6. Lösung zu algebraischen Strukturen: Gruppenhomomorphismen

Lösung (6.1) Wir definieren f durch

$$f(z) \;:=\; \left(|z|, \frac{z}{|z|}\right).$$

Dies ist offensichtlich eine Bijektion von $\mathbb{C}^\times$ auf $\mathbb{R}^+ \times T$, deren Umkehrabbildung gegeben ist durch $g(r,\zeta) = r\zeta$. Daß f ein Gruppenhomomorphismus ist, ergibt sich aus der folgenden Rechnung:

$$\begin{aligned} f(z_1 z_2) \;&=\; \left(|z_1 z_2|, \frac{z_1 z_2}{|z_1 z_2|}\right) \;=\; \left(|z_1|\cdot|z_2|, \frac{z_1}{|z_1|}\cdot\frac{z_2}{|z_2|}\right) \\ &=\; \left(z_1, \frac{z_1}{|z_1|}\right)\cdot\left(z_2, \frac{z_2}{|z_2|}\right) \;=\; f(z_1)\cdot f(z_2). \end{aligned}$$

Hierbei folgt die zweite Gleichung daraus, daß $|z_1 z_2| = |z_1|\,|z_2|$ für alle komplexen Zahlen $z_1, z_2 \in \mathbb{C}$ gilt, während die dritte Gleichung unmittelbar aus der Definition der Verknüpfung eines direkten Produkts zweier Gruppen folgt. (Die erste und die letzte Gleichung ergeben sich unmittelbar aus der Definition von f.) Das Bild von $\mathbb{R}^\times$ ist gerade $\mathbb{R}^+ \times \{\pm 1\}$; die Einschränkung von f auf $\mathbb{R}^+$ ist einfach gegeben durch

$$f(x) \;=\; (|x|, \operatorname{sign}(x)).$$

Lösung (6.2) Wir können $\alpha(M) := \det(M)$, $\beta(M) := |\det(M)|$ und $\gamma(M) := \ln|\det(M)|$ wählen. Der Kern von α ist dann die Gruppe $\mathrm{SL}(n,\mathbb{R})$ aller reellen $(n\times n)$-Matrizen mit der Determinante 1, während der Kern von β und auch derjenige von γ gleich der Menge aller Matrizen M mit $|\det(M)| = 1$ ist.

Lösung (6.3) Die Hintereinanderausführung zweier affiner Abbildungen f_{A_1,b_1} und f_{A_2,b_2} ist gegeben durch

$$\begin{aligned} (f_{A_1,b_1}\circ f_{A_2,b_2})(x) \;&=\; f_{A_1,b_1}\big(f_{A_2,b_2}(x)\big) \\ &=\; f_{A_1,b_1}(A_2x + b_2) \\ &=\; A_1(A_2x+b_2)+b_1 \\ &=\; A_1A_2x + A_1b_2 + b_1 \\ &=\; f_{A_1A_2,A_1b_2+b_1}(x). \end{aligned}$$

Die Multiplikation (Hintereinanderausführung) zweier Matrizen der angegebenen Art ist gegeben durch

$$\begin{bmatrix} A_1 & b_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} A_2 & b_2 \\ 0 & 1 \end{bmatrix} \;=\; \begin{bmatrix} A_1A_2 & A_1b_2+b_1 \\ 0 & 1 \end{bmatrix}.$$

Wir sehen also, daß sich die Multiplikation solcher Matrizen "genauso" verhält wie die Hintereinanderausführung der zugehörigen affinen Abbildungen. Also ist

$$f_{A,b} \;\mapsto\; \begin{bmatrix} A & b \\ 0 & 1 \end{bmatrix}$$

ein (offensichtlich injektiver) Homomorphismus von der Gruppe aller invertierbaren affinen Abbildungen $K^n \to K^n$ in die Gruppe aller invertierbaren $(n+1)\times(n+1)$-Matrizen über K. Wir können daher die affine Gruppe $\mathrm{Aff}(K^n)$ mit einer Matrizengruppe identifizieren.

Lösung (6.4) (a) Es gelten die folgenden Äquivalenzen:

$$\begin{aligned} g \in Z(G) \;&\Leftrightarrow\; gx = xg \text{ für alle } x \in G \\ &\Leftrightarrow\; f(gx) = f(xg) \text{ für alle } x \in G \\ &\Leftrightarrow\; f(g)f(x) = f(x)f(g) \text{ für alle } x \in G \\ &\Leftrightarrow\; f(g)y = yf(g) \text{ für alle } y \in H \\ &\Leftrightarrow\; f(g) \in Z(H). \end{aligned}$$

Dabei gilt die erste Äquivalenz aufgrund der Definition des Zentrums einer Gruppe, die zweite aufgrund der Injektivität von f, die dritte aufgrund der Homomorphieeigenschaft von f, die vierte aufgrund der Surjektivität von f und die letzte wieder aufgrund der Definition des Zentrums einer Gruppe.

