2. Lösung zu algebraischen Strukturen: Rechnen mit Gruppenoperationen

Lösung (2.1) (a) Es gilt $(a \star b) \star c = \big((a+b)/2 + c\big)/2 = (a/4) + (b/4) + (c/2)$, und das ist für $a \neq c$ etwas anderes als $a \star (b \star c) = \big(a + (b+c)/2\big)/2 = (a/2) + (b/4) + (c/4)$. Das Assoziativgesetz gilt also nicht. Es gibt auch kein Neutralelement, denn die Gleichung $a \star x = a$, also $(a+x)/2 = a$, ist nur für $x = a$ erfüllbar. Da es kein neutrales Element gibt, kann man die Frage nach der Existenz inverser Elemente gar nicht mehr sinnvoll stellen.

(b) Das Assoziativgesetz gilt, denn für alle $x, y, z \in \mathbb{R}$ haben wir

$$\begin{aligned} x \circ (y \circ z) &= \sqrt{x^2 + (\sqrt{y^2+z^2})^2} = \sqrt{x^2+y^2+z^2} \\ &= \sqrt{(\sqrt{x^2+y^2})^2 + z^2} = (x \circ y) \circ z. \end{aligned}$$

(Offensichtlich gilt auch das Kommutativgesetz.) Wir fragen, ob es ein Neutralement e gibt; dieses müßte dann für alle $x \in \mathbb{R}$ die Bedingung $x \circ e = x$ bzw. $\sqrt{x^2+e^2} = x$ erfüllen, was für negative Zahlen $x < 0$ offenbar nicht möglich ist. Also existiert kein Neutralelement. Die Frage nach der Existenz inverser Elemente kann man daher gar nicht mehr sinnvoll stellen. Es liegt keine Gruppenstruktur vor.

(c) Das Assoziativgesetz gilt, denn für alle $x, y, z \in \mathbb{R}$ haben wir

$$\begin{aligned} x \circ (y \circ z) &= \sqrt[3]{x^3 + (\sqrt[3]{y^3+z^3})^3} = \sqrt[3]{x^3+y^3+z^3} \\ &= \sqrt[3]{(\sqrt[3]{x^3+y^3})^3 + z^3} = (x \circ y) \circ z. \end{aligned}$$

(Offensichtlich gilt auch das Kommutativgesetz.) Die Zahl 0 ist ein Neutralelement für $\circ$, denn es gilt $x \circ 0 = 0 \circ x = \sqrt[3]{x^3} = x$ für alle $x \in \mathbb{R}$. Schließlich ist für jede Zahl $x \in \mathbb{R}$ die Zahl $-x$ invers zu x bezüglich $\circ$, denn es gilt $x \circ (-x) = (-x) \circ x = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} = \sqrt[3]{0} = 0$. Also liegt eine Gruppenoperation vor.

(d) Das Assoziativgesetz gilt, denn für alle $x, y, z \in \mathbb{R}$ gilt

$$\begin{aligned} x \circ (y \circ z) &= x(yz+y+z) + x + (yz+y+z) \\ &= xyz + xy + xz + yz + x + y + z \\ &= (xy + x + y)z + (xy + x + y) + z \\ &= (x \circ y) \circ z. \end{aligned}$$

(Offensichtlich gilt auch das Kommutativgesetz.) Die Zahl 0 ist ein Neutralelement für $\circ$, denn es gilt $x \circ 0 = 0 \circ x = x$ für alle $x \in \mathbb{R}$. Wir fragen, ob es zu jedem Element $x \in \mathbb{R}$ ein inverses Element y gibt; dieses müßte dann $0 = xy + x + y = (x+1)y + x$ bzw. $y(x+1) = -x$ erfüllen. Wir sehen, daß jedes Element $x \neq -1$ ein Inverses besitzt (nämlich $y = -x/(x+1)$), das Element $x = -1$ dagegen nicht (denn die Gleichung $y \cdot 0 = 1$ ist nicht erfüllbar). Also liegt keine Gruppenstruktur vor. (Allerdings kann man nachrechnen, daß die Operation $\circ$ nicht aus $\mathbb{R} \setminus \{-1\}$ herausführt und daher eine innere Verknüpfung auf $\mathbb{R} \setminus \{-1\}$ definiert. Die obigen Rechnungen zeigen dann, daß $(\mathbb{R} \setminus \{-1\}, \circ)$ eine Gruppe ist.)

(e) Das Assoziativgesetz gilt, denn für alle $x, y, z \in \mathbb{R}$ haben wir $(x \circ y) \circ z = x \circ z = x = x \circ y = x \circ (y \circ z)$. Offensichtlich ist sogar *jedes* Element y rechtsneutral für die Operation $\circ$. Andererseits gibt es kein linksneutrales Element e, denn ein solches müßte $x = e \circ x = e$ für alle $x \in \mathbb{R}$ erfüllen. Es existiert also kein Neutralelement; die Frage nach der Existenz inverser Elemente stellt sich daher gar nicht mehr. Eine Gruppenstruktur liegt nicht vor.

