Übungsaufgaben und Musterlösungen zur Einführung in die Algebra im Sommersemester 2004

Aufgabe (1). *Sei D eine nichtleere Menge und $M := Abb(D, D)$.*

(a) Zeigen Sie: M ist bzgl. der Hintereinanderausführung von Abbildungen ein Monoid.

(b) Kann es vorkommen, dass M eine Gruppe wird?

(c) Bestimmen Sie das Zentrum $Z(M) = \{g \in M \ : \ \forall f \in M \ : \ f \circ g = g \circ f\}$.

Lösung. a) M ist ein Monoid, da folgende Eigenschaften gelten:

(i) Die Komposition zweier Abbildungen aus M ist wieder in M, d.h. $\circ$ ist tatsächlich eine Verknüpfung auf M.

(ii) Die Assoziativität ist gegeben, da für alle $f, g, h \in M$ und $x \in D$ gilt:

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x).$$

(iii) Es existiert ein neutrales Element, nämlich id_D, für das $\mathrm{id}_D \circ f = f \circ \mathrm{id}_D = f$ für alle $f \in M$ gilt.

b) Für $|D| = 1$ ist $M = \{\mathrm{id}_D\}$ eine Gruppe. Für $|D| \neq 1$ seien $a, b \in D$, $a \neq b$ und c_a die konstante Abbildung auf a. Für jedes $g \in M$ gilt somit

$$(c_a \circ g)(b) = c_a(g(b)) = a \neq b = \mathrm{id}_D(b),$$

d.h. es kann kein Inverses zu c_a geben.

c) Sei $g \in Z(M)$ und $x \in D$. Dann gilt mit c_x der konstanten Abbildung auf x:

$$g(x) = g(c_x(x)) \underset{g \in Z(M)}{=} c_x(g(x)) = x.$$

Also ist $g = \mathrm{id}_D$ und $Z(M) = \{id_D\}$.

Aufgabe (2). *Sei A ein nichtleeres Alphabet und zu $n \in \mathbb{N}_+$ sei $W_n = \{$"Worte" der Länge $n\}$. Betrachtet werde die folgende Verknüpfung auf W_n:*

$$a_1 \cdots a_n \circ b_1 \cdots b_n := a_{i_1} \cdots a_{i_r} b_{j_1} \cdots b_{j_s},$$

wobei $r \geq 1$, $s \geq 1$, $r + s = n$ und $i_1, \ldots i_r, j_1, \ldots j_s \in \{1, \ldots, n\}$. Geben Sie Bedingungen an dafür, dass eine Halbgruppe entsteht. Kann unter Umständen auch ein Monoid entstehen?

Lösung. Gilt $|A| = 1$ so ist auch W_n einelementig und wir haben ein Monoid.

Gilt $|A| \neq 1$, d.h. es gibt $x, y \in A$, $x \neq y$, so müsste für ein neutrales Element $e_1 \cdots e_n$ gelten:

$$e_1 \cdots e_n \circ b_1 \cdots b_n = e_{i_1} \cdots e_{i_r} b_{j_1} \cdots b_{j_s} = b_1 \cdots b_n.$$

Für $b_1 \cdots b_n = x \cdots x$ folgt einerseits $e_{i_1} = x$ und für $b_1 \cdots b_n = y \cdots y$ andererseits $e_{i_1} = y$, was ein Widerspruch ist. Also entsteht außer im trivialen Fall nie ein Monoid.

Damit eine Halbgruppe entsteht, muss für alle $a = a_1 \cdots a_n$, $b = b_1 \cdots b_n$ und $c = c_1 \cdots c_n$ aus W_n mit $d_1 \cdots d_n := a_{i_1} \cdots a_{i_r} b_{j_1} \cdots b_{j_s} = a \circ b$ und $e_1 \cdots e_n := b_{i_1} \cdots b_{i_r} c_{j_1} \cdots c_{j_s} = b \circ c$ gelten:

$$a \circ (b \circ c) = (a \circ b) \circ c, \text{ also } a_{i_1} \cdots a_{i_r} e_{j_1} \cdots e_{j_s} = d_{i_1} \cdots d_{i_r} c_{j_1} \cdots c_{j_s}.$$

Setzt man $b = c = x \cdots x$, $a = y \cdots y$ folgt (I) $i_1, \ldots, i_r \in \{1, \ldots, r\}$ und für $a = b = x \cdots x$, $c = y \cdots y$ ebenso (II) $j_1, \ldots j_s \in \{r + 1, \ldots, n\}$.

