4. Lösung zu algebraischen Strukturen: Untergruppen und Nebenklassen

Lösung (4.1) (a) Wenn U eine Untergruppe von G ist, so gilt selbstverständlich $UU \subseteq U$; nur die umgekehrte Implikation ist zu zeigen. Es sei $U = \{u_1, \ldots, u_m\}$ mit paarweise verschiedenen Elementen u_i. Wir wählen ein beliebiges Element $u \in U$ und halten dieses fest. Weil die Abbildung $x \mapsto ux$ die Menge U nach Voraussetzung in sich abbildet und injektiv ist, gilt dann auch $U = \{uu_1, \ldots, uu_m\}$. Insbesondere gibt es einen Index i mit $uu_i = u$ und damit $u_i = e$. Also enthält U das Neutralelement e von G. Folglich gibt es auch einen Index j mit $uu_j = e$ und damit $u_j = u^{-1}$. Mit u liegt also auch u^{-1} in U. Da $u \in U$ beliebig war, ist damit die Inkusion $U^{-1} \subseteq U$ gezeigt. Wir haben also $e \in U$, $UU \subseteq U$ und $U^{-1} \subseteq U$; damit ist U eine Untergruppe von G.

(b) Nach (a) kommt nur eine unendliche Menge U in Frage. Wir können etwa $G = (\mathbb{Z}, +)$ und $U = \mathbb{N}$ wählen.

Lösung (4.2) Gilt $A \subseteq B$, so gilt $A \cup B = B$, und dies ist nach Voraussetzung eine Untergruppe von G. Gilt $B \subseteq A$, so gilt $A \cup B = A$, und dies ist nach Voraussetzung ebenfalls eine Untergruppe von G. Es gelte weder $A \subseteq B$ noch $B \subseteq A$; wir müssen zeigen, daß in diesem Fall $A \cup B$ keine Untergruppe von G ist. Wegen $A \not\subseteq B$ und $B \not\subseteq A$ gibt es Elemente $a \in A \setminus B$ und $b \in B \setminus A$. Wäre $A \cup B$ eine Gruppe, so müßte das Produkt ab in $A \cup B$ liegen, also in A oder in B. Gälte $ab \in A$, dann auch $b \in a^{-1}A \subseteq A$ im Widerspruch zur Wahl von b. Gälte $ab \in B$, dann auch $a \in Bb^{-1} \subseteq B$ im Widerspruch zur Wahl von a. Die Annahme, $A \cup B$ sei eine Untergruppe von G, führt also auf einen Widerspruch.

Lösung (4.3) Genau dann gilt $G = SS$, wenn es zu jedem Element $g \in G$ Elemente $s_1, s_2 \in S$ mit $g = s_1 s_2$ bzw. $gs_2^{-1} = s_1$ gibt, wenn also für jedes Element $g \in G$ die Menge $gS^{-1} \cap S$ nicht leer ist. Wir betrachten also ein beliebiges Element $g \in G$ und müssen zeigen, daß die Mengen gS^{-1} und S nicht disjunkt sein können. Da die Abbildung $s \mapsto gs^{-1}$ injektiv ist, hat die Menge gS^{-1} genau so viele Elemente wie die Menge S. Wären gS^{-1} und S disjunkt, so enthielte $gS^{-1} \cup S$ genau doppelt so viele Elemente wie S und damit mehr Elemente als G, was wegen $gS^{-1} \cup S \subseteq G$ natürlich nicht sein kann. Damit ist gezeigt, daß die Mengen gS^{-1} und S nicht disjunkt sein können.

Lösung (4.4) Es sei U eine Untergruppe von G; wir zeigen, daß in diesem Fall $\sim$ eine Äquivalenzrelation ist.

- Ist $a \in G$ beliebig, so gilt $aa{-}1 = e \in U$ und damit $a \sim a$. Also ist $\sim$ reflexiv.
- Gilt $a \sim b$, so gilt $ab^{-1} \in U$. Dann liegt aber auch $(ab^{-1})^{-1} = ba^{-1}$ in U, so daß $b \sim a$ gilt. Also ist $\sim$ symmetrisch.
- Es mögen die Bedingungen $a \sim b$ und $b \sim c$ gelten, also $ab^{-1} \in U$ und bc^{-1} in U. Dann liegt aber auch $ac^{-1} = (ab^{-1})(bc^{-1})$ in U, so daß $a \sim c$ gilt. Also ist $\sim$ transitiv.

