Lösung 2: Relationen, Abbildungen, Mächtigkeit, Gruppen

1. Gegeben $n, m \in \mathbb{Z}$ schreiben wir

$$m \mid n \Leftrightarrow \exists k \in \mathbb{Z} : n = km$$

Wir sagen m teilt n. Eine Zahl $n \in \mathbb{Z}$ ist gerade, genau dann wenn $2 \mid n$.

a) Gegeben $n \in \mathbb{Z}$ gilt $n - n = 0$ und also ist $\equiv$ reflexiv.
Angenommen $2 \mid n - m$, dann $n - m = 2k$ für ein $k \in \mathbb{Z}$ und also $m - n = -2k = 2(-k)$, so dass $2 \mid m - n$. Das zeigt

$$n \equiv m \Rightarrow m \equiv n$$

und somit ist $\equiv$ symmetrisch.
Angenommen $n_1, n_2, n_3 \in \mathbb{Z}$ so dass $n_1 \equiv n_2$ und $n_2 \equiv n_3$, und seien $k_1, k_2 \in \mathbb{Z}$ so dass

$$n_i - n_{i+1} = 2k_i \quad i = 1, 2$$

Dann gilt

$$n_1 - n_3 = (n_1 - n_2) + (n_2 - n_3) = 2k_1 + 2k_2 = 2(k_1 + k_2)$$

Es gilt also $2 \mid n_1 - n_3$ und da n_1, n_2, n_3 beliebig waren, folgt die Transitivität von $\equiv$.
Seien $[0] \subset \mathbb{Z}$ und $[1] \subset \mathbb{Z}$ die Restklassen von 0 und 1. Da $1 \not\equiv 0$, gilt $[1] \cap [0] = \emptyset$. Sei nun $n \in \mathbb{Z}$, dann ist entweder n gerade, in welchem Falle $n \equiv 0$, oder n ist ungerade, also $n \equiv 1$. Tatsächlich sei $k = \max\{l \in \mathbb{Z} \mid 2l \leq n\}$, dann folgt aus $2 \nmid n$, dass $2k < n$, und aus der Maximalität von k, dass $2(k+1) > n$, also

$$2k < n < 2k + 2$$

und folglich $n = 2k + 1$, bzw. $n \equiv 1$. Es gilt also $[0] \sqcup [1] = \mathbb{Z}$ – wobei $\sqcup$ die disjunkte Vereinigung bezeichnet – und somit ist

$$(\mathbb{Z}/\equiv) = \{[0], [1]\}$$

Bitte wenden!

b) Die resultierende Relation ist keine äquivalenzrelation, da sie zwar symmetrisch, aber weder reflexiv noch transitiv ist. Für $n, m \in \mathbb{Z}$ ist wegen Teil (a) $n - m$ ungerade genau dann, wenn $n - m = 2k + 1$ für ein $k \in \mathbb{Z}$. Aber $n - n = 0$ und also wäre die neue Relation nicht reflexiv. Sie wäre symmetrisch, da

$$m - n = -(2k + 1) = 2(-k) + (1 - 2) = 2(-k - 1) + 1$$

Transitivität wäre ebenfalls nicht erfüllt. Seien $k_1, k_2 \in \mathbb{Z}$ so dass

$$n_i - n_{i+1} = 2k_i + 1 \quad i = 1, 2$$

dann folgt

$$n_1 - n_3 = (n_1 - n_2) + (n_2 - n_3) = 2k_1 + 1 + 2k_2 + 1 = 2(k_1 + k_2 + 2)$$

und also $2 \mid n_1 - n_3$.

c) Die Vorgehensweise ist dieselbe wie für die Relation $\equiv$ von oben. Da $n \mid 0$, gilt $m \sim_n m$ für alle $m \in \mathbb{Z}$ und folglich ist die Relation reflexiv.

