1. Gruppen

Wie schon in der Einleitung erläutert wollen wir uns in dieser Vorlesung mit Mengen beschäftigen, auf denen algebraische Verknüpfungen mit gewissen Eigenschaften definiert sind. Die in der Mathematik wichtigste derartige Struktur ist die einer Gruppe.

Definition 1.1 (Gruppen)**.**

(a) Eine **Gruppe** ist eine Menge G zusammen mit einer „Verknüpfung“, d. h. einer Abbildung

$$\begin{aligned} \cdot : G \times G &\to G \\ (a,b) &\mapsto a \cdot b \end{aligned}$$

so dass die folgenden Eigenschaften (auch *Gruppenaxiome* genannt) gelten:

(G1) Für alle $a,b,c \in G$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (**Assoziativität**).

(G2) Es gibt ein $e \in G$, so dass $e \cdot a = a$ für alle $a \in G$ gilt (man nennt ein solches e ein **linksneutrales Element**), und für das die folgende Eigenschaft gilt:

(G3) Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $a' \cdot a = e$ (man nennt ein solches a' ein zu a **linksinverses Element**).

Wir schreiben eine solche Gruppe als $(G, \cdot)$, oder manchmal auch einfach nur als G, wenn die betrachtete Verknüpfung aus dem Zusammenhang klar ist.

Statt eines Punktes „$\cdot$“ kann natürlich auch ein anderes Symbol für die Verknüpfung gewählt werden. In einer allgemeinen Gruppe werden wir jedoch in der Regel einen Punkt verwenden oder diesen oft auch ganz weglassen, also eine Verknüpfung $a \cdot b$ einfach als ab schreiben.

(b) Gilt zusätzlich zu den Gruppenaxiomen (G1), (G2) und (G3) noch

(G4) Für alle $a,b \in G$ gilt $a \cdot b = b \cdot a$ (**Kommutativität**),

so heißt $(G, \cdot)$ eine **kommutative** oder **abelsche Gruppe**.

(c) Hat G nur endlich viele Elemente, so heißt G eine **endliche Gruppe** und die Anzahl ihrer Elemente die **Ordnung** von G. Wie für eine beliebige Menge schreibt man diese Anzahl Elemente als $|G|$.

Beispiel 1.2. Wir wollen in dieser Vorlesung die „Standardzahlbereiche“

$\mathbb{N} = \{0,1,2,\dots\}$ der **natürlichen Zahlen**,

$\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$ der **ganzen Zahlen**,

$\mathbb{Q}$ der **rationalen Zahlen**,

$\mathbb{R}$ der **reellen Zahlen**

zusammen mit den üblichen darauf definierten Verknüpfungen (z. B. Addition und Multiplikation) und ihren Eigenschaften als aus der Schule bekannt voraussetzen. Man könnte diese Mengen und Verknüpfungen zwar auch allein aus den Prinzipien der Mengenlehre konstruieren und ihre Eigenschaften dann beweisen (siehe z. B. [E, Kapitel 1 und 2]) – dies soll aber nicht der Inhalt dieser Vorlesung sein und würde zum momentanen Zeitpunkt auch mehr verwirren als helfen.

Setzen wir die Eigenschaften dieser Zahlbereiche also als bekannt voraus, so können wir daraus die folgenden einfachen Beispiele für Gruppen gewinnen:

(a) $(\mathbb{R},+)$, also die reellen Zahlen zusammen mit der Addition als Verknüpfung, bilden eine abelsche Gruppe, denn es gilt:

(G1) $(a+b)+c = a+(b+c)$ für alle $a,b,c \in \mathbb{R}$;

(G2) die Zahl 0 ist ein linksneutrales Element, denn es ist $0+a=a$ für alle $a \in \mathbb{R}$;

(G3) zu $a \in \mathbb{R}$ ist $-a \in \mathbb{R}$ ein linksinverses Element, denn es ist stets $(-a)+a=0$;

(G4) $a+b=b+a$ für alle $a,b \in \mathbb{R}$.

Genauso sind auch $(\mathbb{Q},+)$ und $(\mathbb{Z},+)$ abelsche Gruppen. Im Gegensatz dazu ist $(\mathbb{N},+)$ keine Gruppe: (G1) und (G2) sind zwar weiterhin erfüllt, aber das Gruppenaxiom (G3) ist hier verletzt, da z. B. die Zahl $1 \in \mathbb{N}$ kein linksinverses Element besitzt (die hierfür benötigte Zahl -1 liegt nicht in $\mathbb{N}$).