(b) Es gelten die folgenden Äquivalenzen:

$$\begin{aligned} g \in G' \;&\Leftrightarrow\; g = \prod_{i=1}^{n} x_i y_i x_i^{-1} y_i^{-1} \text{ mit } n \in \mathbb{N}_0, x_i, y_i \in G \\ &\Leftrightarrow\; f(g) = f\left(\prod_{i=1}^{n} x_i y_i x_i^{-1} y_i^{-1}\right) \text{ mit } n \in \mathbb{N}_0, x_i, y_i \in G \\ &\Leftrightarrow\; f(g) = \prod_{i=1}^{n} f(x_i)f(y_i)f(x_i)^{-1}f(y_i)^{-1} \\ &\qquad\qquad \text{mit } n \in \mathbb{N}_0, x_i, y_i \in G \\ &\Leftrightarrow\; f(g) = \prod_{i=1}^{n} \xi_i\eta_i\xi_i^{-1}\eta_i^{-1} \text{ mit } n \in \mathbb{N}_0, \xi_i, \eta_i \in H \\ &\Leftrightarrow\; f(g) \in H'. \end{aligned}$$

Dabei gilt die erste Äquivalenz aufgrund der Definition der Kommutatorgruppe einer Gruppe, die zweite aufgrund der Injektivität von f, die dritte aufgrund der Homomorphieeigenschaft von f, die vierte aufgrund der Surjektivität von f und die letzte wieder aufgrund der Definition der Kommutatorgruppe einer Gruppe.

(c) Für $x \in G$ und $n \in \mathbb{N}$ gilt wegen der Injektivität von f genau dann $x^n = e_G$, wenn $f(x^n) = f(e_G)$ bzw. $f(x)^n = e_H$ gilt.

(d) Wir haben $F(\mathrm{id}_G) = f\circ\mathrm{id}_G\circ f^{-1} = f\circ f^{-1} = \mathrm{id}_H$ sowie

$$\begin{aligned} F(\sigma_2\circ\sigma_1) \;&=\; f\circ\sigma_2\circ\sigma_1\circ f^{-1} \\ &=\; (f\circ\sigma_2\circ f^{-1})\circ(f\circ\sigma_1\circ f^{-1}) \\ &=\; F(\sigma_2)\circ F(\sigma_1), \end{aligned}$$

so daß F ein Gruppenhomomorphismus von $\mathrm{Aut}(G)$ nach $\mathrm{Aut}(H)$ ist. Da F offensichtlich bijektiv ist (mit $F^{-1}(\widehat{\sigma}) = f^{-1}\circ\widehat{\sigma}\circ f$ für $\widehat{\sigma} \in \mathrm{Aut}(H)$), ist F daher ein Gruppenisomorphismus.

Lösung (6.5) Zwei gegebene Gruppen G und H sind nach der vorigen Aufgaben sicher dann nicht isomorph, wenn

- die Mächtigkeiten von G und H nicht übereinstimmen,
- die Anzahl der Elemente einer gegebenen Ordnung in G und in H nicht übereinstimmen,
- die Zentren $Z(G)$ und $Z(H)$, die Kommutatorgruppen G' und H' oder die Automorphismengruppen $\mathrm{Aut}(G)$ und $\mathrm{Aut}(H)$ nicht isomorph sind.

Lösung (6.6) Jede Abbildung der Form κ_g ist tatsächlich ein Automorphismus von G, so daß φ wohldefiniert ist. Es gilt $\varphi(e) = \kappa_e = \mathrm{id}_G$, und für alle $g_1, g_2 \in G$ und alle $x \in G$ gilt $\kappa_{g_1g_2}(x) = (g_1g_2)x(g_1g_2)^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = \kappa_{g_1}(g_2xg_2^{-1}) = \kappa_{g_1}\big(\kappa_{g_2}(x)\big) = (\kappa_{g_1} \circ \kappa_{g_2})(x)$ und damit

$$\varphi(g_1g_2) \;=\; \kappa_{g_1g_2} \;=\; \kappa_{g_1} \circ \kappa_{g_2} \;=\; \varphi(g_1)\varphi(g_2).$$

Also ist φ ein Gruppenhomomorphismus. Genau dann liegt g im Kern von φ, wenn $\varphi_g = \mathrm{id}_G$ gilt, also $gxg^{-1} = x$ bzw. $gx = xg$ für alle $x \in G$. Das ist aber genau die Bedingung dafür, daß g im Zentrum von G liegt.

