6. Faktorgruppen

Im vorangegangenen Kapitel haben wir zu einer Untergruppe U einer gegebenen Gruppe G die Menge der Linksnebenklassen $G/U = \{aU : a \in G\}$ untersucht und damit bereits einige interessante Resultate wie z. B. den Satz 5.10 von Lagrange erhalten.

Eine Menge ist für sich genommen aber noch keine besonders interessante Struktur. Wünschenswert wäre es natürlich, wenn wir G/U nicht nur als *Menge*, sondern ebenfalls wieder als *Gruppe* auffassen könnten, also wenn wir aus der gegebenen Verknüpfung in G auch eine Verknüpfung in G/U konstruieren könnten. Wir wollen daher in diesem Kapitel untersuchen, wann und wie dies möglich ist.

Als Erstes benötigen wir dazu eine wichtige Vorbemerkung, die immer dann relevant ist, wenn wir auf einer Menge von Äquivalenzklassen eine Funktion (oder Verknüpfung) definieren wollen.

Bemerkung 6.1 (Wohldefiniertheit)**.** Erinnern wir uns noch einmal an die Konstruktion des Signums einer Permutation $\sigma \in S_n$ aus Definition 2.13: Wir mussten hierfür eine Darstellung $\sigma = \tau_1 \cdots \tau_r$ von σ als Verkettung von Transpositionen $\tau_1, \ldots, \tau_r$ wählen, und haben dann $\operatorname{sign}\sigma := (-1)^r$ gesetzt. Damit dies die Zahl $\operatorname{sign}\sigma$ auch wirklich widerspruchsfrei definiert, mussten wir dabei natürlich überprüfen, dass das Gesamtresultat dieser Vorschrift von der zwischendurch nötigen Wahl der Verkettung von Transpositionen unabhängig ist: Lemma 2.12 (b) hat uns gesagt, dass bei einer anderen solchen Darstellung $\sigma = \tilde{\tau}_1 \cdots \tilde{\tau}_s$ in jedem Fall r und s beide gerade oder beide ungerade sind, so dass das Endergebnis $(-1)^r = (-1)^s$ immer dasselbe ist.

Abstrakt formuliert passiert es bei der Definition mathematischer Funktionen manchmal, dass die Abbildungsvorschrift an irgendeiner Stelle eine nicht eindeutig bestimmte Wahl erfordert. Wenn dies wie im Beispiel des Signums oben der Fall ist, ist es klar, dass wir am Ende überprüfen müssen, dass das Endresultat der Vorschrift nicht von dieser Wahl abhängt. Die mathematische Sprechweise hierfür ist, dass wir überprüfen müssen, ob die Funktion durch die gegebene Vorschrift **wohldefiniert** ist.

Besonders oft tritt dies bei der Untersuchung von Äquivalenzrelationen wie in Kapitel 5 auf. Ist $\sim$ eine Äquivalenzrelation auf einer Menge M und will man eine Abbildung $f\colon M/\sim \to N$ von der Menge der zugehörigen Äquivalenzklassen in eine weitere Menge N definieren, so ist die Idee hierfür in der Regel, dass man eine Abbildung $g\colon M \to N$ wählt und dann

$$f\colon M/\sim \to N,\ f(\overline{a}) := g(a)$$

setzt. Man möchte das Bild einer Äquivalenzklasse unter f also dadurch definieren, dass man einen Repräsentanten dieser Klasse wählt und diesen Repräsentanten dann mit g abbildet. Damit diese Vorschrift wohldefiniert ist, brauchen wir also offensichtlich, dass verschiedene Repräsentanten derselben Klasse das gleiche Endergebnis liefern, also dass gilt:

$$\text{Für alle } a,b \in M \text{ mit } \overline{a} = \overline{b} \text{ ist } g(a) = g(b).$$

Beispiel 6.2 (Verknüpfungen auf G/U)**.** Wir wollen nun wieder unsere ursprüngliche Situation betrachten, nämlich eine Menge G/U von Linksnebenklassen zu einer Untergruppe U einer gegebenen Gruppe G. Es ist natürlich sehr naheliegend, auf G/U eine Verknüpfung durch

$$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

definieren zu wollen: Um zwei Äquivalenzklassen in G/U miteinander zu verknüpfen, verknüpfen wir einfach zwei zugehörige Repräsentanten in G und nehmen dann vom Ergebnis wieder die Äquivalenzklasse.