Wenn wir im Folgenden ohne weitere Angaben von $\mathbb{R}$, $\mathbb{Q}$ oder $\mathbb{Z}$ als Gruppe reden, wollen wir vereinbaren, dass immer die Addition als Verknüpfung gemeint ist.

(b) $(\mathbb{R},\cdot)$, also die reellen Zahlen zusammen mit der gewöhnlichen Multiplikation, bilden ebenfalls keine Gruppe: (G1) und (G2) sind hier zwar erfüllt (mit dem einzig möglichen linksneutralen Element 1), aber zu der Zahl 0 gibt es kein linksinverses Element, also kein $a' \in \mathbb{R}$ mit $a' \cdot 0 = 1$.

Dieses „Problem“ lässt sich jedoch leicht beheben, indem man die 0 einfach aus der Menge herausnimmt: $(\mathbb{R}\backslash\{0\},\cdot)$ ist eine abelsche Gruppe, denn die Assoziativität und die Existenz eines linksneutralen Elementes 1 gelten immer noch, und zusätzlich haben wir:

(G3) Jedes $a \in \mathbb{R}\backslash\{0\}$ hat ein linksinverses Element $a' = \frac{1}{a}$ (mit $\frac{1}{a} \cdot a = 1$);

(G4) $a \cdot b = b \cdot a$ für alle $a,b \in \mathbb{R}\backslash\{0\}$.

Genauso ist auch $(\mathbb{Q}\backslash\{0\},\cdot)$ eine abelsche Gruppe. Dagegen sind $(\mathbb{Z}\backslash\{0\},\cdot)$ und $(\mathbb{N}\backslash\{0\},\cdot)$ keine Gruppen: (G1) und (G2) gelten zwar weiterhin (wiederum mit linksneutralem Element 1), aber das Gruppenaxiom (G3) ist verletzt, da z. B. die Zahl 2 kein linksinverses Element besitzt (die hierfür benötigte Zahl $\frac{1}{2}$ liegt nicht in $\mathbb{Z}$ bzw. $\mathbb{N}$).

Analog zu (a) wollen wir vereinbaren, dass immer die Multiplikation gemeint ist, wenn wir ohne Angabe einer Verknüpfung von der Gruppe $\mathbb{R}\backslash\{0\}$ oder $\mathbb{Q}\backslash\{0\}$ sprechen.

(c) Die Menge $G = \{-2,-1,0,1,2\}$ mit der gewöhnlichen Addition ist *keine* Gruppe, obwohl es auf den ersten Blick vielleicht so aussieht, als ob (G1), (G2) und (G3) erfüllt wären. Die Addition ist nämlich nicht einmal eine Verknüpfung auf G, da sie zwei Elemente von G nicht unbedingt wieder nach G abbildet: Es gilt zwar $1,2 \in G$, aber $1+2=3 \notin G$. In diesem Sinne steckt in Definition 1.1 also schon in der allerersten Formulierung „eine Gruppe ist eine Menge zusammen mit einer Verknüpfung“ eine Bedingung.

(d) Nach (G2) hat jede Gruppe mindestens ein Element – und zwar ein linksneutrales. Mehr braucht es jedoch nicht: Die einelementige Menge $G = \{e\}$ mit der durch $e \cdot e := e$ definierten trivialen Verknüpfung ist bereits eine Gruppe (wenn auch keine sehr interessante). Sie wird die **triviale Gruppe** genannt.

Bemerkung 1.3 (Verknüpfungstafeln)**.** Verknüpfungen auf Mengen mit nur wenigen Elementen lassen sich mit Hilfe einer **Verknüpfungstafel** angeben – so wie im Bild rechts, das auf der Menge $G = \{0,1\}$ eine Verknüpfung $*$ definiert, indem die Werte $a*b$ für alle $a,b \in G$ einfach in einer Tabelle angegeben werden. Um festzustellen, ob eine so definierte Verknüpfung alle Gruppenaxiome erfüllt, muss man die Eigenschaften aus Definition 1.1 dann für alle Elemente von G durchgehen.

$*$	0	1
0	0	1
1	1	0

Bei der hier angegebenen Verknüpfungstafel ist dies der Fall, wobei 0 ein linksneutrales Element und jedes Element zu sich selbst linksinvers ist. Die so definierte (abelsche) Gruppe wird mit $\mathbb{Z}_2$ bezeichnet; man kann sie sich vorstellen als „gerade Zahlen (entsprechend 0) und ungerade Zahlen (entsprechend 1) unter Addition“, so dass also z. B. $1*1=0$ bedeutet, dass die Summe zweier ungerader Zahlen gerade ist. Eine deutlich allgemeinere Konstruktion von Gruppen dieser Art werden wir in Beispiel 6.15 kennenlernen.