Lösung (6.7) Offensichtlich ist für jede invertierbare Matrix A auch $\Phi(A) = A^{T-1}$ invertierbar, und es gilt $\Phi(\mathbf{1}) = \mathbf{1}$. Für alle $A, B \in G$ gilt ferner $\Phi(AB) = (AB)^{T-1} = (B^TA^T)^{-1} = A^{T-1}B^{T-1} = \Phi(A)\Phi(B)$. Also ist $\Phi : G \to G$ ein Gruppenhomomorphismus. Für alle $A \in G$ haben wir $(\Phi \circ \Phi)(A) = (A^{T-1})^{T-1} = A$, so daß $\Phi^2 = \mathrm{id}_G$ gilt. Insbesondere ist also Φ invertierbar (mit $\Phi^{-1} = \Phi$) und damit ein Automorphismus von G. Genau dann ist Φ ein *innerer* Automorphismus von G, wenn es eine Matrix $M \in G$ gibt mit $\Phi(A) = MAM^{-1}$ für alle $A \in G$, also

$$(\star) \qquad A^{T-1}M \;=\; MA \quad \text{für alle } A \in G.$$

Bilden wir auf beiden Seiten von $(\star)$ die Determinante, so folgt $1/\det(A) = \det(A)$ bzw. $\det(A)^2 = 1$ für alle $A \in G$ und damit $\lambda^2 = 1$ für alle $\lambda \in K\setminus\{0\}$. Dies ist nur für $K = \mathbb{Z}_2$ und $K = \mathbb{Z}_3$ erfüllt. Für alle anderen Körper ist also Φ auf jeden Fall ein äußerer Automorphismus (egal, welchen Wert n hat). Für welche Werte von n in den Fällen $K = \mathbb{Z}_2$ und $K = \mathbb{Z}_3$ ein innerer Automorphismus vorliegt, untersuchen wir nun gesondert.

• $n = 1$: In diesem Fall lautet $(\star)$ (mit (1×1)-Matrizen $A = (a)$ und $M = (m)$) einfach $a^{-1} = a$ für alle $a \neq 0$ (und zwar unabhängig von $m \neq 0$), und dies ist sowohl für $K = \mathbb{Z}_2$ als auch für $K = \mathbb{Z}_3$ erfüllt. Also ist Φ jeweils ein innerer Automorphismus (mit $m = 1$ bzw. $m = \pm1$).

• $n = 2$: In diesem Fall schreiben wir

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{und} \quad M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix};$$

Bedingung $(\star)$ geht dann über in

$(\star\star)$

$$\frac{1}{ad-bc}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}\begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \;=\; \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

für alle $a, b, c, d \in K$ mit $ad - bc \neq 0$. Für $K = \mathbb{Z}_2$ folgt aus $ad - bc \neq 0$ automatisch $ad - bc = 1$, und wir haben $-b = b$ und $-c = c$, so daß sich die obige Gleichung zu

$$\begin{bmatrix} d & c \\ b & a \end{bmatrix}\begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \;=\; \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

vereinfacht. Diese Gleichung ist genau dann für alle invertierbaren Matrizen A erfüllt, wenn

$$M \;=\; \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

gilt, so daß für $K = \mathbb{Z}_2$ ein innerer Automorphismus vorliegt. Für $K = \mathbb{Z}_3$ wenden wir $(\star)$ mit $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ und dann mit $A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ an. Die resultierenden Gleichungen liefern $m_1 = m_2 = m_3 = m_4 = 0$, obwohl doch M invertierbar sein sollte. Die Annahme, es gäbe eine invertierbare Matrix M, die $(\star)$ erfüllt, führt also auf einen Widerspruch. Für $K = \mathbb{Z}_3$ ist im Fall $n = 2$ also Φ ein äußerer Automorphismus.