(a) Als konkretes Beispiel betrachten wir noch einmal die Menge $\mathbb{Z}_{12} = \{\overline{0}, \dots, \overline{11}\}$ der Stände einer Uhr aus Beispiel 5.2 (b) bzw. Beispiel 5.8 (a). Wir würden also die Addition von $\mathbb{Z}$ auf $\mathbb{Z}_{12}$ übertragen wollen, indem wir z. B.

$$\overline{6} + \overline{8} = \overline{6+8} = \overline{14} = \overline{2}$$

rechnen: Wenn seit Mitternacht zuerst 6 und dann nochmal 8 Stunden vergehen, zeigt die Uhr anschließend auf die 2. Nach Bemerkung 6.1 müssen wir allerdings noch überprüfen, ob diese neue Verknüpfung auf $\mathbb{Z}_{12}$ wirklich wohldefiniert ist: Im Beispiel hätten wir statt der Repräsentanten 6 und 8 von $\overline{6}$ und $\overline{8}$ ja z. B. auch 18 bzw. 20 wählen können. In der Tat hätten wir dann allerdings ebenfalls wieder dasselbe Endergebnis

$$\overline{6} + \overline{8} = \overline{18+20} = \overline{38} = \overline{2}$$

erhalten: Auch wenn zuerst 18 und dann nochmal 20 Stunden vergehen, zeigt die Uhr danach auf die 2. In diesem Beispiel scheint die Situation also erst einmal in Ordnung zu sein. In der Tat ist die Verknüpfung in diesem Fall wohldefiniert, wie wir gleich in Beispiel 6.15 noch allgemein sehen werden. Leider ist dies jedoch nicht immer der Fall, wie das folgende Beispiel zeigt.

(b) Wir betrachten noch einmal das Beispiel 5.8 (b) der Untergruppe

$$U = \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\}$$

von S_3 mit den drei Linksnebenklassen

$$\overline{\mathrm{id}} = \{\mathrm{id}, (1\ 2)\}, \quad \overline{\sigma_1} = \{(1\ 2\ 3), (1\ 3)\}, \quad \overline{\sigma_2} = \{(1\ 3\ 2), (2\ 3)\},$$

wobei $\sigma_1 = (1\ 2\ 3)$ und $\sigma_2 = (1\ 3\ 2)$. Angenommen, wir könnten auch hier die Nebenklassen dadurch miteinander verknüpfen, dass wir einfach Repräsentanten der beiden Klassen miteinander verknüpfen und vom Ergebnis wieder die Nebenklasse nehmen. Um z. B. $\overline{\mathrm{id}} \circ \overline{\sigma_1}$ zu berechnen, könnten wir also den jeweils ersten oben aufgeführten Repräsentanten wählen und

$$\overline{\mathrm{id}} \circ \overline{\sigma_1} = \overline{\mathrm{id} \circ (1\ 2\ 3)} = \overline{(1\ 2\ 3)} = \overline{\sigma_1}$$

rechnen. Hätten wir für die erste Nebenklasse $\overline{\mathrm{id}}$ jedoch den zweiten Repräsentanten gewählt, so hätten wir als Ergebnis

$$\overline{\mathrm{id}} \circ \overline{\sigma_1} = \overline{(1\ 2) \circ (1\ 2\ 3)} = \overline{(2\ 3)} = \overline{\sigma_2}$$

erhalten, also nicht das gleiche wie vorher! Die Verknüpfung auf der Menge der Nebenklassen ist hier also nicht wohldefiniert.

Wir wollen diese Situation nun klären und herausfinden, in welchen Fällen die Gruppenverknüpfung in G auf eine in G/U übertragen werden kann. Die Eigenschaft von U, die wir hierfür benötigen, ist die folgende.

Definition 6.3 (Normalteiler)**.** Eine Teilmenge U einer Gruppe G heißt ein **Normalteiler**, in Zeichen $U \trianglelefteq G$, wenn gilt:

(a) U ist eine Untergruppe von G;

(b) für alle $a \in G$ und $u \in U$ ist $aua^{-1} \in U$.

Bemerkung 6.4. Da die Bedingung (b) in Definition 6.3 für alle $a \in G$ gelten muss, können wir dort auch genauso gut a durch a^{-1} ersetzen und erhalten die äquivalente Bedingung $a^{-1}ua \in U$.