Beispiel 1.4. Wir definieren auf der Menge $G = \mathbb{R}$ eine Verknüpfung „$*$“ durch

$$a*b := a+b+1 \quad \text{für } a,b \in \mathbb{R}$$

(wobei „+“ die gewöhnliche Addition reeller Zahlen bezeichnet) und behaupten, dass $(\mathbb{R},*)$ damit zu einer abelschen Gruppe wird. Im Gegensatz zu Beispiel 1.2 (a) und (b), wo wir die Gruppeneigenschaften von $\mathbb{R}$ bezüglich der gewöhnlichen Addition und Multiplikation einfach als bekannt vorausgesetzt haben, müssen wir bei dieser speziell konstruierten Verknüpfung nun natürlich *beweisen*, dass die Gruppenaxiome gelten. Dies rechnet man einfach nach:

(G1) Für alle $a,b,c \in \mathbb{R}$ ist
$$(a*b)*c = (a+b+1)*c = (a+b+1)+c+1 = a+b+c+2$$
und genauso
$$a*(b*c) = a*(b+c+1) = a+(b+c+1)+1 = a+b+c+2,$$
woraus die Assoziativität der Verknüpfung folgt (natürlich haben wir hierbei wieder die Eigenschaften der Addition reeller Zahlen als bekannt vorausgesetzt).

(G2) Die Zahl $e := -1 \in \mathbb{R}$ ist ein linksneutrales Element der Verknüpfung, denn für alle $a \in \mathbb{R}$ gilt
$$(-1)*a = (-1)+a+1 = a.$$

(G3) Zu jedem $a \in \mathbb{R}$ ist $-2-a \in \mathbb{R}$ ein linksinverses Element, denn es gilt
$$(-2-a)*a = (-2-a)+a+1 = -1 = e.$$

(G4) Für alle $a,b \in \mathbb{R}$ gilt
$$a*b = a+b+1 = b+a+1 = b*a.$$

Also ist $(\mathbb{R},*)$ eine abelsche Gruppe – allerdings eine ziemlich langweilige und unwichtige, die euch wohl nie wieder begegnen wird. Der Sinn dieses einfachen Beispiels war es lediglich zu sehen, wie man bei einer konkret gegebenen Verknüpfung die Gruppenaxiome überprüfen kann.

Konstruktion 1.5 (Produkte von Gruppen)**.** Es seien $(G,*)$ und $(H,\circ)$ zwei Gruppen – wir verwenden hier verschiedene Symbole, um die beiden Verknüpfungen unterscheiden zu können. Wir können dann auch auf dem Produkt
$$G \times H = \{(a_1,a_2) : a_1 \in G, a_2 \in H\}$$
eine Verknüpfung definieren, indem wir die beiden gegebenen Verknüpfungen komponentenweise anwenden: Wir setzen einfach
$$(a_1,a_2)\cdot(b_1,b_2) := (a_1*b_1, a_2\circ b_2) \quad \text{für } (a_1,a_2),(b_1,b_2) \in G\times H.$$
Dies macht $G\times H$ zu einer Gruppe, die wir das **Produkt** der Gruppen G und H nennen. In der Tat folgen die Gruppenaxiome für $(G\times H,\cdot)$ sofort aus denen für $(G,*)$ und $(H,\circ)$:

(G1) Für alle $a_1,b_1,c_1 \in G$ und $a_2,b_2,c_2 \in H$ gilt nach Definition der Verknüpfung in $G\times H$
$$\begin{aligned}((a_1,a_2)\cdot(b_1,b_2))\cdot(c_1,c_2) &= (a_1*b_1, a_2\circ b_2)\cdot(c_1,c_2)\\ &= ((a_1*b_1)*c_1, (a_2\circ b_2)\circ c_2)\end{aligned}$$
und
$$\begin{aligned}(a_1,a_2)\cdot((b_1,b_2)\cdot(c_1,c_2)) &= (a_1,a_2)\cdot(b_1*c_1, b_2\circ c_2)\\ &= (a_1*(b_1*c_1), a_2\circ(b_2\circ c_2)).\end{aligned}$$
Wegen der Assoziativität der Verknüpfungen in G und H stimmen diese beiden Ausdrücke überein – was die Assoziativität in $G\times H$ zeigt.

(G2) Das Paar (e_G,e_H) der beiden neutralen Elemente von G und H ist ein linksneutrales Element in $G\times H$, denn es ist
$$(e_G,e_H)\cdot(a_1,a_2) = (e_G*a_1, e_H\circ a_2) = (a_1,a_2)$$
für alle $(a_1,a_2) \in G\times H$.