• $n \geq 3$: Wir nehmen an, eine Matrix $M \in G$ erfülle $(\star)$. Wir wählen in $(\star)$ dann speziell eine Blockdiagonalmatrix $A = \begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix}$ mit invertierbaren Matrizen $U \in K^{n_1\times n_1}$ und $V \in K^{n_2\times n_2}$, wobei $n_1 + n_2 = n$ gilt. Schreiben wir $M = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}$ als Blockmatrix mit $M_1 \in K^{n_1\times n_1}$ und $M_4 \in K^{n_2\times n_2}$, so geht $(\star)$ über in

$$\begin{bmatrix} U^{T-1}M_1 & U^{T-1}M_2 \\ V^{T-1}M_3 & V^{T-1}M_4 \end{bmatrix} \;=\; \begin{bmatrix} M_1U & M_2V \\ M_3U & M_4V \end{bmatrix}.$$

Dies muß für alle invertierbaren Matrizen U und V gelten, was nur für $M_2 = 0$ und $M_3 = 0$ gelten kann. Da die Größe von U beliebig war, muß also M eine Diagonalmatrix sein. Andererseits müssen die Gleichungen $U^{T-1} = M_1UM_1^{-1}$ und $V^{T-1} = M_4VM_4^{-1}$ für alle invertierbaren Matrizen U und V gelten, und zwar auch dann, wenn wir $n_1 = 2$ wählen. Nach dem vorher diskutierten Fall haben wir dann aber zwangsläufig $K = \mathbb{Z}_2$ und $M_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, was aber der gerade bewiesenen Tatsache widerspricht, daß M eine Diagonalmatrix sein muß. Die Annahme, es gebe eine Matrix $M \in G$ mit $(\star)$, führt also auf einen Widerspruch. Für $n \geq 3$ ist daher Φ in jedem Fall ein äußerer Automorphismus.

Lösung (6.8) Für $k \in \mathbb{N}$ definieren wir $\sigma_k : \mathbb{Z} \to \mathbb{Z}$ durch

$$(\star) \qquad \sigma_k(x) \;:=\; kx.$$

Dies ist offensichtlich ein Endomorphismus von $\mathbb{Z}$, denn für alle $x, y \in \mathbb{Z}$ erhalten wir $\sigma_k(x+y) = k(x+y) = kx + ky = \sigma_k(x) + \sigma_k(y)$. Ist umgekehrt $\sigma : \mathbb{Z} \to \mathbb{Z}$ ein beliebiger Endomorphismus, so gilt zunächst $\sigma(0) = 0$, dann

$$\begin{aligned}\sigma(n) &= \sigma(1+1+\cdots+1)\\ &= \sigma(1)+\sigma(1)+\cdots+\sigma(1)\\ &= n\cdot\sigma(1)\end{aligned}$$

für alle $n \in \mathbb{N}$ und schließlich $\sigma(-n) = -\sigma(n) = -n\cdot\sigma(1)$, insgesamt also $\sigma(x) = x\cdot\sigma(1)$ für alle $x \in \mathbb{Z}$, also $\sigma = \sigma_k$ mit $k := \sigma(1)$. Jeder beliebige Endomorphismus von $\mathbb{Z}$ ist also von der Form $(\star)$. Ein solcher Endomorphismus ist genau dann ein Automorphismus, wenn er bijektiv ist; dies ist genau für $k = \pm 1$ der Fall.

Lösung (6.9) Wegen $\sigma_k(0) = 0$ und $\sigma_k(x+y) = k(x+y) = kx + ky = \sigma_k(x) + \sigma_k(y)$ für alle $x, y \in \mathbb{Z}_n$ ist jede der Abbildungen σ_k ein Endomorphismus von $\mathbb{Z}_n$. Ist umgekehrt $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ ein beliebiger Endomorphismus von $\mathbb{Z}_n$, so setzen wir $k := \sigma(1)$ und erhalten für alle $x \in \mathbb{Z}_n$ dann $\sigma(x) = \sigma(1+1+\cdots+1) = \sigma(1)+\sigma(1)+\cdots+\sigma(1) = k+k+\cdots+k = xk = kx = \sigma_k(x)$; also gilt $\sigma = \sigma_k$. Genau dann ist σ_k ein Automorphismus, wenn σ_k injektiv ist, wenn also k kein Nullteiler in $\mathbb{Z}_n$ ist, wenn also k in $\mathbb{Z}_n^\times$ liegt.

Für alle $x \in \mathbb{Z}_n$ gilt $\sigma_1(x) = 1\cdot x = x$; also ist $\sigma_1 = \mathrm{id}$. Für alle $x \in \mathbb{Z}_n$ gilt ferner $\sigma_{k\ell}(x) = (k\ell)x = k\cdot(\ell\cdot x) = \sigma_k\big(\sigma_\ell(x)\big) = (\sigma_k \circ \sigma_\ell)(x)$; also ist $\sigma_{k\ell} = \sigma_k \circ \sigma_\ell$. Damit ist gezeigt, daß $k \mapsto \sigma_k$ ein Homomorphismus $\mathbb{Z}_n^\times \to \mathrm{Aut}(\mathbb{Z}_n)$ ist.