Lemma 6.5. *Eine Untergruppe U einer Gruppe G ist genau dann ein Normalteiler, wenn $aU = Ua$ für alle $a \in G$ gilt, also wenn die Links- und Rechtsnebenklassen von U übereinstimmen.*

Beweis.

„⇒“ Ist $U \trianglelefteq G$, so gilt für alle $a \in G$ und $u \in U$ nach Bemerkung 6.4

$$aua^{-1} \in U \overset{\cdot a}{\Rightarrow} au \in Ua \Rightarrow aU \subset Ua$$
$$\text{und} \quad a^{-1}ua \in U \overset{a\cdot}{\Rightarrow} ua \in aU \Rightarrow Ua \subset aU,$$

und damit insgesamt $Ua = aU$.

„⇐“ Gilt $aU = Ua$ für alle $a \in G$, so ist $au \in aU = Ua$ und damit $aua^{-1} \in Uaa^{-1} = U$ für alle $u \in U$. □

Beispiel 6.6.

(a) Ist G abelsch, so ist jede Untergruppe U von G ein Normalteiler: Die Eigenschaft (b) aus Definition 6.3 ist hier natürlich stets erfüllt, denn es ist ja $aua^{-1} = aa^{-1}u = u \in U$ für alle $a \in G$ und $u \in U$.

(b) Die trivialen Untergruppen $\{e\}$ und G sind immer Normalteiler von G: In beiden Fällen sind die Eigenschaften aus Definition 6.3 offensichtlich.

(c) Die in Beispiel 6.2 (b) betrachtete Untergruppe $U = \langle (1\ 2) \rangle$ von S_3 ist kein Normalteiler: In der Tat haben wir in Beispiel 5.8 (b) konkret nachgeprüft, dass die äquivalente Normalteilerbedingung aus Lemma 6.5 in diesem Fall nicht erfüllt ist.

Ein weiteres, sehr wichtiges Beispiel von Normalteilern ist das folgende:

Lemma 6.7. *Ist $f\colon G \to H$ ein Gruppenhomomorphismus, so ist* $\operatorname{Ker} f$ *ein Normalteiler von G.*

Beweis. Wir wissen bereits (siehe Definition 4.14), dass $\operatorname{Ker} f$ eine Untergruppe von G ist. Weiterhin gilt für alle $a \in G$ und $u \in \operatorname{Ker} f$ nach Lemma 4.4

$$f(aua^{-1}) = f(a)\underbrace{f(u)}_{=e}f(a^{-1}) = f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e,$$

also $aua^{-1} \in \operatorname{Ker} f$. Damit ist $\operatorname{Ker} f$ ein Normalteiler von G. □

Beispiel 6.8. Die alternierende Gruppe (siehe Definition 4.16)

$$A_n = \{\sigma \in S_n : \operatorname{sign}\sigma = 1\}$$

ist als Kern der Signumsabbildung ein Normalteiler von S_n.

Aufgabe 6.9. Es sei U eine Untergruppe einer endlichen Gruppe G. Man zeige:

(a) Gibt es keine weitere Untergruppe von G, die genauso viele Elemente wie U hat, so ist U ein Normalteiler von G.

(b) Ist $|U| = \frac{1}{2}|G|$, so ist U ein Normalteiler von G.

Aufgabe 6.10. Welche der folgenden Teilmengen $U \subset G$ sind Normalteiler?

(a) $G = \mathbb{Z}$, $U = \{1, -1\}$;

(b) $G = S_n$, $U = \{\sigma \in S_n : \sigma(1) = 1\}$ für ein $n \in \mathbb{N}_{\geq 2}$;

(c) G eine beliebige Gruppe, $U = f^{-1}(N)$ für einen Gruppenhomomorphismus $f\colon G \to H$ und $N \trianglelefteq H$;

(d) G eine Gruppe mit $|G| = 24$, $U = \langle a, b \rangle$ für gewisse $a, b \in G$ mit $\operatorname{ord}(a) = 4$ und $\operatorname{ord}(b) = 3$.

Aufgabe 6.11. In einer Gruppe G seien U eine Untergruppe und N ein Normalteiler. Zeige, dass $UN := \{un : u \in U, n \in N\}$ dann eine Untergruppe von G ist.

Aufgabe 6.12. Es sei U eine Untergruppe einer Gruppe G.

Zeige, dass

$$V := \{(a, ua) : a \in G, u \in U\} \quad \subset G \times G$$

genau dann eine Untergruppe von $G \times G$ ist, wenn U ein Normalteiler von G ist.