(G3) Sind a_1' und a_2' linksinverse Elemente zu a_1 in G bzw. zu a_2 in H, so ist (a_1', a_2') linksinvers zu (a_1, a_2) in $G \times H$, denn

$$(a_1', a_2') \cdot (a_1, a_2) = (a_1' * a_1, a_2' \circ a_2) = (e_G, e_H).$$

Sind zudem G und H abelsch, so folgt natürlich auf die gleiche Art, dass dann auch $G \times H$ abelsch ist.

Das einfachste Beispiel für ein Produkt von Gruppen kennt ihr sicher schon aus der Schule: Die Menge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ aller Vektoren in der Ebene mit der komponentenweisen Addition

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2).$$

Es hindert uns aber auch nichts daran, das Produkt von zwei „ganz verschiedenen" Gruppen zu bilden, also z. B. $(\mathbb{Z}, +) \times (\mathbb{R} \backslash \{0\}, \cdot)$. Auch kann man natürlich ganz analog das Produkt von mehr als zwei Gruppen bilden.

Aufgabe 1.6. Untersuche, ob es sich bei den folgenden Mengen und Verknüpfungen um Gruppen handelt. (Man gebe also einen Beweis der Gruppenaxiome oder ein Gegenbeispiel für ein verletztes Axiom an.)

(a) $G = 5\mathbb{Z} := \{5n : n \in \mathbb{Z}\}$, also die Menge aller durch 5 teilbaren ganzen Zahlen, mit der gewöhnlichen Addition als Verknüpfung;

(b) $G = 5\mathbb{Z}$ mit der gewöhnlichen Multiplikation als Verknüpfung;

(c) $G = \mathbb{Q}_{>0}$ mit der Verknüpfung $a * b := \frac{ab}{2}$;

(d) $G = \mathbb{R} \times \mathbb{R}$ mit der Verknüpfung $(a_1, a_2) * (b_1, b_2) := (a_1 + b_2, a_2 + b_1)$;

(e) $G = \mathbb{R} \times \mathbb{R}$ mit der Verknüpfung $(a_1, a_2) * (b_1, b_2) := (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$.

Wir werden später noch mehr Beispiele für Gruppen sehen. Zunächst wollen wir aber ein kleines Resultat beweisen, das es uns erlaubt, etwas einfacher über Gruppen reden zu können. Schauen wir uns dazu einmal das Gruppenaxiom (G2) an: Wir haben hier für $e \in G$ die Beziehung $e \cdot a = a$ für alle $a \in G$ gefordert und e *links*neutral genannt – weil es ein gegebenes a nicht ändert, wenn man es von links mit e verknüpft. Da wir für eine allgemeine Gruppe keine Kommutativität vorausgesetzt haben, folgt daraus natürlich zunächst einmal *nicht*, dass auch $a \cdot e = a$ für alle $a \in G$ gelten muss, dass e also auch *rechts*neutral ist. Wir wollen nun allerdings zeigen, dass dies doch immer der Fall ist und wir e deswegen einfach als *neutrales Element* bezeichnen können. Außerdem wollen wir zeigen, dass ein solches neutrales Element nicht nur existiert (wie es ja in den Gruppenaxiomen gefordert ist), sondern sogar *eindeutig* ist, so dass wir in Zukunft nicht nur von *einem* neutralen Element, sondern von *dem* neutralen Element reden können.

Die gleichen Aussagen gelten übrigens analog auch für inverse Elemente: Ein linksinverses Element ist immer auch rechtsinvers, und ist darüber hinaus auch eindeutig bestimmt. Alles dies besagt der folgende Satz, den wir jetzt beweisen wollen.

Satz 1.7 (Existenz und Eindeutigkeit neutraler und inverser Elemente)**.** *In jeder Gruppe G gilt:*

(a) *Es gibt genau ein linksneutrales Element $e \in G$;*

(b) *dieses linksneutrale Element ist dann auch* ***rechtsneutral****, d. h. es gilt $a \cdot e = a$ für alle $a \in G$;*

(c) *jedes $a \in G$ besitzt genau ein linksinverses Element $a' \in G$;*

(d) *dieses linksinverse Element ist dann auch* ***rechtsinvers****, d. h. es gilt $a \cdot a' = e$.*

Wir werden in Zukunft statt von links- und rechtsneutralen bzw. -inversen Elementen also einfach von dem ***neutralen*** *und dem zu einem $a \in G$* ***inversen Element*** *reden.*

Beweis. Nach (G2) existiert in G ein linksneutrales Element e, das (G3) erfüllt. Wir beweisen die vier Aussagen in etwas anderer Reihenfolge, als sie in der Behauptung aufgeführt sind.