Lösung (6.10) Wir schreiben $\sigma(x) := x^{-1}$; dann ist $\sigma : G \to G$ eine bijektive Abbildung. Genau dann ist σ ein Automorphismus, wenn für alle $x, y \in G$ die Gleichung $\sigma(xy) = \sigma(x)\sigma(y)$ gilt, also $(xy)^{-1} = x^{-1}y^{-1}$ bzw. $y^{-1}x^{-1} = x^{-1}y^{-1}$. Das ist aber gleichbedeutend damit, daß $\eta\xi = \xi\eta$ für alle $\xi, \eta \in G$ gilt, daß also G abelsch ist.

Lösung (6.11) (a) Wir definieren $f : G \to G$ durch $f(x) := x^{-1}\sigma(x)$. Aus $f(x) = f(y)$, also $x^{-1}\sigma(x) = y^{-1}\sigma(y)$, folgt dann $xy^{-1} = \sigma(x)\sigma(y)^{-1} = \sigma(xy^{-1})$, so daß xy^{-1} ein Fixpunkt von σ ist. Nach Voraussetzung gilt also $xy^{-1} = e$ und damit $x = y$. Wir haben gezeigt, daß aus $f(x) = f(y)$ schon $x = y$ folgt; also ist f injektiv. Da G endlich ist, ist f daher auch surjektiv, und dies ist die Behauptung.

(b) Es sei $a \in G$ beliebig. Nach Teil (a) gibt es ein Element $x \in G$ mit $a = x^{-1}\sigma(x)$. Es folgt $\sigma(a) = \sigma\big(x^{-1}\sigma(x)\big) = \sigma(x^{-1})\sigma\big(\sigma(x)\big) = \sigma(x)^{-1}x = a^{-1}$.

(c) Hier wird also vorausgesetzt, daß die Inversionsabbildung σ ein Automorphismus ist. Für alle $a, b \in G$ gilt dann $ba = (a^{-1}b^{-1})^{-1} = \sigma\big(\sigma(a)\sigma(b)\big) = \sigma^2(a)\sigma^2(b) = ab$; also ist G abelsch. (Das wurde in Aufgabe (6.10) schon einmal bewiesen.)

Lösung (6.12) (a) Es gilt

$$\begin{aligned}|S \cap s_0^{-1}S| &= |S| + |s_0^{-1}S| - |S \cup s_0^{-1}S|\\ &= |S| + |S| - |S \cup s_0^{-1}S|\\ &\geq 2|S| - |G| \;>\; 2\cdot(3|G|/4) - |G| \;=\; |G|/2.\end{aligned}$$

(b) Ein Element von $S \cap s_0^{-1}S$ hat die Form $x = s_0^{-1}\xi$ mit $x, \xi \in S$. Dann ist $\xi = s_0 x$, folglich $\xi^{-1} = \sigma(\xi) = \sigma(s_0 x) = \sigma(s_0)\sigma(x) = s_0^{-1}x^{-1}$ und daher $\xi = x s_0$. Wir haben also $s_0 x = \xi = x s_0$ und daher $x \in Z_G(s_0)$.

(c) Wegen (a) und (b) gilt $|Z_G(s_0)| > |G|/2$. Da $|Z_G(s_0)|$ nach dem Satz von Lagrange ein Teiler von $|G|$ sein muß, folgt hieraus $|Z_G(s_0)| = |G|$ und damit $Z_G(s_0) = G$. (Vgl. auch Aufgabe (4.3).)

(d) Wegen (c) gilt $S \subseteq Z(G)$, wenn $Z(G)$ das Zentrum von G bezeichnet. Also gilt $|Z(G)| \geq |S| > 3|G|/4$; andererseits muß $|Z(G)|$ nach dem Satz von Lagrange ein Teiler von $|G|$ sein. Es folgt $|Z(G)| = |G|$ und damit $Z(G) = G$. Das bedeutet aber, daß G abelsch ist.

(e) Wegen $|\langle\langle S\rangle\rangle| \geq |S| > 3|G|/4$ gilt $\langle\langle S\rangle\rangle = G$; jedes Element $g \in G$ läßt sich daher in der Form $g = s_1 \cdots s_m$ mit Elementen $s_i \in S$ schreiben. Es folgt $\sigma(g) = \sigma(s_1)\cdots\sigma(s_m) = s_1^{-1}\cdots s_m^{-1} = (s_m \cdots s_1)^{-1} = (s_1 \cdots s_m)^{-1} = g^{-1}$, wobei wir bei der vorletzten Gleichung ausnutzten, daß G nach Teil (d) abelsch ist.