Wie bereits angekündigt wollen wir nun sehen, dass sich die Gruppenverknüpfung von G auf eine in G/U überträgt, wenn U ein Normalteiler ist.

Satz und Definition 6.13 (Faktorgruppen)**.** *Es sei G eine Gruppe und $U \trianglelefteq G$. Dann gilt:*

(a) *Die Verknüpfung $\overline{a} \cdot \overline{b} := \overline{ab}$ ist wohldefiniert auf G/U und macht G/U zu einer Gruppe. Das neutrale Element dieser Gruppe ist $\overline{e}$, das zu $\overline{a}$ inverse Element ist $\overline{a^{-1}}$. Die Gruppe G/U wird als eine **Faktorgruppe** von G bezeichnet.*

(b) *Die Abbildung $\pi \colon G \to G/U$, $\pi(a) = \overline{a}$ ist ein surjektiver Morphismus mit Kern U. Man nennt sie die **Restklassenabbildung** von G/U.*

Beweis.

(a) Die Verknüpfung ist wohldefiniert: Sind $a, a', b, b' \in G$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, gilt also $a^{-1}a' =: u \in U$ und $b^{-1}b' =: v \in U$, so ist

$$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = b^{-1}ub' = b^{-1}ubb^{-1}b' = \underbrace{b^{-1}ub}_{\in U}v \in U,$$

wobei $b^{-1}ub \in U$ aus der Normalteilereigenschaft folgt. Also ist $\overline{ab} = \overline{a'b'}$ und die Verknüpfung damit wohldefiniert. Die Gruppenaxiome für G/U rechnet man nun ganz einfach nach:

(G1) Für alle $a, b, c \in G$ gilt

$$\left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} \overset{(*)}{=} \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right),$$

wobei $(*)$ die Assoziativität in G ist und alle anderen Gleichungen einfach nur die Definition der Verknüpfung auf G/U sind.

(G2) Für alle $a \in G$ ist $\overline{e} \cdot \overline{a} = \overline{ea} = \overline{a}$.

(G3) Für alle $a \in G$ ist $\overline{a^{-1}} \cdot \overline{a} = \overline{a^{-1}a} = \overline{e}$.

(b) Die Abbildung π ist nach Definition der Verknüpfung auf G/U ein Morphismus: Für alle $a, b \in G$ gilt nämlich

$$\pi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \pi(a) \cdot \pi(b).$$

Nach Definition von G/U ist π surjektiv. Der Kern von π ist

$$\operatorname{Ker} \pi = \{a \in G : \overline{a} = \overline{e}\} = \overline{e} = U. \qquad \square$$

Bemerkung 6.14.

(a) Die Normalteilereigenschaft von U ist für Satz 6.13 wirklich notwendig: Ist die Verknüpfung auf G/U wohldefiniert, so muss wegen $\overline{au} = \overline{a}$ für alle $a \in G$ und $u \in U$ insbesondere $\overline{au \cdot a^{-1}} = \overline{a \cdot a^{-1}} = \overline{e}$, also $aua^{-1} \in U$ gelten, und damit U ein Normalteiler sein.

(b) Ist G eine abelsche Gruppe, so auch jede Faktorgruppe G/U: Für alle $a, b \in G$ ist dann nämlich $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$.

(c) Wir hatten in Lemma 6.7 gesehen, dass jeder Kern eines Morphismus ein Normalteiler ist. Nach Satz 6.13 (b) gilt hier auch die Umkehrung: Jeder Normalteiler kann als Kern eines Morphismus geschrieben werden (nämlich als Kern der Restklassenabbildung).

Beispiel 6.15 ($\mathbb{Z}_n$ als Gruppe)**.** Es sei $n \in \mathbb{N}_{>0}$. Die Untergruppe $n\mathbb{Z}$ von $\mathbb{Z}$ ist natürlich ein Normalteiler, da $\mathbb{Z}$ abelsch ist (siehe Beispiel 6.6 (a)). Also ist die Menge $\mathbb{Z}_n$ mit der Verknüpfung $\overline{k} + \overline{l} := \overline{k+l}$, wie wir sie schon in Beispiel 6.2 (a) untersucht haben, nach Satz 6.13 und Bemerkung 6.14 (b) eine abelsche Gruppe. Wir können uns die Verknüpfung dort vorstellen als die gewöhnliche Addition in $\mathbb{Z}$, wobei wir uns bei der Summe aber immer nur den Rest bei Division durch n merken. Die Tabelle rechts zeigt die Verknüpfung dieser Gruppe im Beispiel $n = 3$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Diese Gruppen $(\mathbb{Z}_n, +)$ sind sicher die wichtigsten Beispiele von Faktorgruppen.