Eine weitere Bedingung (III) $i_{i_k} = i_k$, $j_{j_l} = j_l$ für $1 \leq k \leq r$ und $1 \leq l \leq s$ erhält man durch Setzen von $a = b = c$, wobei c das Wort ist, was nur aus x besteht außer an der Stelle c_k bzw. c_{r+l}.

Dass diese Bedingungen auch hinreichend sind, rechnet man kurz nach:

$$a \circ (b \circ c) \underset{\text{(II)}}{=} a_{i_1} \cdots a_{i_r} c_{j_{j_1}} \cdots c_{j_{j_s}} \underset{\text{(III)}}{=} a_{i_{i_1}} \cdots a_{i_{i_r}} c_{j_1} \cdots c_{j_s} \underset{\text{(I)}}{=} (a \circ b) \circ c.$$

(Bemerkung: Hier hätte eine hinreichende Bedingung, damit $(A, \circ)$ eine Halbgruppe wird, zur Lösung der Aufgabe bereits genügt.)

Aufgabe (3). *In dem euklidischen Vektorraum $\mathbb{R}^2$ mit Standardskalarprodukt $((\cdot,\cdot))$ sei $K = \{v \in \mathbb{R} : ((v,v)) = 1\}$ der sogenannte Einheitskreis. Seien $v^{(1)}, v^{(2)}, v^{(3)}$ gleichabständige Punkte auf K und $v^{(1)} = (1,0)$. Bestimmen Sie die Untergruppe $G_\triangle$ von $\mathbb{R}^{2\times 2}$ aller orthogonalen 2×2-Matrizen, deren zugehörige lineare Abbildung (bzgl. der kanonischen Basis) die Menge $\{v^{(1)}, v^{(2)}, v^{(3)}\}$ in sich abbildet.*

Lösung. Mit $v^{(2)} = (\cos(2\pi/3), \sin(2\pi/3))$ und $v^{(3)} = (\cos(2\pi/3), -\sin(2\pi/3))$ haben wir gleichabstandige Punkte. Sei $A \in G_\triangle$. Dann ist die zugehörige lineare Abbildung F_A durch die Bilder auf der Basis $(v^{(1)}, v^{(2)})$ schon vollständig festgelegt. Wählen wir für $F_A(v^{(1)})$ einen der drei Punkte aus $\{v^{(1)}, v^{(2)}, v^{(3)}\}$, so bleiben für $F_A(v^{(2)})$ nur noch zwei Wahlmöglichkeiten, da orthogonale Matrizen vollen Rang haben. Wir bekommen also folgende sechs Matrizen:

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1/2 & -\sqrt{3}/2\\ \sqrt{3}/2 & -1/2\end{bmatrix}, \begin{bmatrix}-1/2 & \sqrt{3}/2\\ \sqrt{3}/2 & 1/2\end{bmatrix}, \begin{bmatrix}-1/2 & \sqrt{3}/2\\ -\sqrt{3}/2 & -1/2\end{bmatrix}, \begin{bmatrix}-1/2 & -\sqrt{3}/2\\ -\sqrt{3}/2 & 1/2\end{bmatrix}.$$

Nachrechnen bestätigt die Orthogonalität.

Da diese Abbildungen jeweils nur die Punkte untereinander vertauschen (und dabei alle Vertauschungen möglich sind), ist zu jeder dieser Abbildungen auch die inverse Abbildung in der Liste, und ebenfalls zu je zwei Abbildungen die Hintereinanderausführung. Damit ist das Untergruppenkritierum erfüllt, womit $G_\triangle$ eine Untergruppe der orthogonalen 2×2-Matrizen ist.

Aufgabe (5). *Sei $\alpha = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Welche Ordnung hat die von*

$$A := \begin{bmatrix}1 & 0 & 0\\ 0 & \alpha & 0\\ 0 & 0 & \alpha^2\end{bmatrix} \in GL(\mathbb{C}, 3) \qquad \text{und} \qquad B := \begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{bmatrix} \in GL(\mathbb{C}, 3)$$

erzeugte Untergruppe und welche Ordnung hat ihr Zentrum?

Lösung.

Behauptung: Es gilt $|\langle A, B\rangle| = 27$ und $|Z(\langle A, B\rangle)| = 3$.

Beweis: Wir bemerken zuerst, dass $\operatorname{ord}\alpha = \operatorname{ord} A = \operatorname{ord} B = 3$ ist und weiter $BAB^{-1} = \alpha A$.