Sei $m - l = kn$ für ein $k \in \mathbb{Z}$, d.h. $m \sim_n l$, dann gilt $l - m = -kn = (-k)n$ und also $n \mid l - m$, i.e. $l \sim_n m$. Somit ist $\sim_n$ symmetrisch.

Seien wieder $m_1, m_2, m_3, k_1, k_2 \in \mathbb{Z}$ so dass

$$m_i - m_{i+1} = k_i n \quad i = 1, 2$$

Dann folgt

$$m_1 - m_3 = (m_1 - m_2) + (m_2 - m_3) = (k_1 + k_2)n$$

und folglich $m_1 \sim_n m_2, m_2 \sim_n m_3 \Rightarrow m_1 \sim_n m_3$.

d) Seien $[0], \ldots, [n-1]$ die Restklassen von $0, \ldots, n-1$. Seien $0 \leq k < l < n$, dann ist $0 \leq l - k < n$ und folglich $n \nmid l - k$, d.h. $[k] \cap [l] = \emptyset$. Sei $l \in \mathbb{Z}$ beliebig und sei $k := \max\{l \in \mathbb{Z} \mid kn \leq l\}$. Per definitionem gilt

$$kn \leq l < kn + n$$

beziehungsweise $0 \leq l - kn < n$, also $l - kn = m$ für ein $0 \leq m < n$ und also $l \sim_n m$, und da $l \in \mathbb{Z}$ beliebig war folgt

$$\mathbb{Z}/\sim_n = \{[m] \mid 0 \leq m < n\}$$

2. a) **"$\Rightarrow$":** Es ist klar, dass $b = c \Rightarrow a \circ b = a \circ c$.

"$\Leftarrow$": Sei $a \circ b = a \circ c$. Da G eine Gruppe ist, existiert $x \in G$ mit $x \circ a = e$, und also wegen Assoziativität:

$$\begin{aligned} b &= e \circ b = (x \circ a) \circ b = x \circ (a \circ b) \\ &= x \circ (a \circ c) = (x \circ a) \circ c = e \circ c = c \end{aligned}$$

Siehe nächstes Blatt!

3. Für $n = 1$ sei $[x] := x$ und für $n = 2$ sei $[x_1, x_2] := x_1 * x_2$. Diese Definitionen erfüllen offensichtlich die drei bedingungen. Seien nun die Produkte $[x_1, \ldots, x_k]$ definiert für $1 \leq k \leq n$. Jede Definition von $[x_1, \ldots, x_{n+1}]$ mit den gewünschten Eigenschaften erfüllt (für den Spezialfall $i = n$) die Gleichung

$$[x_1, \ldots, x_{n+1}] = [x_1, \ldots, x_n] * [x_{n+1}]$$

Die rechte Seite ist aber von der Form $y * x_{n+1}$, mit $y = [x_1, \ldots, x_n]$ und somit liefert die rechte Seite die eindeutige Definition von $[x_1, \ldots, x_{n+1}]$. Es bleibt zu zeigen, dass

$$[x_1, \ldots, x_{n+1}] = [x_1, \ldots, x_i] * [x_{i+1}, \ldots, x_{n+1}] \quad \forall 1 \leq i \leq n$$

Per definitionem können wir annehmen, dass $i < n$ und es folgt also unter Verwendung der Assoziativität

$$\begin{aligned}[x_1, \ldots, x_{n+1}] =& [x_1, \ldots, x_n] * x_{n+1} \\ =& ([x_1, \ldots, x_i] * [x_{i+1}, \ldots, x_n]) * x_{n+1} \\ =& [x_1, \ldots, x_i] * ([x_{i+1}, \ldots, x_n] * x_{n+1}) \\ =& [x_1, \ldots, x_i] * [x_{i+1}, \ldots, x_{n+1}]\end{aligned}$$

da das eindeutige Produkt von $n + 1 - i$ Elementen $x_{i+1}, \ldots, x_{n+1}$ gegeben ist durch

$$[x_{i+1}, \ldots, x_{n+1}] = [x_{i+1}, \ldots, x_n] * x_{n+1}$$

4. a) Sei $G = \{e, a, b\}$ mit Verknüpfung $\circ$ und neutralem Element e. Dann wissen wir