Umgekehrt sei $\sim$ eine Äquivalenzrelation; wir zeigen, daß in diesem Fall U eine Untergruppe ist.

- Wähle irgendein Element $a \in G$. Wegen $a \sim a$ liegt dann aa^{-1} in U. Also gilt $e \in U$.
- Es sei $u \in U$. Dann gilt $u \sim e$, folglich auch $e \sim u$ und damit $eu^{-1} \in U$. Aus $u \in U$ folgt also $u^{-1} \in U$.
- Es seien $u_1, u_2 \in U$. Wie wir gerade sahen, gilt dann auch $+\, u_2^{-1} \in U$. Wir haben also $u_1 \sim e$ und $u_2^{-1} \sim e$, folglich $u_1 \sim e$ und $e \sim u_2^{-1}$ und damit $u_1(u_2^{-1})^{-1} \in U$, also $u_1 u_2 \in U$. Aus $u_1, u_2 \in U$ folgt also $u_1 u_2 \in U$.

Lösung (4.5) Es gelte $A \subseteq C$. Wir beweisen die beiden Inklusionen $(AB) \cap C \subseteq A(B \cap C)$ und $(AB) \cap C \supseteq A(B \cap C)$ separat.

$\subseteq$: Es sei $x \in (AB) \cap C$, sagen wir $x = ab = c$ mit $a \in A$, $b \in B$ und $c \in C$. Dann gilt $b = a^{-1}c \in AC \subseteq CC \subseteq C$, folglich $b \in B \cap C$ und damit $x = ab \in A(B \cap C)$.

$\supseteq$: Wir haben $A(B \cap C) \subseteq AB$ und $A(B \cap C) \subseteq CC \subseteq C$, insgesamt also $A(B \cap C) \subseteq (AB) \cap C$.

Lösung (4.6) Die Zahl $|A| \cdot |B|$ ist die Mächtigkeit des direkten Produkts $A \times B$, also der Menge aller Paare (a, b) mit $a \in A$ und $b \in B$. Zwei Paare (a_1, b_1) und (a_2, b_2) bestimmen nun genau dann das gleiche Element $a_1 b_1 = a_2 b_2$ von G, wenn $a_2^{-1} a_1 = b_2 b_1^{-1}$ in $A \cap B$ liegt. Zählt man also statt der Produkte ab die Paare (a, b), so wird jedes Produkt genau $|A \cap B|$-mal gezählt. Diese Beobachtung liefert schon die Behauptung.

Lösung (4.7) (a) Ist AB eine Untergruppe, so haben wir $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$. Gilt umgekehrt $AB = BA$, so haben wir $(AB)^{-1} = B^{-1}A^{-1} = BA = AB$ und $(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) \subseteq AB$, so daß wegen $e = e \cdot e \in AB$ die Menge AB eine Untergruppe von G ist.

(b) Für alle $m \in \mathbb{Z}$ haben wir

$$a^m = \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix} \quad \text{und} \quad b^m = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}.$$

Also ist AB die Menge aller Matrizen der Form

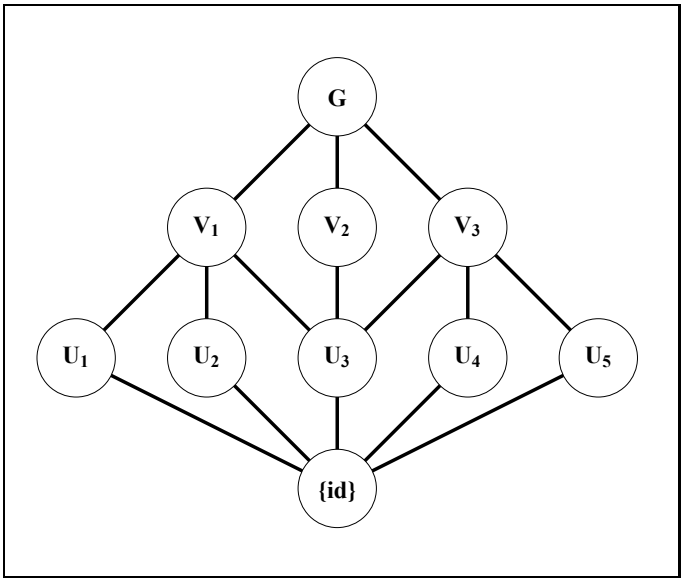
$$a^m b^n = \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ m & mn{+}1 \end{bmatrix}$$