Bemerkung 1. Beweistechnisch bemerkenswert ist die Tatsache, daß wir nicht zuerst beweisen, daß $\sigma(x) = x^{-1}$ für alle $x \in G$ gilt, und dann wie in Aufgabe (6.10) nachweisen, daß G abelsch sein muß. Stattdessen müssen wir die Kommutativität von G schon vorher feststellen, um dann zu schließen, daß σ die Inversionsabbildung ist.

Bemerkung 2. Es gibt nichtabelsche Gruppen, die einen Automorphismus besitzen, der genau drei Viertel aller Elemente auf ihr jeweiliges Inverses abbildet. Ein Beispiel ist etwa die Quaternionengruppe, die uns in Aufgabe (4.9) begegnet ist. Für diese Gruppe G definieren wir $\sigma : G \to G$ als diejenige Abbildung, die sowohl I und $-I$ als auch J und $-J$ als auch K und $-K$ jeweils miteinander vertauscht und $\mathbf{1}$ und $-\mathbf{1}$ festläßt. Dann ist σ ein Automorphismus, und es gilt $\sigma(x) = x^{-1}$ für $x \in \{\pm I, \pm J, \pm K\}$; diese Menge umfaßt genau drei Viertel der Elemente von G. Ein anderes Beispiel ist die Diedergruppe D_8, also die Symmetriegruppe eines Quadrats. Die Abbildung $\sigma : D_8 \to D_8$, die die 90^0-Drehung und die 270^0-Drehung miteinander vertauscht und alle anderen Elemente von D_8 festläßt, ist ein Automorphismus von D_8. Da alle Elemente von D_8 außer der 90^0- und der 270^0-Drehung zu sich selbst invers sind, bildet σ also 6 Elemente der Gruppe (und damit drei Viertel aller Gruppenelemente) auf ihre jeweiligen Inversen ab.

Lösung (6.13) Es gelten die folgenden Äquivalenzen:

$$\begin{aligned}&[k_1] = [k_2] \;\Leftrightarrow\; k_1 - k_2 \text{ ist durch } n \text{ teilbar}\\ &\Leftrightarrow\; g^{k_1-k_2} = e \;\Leftrightarrow\; g^{k_1} = g^{k_2}.\end{aligned}$$

Die Richtung $\Rightarrow$ zeigt dabei, daß $\exp_g$ eine wohldefinierte Abbildung ist; die Richtung $\Leftarrow$ zeigt, daß diese Abbildung injektiv ist. Da nach Voraussetzung $G = \langle\langle g \rangle\rangle$ gilt, ist $\exp_g$ auch surjektiv und folglich eine Bijektion. Daß $\exp_g$ ein Gruppenhomomorphismus ist, folgt aus der Rechnung

$$\exp_g([k_1]+[k_2]) \;=\; \exp_g([k_1+k_2]) \;=\; g^{k_1+k_2} \;=\; g^{k_1}g^{k_2}.$$

Also ist $\exp_g$ ein Gruppenisomorphismus.

Lösung (6.14) (a) Die gesuchte Zahl x besitzt eine eindeutige Darstellung $x = km + r$ mit $k \geq 0$ und $0 \leq r \leq m-1$ (Division mit Rest). Dabei ist zwangsläufig $k \leq m-1$, denn aus $k \geq m$ folgte $x \geq m^2 \geq (\sqrt{n})^2 = n$. Wir haben dann $a = g^x = g^{km+r}$ und damit $g^r = a(g^{-m})^k = a\gamma^k$ mit $k \leq m-1$. Dies ist schon die Behauptung.

Lösung (6.15) Mit $m := [\sqrt{12}] + 1 = 4$ erhalten wir in $\mathbb{Z}_{13}^\times$ die Gleichung $\gamma = 2^{-4} = (2^{-1})^4 = 7^4 = 9$ (nachrechnen!). Nach dem Algorithmus von Shanks berechnen wir also zunächst

r	0	1	2	3	4
2^r	1	2	4	8	3

und dann

k	0	1	2 $\cdots$
$5 \cdot 9^k$	5	6	2 $\cdots$

Für $r = 1$ und $k = 2$ tritt Übereinstimmung auf; wir haben also $\log_2 5 = km + r = 2 \cdot 4 + 1 = 9$. (Zur Probe kann man natürlich nachprüfen, daß tatsächlich $2^9 = 5$ in $\mathbb{Z}_{13}^\times$ gilt.)