(d) Es seien $a \in G$ beliebig und $a' \in G$ ein dazu linksinverses Element, d. h. es gilt $a' \cdot a = e$. Nach (G3) existiert zu diesem a' wiederum ein linksinverses Element $a'' \in G$, es ist also $a'' \cdot a' = e$. Damit folgt nun (wir schreiben zur besseren Verständlichkeit des Beweises hinter jede Gleichheit die zugehörige Begründung)

$$\begin{aligned}
a \cdot a' &= e \cdot (a \cdot a') && \text{(G2)} \\
&= (a'' \cdot a') \cdot (a \cdot a') && (a'' \text{ ist linksinvers zu } a') \\
&= a'' \cdot (a' \cdot (a \cdot a')) && \text{(G1)} \\
&= a'' \cdot ((a' \cdot a) \cdot a') && \text{(nochmal G1)} \\
&= a'' \cdot (e \cdot a') && (a' \text{ ist linksinvers zu } a) \\
&= a'' \cdot a' && \text{(G2)} \\
&= e. && (a'' \text{ ist linksinvers zu } a')
\end{aligned}$$

Also ist a' auch ein rechtsinverses Element zu a.

(b) Es sei $a \in G$ beliebig. Nach (G3) existiert zu a ein linksinverses Element $a' \in G$, d. h. es gilt $a' \cdot a = e$. Damit folgt

$$\begin{aligned}
a \cdot e &= a \cdot (a' \cdot a) && (a' \text{ ist linksinvers zu } a) \\
&= (a \cdot a') \cdot a && \text{(G1)} \\
&= e \cdot a && (a' \text{ ist nach (d) auch rechtsinvers zu } a) \\
&= a, && \text{(G2)}
\end{aligned}$$

und damit ist e auch rechtsneutral. (Beachte, dass wir beim Beweis dieser Aussage u. a. den schon bewiesenen Teil (d) des Satzes verwendet haben.)

(a) Es sei $\tilde{e} \in G$ ein weiteres linksneutrales Element. Dann folgt sofort

$$\begin{aligned}
e &= \tilde{e} \cdot e && (\tilde{e} \text{ ist linksneutral}) \\
&= \tilde{e}. && (e \text{ ist nach (b) rechtsneutral})
\end{aligned}$$

Also sind e und $\tilde{e}$ notwendigerweise gleich, d. h. es gibt nur ein neutrales Element. 01

(c) Es seien nun $a \in G$ beliebig und $a', \tilde{a}' \in G$ zwei linksinverse Elemente zu a, die dann nach (d) auch beide zu a rechtsinvers sind. Damit ergibt sich

$$\begin{aligned}
a' &= e \cdot a' && \text{(G2)} \\
&= (\tilde{a}' \cdot a) \cdot a' && (\tilde{a}' \text{ ist linksinvers zu } a) \\
&= \tilde{a}' \cdot (a \cdot a') && \text{(G1)} \\
&= \tilde{a}' \cdot e && (a' \text{ ist rechtsinvers zu } a) \\
&= \tilde{a}'. && (e \text{ ist rechtsneutral nach (b)})
\end{aligned}$$

Also müssen a' und $\tilde{a}'$ gleich sein, d. h. es gibt zu a nur ein inverses Element. □

Das Symbol „□“ steht hierbei übrigens (wie in der Mathematik üblich) für das Ende eines Beweises.

Bemerkung 1.8. Nach Satz 1.7 hätten wir in Definition 1.1 (a) anstatt der Teile (G2) und (G3) also auch genauso gut schreiben können

(G2′) es gibt *genau ein* $e \in G$ mit $e \cdot a = a \cdot e = a$ für alle $a \in G$;

(G3′) für alle $a \in G$ gibt es *genau ein* $a' \in G$ mit $a' \cdot a = a \cdot a' = e$.

Unser gerade bewiesener Satz zeigt uns, dass die so entstehende Definition zu unserer ursprünglichen äquivalent gewesen wäre. In der Tat wird man wohl auch in manchen Büchern diese abgeänderte Definition finden. Unsere Definition 1.1 (a) hat aber in der Praxis den Vorteil, dass die Bedingungen in konkreten Fällen leichter nachprüfbar sind, weil sie (scheinbar) schwächer sind.

Notation 1.9.