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

wobei die "$*$" Platzhalter für noch nicht bestimmte Einträge sind. Beachte, dass in jeder Spalte und jeder Zeile jedes Element von G genau einmal auftaucht. Andernfalls existiert (allgemein für endliche G) ein $h \in G$, das zweimal auftaucht und also $g_i, g_j, g \in G$ mit $g_i \neq g_j$ und $g_i \circ g = g_j \circ g = h$ (bzw. $g \circ g_i = g \circ g_j = h$), was absurd ist (siehe Aufgabe 2). Wir wissen also $a \circ a \in \{e, b\}$. Falls $a \circ b = b = e \circ b$, dann gilt ebenfalls wegen der Kürzungsregel $a = e$. Also ist $a \circ b = e$ und $a \circ a = b$ und somit

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

Bitte wenden!

b) Ohne Musterlösung. Die Vorgehensweise ist wie in Teilaufgabe (a).

c) G ist abelsch genau dann, wenn $g_i \circ g_j = g_j \circ g_i$ für alle i, j genau dann, wenn die Gruppentafel symmetrisch ist.

d) Wir führen die folgende Notation ein: Gegeben ein Winkel $\phi \in [0, 2\pi)$ bezeichne r_ϕ die Rotation der Ebene um den Mittelpunkt M um den Winkel ϕ im Gegenuhrzeigersinn. Die Menge solcher Rotationen, die das Quadrat auf sich selber abbilden, ist

$$\mathcal{R} := \left\{ r_\phi \mid \phi = \frac{k\pi}{2} \text{ für } 0 \leq k < 4 \right\}$$

Im folgenden bezeichnen wir $r := r_{\pi/2}$ und man sieht leicht, dass

$$\mathcal{R} = \{ r^k \mid 0 \leq k < 4 \}$$

wobei $r^k := \mathrm{id}$ falls $k = 0$ und $r^k := r^{k-1} \circ r$ falls $k \geq 1$. Man beachte, dass $\mathcal{R}$ bereits eine Gruppe bildet, mit neutralem Element id und Inversen $(r^k)^{-1} = r^{4-k}$. Wir bezeichnen im Gegenuhrzeigersinn mit S_k, $0 \leq k < 4$, die Symmetrieachsen des Quadrats, beginnend mit der horizontalen Symmetrieachse und wir bezeichnen mit s_k die Spiegelung der Ebene entlang der Achse S_k. Zur Vereinfachung der Notation schreiben wir $s := s_0$. Im Folgenden sei $s_n := s_k$ für $n \in \mathbb{Z}$, wobei $0 \leq k < 4$ so dass $n \sim_4 k$.

Als erstes bemerken wir drei spezielle Relationen, die wir verwenden werden, um die gewünschte Beschreibung der Gruppe D_4 zu erhalten. Zuerst überprüft man für die vier Spiegelungen explizit, dass

$$s_k = r^k s \quad \forall 0 \leq k < 4 \tag{1}$$

Andererseits gilt aber auch

$$s_k = r^k_{\pi/4} s r^{-k}_{\pi/4} \quad \forall k \in \mathbb{Z} \tag{2}$$

Falls $0 \leq k < 3$, dann überlegt man sich das konkret anhand des Quadrates. Andernfalls sei $k \in \mathbb{Z}$ und sei $k = 4l + n$ für $l \in \mathbb{Z}$ und $0 \leq n < 3$. Beachte, dass $r^2_{\pi/4} = r$. Dann ist per Definition $s_k = s_n = r^n_{\pi/4} s r^{-n}_{\pi/4}$. Des Weiteren ist $r^2 s r^{-2}$ eine Rotation um Winkel π um den Nullpunkt, gefolgt von einer Spiegelung entlang der x-Achse, gefolgt von einer Rotation um π um den Nullpunkt dasselbe wie eine Spiegelung entlang der x-Achse, denn die Rotation um Winkel π ist eine Spiegelung am Nullpunkt und sendet (x, y) nach $(-x, -y)$, während die Spiegelung s den Punkt (x, y) auf $(x, -y)$ abbildet, also