Weiterhin ist auch $\langle \alpha E_3, A\rangle \cap \langle B\rangle = \{E_3\}$, was man daran sehen kann, dass A^2 sowohl 1 als auch $\alpha^2 \neq 1$ enthält. Somit enthält jede Matrix in $\langle \alpha E_3, A\rangle \setminus \{E_3\}$ ein α, und in den Potenzen von B ist nie ein α enthalten.

Setze $G := \{\alpha^a A^b B^c \mid a, b, c \in \{0, 1, 2\}\}$. Wir zeigen nun $|G| = 27$ und $\langle A, B\rangle = G$, womit der erste Teil der Behauptung folgt.

Teilbehauptung 1: Es ist $G \subseteq \langle A, B\rangle$.

Denn:

Sei $\alpha^a A^b B^c \in G$. Es ist $\alpha^a = (BAB^{-1}A^{-1})^a$, und somit gilt $\alpha^a A^b B^c \in \langle A, B\rangle$.

Teilbehauptung 2: Es ist $\langle A, B\rangle \subseteq G$.

Denn:

Sei $x = x_1^{e_1} \cdots x_n^{e_n} \in \langle A, B\rangle$ mit $x_i \in \{A, B\}$ und $e_i \in \{-1, 1\}$ für $1 \leq i \leq n$. Nun ist $A^{-1} = A^2$ und $B^{-2} = B^2$, womit ohne Einschränkung $e_i = 1$ vorausgesetzt werden kann für alle $i \in \{1, \ldots, n\}$.

Nun ist $BA = \alpha AB$. Gibt es also ein $i \in \{1, \dots, n-1\}$ mit $x_i = B$ und $x_{i+1} = A$, so ist

$$x = \alpha x_1 \cdots x_{i-1} AB x_{i+2} \cdots x_n.$$

Nun kann man so lange die Kombination BA in x durch αAB ersetzen und die αs nach vorne ziehen, so dass es $a', b', c' \in \mathbb{N}$ gibt mit

$$x = \alpha^{a'} A^{b'} B^{c'}.$$

Nun ist $\operatorname{ord} \alpha = \operatorname{ord} A = \operatorname{ord} B = 3$, womit man $a, b, c \in \{0, 1, 2\}$ wählen kann mit $\alpha^{a'} = \alpha^a$, $A^{b'} = A^b$ und $B^{c'} = B^c$ (Division mit Rest; Eigenschaft der Ordnung).

Damit gilt $|\langle A, B\rangle| = |G| \leq 27$.

Teilbehauptung 3: Es ist $|G| = 27$.

Denn:

Da wir bereits wissen, dass G maximal 27 Elemente enthält, reicht es zu zeigen, das zwei dieser Elemente, die zu verschiedenen Exponententripeln gehören, paarweise verschieden sind. Seien $\alpha^a A^b B^c \in G$ und $\alpha^{a'} A^{b'} B^{c'} \in G$ mit

$$\alpha^a A^b B^c = \alpha^{a'} A^{b'} B^{c'}.$$

Durch Multiplizieren von Links mit $\alpha^{-a'} A^{-b'}$ und mit B^{-c} von Rechts erhalten wir

$$\alpha^{a-a'} A^{b-b'} = B^{c'-c}.$$

Wie oben bemerkt, gilt nun $\langle \alpha E_3, A\rangle \cap \langle B\rangle = \{E_3\}$, womit daraus

$$\alpha^{a-a'} A^{b-b'} = E_3 = B^{c'-c}$$

folgt. Nun sind $a, a', b, b', c', c \in \{0, 1, 2\}$, womit $a' - a, b' - b, c' - c \in \{-2, -1, 0, 1, 2\}$ folgt, und wegen $\operatorname{ord} \alpha = \operatorname{ord} A = \operatorname{ord} B = 3$ dann

$$a = a', \quad b = b' \quad \text{und} \quad c = c'$$

sein muss.

Teilbehauptung 4: Es ist

$$Z(G) = \{\alpha^a E_3 \mid a \in \mathbb{Z}\} = \{\alpha^a E_3 \mid a \in \{0, 1, 2\}\}.$$

Denn:

Die hintere Gleichheit folgt aus $\operatorname{ord} \alpha = 3$. Es ist $\alpha^a E_3 \in Z(G)$, da für alle $M \in G$ gilt

$$(\alpha^a E_3) M = \alpha^a M = \alpha^a M E_3 = M(\alpha^a E_3).$$

Sei $C = (c_{ij})_{ij}$ und $D = diag(d_1, \dots, d_3) \in \mathbb{C}^{3\times 3}$. Damit $CD = DC$ gilt, muss $c_{ij} d_i = c_{ij} d_j$ sein für alle $1 \leq i, j \leq 3$.