Bemerkung. Die Gruppenstrukturen in (c) für $\mathbb{R}$ und in (d) für $\mathbb{R} \setminus \{-1\}$ ergeben sich aus der folgenden allgemeinen Konstruktion: Es seien $(G, \circ)$ eine Gruppe, X eine Menge und $f : X \to G$ eine bijektive Abbildung. Dann ist eine Gruppenstruktur auf X gegeben durch

$$x_1 \star x_2 := f^{-1}\big(f(x_1) \circ f(x_2)\big).$$

(Die Gruppenstruktur von G wird also einfach nach X übertragen.) In (c) betrachten wir $(G, \circ) = (\mathbb{R}, +)$ und $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) := x^3$. In (d) betrachten wir $(G, \circ) = (\mathbb{R} \setminus \{0\}, \cdot)$ und $f : \mathbb{R} \setminus \{-1\} \to \mathbb{R} \setminus \{0\}$ mit $f(x) := x + 1$.

Lösung (2.2) Die Implikationen (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (1) sind trivial; nur die Implikation (1) $\Rightarrow$ (2) ist wirklich zu zeigen. Es gelte also (1). Wir wählen ein festes Element $a \in G$; nach Voraussetzung gibt es dann ein (a priori von a abhängiges) Element $e \in G$ mit $ae = a$. Wir behaupten, daß dann auch $be = b$ für alle $b \in G$ gilt (so daß e ein rechtsneutrales Element für die Operation $\circ$ ist). Dazu geben wir uns $b \in G$ beliebig vor. Nach Voraussetzung existiert ein Element $x \in G$ mit $b = xa$. Es folgt dann

$$be = (xa)e = x(ae) = xa = b$$

wie behauptet. Vollkommen analog sieht man, daß ein linksneutrales Element f existiert. Wegen $f = fe = e$ ist damit die Existenz (und Eindeutigkeit) eines Neutralelements nachgewiesen.

Nun sei $x \in G$ beliebig. Nach Voraussetzung gibt es ein Element $x' \in G$ mit $x'x = e$. Wir behaupten, daß dann auch $xx' = e$ gilt, daß also x' invers (und nicht nur linksinvers) zu x ist. Zum Nachweis setzen wir $y := xx'$ und erhalten

$$yy = (xx')(xx') = x(x'x)x' = xex' = xx' = y.$$

Wiederum nach Voraussetzung gibt es ein Element y' mit $y'y = e$. Es folgt dann $e = y'y = y'(yy) = (y'y)y = ey = y$, also $y = e$ bzw. $xx' = e$. Damit ist gezeigt, daß jedes Element $x \in G$ ein inverses Element besitzt. Die Gruppenaxiome sind damit nachgewiesen.

Für eine endliche Menge G besagt Bedingung (3), daß eine assoziative Verknüpfung auf G genau dann eine Gruppenstruktur definiert, wenn in jeder Zeile und jeder Spalte der Verknüpfungstafel jedes Element von G genau einmal auftritt.

Lösung (2.3) Aus der ersten Zeile und Spalte der Verknüpfungstafel ergibt sich, daß das Element u sowohl links- als auch rechtsneutral ist. (Dies allein zeigt schon die Eindeutigkeit des Neutralelements, denn sind allgemein e_1 und e_2 sowohl links- als auch rechtsneutral, so folgt $e_1 = e_1e_2 = e_2$. Natürlich kann man auch an der Verknüpfungstafel unmittelbar ablesen, daß jedes Element außer u weder links- noch rechtsneutral ist.) In jeder Zeile und Spalte tritt jedes Element genau einmal auf; also besitzt jedes Element ein eindeutig bestimmtes Links- bzw. Rechtsinverses. Die Symmetrie der Verknüpfungstafel bezüglich der Hauptdiagonalen zeigt, daß das Kommutativgesetz gilt. (Auch deswegen fallen die Begriffe links- und rechtsneutral bzw. links- und rechtsinvers in diesem Beispiel zusammen.) Allerdings gilt das Assoziativgesetz nicht, denn beispielsweise haben wir $(xy)w = vw = u$, aber $x(yw) = xx = w$. (Dieses Beispiel zeigt, daß das Assoziativgesetz unabhängig von den anderen Gruppenaxiomen ist.)

Lösung (2.4) (a) Wir erhalten $(a \star c) \star (b \star c) = (ac^{-1}) \cdot (bc^{-1})^{-1} = (ac^{-1}) \cdot (cb^{-1}) = ab^{-1} = a \star b$, so daß (A) gilt. Die Gleichung $a \star x = b$ lautet $ax^{-1} = b$ und hat die (eindeutige) Lösung $x = b^{-1}a$, so daß auch (B) gilt.

(b) Wir wählen ein beliebiges Element $a \in G$ und definieren $e := a \star a$. Ist nun $b \in G$ ein weiteres Element von G, so gibt es wegen (B) ein Element $x \in G$ mit $a \star x = b$; wir erhalten dann $b \star b = (a \star x) \star (a \star x) = a \star a = e$. Damit ist gezeigt, daß die Elemente $x \star x$ mit $x \in G$ allesamt gleich e sind. Wir beweisen nun die angegebenen Aussagen.

(1) Es seien $a, b \in G$ beliebig. Es gibt ein Element $x \in G$ mit $a \star x = b$. Hieraus folgt $b \star e = (a \star x) \star (x \star x) = a \star x = b$. Da $b \in G$ beliebig war, ist die Behauptung bewiesen.

(2) Für alle $a \in G$ erhalten wir $a \cdot e = a \star (e \star e) = a \star e = a$ und $e \cdot a = e \star (e \star a) = (a \star a) \star (e \star a) = a \star e = a$, wobei wir jeweils (1) benutzten.