Bemerkung 6.16. Eine interessante Anwendung von Faktorgruppen besteht darin, dass man mit ihnen „aus jedem Morphismus einen Isomorphismus machen kann“. Um zu sehen, was damit gemeint ist, betrachten wir einmal einen beliebigen Morphismus $f\colon G \to H$ von Gruppen. Wir haben in Bemerkung 4.9 bereits gesehen, dass Isomorphismen, also bijektive Morphismen, besonders schön sind, da sie bedeuten, dass Start- und Zielraum „als Gruppen ununterscheidbar“ sind und daher miteinander identifiziert werden können.

Nun muss ein Morphismus f im Allgemeinen natürlich weder surjektiv noch injektiv sein. Dies lässt sich aber beheben: Klar ist zunächst einmal, dass man f natürlich immer zu einem surjektiven Morphismus machen kann, indem man den Zielraum H einfach durch die Untergruppe $\operatorname{Im} f$ ersetzt. Wie kann man f nun auch noch injektiv machen, d. h. (nach Lemma 4.18) den Kern von f zur trivialen Untergruppe machen, die nur aus einem (nämlich dem neutralen) Element besteht? Die Idee hierfür besteht darin, alle Elemente in $\operatorname{Ker} f$ miteinander zu identifizieren, so dass sie zu einem einzigen Element werden — mit anderen Worten also, beim Startraum von G zur Faktorgruppe $G/\operatorname{Ker} f$ überzugehen.

Kombinieren wir diese Ideen miteinander, so erhalten wir den folgenden wichtigen Satz:

Satz 6.17 (**Homomorphiesatz** für Gruppen)**.** *Es sei $f\colon G \to H$ ein Morphismus von Gruppen. Dann ist die Abbildung*

$$\begin{aligned} g\colon G/\operatorname{Ker} f &\to \operatorname{Im} f \\ \overline{a} &\mapsto f(a) \end{aligned}$$

zwischen der Faktorgruppe $G/\operatorname{Ker} f$ von G und der Untergruppe $\operatorname{Im} f$ von H ein Isomorphismus.

Beweis. Zunächst einmal ist $\operatorname{Ker} f$ nach Lemma 6.7 ein Normalteiler von G, so dass $G/\operatorname{Ker} f$ nach Satz 6.13 also wirklich eine Gruppe ist. Die im Satz angegebene Abbildung g ist außerdem wohldefiniert, denn für $a, b \in G$ mit $\overline{a} = \overline{b}$, also $a^{-1}b \in \operatorname{Ker} f$, gilt

$$e = f(a^{-1}b) = f(a)^{-1} f(b)$$

und damit $f(a) = f(b)$. Weiterhin ist g ein Morphismus, denn für $a, b \in G$ gilt

$$\begin{aligned} g\big(\overline{a} \cdot \overline{b}\big) &= g\big(\overline{ab}\big) && \text{(Definition der Verknüpfung in } G/\operatorname{Ker} f) \\ &= f(ab) && \text{(Definition von } g) \\ &= f(a) \cdot f(b) && (f \text{ ist Morphismus}) \\ &= g\big(\overline{a}\big) \cdot g\big(\overline{b}\big). && \text{(Definition von } g) \end{aligned}$$

Wir müssen also nur noch zeigen, dass g surjektiv und injektiv ist. Beides folgt im Prinzip unmittelbar aus der Konstruktion von g bzw. der Idee aus Bemerkung 6.16:

- g ist surjektiv: Ist b ein Element in der Zielgruppe $\operatorname{Im} f$, so gibt es also ein $a \in G$ mit $f(a) = b$, d. h. mit $g\big(\overline{a}\big) = b$.
- g ist injektiv: Ist $a \in G$ mit $g\big(\overline{a}\big) = f(a) = e$, so ist also $a \in \operatorname{Ker} f$ und damit $\overline{a} = \overline{e}$ nach Bemerkung 5.7 (a). Also ist $\operatorname{Ker} g = \{\overline{e}\}$ und g damit nach Lemma 4.18 injektiv. □