(b) Mit $m := [\sqrt{30}] + 1 = 6$ erhalten wir in $\mathbb{Z}_{31}^\times$ die Gleichung $\gamma = 3^{-6} = (3^{-1})^6 = 21^6 = 2$ (nachrechnen!). Nach dem Algorithmus von Shanks berechnen wir also zunächst

r	0	1	2	3	4	5	6
3^r	1	3	9	27	19	26	16

und dann

k	0	1	2	3	4 $\cdots$
$7 \cdot 2^k$	7	14	28	25	19 $\cdots$

Für $r = 4$ und $k = 4$ tritt Übereinstimmung auf; wir haben also $\log_3 7 = km + r = 4 \cdot 6 + 4 = 28$. (Zur Probe kann man natürlich nachprüfen, daß tatsächlich $3^{28} = 7$ in $\mathbb{Z}_{31}^\times$ gilt.)

(c) Mit $m := [\sqrt{28}] + 1 = 6$ erhalten wir in $\mathbb{Z}_{29}^\times$ die Gleichung $\gamma = 11^{-6} = (11^{-1})^6 = 8^6 = 13$ (nachrechnen!). Nach dem Algorithmus von Shanks berechnen wir also zunächst

r	0	1	2	3	4	5	6
11^r	1	11	5	26	25	14	9

und dann

k	0	1	2	3	4 $\cdots$
$19 \cdot 13^k$	19	15	21	12	11 $\cdots$

Für $r = 1$ und $k = 4$ tritt Übereinstimmung auf; wir haben also $\log_{11} 19 = km + r = 4 \cdot 6 + 1 = 25$. (Zur Probe kann man natürlich nachprüfen, daß tatsächlich $11^{25} = 19$ in $\mathbb{Z}_{29}^\times$ gilt.)

Lösung (6.16) Wir wollen zunächst die Inklusion $f^{-1}\big(f(U)\big) \subseteq U \cdot \mathrm{Kern}(f)$ beweisen. Dazu sei $x \in f^{-1}\big(f(U)\big)$, also $f(x) \in f(U)$. Es gibt dann ein Element $u \in U$ mit $f(x) = f(u)$. Dann liegt $u^{-1}x$ im Kern von f (denn $f(u^{-1}x) = f(u)^{-1}f(x) = e$), und es folgt $x = u \cdot u^{-1}x \in U \cdot \mathrm{Kern}(f)$.

Nun wollen wir die umgekehrte Inklusion $U \cdot \mathrm{Kern}(f) \subseteq f^{-1}\big(f(U)\big)$ beweisen. Dazu sei $x \in U \cdot \mathrm{Kern}(f)$, sagen wir $x = uy$ mit $y \in \mathrm{Kern}(f)$. Dann gilt $f(x) = f(uy) = f(u)f(y) = f(u)$; also liegt x in $f^{-1}\big(f(u)\big) \subseteq f^{-1}\big(f(U)\big)$.

Lösung (6.17) Ist U eine Untergruppe von G, so ist $f(U)$ eine Untergruppe von H. Ist umgekehrt V eine Untergruppe von H, so ist $f^{-1}(V)$ eine Untergruppe von G, die den Kern von f umfaßt. Gilt $V \leq H$, so ist $f\big(f^{-1}(V)\big) = V$, weil f surjektiv ist. Gilt umgekehrt $U \leq G$ mit $\mathrm{Kern}(f) \subseteq U$, so gilt $f^{-1}\big(f(U)\big) = U \cdot \mathrm{Kern}(f) = U$ nach Aufgabe (6.16). Damit ist gezeigt, daß die Abbildungen $U \mapsto f(U)$ und $V \mapsto f^{-1}(V)$ zueinander inverse Bijektionen zwischen der Menge der den Kern von f umfassenden Untergruppen von G und der Menge der Untergruppen von H sind.