(3) Mit $a^{-1} := e \star a$ erhalten wir $a \cdot a^{-1} = a \cdot (e \star a) = a \star \big(e \star (e \star a)\big) = a \star \big((a \star a) \star (e \star a)\big) = a \star (a \star e) = a \star a = e$ und $a^{-1} \cdot a = (e \star a) \cdot a = (e \star a) \star (e \star a) = e$.

(4) Der angegebene Ausdruck ist einerseits gleich

$$\begin{aligned} &\big(a \star (e \star b)\big) \star \big(e \star (e \star c^{-1})\big) \\ &= (a \cdot b) \star (e \cdot c^{-1}) \;=\; (a \cdot b) \star c^{-1} \;=\; (a \cdot b) \cdot c, \end{aligned}$$

andererseits auch gleich

$$\begin{aligned} &\big(a \star (e \star b)\big) \star \big[\big(e \star (b \star c^{-1})\big) \star (e \star b)\big] \\ &= a \star \big(e \star (b \star c^{-1})\big) \;=\; a \cdot (b \star c^{-1}) \;=\; a \cdot (b \cdot c). \end{aligned}$$

Damit ist bewiesen, daß $(G, \cdot)$ eine Gruppe ist, in der das Inverse eines Elements $a \in G$ gegeben ist durch $e \star a$. Der Zusammenhang zwischen $\cdot$ und $\star$ ergibt sich dann aus der Rechnung $a \cdot b^{-1} = a \star (e \star b^{-1}) = a \star \big(e \star (e \star b)\big) = a \star \big((b \star b) \star (e \star b)\big) = a \star (b \star e) = a \star b$.

Lösung (2.5) Es sei $S^\times$ die Menge der invertierbaren Elemente von S. Dann ist $S^\times$ abgeschlossen unter $\circ$, denn sind x_1 und x_2 invertierbar (mit den Inversen y_1 bzw. y_2), so ist auch $x_1 \circ x_2$ invertierbar (mit dem Inversen $y_2 \circ y_1$). Also ist $\circ$ eine innere assoziative Verknüpfung auf $S^\times$. Wegen $e \circ e = e$ gilt $e \in S^\times$, so daß $S^\times$ ein Neutralelement besitzt. Unmittelbar nach Definition besitzt jedes Element von $S^\times$ ein Inverses in S, und dieses Inverse liegt natürlich wieder in $S^\times$. Damit ist $(S^\times, \circ)$ als Gruppe nachgewiesen. Wir bestimmen nun noch $S^\times$ für jedes der Monoide S in der Aufgabenstellung.

(a) Offensichtlich ist S ein Monoid, dessen Neutralelement die Einheitsmatrix $\mathbf{1}$ ist. Eine Matrix $M \in S$ ist offenbar genau dann invertierbar in S, wenn die inverse Matrix M^{-1} existiert und wieder ganzzahlige Einträge hat. In diesem Fall sind sowohl $\det(M)$ als auch $\det(M^{-1}) = 1/\det(M)$ ganzzahlig, was nur für $\det(M) = \pm 1$ möglich ist. Gilt umgekehrt $\det(M) = \pm 1$, so ist M in $\mathbb{Z}^{2\times 2}$ invertierbar. Also gilt

$$S^\times \;=\; \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{Z}^{2\times 2} \mid ad - bc = \pm 1\}.$$

(b) Offensichtlich ist S ein Monoid, dessen Neutralelement die Einheitsmatrix $\mathbf{1}$ ist. Eine Matrix $M \in S$ ist offenbar genau dann invertierbar in S, wenn die inverse Matrix M^{-1} existiert und wieder nichtnegative Einträge hat. Wegen

$$M^{-1} \;=\; \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

ist dies genau dann der Fall, wenn die Bedingungen $a > 0, d > 0, b = c = 0$ oder $a = d = 0, b > 0, c > 0$ gelten. Also ist

$$S^\times \;=\; \{\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mid a, d > 0\} \cup \{\begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} \mid b, c > 0\}.$$

(c) Offensichtlich ist S ein Monoid, dessen Neutralelement die identische Abbildung $\mathrm{id}_\mathbb{R}$ ist. Eine Funktion $f \in S$ ist genau dann invertierbar in S, wenn sie eine Umkehrfunktion besitzt. Also ist

$$S^\times \;=\; \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ bijektiv}\}.$$

(d) Offensichtlich ist S ein Monoid, dessen Neutralelement die konstante Funktion mit dem Wert 1 ist. Eine Funktion $f \in S$ ist genau dann invertierbar in S, wenn $1/f$ existiert. Also gilt

$$S^\times \;=\; \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ hat keine Nullstelle}\}.$$

Lösung (2.6) Offenbar ist $\star$ eine innere Verknüpfung auf G. Diese Verknüpfung ist assoziativ, denn für alle $a, b, c \in G$ gilt

$$(a \star b) \star c \;=\; (axb)xc \;=\; ax(bxc) \;=\; a \star (b \star c).$$

Das Element x^{-1} ist ein Neutralelement für $\star$, denn für alle $a, b \in G$ haben wir $a \star x^{-1} = axx^{-1} = a$ und $x^{-1} \star b = x^{-1}xb = b$. Wir behaupten schließlich, daß für jedes Element $a \in G$ das Element $a' := x^{-1}a^{-1}x^{-1}$ invers zu a bezüglich der Operation $\star$ ist. Dies folgt aus den Gleichungen $a \star a' = ax(x^{-1}a^{-1}x{-}1) = x^{-1}$ und $a' \star a = (x^{-1}a^{-1}x^{-1})xa = x^{-1}$. Damit ist $(G, \star)$ als Gruppe nachgewiesen.