$$(x, y) \overset{r^{-2}}{\mapsto} (-x, -y) \overset{s}{\mapsto} (-x, y) \overset{r^2}{\mapsto} (x, -y)$$

Also ist $r^{4l} s r^{-4l} = s$ und folglich

$$s_k = s_n = r^n_{\pi/4} s r^{-n}_{\pi/4} = r^n_{\pi/4} (r^{4l}_{\pi/4} s r^{-4l}_{\pi/4}) r^{-n}_{\pi/4} = r^k s r^{-k}$$

Siehe nächstes Blatt!

wie behauptet.

Wir zeigen nun, unter Verwendung dieser Relationen, dass sich jedes Element in D_4 in der Form $s^l r^k$ mit $l \in \{0,1\}$ und $0 \leq k < 4$ schreiben lässt. Seien $0 \leq i < 4$ und $k \in \mathbb{Z}$, dann bemerken wir zuerst, dass

$$s_i r^k \overset{(1)}{=} (r^i s) r^k = r^{i+k}(r^{-k} s r^k) = r^{i+k}(r_{\pi/4}^{-2k} s r_{\pi/4}^{2k}) = r^{i+k} s_{-2k} = r^{i-k} s \qquad (3)$$

Falls nun $\sigma = s_i$ oder $\sigma = r^k$, dann sind wir fertig, denn wegen $s^2 = \mathrm{id}$ und (3) hat

$$\sigma = s_i = r^i s = (s r^{-i})^{-1} \overset{(3)}{=} (r^i s)^{-1} = s r^{-i} = s r^{4-i}$$

die gewünschte Form und im Falle $\sigma = r^k$ ist nichts zu zeigen. Seien nun also $m \geq 1$ und τ_i, $1 \leq i \leq m+1$, Rotationen und Spiegelungen. Angenommen, die Behauptung gilt für Kompositionen von m oder weniger Rotationen und Spiegelungen, dann folgt aus der Assoziativität, dass

$$\tau_{m+1} \circ \cdots \circ \tau_1 = \tau_{m+1} \circ (\tau_m \cdots \circ \tau_1) = \tau_{m+1} \circ (s^l r^k)$$

für $0 \leq k < 4$ und $l \in \{0,1\}$. Wenn τ_{m+1} eine Spiegelung ist, dann sind wir fertig. Sei also $\tau_{m+1} = r^n$ für $0 \leq n < 4$. Falls $l = 0$, dann sind wir fertig. Andernfalls folgt

$$\tau_{m+1} \circ \cdots \circ \tau_1 = r^n s r^k \overset{(3)}{=} s r^{-n+k}$$

wie gewünscht, da $r^{-n+k} = r^{k'}$ für $0 \leq k' < 4$. Dies löst die Aufgabe. Wir zeigen zusätzlich, dass $|D_4| = 8$, d.h. dass die $s^l r^k$ tatsächlich alle verschieden sind. Angenommen $l, l' \in \{0,1\}$ und $0 \leq k, k' < 4$ so dass $s^l r^k = s^{l'} r^{k'}$, dann ist auch $s^{l-l'} = r^{k'-k}$, und da r die Orientierung der Ebene erhält während s die Orientierung ändert, gilt $l = l'$. Es folgt $k' \sim_4 k$, und also ist $k = k'$.

e) Suchen Sie ein Gegenbeispiel, d.h. zwei Elemente $\tau, \sigma \in D_4$ so dass $\tau \circ \sigma \neq \sigma \circ \tau$.