Folgerung 6.18. *Für jeden Morphismus $f\colon G \to H$ mit endlicher Startgruppe G gilt*

$$|G| = |\operatorname{Im} f| \cdot |\operatorname{Ker} f|.$$

Beweis. Nach dem Homomorphiesatz 6.17 ist $G/\operatorname{Ker} f$ isomorph zu $\operatorname{Im} f$. Insbesondere gilt also $|G/\operatorname{Ker} f| = |\operatorname{Im} f|$. Mit dem Satz 5.10 von Lagrange bedeutet dies aber sofort

$$\frac{|G|}{|\operatorname{Ker} f|} = |\operatorname{Im} f|, \quad \text{also} \quad |G| = |\operatorname{Im} f| \cdot |\operatorname{Ker} f|. \qquad \square$$

Beispiel 6.19.

(a) Wir betrachten für $n \in \mathbb{N}_{\geq 2}$ noch einmal den Morphismus $\operatorname{sign}\colon S_n \to \mathbb{R}\backslash\{0\}$ aus Beispiel 4.3 (d). Der Kern dieser Abbildung ist nach Definition 4.16 die alternierende Gruppe A_n, das Bild ist $\{\pm 1\}$ und hat damit Ordnung 2. Mit Folgerung 6.18 erhalten wir demnach

$$|S_n| = 2 \cdot |A_n|, \quad \text{also} \quad |A_n| = \frac{1}{2}|S_n| \overset{2.6}{=} \frac{n!}{2}.$$

(b) Ist G eine beliebige Gruppe und $f = \mathrm{id}\colon G \to G$ die Identität, so ist natürlich $\operatorname{Ker} f = \{e\}$ und $\operatorname{Im} f = G$. Nach dem Homomorphiesatz ist also $G/\{e\} \cong G$ (mit der Abbildung $\overline{a} \mapsto a$). Dies ist auch anschaulich klar: wenn man aus G „nichts herausteilt“, also keine nicht-trivialen Identifizierungen von Elementen aus G vornimmt, so ist die resultierende Gruppe immer noch G.

(c) Im anderen Extremfall, dem konstanten Morphismus $f\colon G \to G$, $a \mapsto e$, ist umgekehrt $\operatorname{Ker} f = G$ und $\operatorname{Im} f = \{e\}$. Hier besagt der Homomorphiesatz also $G/G \cong \{e\}$ (mit Isomorphismus $\overline{a} \mapsto e$): Wenn man aus G „alles herausteilt“, so bleibt nur noch die triviale Gruppe $\{e\}$ übrig.

07

Eine sehr schöne Anwendung des Homomorphiesatzes findet sich im Bereich der sogenannten Gruppenklassifikation. Natürlich wäre es wünschenswert, eine „vollständige Liste aller Gruppen“ hinschreiben zu können — also konkrete Beispiele von Gruppen so anzugeben, dass *jede beliebige* Gruppe zu (genau) einer dieser angegebenen Gruppen isomorph ist. Da isomorphe Gruppen ja ununterscheidbar sind, würde das nämlich bedeuten, dass wir dann eigentlich gar keine allgemeinen Gruppen mehr studieren müssten, sondern dass es reichen würde, stattdessen einfach nur alle Beispiele dieser Liste zu untersuchen. Falls ihr aus den Grundlagen der Mathematik schon Vektorräume kennt, werdet ihr vielleicht gemerkt haben, dass ihr dort auf genau diese Art vorgegangen seid: Ihr habt gezeigt, dass jeder (endlich-dimensionale) Vektorraum über $\mathbb{R}$ isomorph ist zu $\mathbb{R}^n$ für ein $n \in \mathbb{N}$ — und aus diesem Grund dann oft nur noch diese speziellen Vektorräume $\mathbb{R}^n$ untersucht (z. B. wenn man lineare Abbildungen durch Matrizen beschreibt).

Da wir uns dennoch schon seit Beginn dieser Vorlesung mit allgemeinen Gruppen beschäftigen, werdet ihr euch schon denken können, dass die Situation bei Gruppen hier nicht ganz so einfach ist. In der Tat wäre eine solche „Liste aller Gruppen“ so lang und kompliziert, dass man mit ihr eigentlich kaum noch etwas anfangen könnte. Wir können aber mit Hilfe des Homomorphiesatzes ein einfaches, aber dennoch verblüffendes Resultat in dieser Richtung zeigen: Wenn wir eine endliche Gruppe G haben, deren Ordnung eine *Primzahl* p ist (d. h. so dass $p \geq 2$ keine natürliche Zahl außer 1 und p als Teiler hat — ein Konzept, das wir in Kapitel 11 noch genauer untersuchen werden), so muss G bereits isomorph zu $\mathbb{Z}_p$ sein. Im Gegensatz zur Liste *aller* Gruppen ist die Liste aller Gruppen mit Primzahlordnung also wieder sehr einfach.