Lösung (2.7) Es seien $f_1, f_2, f_3 \in \mathcal{F}$. Für alle $x \in X$ haben wir dann

$$\begin{aligned}\big(f_1 \star f_2\big) \star f_3\big)(x) \;&=\; \big(f_1(x) \circ f_2(x)\big) \circ f_3(x)\\ &=\; f_1(x) \circ \big(f_2(x) \circ f_3(x)\big) \;=\; \big(f_1 \star (f_2 \star f_3)\big)(x).\end{aligned}$$

Da zwei Funktionen zwischen zwei Mengen genau dann gleich sind, wenn sie für alle Argumente die gleichen Werte annehmen, bedeutet dies $f_1 \star (f_2 \star f_3) = (f_1 \star f_2) \star f_3$. Also ist die Verknüpfung $\star$ assoziativ. Die konstante Funktion mit dem Wert e ist offensichtlich ein Neutralelement für $(\mathcal{F}, \star)$. Definieren wir zu $f : X \to G$ die Funktion $\widehat{f} : X \to G$ durch $\widehat{f}(x) := f(x)^{-1}$, so ist offenbar $\widehat{f}$ sowohl links- als auch rechtsinvers zu f in $(\mathcal{F}, \star)$. Damit ist $(\mathcal{F}, \star)$ als Gruppe nachgewiesen.

Lösung (2.8) Es gelte $x_1x_2 \cdots x_n = e$. Multiplizieren wir diese Gleichung von links mit x_1^{-1} und von rechts mit x_1 durch, so erhalten wir $x_2 \cdots x_nx_1 = x_1^{-1}x_1 = e$, und das ist schon die Behauptung.

Lösung (2.9) Gilt in einer Gruppe $ab = e$, dann auch $ba = e$. Das Auftreten des Elements e in der Gruppentafel erfolgt also symmetrisch zur Hauptdiagonalen. Genau dann ist eine Gruppe G kommutativ, wenn $ab = ba$ für alle $a, b \in G$ gilt, was genau dann der Fall ist, wenn die Gruppentafel von G symmetrisch zur Hauptdiagonalen ist.

Lösung (2.10) Wir betrachten die n Elemente

$$(\star) \qquad g_1, \quad g_1g_2, \quad g_1g_2g_3, \quad \ldots, \quad g_1g_2g_3 \cdots g_n\,.$$

Sind diese paarweise verschieden, so repräsentieren sie genau die n Elemente, die es in G gibt. Da eines davon das Neutralelement e ist, gibt es also eine Darstellung der Form $e = g_1g_2 \ldots g_j$; damit ist in diesem Fall die Behauptung bewiesen (und zwar mit $i = 1$). Sind die Elemente $(\star)$ dagegen nicht paarweise verschieden, so gibt es Indices $1 \le i - 1 \le j$ mit

$$g_1g_2 \cdots g_{i-1} \;=\; g_1g_2 \cdots g_{i-1}g_i \cdots g_j.$$

Multiplizieren wir diese Gleichung mit $(g_1 \cdots g_{i-1})^{-1}$ von links durch, so ergibt sich $e = g_ig_{i+1} \cdots g_j$. Also erhalten wir auch in diesem Fall eine Darstellung der behaupteten Art.

Lösung (2.11) (1) Für alle $x, y, a \in G$ gilt $\kappa_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \kappa_a(x)\kappa_a(y)$.

(2) Für alle $x, a, b \in G$ gilt $(\kappa_a \circ \kappa_b)(x) = \kappa_a\big(\kappa_b(x)\big) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \kappa_{ab}(x)$. Da das Argument x beliebig war, bedeutet dies $\kappa_a \circ \kappa_b = \kappa_{ab}$.

(3) Wegen (2) haben wir $\kappa_{a^{-1}} \circ \kappa_a = \kappa_{a^{-1}a} = \kappa_e = \mathrm{id}_G$ und $\kappa_a \circ \kappa_{a^{-1}} = \kappa_{aa^{-1}} = \kappa_e = \mathrm{id}_G$. Also ist κ_a bijektiv mit der Umkehrabbildung $\kappa_{a^{-1}}$.

(4) Wegen $x = \kappa_e(x)$ gilt $x \sim x$ für alle $x \in G$ (Reflexivität). Gilt $x \sim y$, sagen wir $y = \kappa_a(x)$ mit $a \in G$, so gilt auch $x = \kappa_a^{-1}(y) = \kappa_{a^{-1}}(y)$ und damit $y \sim x$ (Symmetrie). Gelten die Bedingungen $x \sim y$ und $y \sim z$, sagen wir $y = \kappa_a(x)$ und $z = \kappa_b(y)$ mit $a, b \in G$, so gilt auch $z = \kappa_b\big(\kappa_a(x)\big) = \kappa_{ba}(x)$ und damit $x \sim z$ (Transitivität).

Lösung (2.12) (a) Trivialerweise gilt $a \cdot a = a \cdot a$ für alle $a \in G$.

(b) Kommutiert a mit b, so gilt $ab = ba$. Wir multiplizieren diese Gleichung sowohl von links als auch von rechts mit b^{-1} durch und erhalten $b^{-1}a = ab^{-1}$; also kommutiert a auch mit b^{-1}.