Ist nun $C \in Z(G)$, so folgt mit $D = A$, dass $a_{ij} = 0$ ist für $i \neq j$, also $C = diag(c_{11}, \dots, c_{33})$.

Ist $D \in Z(G)$, so wähle $C = B$. Daraus folgt $d_1 = d_2 = d_3$, und somit $D = \lambda E_3$ mit $\lambda \in \mathbb{C}$. Nun sind die einzigen Matrizen in G mit dieser Form gerade $\alpha^k E_3$ mit $k \in \mathbb{Z}$, womit die Behauptung folgt.

Damit ist die Behauptung vollständig gezeigt. □

Aufgabe (6). *Bestimme die Konjugationsklassen von*

(a) der Gruppe $G_\triangle$ aus Aufgabe (3) und

(b) der Gruppe $\langle A, B\rangle$ aus Aufgabe (5).

Lösung. a) Mit den Bezeichnungen aus Aufgabe (3) betrachten wir die Untergruppe

$$G_\triangle = \{O \subseteq \mathbb{R}^{2\times 2} \mid O \text{ orthogonal}, \forall i \in \{0,1,2\}\ \exists j \in \{0,1,2\}\ :\ Ov^{(i)} = v^{(j)}\}$$

der orthogonalen 2×2-Matrizen.

Diese wird von einer Spiegelung an der x-Achse und einer Drechung um 120° nach links erzeugt.

Wir sehen, dass in $[E_2]_\approx$ keine weiteren Matrizen außer E_2 liegen, da aus $CE_2 = BC$ mit $C, B \in G_\triangle$ mit der Identität $CE_2 = E_2C$ und der Rechtskürzungsregel $B = E_2$ folgt.

Die beiden echten Drehungen sind konjugiert, da folgende Gleichung gilt:

$$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}-1/2 & -\sqrt{3}/2\\ \sqrt{3}/2 & -1/2\end{bmatrix} = \begin{bmatrix}-1/2 & -\sqrt{3}/2\\ -\sqrt{3}/2 & 1/2\end{bmatrix} = \begin{bmatrix}-1/2 & \sqrt{3}/2\\ -\sqrt{3}/2 & -1/2\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}.$$

Da für die restlichen drei Matrizen die Determinante gleich -1 ist, können sie nicht zu den beiden gerade betrachteten (mit Determinante 1) konjugiert sein. Für $A, B, C \in G_\triangle$ folgt aus $CA = BC$ nämlich $\det(CA) = \det(C) \cdot \det(A) = \det(B) \cdot \det(C) = \det(BC)$, also $\det(B) = \det(A)$. Damit haben wir eine zweite vollständige Konjugationsklasse gefunden.

Die restlichen drei Matrizen, die das Produkt einer echten Drehung und Spiegelung sind, bilden die letzte Konjugationsklasse, da die folgenden zwei Gleichungen gelten:

$$\begin{bmatrix}-1/2 & -\sqrt{3}/2\\ \sqrt{3}/2 & -1/2\end{bmatrix}\begin{bmatrix}-1/2 & -\sqrt{3}/2\\ -\sqrt{3}/2 & 1/2\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}-1/2 & \sqrt{3}/2\\ \sqrt{3}/2 & 1/2\end{bmatrix}\begin{bmatrix}-1/2 & -\sqrt{3}/2\\ \sqrt{3}/2 & -1/2\end{bmatrix}$$

$$\begin{bmatrix}-1/2 & \sqrt{3}/2\\ -\sqrt{3}/2 & -1/2\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}-1/2 & -\sqrt{3}/2\\ -\sqrt{3}/2 & 1/2\end{bmatrix} = \begin{bmatrix}-1/2 & \sqrt{3}/2\\ \sqrt{3}/2 & 1/2\end{bmatrix}\begin{bmatrix}-1/2 & \sqrt{3}/2\\ -\sqrt{3}/2 & -1/2\end{bmatrix}.$$

b) Wir betrachten nun die Gruppe $\langle A, B\rangle$ aus Aufgabe (5).