(a) Da neutrale und inverse Elemente in Gruppen nach Satz 1.7 eindeutig sind, gibt man ihnen oft besondere Namen: Das zu einem Element a inverse Element schreibt man als a^{-1}, und das neutrale Element manchmal einfach als 1. Eine Ausnahme macht man hierbei nur, wenn man die Gruppenverknüpfung mit dem Symbol „+“ schreibt: Hier ist es (aufgrund von Beispiel 1.2 (a)) natürlicher, das zu a inverse Element als $-a$ und das neutrale Element als 0 zu schreiben.

(b) Schreibt man die Gruppenverknüpfung als „+“, so verwendet man oft die Notation $a-b$ für $a+(-b)$. Die analoge Notation $\frac{a}{b}$ bei multiplikativ geschriebener Gruppenverknüpfung ist jedoch mit Vorsicht zu genießen, da man sie sowohl als $a \cdot b^{-1}$ als auch als $b^{-1} \cdot a$ interpretieren könnte – und in allgemeinen Gruppen ist das ja nicht dasselbe. Man sollte diese Schreibweise daher (wenn überhaupt) nur bei abelschen Gruppen anwenden.

(c) Wir haben im Beweis von Satz 1.7 gesehen, dass die Assoziativität (G1) in der Praxis einfach dazu führt, dass Klammern bei mehrfachen Verknüpfungen beliebig umgesetzt werden können, ohne das Resultat zu verändern. Man lässt diese Klammern daher in der Regel einfach ganz weg und schreibt z. B. für $a,b,c \in G$ einfach $a \cdot b \cdot c$ oder abc an Stelle von $(a \cdot b) \cdot c$ oder $a \cdot (b \cdot c)$.

Zum Abschluss dieses Kapitels wollen wir nun noch ein paar allgemeine Rechenregeln herleiten, die in beliebigen Gruppen gelten und die wir später immer wieder benötigen werden. Die wichtigsten dieser Regeln enthält das folgende Lemma („Lemma“ ist griechisch und bedeutet eigentlich „Annahme“, aber in der Mathematik wird dieser Begriff für einen *Hilfssatz* verwendet – also für ein kleines Zwischenresultat, das vielleicht für sich genommen nicht übermäßig schwierig oder spannend ist, aber das in späteren Untersuchungen immer wieder nützlich sein wird).

Lemma 1.10 (Rechenregeln in Gruppen)**.** *Es sei G eine Gruppe. Dann gilt für alle $a,b \in G$:*

(a) $(a^{-1})^{-1} = a$.

(b) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

(c) ***(Kürzungsregel)*** *Für alle $x \in G$ ist*

$$\begin{aligned} x \cdot a = x \cdot b &\Leftrightarrow a = b, \\ \textit{und analog} \qquad a \cdot x = b \cdot x &\Leftrightarrow a = b. \end{aligned}$$

Beweis.

(a) Nach Satz 1.7 (d) ist $aa^{-1} = e$. Dies bedeutet aber genau, dass a das inverse Element zu a^{-1} ist, d. h. dass $(a^{-1})^{-1} = a$ gilt.

(b) ist analog zu (a): Es ist $b^{-1}a^{-1}ab = b^{-1}b = e$. Lesen wir dies als $(b^{-1}a^{-1})(ab) = e$, so bedeutet dies gerade, dass $b^{-1}a^{-1}$ wie behauptet das inverse Element zu ab ist.

(c) Gilt $xa = xb$, so folgt daraus durch Verknüpfung mit x^{-1} von links auch $x^{-1}xa = x^{-1}xb$ und damit $a = b$. Umgekehrt folgt aus $a = b$ durch Verknüpfung mit x von links natürlich $xa = xb$. Die zweite Äquivalenz zeigt man analog. □

Neben diesen elementaren Rechenregeln sind noch mehrfache Verknüpfungen eines Gruppenelements mit sich selbst wichtig. Wir können diese als Potenzen auffassen:

Definition 1.11 (**Potenzen**)**.** Es sei G eine Gruppe, $a \in G$ und $n \in \mathbb{Z}$. Dann setzen wir

$$a^n := \begin{cases} a \cdot \dots \cdot a \quad (n\text{-mal}) & \text{falls } n > 0, \\ e & \text{falls } n = 0, \\ a^{-1} \cdot \dots \cdot a^{-1} \quad ((-n)\text{-mal}) & \text{falls } n < 0. \end{cases}$$

Schreiben wir die Gruppenverknüpfung mit dem Symbol „+“, so verwenden wir die Schreibweise $n \cdot a$ statt a^n, um Verwirrungen zu vermeiden.