(c) Zunächst sei $k \in \mathbb{N}$. Kommutiert a mit b, so folgt

$$ab^k \;=\; bab^{k-1} \;=\; b^2ab^{k-2} \;=\; \cdots \;=\; b^{k-1}ab \;=\; b^ka,$$

denn wir können das Element a durch Ausnutzen der Gleichung $ab = ba$ stets um eine Position nach rechts verschieben. (Formal kann man Induktion über k benutzen.) Also kommutiert a mit b^k für $k \in \mathbb{N}$. Nach (b) kommutiert a dann auch mit $(b^k)^{-1} = b^{-k}$. Trivialerweise kommutiert a mit $b^0 = e$. Also kommutiert a mit allen Potenzen von b.

(d) Kommutiert a mit b_1 und b_2, so erhalten wir

$$a(b_1b_2) = (ab_1)b_2 = (b_1a)b_2 = b_1(ab_2) = b_1(b_2a) = (b_1b_2)a,$$

so daß a auch mit b_1b_2 kommutiert.

Daß die Relation des Miteinanderkommutierens im allgemeinen nicht transitiv ist, sieht man sofort, indem man irgendwelche nicht kommutierenden Elemente a und c in einer Gruppe wählt und für b dann das Neutralelement dieser Gruppe nimmt. Es kommutieren dann a und b sowie b und c, aber nicht a und c.

Lösung (2.13) (a) Es gilt

$$\begin{aligned}[x, y]^{-1} \;&=\; (xyx^{-1}y^{-1})^{-1}\\ &=\; yxy^{-1}x^{-1} \;=\; [y, x].\end{aligned}$$

(b) Es gelten die Gleichungen

$$x^{-1}[x, y] \;=\; x^{-1}(xyx^{-1}y^{-1}) \;=\; yx^{-1}y^{-1} \;=\; \kappa_y(x^{-1})$$

und

$$[x, y]y \;=\; (xyx^{-1}y^{-1})y \;=\; xyx^{-1} \;=\; \kappa_x(y).$$

(c) Es gelten die Gleichungen

$$\begin{aligned}[xy, z] \;&=\; (xy)z(xy)^{-1}z^{-1} \;=\; xyzy^{-1}x^{-1}z^{-1}\\ &=\; xyzy^{-1}(z^{-1}x^{-1}xz)x^{-1}z^{-1}\\ &=\; x(yzy^{-1}z^{-1})x^{-1}(xzx^{-1}z^{-1})\\ &=\; x[y, z]x^{-1}[x, z] \;=\; \kappa_x\big([y, z]\big)[x, z]\end{aligned}$$

und

$$\begin{aligned}[x,yz] &= x(yz)x^{-1}(yz)^{-1} = xyzx^{-1}z^{-1}y^{-1}\\ &= xy(x^{-1}y^{-1}yx)zx^{-1}z^{-1}y^{-1}\\ &= (xyx^{-1}y^{-1})y(xzx^{-1}z^{-1})y^{-1}\\ &= [x,y]y[x,z]y^{-1} = [x,y]\kappa_y\big([x,z]\big).\end{aligned}$$

(d) Es gelten die Gleichungen

$$\begin{aligned}[x,y^{-1}] &= xy^{-1}x^{-1}y = x(y^{-1}x^{-1}yx)x^{-1}\\ &= x[y^{-1},x^{-1}]x^{-1} = \kappa_x\big([y^{-1},x^{-1}]\big)\end{aligned}$$

und

$$\begin{aligned}[x^{-1},y] &= x^{-1}yxy^{-1} = x^{-1}(yxy^{-1}x^{-1})x\\ &= x^{-1}[y,x]x = \kappa_{x^{-1}}\big([y,x]\big).\end{aligned}$$

(e) Wir erhalten zunächst

$$\begin{aligned}&\kappa_x\big(\big[[x^{-1},y],\,z\big]\big) = x\,[x^{-1}yxy^{-1},\,y]\,x^{-1}\\ &= x(x^{-1}yxy^{-1})z(yx^{-1}y^{-1}x)z^{-1}x^{-1}\\ &= (yxy^{-1}zy)(x^{-1}y^{-1}xz^{-1}x^{-1})\end{aligned}$$

und völlig analog dann

$$\begin{aligned}\kappa_z\big(\big[[z^{-1},x],\,y\big]\big) &= (xzx^{-1}yx)(z^{-1}x^{-1}zy^{-1}z^{-1}),\\ \kappa_y\big(\big[[y^{-1},z],\,x\big]\big) &= (zyz^{-1}xz)(y^{-1}z^{-1}yx^{-1}y^{-1}).\end{aligned}$$

Mit den Abkürzungen

$$\begin{aligned}u &:= yxy^{-1}zy,\\ v &:= xzx^{-1}yx,\\ w &:= zyz^{-1}xz\end{aligned}$$

gehen diese Gleichungen über in die Gleichungen

$$\begin{aligned}\kappa_x\big(\big[[x^{-1},y],\,z\big]\big) &= uv^{-1},\\ \kappa_z\big(\big[[z^{-1},x],\,y\big]\big) &= vw^{-1},\\ \kappa_y\big(\big[[y^{-1},z],\,x\big]\big) &= wu^{-1}.\end{aligned}$$

Als Produkt dieser drei Elemente ergibt sich dann

$$\begin{aligned}&\kappa_x\big(\big[[x^{-1},y],\,z\big]\big)\kappa_z\big(\big[[z^{-1},x],\,y\big]\big)\kappa_y\big(\big[[y^{-1},z],\,x\big]\big)\\ &= uv^{-1}vw^{-1}wu^{-1} = uu^{-1} = e.\end{aligned}$$