mit $m, n \in \mathbb{Z}$, während BA die Menge aller Matrizen der Form

$$b^n a^m = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix} = \begin{bmatrix} mn{+}1 & n \\ m & 1 \end{bmatrix}$$

mit $m, n \in \mathbb{Z}$ ist. Es gilt also $BA \neq AB$; nach (a) ist daher AB keine Untergruppe von G.

Lösung (4.8) Die Diedergruppe D_4 ist die Symmetriegruppe eines Quadrats und besteht aus den vier Drehungen um 0^0, 90^0, ${}^80^0$ und 270^0 um den Mittelpunkt des Quadrats sowie den Spiegelungen σ_1 und σ_2 an den beiden Diagonalen und den Spiegelungen σ_3 und σ_4 an den beiden Verbindungsgeraden gegenüberliegender Kantenmittelpunkte. Dann sind die von den einzelnen Spiegelungen und von der 180^0-Drehung erzeugten Untergruppen jeweils von der Ordnung 2; es sind dies die Untergruppen $U_1 = \{\mathrm{id}, \sigma_1\}$, $U_2 = \{\mathrm{id}, \sigma_2\}$, $U_3 = \{\mathrm{id}, D_{180}\}$, $U_4 = \{\mathrm{id}, \sigma_3\}$ und $U_4 = \{\mathrm{id}, \sigma_4\}$. Die Gruppen $V_1 := \{\mathrm{id}, \sigma_1, \sigma_2, D_{180}\}$ und $V_3 := \{\mathrm{id}, \sigma_3, \sigma_4, D_{180}\}$ haben jeweils die Ordnung 4, ebenso die Gruppe V_2 der vier Drehungen. Ansonsten gibt es nur noch die trivialen Untergruppen $\{\mathrm{id}\}$ und D_4. Der Untergruppenverband sieht folgendermaßen aus.

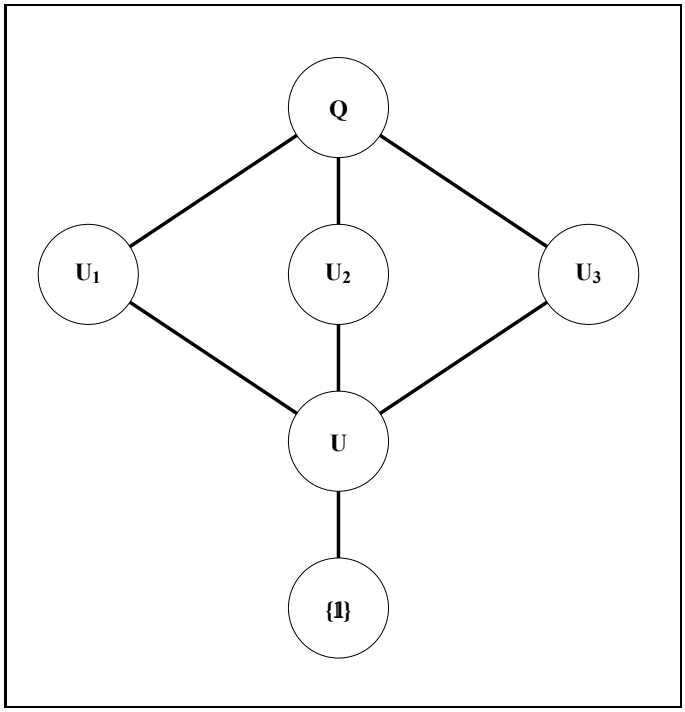


Untergruppenverband der Diedergruppe D_4.

Lösung (4.9) Die angegebenen Gleichungen rechnet man sofort nach; es ergibt sich daher die folgende Verknüpfungstafel.