Um diese Aussage zeigen zu können, benötigen wir zuerst noch eine Definition.

Definition 6.20 (Zyklische Gruppen)**.** Eine Gruppe G heißt **zyklisch**, wenn sie von einem Element erzeugt werden kann, also wenn es ein $a \in G$ gibt mit $G = \langle a \rangle$.

Satz 6.21 (Klassifikation zyklischer Gruppen)**.** *Es sei G eine Gruppe.*

(a) *Ist G zyklisch, so ist G isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}_n$ für ein $n \in \mathbb{N}_{>0}$.*

(b) *Ist G endlich und $p := |G|$ eine Primzahl, so ist G isomorph zu $\mathbb{Z}_p$.*

Beweis.

(a) Es sei $a \in G$ mit $G = \langle a \rangle$. Wir betrachten die Abbildung

$$f\colon \mathbb{Z} \to G,\ k \mapsto a^k,$$

die aufgrund der Rechenregeln für Potenzen aus Lemma 1.12 ein Morphismus ist. Nach Beispiel 3.13 (a) ist dann

$$\operatorname{Im} f = \{a^k : k \in \mathbb{Z}\} = \langle a \rangle = G,$$

d. h. f ist surjektiv. Es ergeben sich nun zwei Fälle:

- Die Abbildung f ist auch injektiv. Dann ist $f\colon \mathbb{Z} \to G$ ein Isomorphismus, also $\mathbb{Z} \cong G$.
- Die Abbildung f ist nicht injektiv, nach Lemma 4.18 also $\operatorname{Ker} f \neq \{0\}$. Als Untergruppe von $\mathbb{Z}$ muss $\operatorname{Ker} f$ nach Satz 3.17 dann die Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}_{>0}$ haben. Aus dem Homomorphiesatz folgt damit $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong G$ (mit Isomorphismus $\overline{k} \mapsto a^k$).

(b) Es sei $a \in G$ ein beliebiges Element mit $a \neq e$. Nach dem Satz 5.10 von Lagrange muss die Ordnung der Untergruppe $\langle a \rangle$ von G ein Teiler der Gruppenordnung p sein. Da p eine Primzahl ist, kommt hier also nur $|\langle a \rangle| = 1$ oder $|\langle a \rangle| = p$ in Frage. Weil aber bereits die beiden Elemente e und a in $\langle a \rangle$ liegen, ist $|\langle a \rangle| = 1$ ausgeschlossen. Damit ist $|\langle a \rangle| = p$, d. h. es ist bereits $\langle a \rangle = G$. Also ist G zyklisch. Die Behauptung folgt damit aus Teil (a). □

Bemerkung 6.22 (S_3 als kleinste nicht-abelsche Gruppe)**.** Wir hatten in Aufgabe 1.15 bereits gesehen, dass jede nicht-abelsche Gruppe mindestens 5 Elemente haben muss. Dieses Ergebnis können wir jetzt verbessern: Da jede Gruppe der Ordnung 5 nach Satz 6.21 (b) isomorph zu $\mathbb{Z}_5$ und damit abelsch ist, muss jede nicht-abelsche Gruppe also sogar mindestens 6 Elemente haben.

In der Tat gibt es natürlich auch eine nicht-abelsche Gruppe der Ordnung 6, nämlich die symmetrische Gruppe S_3. Man kann zeigen, dass S_3 und $\mathbb{Z}_6$ bis auf Isomorphie die einzigen Gruppen der Ordnung 6 sind.

Aufgabe 6.23. Es sei $G = \mathbb{R}/\mathbb{Z}$.

(a) Für welche $a, b \in \mathbb{R}$ ist $f\colon G \to G$, $\overline{x} \mapsto \overline{ax+b}$ eine wohldefinierte Abbildung?

(b) Zeige, dass für jedes $n \in \mathbb{N}_{>0}$ die von $\overline{\frac{1}{n}}$ erzeugte Untergruppe von G isomorph zu $\mathbb{Z}_n$ ist.