Lösung (2.14) (a) Wir benutzen Induktion über n; der Induktionsanfang $n = 1$ ist dabei gerade die Voraussetzung. Gilt $a^nba^{-n} = b^{k^n}$ nach Induktionsannahme, so erhalten wir

$$\begin{aligned}b^{k^{n+1}} &= b^{k^n\cdot k} = (b^{k^n})^k = (a^nba^{-n})^k\\ &= a^nba^{-n}\cdot a^nba^{-n}\cdots a^nba^{-n}\\ &= a^nb^ka^{-n} = a^n(aba^{-1})^ka^{-n}\\ &= a^n\cdot aba^{-1}\cdot aba^{-1}\cdots aba^{-1}a^{-n}\\ &= a^nab^ka^{-1}a^{-n} = a^{n+1}b^ka^{-(n+1)}.\end{aligned}$$

Damit ist der Induktionsschritt abgeschlossen.

(b) Aus $aba^{-1} = b^2$ folgt $a^5ba^{-5} = b^{32}$ nach Teil (a). Wegen $a^5 = e$ bedeutet dies $b = b^{32}$ und damit $b^{31} = e$.

(c) Die Bedingung $aba^{-1} = b^{-1}$ lautet umgeschrieben $bab = a$. Unter Benutzung dieser Bedingung erhalten wir für alle $n \in \mathbb{N}$ die Gleichung

$$(ba)^{2n} = (baba)^n = (a^2)^n = a^{2n}$$

und damit $(ba)^{2n+1} = (ba)(ba)^{2n} = (ba)a^{2n} = ba^{2n+1}$. Speziell für $n = m$ erhalten wir $(ba)^{2m+1} = ba^{2m+1} = b$ und damit

$$\begin{aligned}a &= a\cdot a^{2m+1} = a^{2m+2} = (ba)^{2m+2}\\ &= (ba)^{2m+1}(ba) = b(ba) = b^2a,\end{aligned}$$

insgesamt also $a = b^2a$ und damit $b^2 = e$.

(d) Die erste Gleichung besagt $ab^2a^{-1} = b^3$. Hieraus folgt $ab^{2k}a^{-1} = b^{3k}$ für alle $k \in \mathbb{Z}$; insbesondere erhalten wir

$$a^2b^4a^{-2} = a(ab^4a^{-1})a^{-1} = ab^6a^{-1} = b^9.$$

Aus der zweiten Gleichung folgt $a^{-1}b = a^2ba^{-2}$ und daher

$$a^2b^4a^{-2} = (a^2ba^{-2})^4 = (a^{-1}b)^4.$$

Insgesamt erhalten wir also $b^9 = (a^{-1}b)^4$. Dieses Element kommutiert offensichtlich sowohl mit b als auch mit $a^{-1}b$, damit aber auch mit b^{-1}, mit $(a^{-1}b)b^{-1} = a^{-1}$ und mit a. Dann kommutiert aber auch $a^{-2}b^9a^2 = b^4$ sowohl mit a als auch mit b. Also kommutieren b^9 und b^4 beide mit a; dann kommutiert aber auch $b = b^9(b^4)^{-2}$ mit a. Die Gleichungen $ab^2 = b^3a$ und $a^3b = ba^2$ gehen daher über in $ab^2 = ab^3$ und $a^3b = a2b$ und daher in $e = b$ und $a = e$. Es ergibt sich $a = b = e$.

Lösung (2.15) (a) Es gebe ein Element $x \in G$ mit $xax = b$. Dann ist $ab = axax = (ax)^2$ ein Quadrat in G. Umgekehrt sei ab ein Quadrat in G, sagen wir $ab = y^2$. Wir wollen ein Element $x \in G$ finden mit $xax = b$. Wie wir schon gesehen haben, muß dann $y^2 = ab = (ax)^2$ gelten; es ist also naheliegend, x so zu wählen, daß $ax = y$ gilt. Wir definieren also $x := a^{-1}y$; dann gilt tatsächlich $xax = a^{-1}yaa^{-1}y = a^{-1}y^2 = a^{-1}ab = b$, so daß x die Gleichung $xax = b$ löst.

(b) Es gelte $x^2ax = a^{-1}$. Dann gilt $x^2axa = e$, also $xaxa = x^{-1}$ und folglich $(xa)^3 = x^{-1}(xa) = a$. Damit ist gezeigt, daß a ein Kubus in G ist. Umgekehrt gebe es ein Element $y \in G$ mit $a = y^3$. Um die Gleichung $x^2ax = a^{-1}$ zu erfüllen, ist es nach der vorigen Überlegung naheliegend, das Element x so zu wählen, daß $y = xa$ gilt; wir setzen also $x := ya^{-1}$. Für dieses Element ergibt sich dann $x^2ax = (ya^{-1})^2a(ya^{-1}) = ya^{-1}ya^{-1}aya^{-1} = ya^{-1}y^2a^{-1} = yy^{-3}y^2y^{-3} = y^{-3} = a^{-1}$ und damit die Gültigkeit der Gleichung $x^2ax = a^{-1}$.