$\cdot$	$\mathbf{1}$	$-\mathbf{1}$	I	$-I$	J	$-J$	K	$-K$
$\mathbf{1}$	$\mathbf{1}$	$-\mathbf{1}$	I	$-I$	J	$-J$	K	$-K$
$-\mathbf{1}$	$-\mathbf{1}$	$\mathbf{1}$	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	$-\mathbf{1}$	$\mathbf{1}$	K	$-K$	$-J$	J
$-I$	$-I$	I	$\mathbf{1}$	$-\mathbf{1}$	$-K$	K	J	$-J$
J	J	$-J$	$-K$	K	$-\mathbf{1}$	$\mathbf{1}$	I	$-I$
$-J$	$-J$	J	K	$-K$	$\mathbf{1}$	$-\mathbf{1}$	$-I$	I
K	K	$-K$	J	$-J$	$-I$	I	$-\mathbf{1}$	$\mathbf{1}$
$-K$	$-K$	K	$-J$	J	I	$-I$	$\mathbf{1}$	$-\mathbf{1}$

Das Element $-\mathbf{1}$ hat die Ordnung 2, erzeugt also eine zweielementige Untergruppe $U = \{\pm\mathbf{1}\}$. Jedes der Elemente $\pm I$, $\pm J$, $\pm K$ hat die Ordnung 4; dies liefert die vierelementigen Untergruppen $U_1 = \{\pm\mathbf{1}, \pm I\}$, $U_2 = \{\pm\mathbf{1}, \pm J\}$, $U_3 = \{\pm\mathbf{1}, \pm K\}$. Der Untergruppenverband von Q sieht daher folgendermaßen aus.



Untergruppenverband der Quaternionengruppe Q.

Lösung (4.10) Wegen $ex = xe = x$ für alle x gilt $e \in Z_G(X)$. Aus $gx = xg$ folgt $xg^{-1} = g^{-1}x$; mit g liegt also auch g^{-1} in $Z_G(X)$. Aus $g_1x = xg_1$ und $g_2x = xg_2$ folgt die Gleichungskette $(g_1g_2)x = g_1(g_2x) = g_1(xg_2) = (g_1x)g_2 = (xg_1)g_2 = x(g_1g_2)$; mit g_1 und g_2 liegt daher auch g_1g_2 in $Z_G(X)$. Wegen $eX = X = Xe$ gilt $e \in N_G(X)$. Aus $gXg^{-1} = X$ folgt $X = g^{-1}Xg = g^{-1}X(g^{-1})^{-1}$; mit g liegt also auch g^{-1} in $N_G(X)$. Aus $g_1Xg_1^{-1} = X = g_2Xg_2^{-1}$ folgt schließlich $(g_1g_2)X(g_1g_2)^{-1} = g_1(g_2Xg_2^{-1})g_1^{-1} = g_1Xg_1^{-1} = X$; mit g_1 und g_2 liegt also auch g_1g_2 in $N_G(X)$. Damit sind $Z_G(X)$ und $N_G(X)$ als Untergruppen von G nachgewiesen. Die Inklusion $Z_G(X) \subseteq N_G(X)$ gilt trivialerweise. Genau dann gilt $gx = xg$ für alle $x \in X$, wenn

$$gx_1^{e_1}x_2^{e_2}\cdots x_n^{e_n} \;=\; x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}g$$

für alle $n \in \mathbb{N}$, alle $x_i \in X$ und alle $e_i \in \mathbb{Z}$ gilt; dies zeigt die Gleichheit $Z_G(X) = Z_G(\langle\!\langle X\rangle\!\rangle)$. Gilt $gXg^{-1} = X$, so gilt

$$\begin{aligned} g\langle\!\langle X\rangle\!\rangle g^{-1} \;&=\; \{gx_1^{e_1}\cdots x_n^{e_n}g^{-1} \mid n \in \mathbb{N}, x_i \in X, e_i \in \mathbb{Z}\} \\ &=\; \{(gx_1g^{-1})^{e_1}\cdots(gx_ng^{-1})^{e_n} \mid n \in \mathbb{N}, x_i \in X, e_i \in \mathbb{Z}\} \\ &=\; \{\xi_1^{e_1}\cdots\xi_n^{e_n} \mid n \in \mathbb{N}, \xi_i \in X, e_i \in \mathbb{Z}\} \;=\; \langle\!\langle X\rangle\!\rangle; \end{aligned}$$

also gilt die Inklusion $N_G(X) \subseteq N_G(\langle\!\langle X\rangle\!\rangle)$.