Diese Potenzen erfüllen nun die erwarteten Eigenschaften:

Lemma 1.12 (Rechenregeln für Potenzen)**.** *In jeder Gruppe G gilt für alle $a \in G$ und $m, n \in \mathbb{Z}$*

(a) $a^m \cdot a^n = a^{m+n}$;

(b) $(a^m)^n = a^{m \cdot n}$.

(Beachte, dass die Verknüpfung „ $\cdot$ “ in diesen Gleichungen in zwei Bedeutungen auftritt: als Gruppenverknüpfung auf der linken Seite von (a) und als gewöhnliche Multiplikation zweier ganzer Zahlen auf der rechten Seite von (b).)

Beweis.

(a) Für $m \geq 0$ und $n \geq 0$ ist die Behauptung klar nach Definition 1.11, da dann auf beiden Seiten einfach $(m+n)$-mal das Element a mit sich selbst verknüpft wird. Ebenso ergibt sich die Behauptung sofort für $m < 0$ und $n < 0$, weil dann auf beiden Seiten die $(-m-n)$-fache Verknüpfung von a^{-1} mit sich selbst steht.

Ist hingegen $m \geq 0$ und $n < 0$, so ist die linke Seite der zu beweisenden Gleichung nach Definition 1.11 gleich

$$\underbrace{a \cdot \dots \cdot a}_{m\text{-mal}} \cdot \underbrace{a^{-1} \cdot \dots \cdot a^{-1}}_{(-n)\text{-mal}}.$$

Durch mehrfaches Herauskürzen von $a a^{-1}$ in der Mitte erhält man daraus

$$\begin{aligned} a \cdot \dots \cdot a \quad & ((m-(-n))\text{-mal}) && \text{falls } m \geq -n, \\ a^{-1} \cdot \dots \cdot a^{-1} \quad & ((-n-m)\text{-mal}) && \text{falls } m < -n. \end{aligned}$$

In beiden Fällen ist das Ergebnis nach Definition 1.11 wie behauptet gleich a^{m+n}.

Den noch fehlenden Fall $m < 0$ und $n \geq 0$ zeigt man natürlich analog.

(b) Abhängig von n unterscheiden wir die folgenden Fälle:

(1) Für $n \geq 0$ gilt nach Definition

$$(a^m)^n = \underbrace{a^m \cdot \dots \cdot a^m}_{n\text{-mal}} \overset{\text{(a)}}{=} a^{\overbrace{m+\dots+m}^{n\text{-mal}}} = a^{mn}.$$

(2) Für $n = -1$ müssen wir $(a^m)^{-1} = a^{-m}$ zeigen, also dass a^{-m} das Inverse zu a^m ist. Dies folgt aber aus Teil (a), da $a^{-m} \cdot a^m = a^{-m+m} = a^0 = e$ gilt.

(3) Für $n < -1$ ergibt sich nun wieder aus der Definition

$$(a^m)^n = \underbrace{(a^m)^{-1} \cdot \dots \cdot (a^m)^{-1}}_{(-n)\text{-mal}} \overset{(2)}{=} \underbrace{a^{-m} \cdot \dots \cdot a^{-m}}_{(-n)\text{-mal}} \overset{\text{(a)}}{=} a^{\overbrace{-m-\dots-m}^{(-n)\text{-mal}}} = a^{mn}.$$

Damit haben wir die Behauptung in allen Fällen gezeigt. □

Wie erwartet haben wir in Definition 1.11 für ein beliebiges Element a einer Gruppe $a^0 := e$ gesetzt. Beachte aber, dass zusätzlich auch $a^n = e$ für ein $n \in \mathbb{N}_{>0}$ gelten kann. Dies führt zum folgenden Begriff der Ordnung eines Gruppenelements, der zunächst einmal nichts mit der Ordnung einer Gruppe wie in Definition 1.1 (c) zu tun hat (wir werden allerdings in Lemma 5.11 noch einen Zusammenhang zwischen diesen beiden Konzepten sehen).

Definition 1.13 (Ordnung eines Gruppenelements)**.** Es sei G eine Gruppe und $a \in G$. Gibt es ein $n \in \mathbb{N}_{>0}$ mit $a^n = e$, so heißt das kleinste solche n die **Ordnung** $\operatorname{ord} a$ von a. Existiert kein solches n, so schreibt man formal $\operatorname{ord} a = \infty$.

Beispiel 1.14.

(a) In $(\mathbb{R}\backslash\{0\},\cdot)$ (mit neutralem Element 1) ist $\operatorname{ord}(-1)=2$, denn $(-1)^1\neq 1$, aber $(-1)^2=1$.