Seien $\alpha^a A^b B^c$ und $\alpha^{a'} A^{b'} B^{c'}$ konjugiert, d. h. es gibt ein $\alpha^{a''} A^{b''} B^{c''}$ mit

$$(\alpha^{a''} A^{b''} B^{c''})(\alpha^a A^b B^c) = (\alpha^{a'} A^{b'} B^{c'})(\alpha^{a''} A^{b''} B^{c''}).$$

Nun ist

$$(\alpha^{a''} A^{b''} B^{c''})(\alpha^a A^b B^c) = \alpha^{a+a''} A^{b''} \alpha^{bc''} A^b B^{c''} B^c = \alpha^{a+a''+bc''} A^{b+b''} B^{c+c''}$$

und

$$(\alpha^{a'} A^{b'} B^{c'})(\alpha^{a''} A^{b''} B^{c''}) = \alpha^{a'+a''} A^{b'} \alpha^{b''c'} A^{b''} B^{c'} B^{c''} = \alpha^{a'+a''+b''c'} A^{b'+b''} B^{c'+c''},$$

woraus wie oben folgt

$$b = b' \qquad \text{und} \qquad c = c'.$$

Weiterhin gilt dann

$$\alpha^{a+bc''} = \alpha^{a'+b''c}$$

und somit $a + bc'' \equiv a' + b''c \pmod 3$. Ist nun $b = c = 0 = b' = c'$, also $\alpha^a A^b B^c = \alpha^a E_3$, so folgt $a = a'$. Die Konjugationsklassen von $\alpha^a E_3$ bestehen also jeweils nur aus $\alpha^a E_3$ und sonst keinem Element.

Ist nun $b \neq 0$, so kann durch Wahl von c'' das Produkt bc'' jeden beliebigen Wert modulo 3 annehmen[1]. Analog kann für $c \neq 0$ durch Wahl von b'' das Produkt $b''c$ jeden beliebigen Wert modulo 3 annehmen. Ist also $(b, c) \neq (0, 0)$, so kann man für alle a, a' passende c'', b'' so finden, dass die Konjugationsgleichung erfüllt ist.

Damit sind die Konjugationsklassen gegeben durch

$$[A^b B^c]_\approx = \{\alpha^a A^b B^c \mid a \in \{0,1,2\}\}, \qquad (b, c) \in \{0,1,2\}^2 \setminus \{(0,0)\},$$
$$[\alpha^a E_3]_\approx = \{\alpha^a E_3\}, \qquad a \in \{0,1,2\}.$$

[1] Dies kann man einfach Nachrechnen, oder sich wie folgt überlegen: Rechnen modulo 3 ist wie Rechnen im $\mathbb{Z}_3$. Nun ist $\mathbb{Z}_3$ ein Körper, also hat jedes Element ungleich 0 ein multiplikatives Inverses. Ist also $a \in \mathbb{Z}_3 \setminus \{0\}$ und $b \in \mathbb{Z}_3$, so gibt es immer ein $c \in \mathbb{Z}_3$ mit $ac = b$.

Aufgabe (7). *Sei G eine Gruppe, und seien $a, b \in G$ mit $\operatorname{ord} a < \infty$ und $\operatorname{ord} b < \infty$. Es gelte weiterhin $\langle a \rangle \cap \langle b \rangle = \{1\}$. Dann gilt $\operatorname{ord}(\langle a, b \rangle) \geq \operatorname{ord} a \cdot \operatorname{ord} b$, wobei sowohl Gleichheit als auch Ungleichheit gelten kann.*

Lösung. Setze

$$H := \{a^i b^j \mid 0 \leq i < \operatorname{ord} a,\ 0 \leq j < \operatorname{ord} b\}.$$

Es gilt $|H| \leq \operatorname{ord} a \cdot \operatorname{ord} b$ und $H \subseteq \langle a, b \rangle$. Wir zeigen nun, dass je zwei Elemente mit verschiedenen Exponenten aus H paarweise verschieden sind, woraus $|H| = \operatorname{ord} a \cdot \operatorname{ord} b$ folgt. Dann muss auch $\langle a, b \rangle$ mindestens $\operatorname{ord} a \cdot \operatorname{ord} b$ Elemente enthalten, was zu zeigen war.