Lösung (4.11) Da G nicht abelsch ist, ist $Z \neq G$; es gibt also ein Element $x \in G$ mit $x \in G \setminus Z$. Dann gelten die beiden echten Inklusionen

$$Z \;\subsetneqq\; Z_G(x) \;\subsetneqq G.$$

(Die erste Inklusion gilt, weil jedes Element von Z mit allen Elementen von G kommutiert, insbesondere also mit

x. Sie ist echt, weil x nicht in Z liegt. Die zweite Inklusion gilt trivialerweise; sie ist echt, weil x nicht im Zentrum von G liegt, also nicht mit allen Elementen von G kommutiert.) Daher ist

$$[G : Z] \;=\; [G : Z_G(x)] \cdot [Z_G(x) : Z]$$

eine Zerlegung von $[G : Z]$ in Faktoren größer als 1; es kann also $[G : Z]$ keine Primzahl sein.

Lösung (4.12) (a) Das Neutralelement $e = (e_i)_{i\in I}$ liegt in U, denn $e_i \in U_i$ für alle i. Mit $u = (u_i)_{i\in I}$ liegt auch $u^{-1} = (u_i^{-1})_{i\in I}$ in U, denn $u_i^{-1} \in U_i$ für alle i. Liegen $u = (u_i)$ und $v = (v_i)$ in U, dann auch $uv = (u_iv_i)$ wegen $u_iv_i \in U_i$ für alle i. Damit ist nachgeprüft, daß U eine Untergruppe von G ist.

(b) Die Gruppentafel sieht folgendermaßen aus.

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Die einzigen Untergruppen von $\mathbb{Z}_2$ sind $U = \{0\}$ und $V = \mathbb{Z}_2$. Nach Teil (a) besitzt daher $\mathbb{Z}_2 \times \mathbb{Z}_2$ die Untergruppen

$$\begin{aligned} U \times U &= \{(0,0)\}, \\ V \times U &= \{(0,0),(1,0)\}, \\ U \times V &= \{(0,0),(0,1)\}, \\ V \times V &= \{(0,0),(1,0),(0,1),(1,1)\}. \end{aligned}$$

Hinzu kommt noch die Untergruppe

$$\Delta \;:=\; \{(x,x) \mid x \in \mathbb{Z}_2\} \;=\; \{(0,0),(1,1)\},$$

die nicht von der in (a) angegebenen Bauart ist. Andere Untergruppen kann es nach dem Satz von Lagrange nicht geben.

Lösung (4.13) Ist G endlich, so hat G sogar nur endlich viele Teilmengen, erst recht also nur endlich viele Untergruppen. Umgekehrt sei G unendlich. Gibt es in G ein Element unendlicher Ordnung, so hat bereits die von diesem erzeugte zyklische Gruppe unendlich viele Untergruppen. Gibt es in G nur Elemente endlicher Ordnung, so enthält jede zyklische Untergruppe von G nur endlich viele Elemente; wegen $|G| = \infty$ muß es daher unendlich viele dieser zyklischen Untergruppen geben.

Lösung (4.14) (a) Jedes Element von $\mathbb{Q}$ (außer der Null) hat die Form m/n mit teilerfremden Zahlen $m \in \mathbb{Z}$ und $n \in \mathbb{N}$, und dieses Element hat in $(\mathbb{Q}, +)$ die Ordnung n. Jedes Element von $(\mathbb{Q}, +)$ hat also endliche Ordnung. Sind endlich viele Elemente $x_1, \ldots, x_r$ von $\mathbb{Q}$ gegeben, so besitzen diese einen Hauptnenner n. Ist p irgendeine Primzahl, durch die n nicht teilbar ist, so ist $1/p$ nicht als $\mathbb{Z}$-Linearkombination von $x_1, \ldots, x_n$ darstellbar; also wird $(\mathbb{Q}, +)$ nicht von $x_1, \ldots, x_n$ erzeugt. Die Gruppe $(\mathbb{Q}, +)$ ist also nicht endlich erzeugt.

