyklisch. Wegen Satz 3 ist G isomorph zu $\mathbb{Z}/p\mathbb{Z}$. □

Aufgaben

1. *Für $m \in \mathbb{N}-\{0\}$ setze man $G_m := \{0, 1, \ldots, m-1\}$. Durch*

$$a \circ b := \text{ der Rest von } a+b \text{ bei Division durch } m$$

wird auf G_m eine Verknüpfung erklärt. Man mache sich in direkter Weise klar, dass "$\circ$" eine Gruppenstruktur auf G_m definiert und dass die entstehende Gruppe isomorph zu $\mathbb{Z}/m\mathbb{Z}$ ist.

2. *Für $m \in \mathbb{N}-\{0\}$ bestimme man alle Untergruppen von $\mathbb{Z}/m\mathbb{Z}$.*

3. Man betrachte $\mathbb{Z}$ als additive Untergruppe von $\mathbb{Q}$ und zeige:
   (i) Jedes Element in $\mathbb{Q}/\mathbb{Z}$ ist von endlicher Ordnung.
   (ii) Für jedes $n \in \mathbb{N}-\{0\}$ besitzt $\mathbb{Q}/\mathbb{Z}$ genau eine Untergruppe der Ordnung n, und diese ist zyklisch.

4. Es seien $m, n \in \mathbb{N}-\{0\}$. Man zeige, dass die Gruppen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ genau dann isomorph sind, wenn m und n teilerfremd sind. Insbesondere ist ein Produkt zweier zyklischer Gruppen mit teilerfremden Ordnungen wieder zyklisch.

5. Es sei $\varphi\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ ein Endomorphismus des n-fachen Produkts der additiven Gruppe $\mathbb{Z}$, wobei $n \in \mathbb{N}$. Man zeige: φ ist genau dann injektiv, wenn $\mathbb{Z}^n/\operatorname{im}\varphi$ eine endliche Gruppe ist. (Hinweis: Man betrachte den zu φ gehörigen Homomorphismus von $\mathbb{Q}$-Vektorräumen $\varphi_{\mathbb{Q}}\colon \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$.)