Aufgabe 6.24.

(a) Es seien G und H zwei endliche Gruppen, deren Ordnungen $|G|$ und $|H|$ keinen gemeinsamen Teiler (größer als 1) besitzen. Zeige, dass es dann nur einen Morphismus von G nach H gibt.

(b) Bestimme alle Morphismen von $\mathbb{Z}_9$ nach $\mathbb{Z}_{11}$ sowie von $\mathbb{Z}_9$ nach $\mathbb{Z}_{12}$.

Aufgabe 6.25. Es sei G eine Gruppe mit $|G| = 10$. Zeige, dass G entweder kein Element der Ordnung 10 oder genau vier Elemente der Ordnung 10 besitzt, und gib für jeden dieser beiden Fälle ein Beispiel an.

Aufgabe 6.26. Es sei N ein Normalteiler einer Gruppe G. Zeige, dass die Abbildung

$$\begin{aligned} \{U\colon U \text{ ist Untergruppe von } G \text{ mit } U \supset N\} &\to \{V\colon V \text{ ist Untergruppe von } G/N\} \\ U &\mapsto U/N \end{aligned}$$

bijektiv ist. (Die Untergruppen einer Faktorgruppe G/N entsprechen in diesem Sinne also genau den Untergruppen von G, die N enthalten.)

Aufgabe 6.27. Der Satz 5.10 von Lagrange besagt bekanntlich, dass die Ordnung jeder Untergruppe einer endlichen Gruppe G ein Teiler von $|G|$ sein muss. Wir wollen nun in zwei einfachen Fällen die umgekehrte Fragestellung untersuchen, ob es zu jedem Teiler von $|G|$ auch eine Untergruppe dieser Ordnung geben muss. Zeige dazu für eine endliche Gruppe G:

(a) Ist 2 ein Teiler von $|G|$, so besitzt G ein Element der Ordnung 2 (und damit auch eine Untergruppe der Ordnung 2).

(b) Ist G abelsch und 2^n ein Teiler von $|G|$ für ein $n \in \mathbb{N}$, so hat G eine Untergruppe der Ordnung 2^n.

Hinweis: Für (a) zeige man, dass G außer dem neutralen Element noch mindestens ein weiteres Element a mit $a^{-1} = a$ besitzen muss. Für (b) empfiehlt sich Induktion über n und die Untersuchung einer geeigneten Faktorgruppe von G.

Aufgabe 6.28.

(a) Bestimme mit Hilfe von Aufgabe 6.26 alle Untergruppen von $\mathbb{Z}_n$ für $n > 0$.

(b) Man zeige: Ist G eine endliche zyklische Gruppe und n ein Teiler der Ordnung von G, so gibt es genau eine Untergruppe von G der Ordnung n, und diese ist ebenfalls zyklisch.

Aufgabe 6.29. Es sei G eine Gruppe. Man zeige:

(a) Sind $a, b \in G$ und ist $\operatorname{ord} a = \operatorname{ord} b$ eine Primzahl, so gilt $\langle a \rangle = \langle b \rangle$ oder $\langle a \rangle \cap \langle b \rangle = \{e\}$.

(b) Ist $|G| = 35$, so gibt es $a, b \in G$ mit $\operatorname{ord} a = 5$ und $\operatorname{ord} b = 7$.

(c) Ist $|G| = 35$ und G abelsch, so ist $G \cong \mathbb{Z}_{35}$.

Aufgabe 6.30. Man zeige: Ist G eine Gruppe, die genau drei Untergruppen besitzt, so ist $G \cong \mathbb{Z}_{p^2}$ für eine Primzahl p.

Aufgabe 6.31. Es seien $n \in \mathbb{N}_{>1}$ und U eine Untergruppe einer endlichen Gruppe G mit $|U| = \frac{1}{n}|G|$. Man zeige für alle $a \in G$:

(a) Ist U ein Normalteiler von G, so gilt $a^n \in U$.

(b) Im Allgemeinen liegt zwar mindestens eines der Elemente $a^1, a^2, \ldots, a^n$ in U, aber nicht notwendig a^n.

Aufgabe 6.32. Man zeige:

(a) Eine Gruppe der Ordnung 60 hat höchstens einen Normalteiler der Ordnung 12.

(b) Eine Gruppe der Ordnung 60 kann mehrere Untergruppen der Ordnung 12 haben.