(b) Es sei $x = m/n \in \mathbb{Q}^\times$ ein gekürzter Bruch. Besitzt n einen Primteiler p, so gilt $x^n \neq 1$ für alle $n \in \mathbb{N}$. Die einzigen Elemente in $(\mathbb{Q}^\times, \cdot)$, die endliche Ordnung haben, sind also ± 1. Sind endlich viele Elemente $x_1, \ldots, x_r$ von $\mathbb{Q}^\times$ gegeben, so besitzen diese einen Hauptnenner n. Ist p irgendeine Primzahl, durch die n nicht teilbar ist, so $1/p$ nicht als Produkt $x_1^{n_1} \cdots x_r^{n_r}$ mit Exponenten $n_i \in \mathbb{N}$ darstellbar; also wird $(\mathbb{Q}^\times, \cdot)$ nicht von $x_1, \ldots, x_n$ erzeugt. Die Gruppe $(\mathbb{Q}^\times, \cdot)$ ist also nicht endlich erzeugt.

Lösung (4.15) Man prüft schnell nach, daß sowohl $(A \star B) \star C$ als auch $A \star (B \star C)$ genau aus denjenigen Elementen $x \in X$ besteht, die entweder in genau einer der drei Mengen A, B, C oder aber in allen dreien dieser Mengen liegen. Insbesondere gilt also $(A \star B) \star C = A \star (B \star C)$, so daß $\star$ das Assoziativgesetz erfüllt. Offensichtlich ist $\star$ auch kommutativ. Offensichtlich ist die leere Menge $\emptyset$ ein Neutralelement für $\star$, und wegen $A \star A = \emptyset$ für alle $A \in \mathfrak{P}(X)$ ist jedes Element $A \in \mathfrak{P}(X)$ zu sich selbst invers ist, also im Fall $A \neq \emptyset$ die Ordnung 2 hat.

Lösung (4.16) (a) Für $z \in \mathbb{C}^\times$ ist $zU_1 = \{rz \mid r > 0\}$ gerade der Ursprungsstrahl durch z. Die Nebenklassen nach U_1 sind also gerade die Ursprungsstrahlen.

(b) Für $z \in \mathbb{C}^\times$ ist $zU_2 = \{rz \mid r \neq 0\}$ gerade die Ursprungsgerade durch z, aus der der Nullpunkt entfernt wurde. Die Nebenklassen nach U_2 sind also gerade die punktierten Ursprungsgeraden.

(c) Für $z \in \mathbb{C}^\times$ ist $zU_3 = \{zw \mid |w| = 1\} = \{\zeta \in \mathbb{C} \mid |\zeta| = |z|\}$ der Kreis durch z mit Mittelpunkt im Nullpunkt. Die Nebenklassen nach U_3 sind also gerade die konzentrischen Kreise mit Mittelpunkt im Nullpunkt.

(d) Für $z \in \mathbb{C}^\times$ ist $zU_4 = \{\pm z\}$. Die Nebenklassen nach U_4 sind also gerade die Mengen $\{\pm z\}$ mit $z \neq 0$, also die Paare aus jeweils einer komplexen Zahl und deren Spiegelbild am Nullpunkt.

(e) Es sei $\varepsilon := e^{2\pi/n}$; für $z \in \mathbb{C}$ ist dann $zU_5 = \{z\varepsilon^k \mid 1 \leq k \leq n\}$ die Menge, die aus den Ecken des regelmäßigen n-Ecks mit Mittelpunkt im Nullpunkt besteht, das z als eine seiner Ecken hat. Die Nebenklassen nach U_5 sind also gerade die Mengen solcher Polygonecken.

Lösung (4.17) (1)⇒(2): Es sei $g \in G$ beliebig. Anwendung von Bedingung (1) mit $g_1 := e$ und $g_2 := g$ zeigt, daß es ein Element $x \in G$ gibt mit $xA = A$ und $xB = gB$, also $x \in A$ und $g \in xB$. Dann gilt $g \in xB \subseteq AB$. Da $g \in G$ beliebig war, ist Bedingung (2) gezeigt.