Lösung (2.16) (1)⇒(2). Aufgrund der Kommutativität erhalten wir $(ab)^n = abab\cdots ab = aa\cdots abb\cdots b = a^nb^n$. Formal verbirgt sich hinter den drei Pünktchen ein Induktionsbeweis, den wir der Vollständigkeit halber auch noch führen wollen. Für $n = 1$ gilt die Behauptung trivialerweise. Gilt $(ab)^n = a^nb^n$ nach Induktionsannahme, so folgt $(ab)^{n+1} = ab(ab)^n = aba^nb^n = aa^nbb^n = a^{n+1}b^{n+1}$, wobei für die zweite Gleichung die Induktionsannahme und für die dritte Gleichung die Kommutativität von G benutzt wurde.

(2)⇒(3): Diese Implikation ist trivial.

(3)⇒(1): Es seien $a, b \in G$ beliebig. Nach Voraussetzung gelten die Bedingungen

$$\begin{aligned}(ab)^N &= a^Nb^N,\\ (ab)^{N+1} &= a^{N+1}b^{N+1},\\ (ab)^{N+2} &= a^{N+2}b^{N+2}.\end{aligned}$$

Einsetzen der ersten in die zweite und der zweiten in die dritte dieser Gleichungen liefert $ab(a^Nb^N) = a^{N+1}b^{N+1}$ und $(ab)a^{N+1}b^{N+1} = a^{N+2}b^{N+2}$, nach Multiplikation mit a^{-1} von links und b^{-N} bzw. $b^{-(N+1)}$ von rechts also

$$ba^N = a^Nb \quad \text{und} \quad ba^{N+1} = a^{N+1}b.$$

Setzen wir hier die erste in die zweite Gleichung ein, so erhalten wir $(a^Nb)a = a^{N+1}b$, nach Durchmultiplizieren mit a^{-N} von links also $ba = ab$. Da $a, b \in G$ beliebig waren, ist damit die Kommutativität von G gezeigt. (Der Beweis zeigt, daß die in der Bedingung auftretende Zahl N nicht fest sein muß, sondern von den jeweils betrachteten Elementen a und b abhängen darf.)

(1)⇔(4): Es gelten die Äquivalenzen $(ab)^2 = a^2b^2 \Leftrightarrow abab = aabb \Leftrightarrow ba = ab$.

(1)⇔(5): Es gelten die Äquivalenzen $(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow ab = (a^{-1}b^{-1})^{-1} = ba$.

Lösung (2.17) Aus der angegebenen Eigenschaft folgt sofort

$$(\star) \qquad (a_1a_2\cdots a_n)^3 = a_1^3a_2^3\cdots a_n^3$$

für alle $n \in \mathbb{N}$ und alle $a_i \in G$; diese Eigenschaft werden wir mehrfach verwenden. Wir beweisen zunächst die im Hinweis enthaltenen Aussagen!

(1) Es gelte $xy^3 = y^3x$. Für das Element $\xi := xyx^{-1}y^{-1}$ gilt dann $\xi^3 = (xyx^{-1}y^{-1})^3 = x^3y^3x^{-3}y^{-3} = x^3x^{-3}y^3y^{-3} = e$. Weil G keine Elemente der Ordnung 3 besitzt, folgt hieraus $\xi = e$; das bedeutet aber $xy = yx$.

(2) Für alle $a, b \in G$ gilt $a^3b^3a^{-3} = (aba^{-1})^3 = ab^3a^{-1}$; hierbei gilt die erste Gleichung wegen $(\star)$, die zweite wegen $(aba^{-1})^3 = aba^{-1}aba^{-1}aba^{-1} = abbba^{-1} = ab^3a^{-1}$. Durchmultiplizieren der Gleichung $a^3b^3a^{-3} = ab^3a^{-1}$ von links mit a^{-1} und von rechts mit a^3 liefert $a^2b^3 = b^3a^2$. Da $a, b \in G$ beliebig waren, kommutiert also in G jedes Quadrat mit jedem Kubus. Nach (1) kommutiert dann jedes Quadrat in G mit jedem Element von G.

(3) Es sei $\xi = xyx^{-1}y^{-1}$ mit $x, y \in G$. Wegen $(\star)$ gilt dann

$$\begin{aligned}\xi^3 &= (xyx^{-1}y^{-1})^3 = (xyx^{-1})^3y^{-3} = xy^3x^{-1}y^{-3}\\ &= xyy^2x^{-1}y^{-3} = xyx^{-1}y^2y^{-3} = xyx^{-1}y^{-1} = \xi;\end{aligned}$$

dabei gilt die erste Gleichung in der zweiten Zeile, weil y^2 nach (2) mit allen Elementen von G kommutiert. Also gilt $\xi^3 = \xi$, damit aber $\xi^2 = e$.

(4) Wegen (3) gilt $(xyx^{-1}y^{-1})^2 = e$, also

$$\begin{aligned}e &= xyx^{-1}y^{-1}xyx^{-1}y^{-1} = xyxx^{-2}yy^{-2}xyx^{-1}y^{-1}\\ &= xyxyxyx^{-3}y^{-3} = (xy)^3x^{-3}y^{-3} = (xyx^{-1}y^{-1})^3;\end{aligned}$$

dabei gilt der Übergang von der ersten zur zweiten Zeile, weil die Elemente x^{-2} und y^{-2} nach (2) mit allen Elementen von G kommutieren, während die letzte Gleichung wegen $(\star)$ gilt. Aus $(xyx^{-1}y^{-1})^3 = e$ folgt aber, weil G keine Elemente der Ordnung 3 besitzt, die Gleichung $xyx^{-1}y^{-1} = e$.

Wegen (4) gilt $xy = yx$ für alle $x, y \in G$. Das bedeutet aber, daß G kommutativ ist.