In $(\mathbb{R},+)$ dagegen ist $\operatorname{ord}(-1)=\infty$, denn $n\cdot(-1)\neq 0$ für alle $n\in\mathbb{N}_{>0}$. In der Tat ist in dieser Gruppe mit dem gleichen Argument $\operatorname{ord} a=\infty$ für alle $a\neq 0$.

(b) Für ein Element a einer Gruppe G gilt genau dann $\operatorname{ord} a=1$, wenn $a=e$.

Beachte, dass es zur Überprüfung der Ordnung eines Elements nicht ausreicht, dass die entsprechende Potenz gleich e ist – es muss sich auch um die *kleinste* (positive) solche Potenz handeln. Andernfalls erhalten wir lediglich die folgende Aussage:

Lemma 1.15. *Es seien a ein Element einer Gruppe G und $n\in\mathbb{N}_{>0}$. Dann gilt $a^n=e$ genau dann, wenn $\operatorname{ord} a$ (endlich und) ein Teiler von n ist, d. h. wenn es ein $k\in\mathbb{N}_{>0}$ gibt mit $n=k\operatorname{ord} a$.*

Beweis. Wir zeigen die beiden Richtungen der Äquivalenz:

„$\Rightarrow$“: Es sei $n\in\mathbb{N}_{>0}$ mit $a^n=e$. Nach Definition 1.13 ist dann zunächst einmal $m:=\operatorname{ord} a\neq\infty$. Wir teilen n mit Rest durch m: Es gibt ein $k\in\mathbb{N}$ (das ganzzahlige Ergebnis der Division) und $r\in\{0,\dots,m-1\}$ (den Rest) mit

$$\frac{n}{m}=k+\frac{r}{m}\quad\text{bzw.}\quad n=km+r.$$

Mit den Rechenregeln aus Lemma 1.12 ist damit $e=a^n=(a^m)^k\cdot a^r=e^k\cdot a^r=a^r$. Nach Definition ist m aber die kleinste positive Zahl mit $a^m=e$. Wegen $a^r=e$ und $r<m$ kann r also nicht positiv sein, d. h. es ist $r=0$ und damit $n=km=k\operatorname{ord} a$. Mit $n>0$ ist dabei schließlich auch $k>0$.

„$\Leftarrow$“: Für $n=k\operatorname{ord} a$ folgt sofort $a^n=(a^{\operatorname{ord} a})^k=e^k=e$. □

Aufgabe 1.16. Es sei $G=\{e,a,b\}$ eine Gruppe der Ordnung 3, wobei e wie üblich das neutrale Element bezeichnet. Bestimme alle möglichen Verknüpfungstafeln für G.

Aufgabe 1.17. Man zeige:

(a) Ist G eine Gruppe mit $(ab)^2=a^2b^2$ für alle $a,b\in G$, so ist G abelsch.

(b) Ist G eine Gruppe mit $a^2=e$ für alle $a\in G$, so ist G abelsch.

Aufgabe 1.18. Zeige, dass jede nicht-abelsche Gruppe mindestens 5 Elemente haben muss.

Aufgabe 1.19. Es seien G eine Gruppe und $a,b\in G$. Man zeige:

(a) Ist G endlich, so ist auch $\operatorname{ord} a\neq\infty$.

(b) $\operatorname{ord}(ab)=\operatorname{ord}(ba)$.

(c) $\operatorname{ord}(a^{-1})=\operatorname{ord} a$.

Aufgabe 1.20. Es sei G eine Gruppe der Ordnung $|G|=10$. Zeige, dass es ein $a\in G\backslash\{e\}$ gibt mit $a^{-1}=a$.

Aufgabe 1.21. Es sei G eine Menge mit einer Verknüpfung, von der wir lediglich wissen, dass sie die Assoziativität (G1) und die Existenz eines linksneutralen Elements (G2) erfüllt, aber nicht notwendig die Existenz eines linksinversen Elements (G3). Man zeige:

(a) Ist G endlich, und gilt die rechtsseitige Kürzungsregel

$$ax=bx\ \Leftrightarrow\ a=b$$

für alle $a,b,x\in G$, so ist G bereits eine Gruppe.

(b) Ist G endlich, und gilt die linksseitige Kürzungsregel

$$xa=xb\ \Leftrightarrow\ a=b$$

für alle $a,b,x\in G$, so muss G nicht notwendig eine Gruppe sein.

(c) Ist G unendlich, so muss G selbst dann keine Gruppe sein, wenn beide Kürzungsregeln gelten.

Aufgabe 1.22. Es sei $G = \{a_1, \ldots, a_n\}$ eine abelsche Gruppe der Ordnung n. Zeige, dass dann $(a_1 \cdot \cdots \cdot a_n)^2 = e$ gilt.