(2)⇒(1): Es seien $g_1, g_2 \in G$ beliebig vorgegeben. Wir müssen ein Element $x \in G$ sowie Elemente $a \in A$ und $b \in B$ finden mit $g_1 = xa$ und $g_2 = xb$ und damit $x = g_1a^{-1} = g_2b^{-1}$, folglich $g_1^{-1}g_2 = a^{-1}b$. Jetzt ist klar, wie die Wahl zu treffen ist. Wegen $G = AB$ nach Vor-

aussetzung (2) gibt es Elemente $a \in A$ und $b \in B$ mit $g_1^{-1}g_2 = a^{-1}b$. Wir setzen dann $x := g_1a^{-1} = g_2b^{-1}$ und erhalten $xA = g_1a^{-1}A = g_1A$ sowie $xB = g_2b^{-1}B = g_2B$. Damit ist Bedingung (1) gezeigt.

Lösung (4.18) (a) Es gelten die folgenden Äquivalenzen:

$$\begin{aligned} & b_1A = b_2A \;\Leftrightarrow\; b_2^{-1}b_1 \in A \\ \Leftrightarrow\; & b_2^{-1}b_1 \in A \cap B \;\Leftrightarrow\; b_1(A\cap B) = b_2(A\cap B). \end{aligned}$$

Die Implikation $\Leftarrow$ zeigt, daß φ wohldefiniert ist; die Implikation $\Rightarrow$ zeigt, daß φ injektiv ist. Es folgt dann, daß U/A mindestens so viele Elemente wie $B/(A\cap B)$ hat, daß also $[B : A\cap B] \le [U : A]$ gilt. Im Fall $[U : A] < \infty$ gilt Gleichheit genau dann, wenn φ bijektiv ist (denn eine injektive Abbildung zwischen gleichmächtigen endlichen Mengen ist automatisch bijektiv), was genau dann der Fall ist, wenn für jedes $u \in U$ ein $b \in B$ existiert mit $uA = bA$, was genau dann der Fall ist, wenn $U = BA$ gilt bzw. $U = U^{-1} = (BA)^{-1} = A^{-1}B^{-1} = AB$.

(b) Es gelten die folgenden Äquivalenzen:

$$\begin{aligned} & (x_1A, x_1B) = (x_2A, x_2B) \\ \Leftrightarrow\; & x_1A = x_2A \text{ und } x_1B = x_2B \\ \Leftrightarrow\; & x_2^{-1}x_1 \in A \text{ und } x_2^{-1}x_1 \in B \\ \Leftrightarrow\; & x_2^{-1}x_1 \in A\cap B \\ \Leftrightarrow\; & x_1(A\cap B) = x_2(A\cap B). \end{aligned}$$

Die Implikation $\Leftarrow$ zeigt, daß ψ wohldefiniert ist; die Implikation $\Rightarrow$ zeigt, daß ψ injektiv ist. Es folgt dann, daß $(G/A)\times(G/B)$ mindestens so viele Elemente wie $G/(A\cap B)$ besitzt, daß also $|G/(A\cap B)| \le |(G/A)\times(G/B)| = |G/A|\cdot|G/B|$ gilt. Das bedeutet aber gerade $[G : A\cap B] \le [G : A]\cdot[G : B]$.

(c) Sind G/A und G/B endliche Mengen, so gilt Gleichheit in (b) genau dann, wenn die Abbildung ψ bijektiv ist, was genau dann der Fall ist, wenn es zu je zwei Elementen $g_1, g_2 \in G$ ein Element $x \in G$ gibt mit $g_1A = xA$ und $g_2B = xB$. Nach der vorigen Aufgabe ist dies genau dann der Fall, wenn $G = AB$ gilt.

(d) Wegen

$$\begin{aligned} [G : A\cap B] &= [G : A]\cdot[A : A\cap B], \\ [G : A\cap B] &= [G : B]\cdot[B : A\cap B] \end{aligned}$$

ist $[G : A\cap B]$ sowohl durch $[G : A]$ als auch durch $[G : B]$ teilbar, wegen der vorausgesetzten Teilerfremdheit dieser beiden Zahlen also auch durch $[G : A]\cdot[G : B]$. Andererseits gilt $[G : A\cap B] \le [G : A]\cdot[G : B]$ nach Teil (b). Also muß $[G : A\cap B] = [G : A]\cdot[G : B]$ gelten, was nach Teil (c) die Bedingung $G = AB$ zur Folge hat.