Lösung (2.18) (a) Es seien $x, y \in G$ beliebige Elemente von G. Nach Voraussetzung gelten dann die Gleichungen $x^2 = e$, $y^2 = e$ und $e = (xy)^2 = xyxy$. Durchmultiplizieren der letzten Gleichung mit x von links und mit y von rechts liefert $xey = x^2yxy^2 = eyxe$ und damit $xy = yx$. Da x und y beliebig waren, ist damit die Kommutativität der Gruppe G gezeigt.

(b) Ein Beispiel ist etwa die Kleinsche Vierergruppe, also die Gruppe der Symmetrieabbildungen eines Rechtecks. (Diese besteht aus der Identität, der 180^0-Drehung um den Mittelpunkt des Rechtecks und den Spiegelungen an den beiden Symmetrieachsen des Rechtecks. Jede dieser Abbildungen ist zu sich selbst invers.) Ein Gegenbeispiel ist etwa die additive Gruppe $\mathbb{Z}_3$.

Lösung (2.19) (a) Gilt $x^2 \neq e$, dann auch $(x^{-1})^2 \neq e$, und es gilt $x^{-1} \neq x$. Die Elemente $x \in G$ mit $x^2 \neq e$ treten also in Paaren (x, x^{-1}) auf.

(b) Nach (a) ist die Anzahl der Elemente x mit $x^2 \neq e$ gerade. Weil $|G|$ gerade ist, muß dann auch die Anzahl der Elemente x mit $x^2 = e$ gerade sein. Weil das Neutralelement e eines dieser Elemente ist, muß es daher mindestens ein Element $x \neq e$ mit $x^2 = e$ geben.

(c) Nach (b) ist die Quadrierungsabbildung

$$f : \begin{array}{ccc} G & \to & G \\ x & \mapsto & x^2 \end{array}$$

nicht injektiv. Da G endlich ist, ist dies gleichbedeutend damit, daß f nicht surjektiv ist. Das ist aber schon die Behauptung.

Lösung (2.20) Eine Gruppe mit zwei Elementen muß aus dem Neutralelement e und einem zweiten Element $a \neq e$ bestehen. Da in der Verknüpfungstafel in jeder Zeile und Spalte jedes Element genau einmal vorkommen muß, bleibt als einzige Möglichkeit die folgende Verknüpfungstafel.

$\circ$	e	a
e	e	a
a	a	e

Daß tatsächlich eine Gruppe vorliegt, ist klar, weil es konkrete Realisierungen dieser Verknüpfungstafel durch bekannte Gruppen gibt, beispielsweise die Gruppe $(\mathbb{Z}_2, +)$ oder auch die Symmetriegruppe einer geometrischen Figur, deren einzige nichttriviale Symmetrieoperation eine Achsenspiegelung ist. (Ein gleichschenkliges, aber nicht gleichseitiges Dreiecks ist etwa eine solche Figur.) Analog kann die Verknüpfungstafel einer Gruppe mit drei Elementen nur die folgende Form haben.

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Auch hier ist klar, daß tatsächlich eine Gruppe vorliegt (daß also zwangsläufig das Assoziativgesetz gilt), weil es konkrete Realisierungen dieser Verknüpfungstafel durch bekannte Gruppen gibt, beispielsweise die Gruppe $(\mathbb{Z}_3, +)$ oder die Symmetriegruppe einer Figur, deren einzige Symmetrieoperationen die Drehungen um 0^0, um 120^0 und um 240^0 sind. (Ein Dreischneuß ist eine solche Figur.) Bei einer Gruppe mit 4 Elementen gibt es gemäß Aufgabe (2.19) entweder genau ein Element $a \neq e$ mit $a^2 = e$, oder alle vier Elemente von G erfüllen die Gleichung $x^2 = e$. Diese Bedingung legt einen Teil der Verknüpfungstafel fest, und zwar gibt es die beiden folgenden Möglichkeiten.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b			e
c	c		e	

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

In jedem der beiden Fälle legt nun die Bedingung, daß jedes Gruppenelement in jeder Zeile und Spalte genau einmal auftreten muß, die Verknüpfungstafel eindeutig fest, und zwar wie folgt.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Es scheint also zwei verschiedene Gruppen mit jeweils vier Elementen zu geben, aber das haben wir noch nicht bewiesen. Wir haben nur gezeigt, daß, wenn es überhaupt eine Gruppe mit vier Elementen gibt, deren Verknüpfungstafel durch eine der beiden obigen Möglichkeiten gegeben ist. Die Gültigkeit des Assoziativgesetzes haben wir in keinem der beiden Fälle nachgeprüft. Das ist aber auch nicht nötig, weil sich beide Verknüpfungstafeln durch bekannte Gruppen realisieren lassen. Die linke Tafel wird etwa realisiert durch die Gruppe $(\mathbb{Z}_4, +)$ oder die Symmetriegruppe einer geometrischen Figur, deren einzige Symmetrieoperationen die Drehungen um 0^0, um 90^0, um 180^0 und um 270^0 sind. (Ein Vierschneuß ist etwa eine solche Figur.) Die rechte Tafel wird etwa realisiert durch das direkte Produkt von $(\mathbb{Z}_2, +)$ mit sich selbst oder die Symmetriegruppe eines nichtquadratischen Rechtecks. Diese zweite Gruppe wird nach dem Mathematik Felix Klein (1849-1925) als **Kleinsche Vierergruppe** bezeichnet.