Es bleibt zu zeigen, daß $[G : U] = [H : f(U)]$ für jede Untergruppe $U \leq G$ mit $\mathrm{Kern}(f) \subseteq U$ gilt. Dazu sei $(g_i)_{i\in I}$ ein minimales System von Repräsentanten für die Linksnebenklassen von G; dann ist G die disjunkte Vereinigung $G = \bigcup_{i\in I} g_iU$. Wir sind fertig, wenn wir zeigen können, daß $\big(f(g_i)\big)_{i\in I}$ ein minimales System von Repräsentanten für die Linksnebenklassen von $f(U)$ in $H = f(G)$ ist. Zunächst gilt

$$H \;=\; f(G) \;=\; f\Big(\bigcup_{i\in I} g_iU\Big) \;=\; \bigcup_{i\in I} f(g_iU) \;=\; \bigcup_{i\in I} f(g_i)f(U).$$

Also bilden die Elemente $f(g_i)$ ein Repräsentantensystem der Linksnebenklassen von $f(U)$ in H. Es bleibt zu zeigen, daß $f(g_i)f(U) \neq f(g_j)f(U)$ für $i \neq j$ gilt, daß also keine Nebenklasse doppelt repräsentiert wird. Es gelte $f(g_i)f(U) = f(g_j)f(U)$, also $f(g_i) = f(g_j)f(u)$

mit einem Element $u \in U$. Dann gilt $f(g_j^{-1}g_iu) = f(g_j)^{-1}f(g_i)f(u) = e_H$ und damit $g_j^{-1}g_iu \in \mathrm{Kern}(f) \subseteq U$, folglich $g_iu \in g_jU$ und damit $g_iU = g_jU$. Da nach Voraussetzung die Elemente g_i ein minimales Repräsentantensystem der Linksnebenklassen von U bilden, folgt hieraus $i \neq j$. Damit ist alles gezeigt.

Lösung (6.18) Jede Linksmultiplikation L_g ist bijektiv und damit ein Element von $\mathrm{Bij}(G)$. Es seien $g_1, g_2 \in G$ beliebige Elemente von G. Dann gilt $L_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = L_{g_1}\big(L_{g_2}(x)\big) = (L_{g_1} \circ L_{g_2})(x)$ für alle $x \in G$, folglich $L_{g_1g_2} = L_{g_1} \circ L_{g_2}$. Dies zeigt, daß $g \mapsto L_g$ ein Gruppenhomomorphismus ist. Liegt g im Kern von L, so gilt $L_g = \mathrm{id}_G$, also $gx = x$ für alle $x \in G$, was nur für $g = e$ möglich ist. Also ist $\mathrm{Kern}(L) = \{e\}$; dies zeigt, daß L injektiv und damit eine Einbettung ist.

Lösung (6.19) Wir numerieren die Elemente von Sym_3 folgendermaßen durch:

$$\sigma_1 = \mathrm{id}, \quad \sigma_2 = (12), \quad \sigma_3 = (23),$$
$$\sigma_4 = (13), \quad \sigma_5 = (123), \quad \sigma_6 = (132).$$

Die Verknüpfungstafel von Sym_3 sieht dann folgendermaßen aus.

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_6	σ_1	σ_5	σ_4	σ_2
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_4	σ_2	σ_3	σ_6	σ_1
σ_6	σ_6	σ_3	σ_4	σ_2	σ_1	σ_5

Für jedes $\sigma \in \mathrm{Sym}_3$ bewirkt nun die Abbildung $\sigma \mapsto \sigma\sigma_i$ eine Permutation der Elemente $\sigma_1, \ldots, \sigma_6$; die Cayley-Einbettung ergibt sich dann gerade durch Identifikation von σ mit dieser Permutation. Wie sich sofort aus der obigen Gruppentafel ablesen läßt, sieht die Cayley-Einbettung folgendermaßen aus:

$$\sigma_1 \to \big((1,2,3,4,5,6) \to (1,2,3,4,5,6)\big) = \mathrm{id},$$
$$\sigma_2 \to \big((1,2,3,4,5,6) \to (2,1,5,6,3,4)\big) = (12)(35)(46),$$
$$\sigma_3 \to \big((1,2,3,4,5,6) \to (3,6,1,5,4,2)\big) = (13)(26)(45),$$
$$\sigma_4 \to \big((1,2,3,4,5,6) \to (4,5,6,1,2,3)\big) = (14)(25)(36),$$
$$\sigma_5 \to \big((1,2,3,4,5,6) \to (5,4,2,3,6,1)\big) = (156)(243),$$
$$\sigma_6 \to \big((1,2,3,4,5,6) \to (6,3,4,2,1,5)\big) = (165)(234).$$

Also ist

$$\{\mathrm{id},\ (12)(35)(46),\ (13)(26)(45),\ (14)(25)(36),\ (156)(243),\ (165)(234)\}$$

eine zu Sym_3 isomorphe Untergruppe von Sym_6. Die explizite Darstellung hängt natürlich von der (willkürlich gewählten) Numerierung der Elemente von Sym_3 ab. Es ist aber klar, daß sich durch eine Änderung der Numerierung keine strukturellen Eigenschaften ändern.