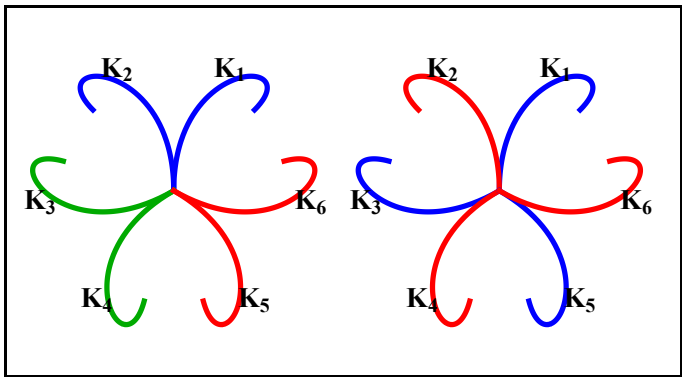
Lösung (4.19) (a) Es gilt $U = \{g \in G \mid g\star\mathfrak{U} = \mathfrak{U}\}$, wenn $\star$ die Wirkung von G auf den Punkten der Figur $\mathfrak{G}$ bezeichnet. Es gelten dann die folgenden Äquivalenzen:

$$\begin{aligned} & g_1U = g_2U \;\Leftrightarrow\; g_2^{-1}g_1U = U \;\Leftrightarrow \\ & g_2^{-1}g_1\star\mathfrak{U} = \mathfrak{U} \;\Leftrightarrow\; \mathfrak{g}_1\star\mathfrak{U} = \mathfrak{g}_2\star\mathfrak{U}. \end{aligned}$$

Also ist durch $gU \mapsto g\star\mathfrak{U}$ eine Bijektion zwischen den Linksnebenklassen von G nach U und den zu $\mathfrak{U}$ unter der Wirkung von G kongruenten Teilfiguren von $\mathfrak{G}$ gegeben. Eine analoge Abbildung für die Rechtsnebenklassen von G nach U ist gegeben durch $Ug \mapsto g^{-1}\star\mathfrak{U}$.

(b) Die Symmetriegruppe G der angegebenen Figur $\mathfrak{G}$ besteht aus drei Drehungen (um 0^0, 120^0 und 240^0) sowie drei Spiegelungen. Wir bezeichnen die Drehungen mit D_0, D_{120} und D_{240} sowie mit S_{12}, S_{34} und S_{56} die Spiegelungen, wobei S_{ij} die Kurven K_i und K_j aneinander spiegle.

- Für $\mathfrak{U} = \{K_1\}$ ist $U = \{\mathrm{id}\}$; die (Links- und Rechts-) Nebenklassen von G nach U sind einfach die einelementen Teilmengen $\{g\}$ mit $g \in G$, und die zu K_1 kongruenten Teilfiguren von $\mathfrak{G}$ sind genau die Mengen $K_1 = \mathrm{id}\star K_1$, $K_2 = S_{12}\star K$, $K_3 = D_{120}\star K_1$, $K_4 = S_{23}\star K_1$, $K_5 = D_{240}\star K_1$ und $K_6 = S_{34}\star K_1$.
- Für $\mathfrak{U} = \{K_1, K_2\}$ ist $U = \{\mathrm{id}, S_{12}\}$. Die Nebenklassen von U sind $\{\mathrm{id}, S_{12}\}$, $\{D_{120}, S_{34}\}$ und $\{D_{240}, S_{56}\}$. Diesen Nebenklassen entsprechen die Teilfiguren $K_1\cup K_2$, $K_3\cup K_4$ und $K_5\cup K_6$.
- Für $\mathfrak{U} = \{K_1, K_3, K_5\}$ ist $U = \{D_0, D_{120}, D_{240}\}$. Die Nebenklassen von U sind $\{D_0, D_{120}, D_{240}\}$ und $\{S_{12}, S_{34}, S_{56}\}$. Diesen Nebenklassen entsprechen die Teilfiguren $K_1\cup K_3\cup K_5$ und $K_2\cup K_4\cup K_6$.



Zusammenhang zwischen den Nebenklassen einer Untergruppe der Symmetriegruppe einer geometrischen Figur und Teilfiguren dieser Figur.