Seien $a^i b^j \in H$ und $a^k b^\ell \in H$ mit $a^i b^j = a^k b^\ell$. Multiplizieren von Links mit a^{-k} und von Rechts mit b^{-j} liefert

$$a^{i-k} = b^{\ell-j},$$

was wegen der Voraussetzung $\langle a \rangle \cap \langle b \rangle = \{1\}$ gerade

$$a^{i-k} = 1 \qquad \text{und} \qquad b^{\ell-j} = 1$$

liefert. Nun ist

$$-\operatorname{ord} a < i - k < \operatorname{ord} a \qquad \text{und} \qquad -\operatorname{ord} b < \ell - j < \operatorname{ord} b,$$

womit $i - k = 0 = \ell - j$ sein muss, also ist $i = k$ und $\ell = j$.

Damit ist $|H| = \operatorname{ord} a \cdot \operatorname{ord} b$ gezeigt, und somit der erste Teil der Behauptung.

Als Beispiel für Gleichheit betrachte die triviale Gruppe $\{1\}$ mit $a = b = 1$. (Die Voraussetzungen sind dann natürlich erfüllt.)

Als Beispiel für Ungleichheit betrachte die Gruppe $\langle A, B \rangle$ aus Aufgabe (5).

Lösungen einiger Präsenzaufgaben

Aufgabe (P1). *Sei M die Menge der 2-elementigen Teilmengen von $\{1,2,3,4\}$. Ist die induzierte Abbildung $\varphi : S_4 \to S(M)$ mit $\varphi(\sigma) : \{i,j\} \mapsto \{\sigma(i),\sigma(j)\}$ injektiv? Ist sie ein Morphismus?*

Lösung. Seien $\sigma, \sigma' \in S_4$. Dann gilt für alle $\{i,j\} \in M$

$$(\varphi(\sigma)\varphi(\sigma'))(\{i,j\}) = \varphi(\sigma)(\{\sigma'(i),\sigma'(j)\}) = \{\sigma(\sigma'(i)),\sigma(\sigma'(j))\} = \varphi(\sigma\circ\sigma')(\{i,j\}),$$

womit φ ein Morphismus ist. Sei nun $\sigma \in S_4$ mit $\varphi(\sigma) = \mathrm{id}_M$. Dann ist

$$\{1,2\} \ = \varphi(\sigma)(\{1,2\}) = \{\sigma(1),\sigma(2)\}.$$

Weiterhin ist

$$\{2,3\} \ = \varphi(\sigma)(\{2,3\}) = \{\sigma(2),\sigma(3)\}.$$

Nun ist $\{1,2\}\cap\{2,3\} = \{2\}$, also ist auch $\{\sigma(1),\sigma(2)\}\cap\{\sigma(2),\sigma(3)\} = \{2\}$. Nun muss $\sigma(1) \neq \sigma(3)$ sein, womit $\sigma(2) = 2$ folgt. Also ist auch $\sigma(1) = 1$ und $\sigma(3) = 3$, woraus sofort $\sigma(4) = 4$ folgt (dies folgt alles, da σ bijektiv ist), also $\sigma = \mathrm{id}$. Damit ist Kern φ trivial, und somit ist φ injektiv.

Aufgabe (P2). *Die Gruppe G sei von 2 Elementen a, b erzeugt und folgende Relationen seien bekannt: Es gibt $r, s, t \in \mathbb{N}_+$ mit $aba^{-1} = b^t$, $\operatorname{ord} a = r$, $\operatorname{ord} b = s$ und es gilt $\langle a\rangle \cap \langle b\rangle = \langle 1\rangle$. Zeige G enthält genau $r \cdot s$ Elemente.*

Lösung. Setze $H := \{a^i b^j \mid 0 \le i < r,\ 0 \le j < s\} \subseteq \langle a,b\rangle$. Genau wie in Aufgabe (7) zeigt man $|H| = \operatorname{ord} a \cdot \operatorname{ord} b$. Wir zeigen nun $\langle a,b\rangle \subseteq H$, womit die Behauptung folgt.

Sei $x = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} \in \langle a,b\rangle$ mit $x_i \in \{a,b\}$ und $e_i \in \{-1,1\}$ für $i = 1,\dots,n$. Da a und b endliche Ordnungen haben ist $a^{-1} = a^{r-1}$ und $b^{-1} = b^{s-1}$, womit man ohne Einschränkung $e_i = 1$ fordern kann für alle $i = 1,\dots,n$.

Die Voraussetzung $aba^{-1} = b^t$ bedeutet gerade, dass $ab = b^t a$ ist, womit jedes a in x in endlich vielen Schritten nach hinten verschoben werden kann. Insgesamt erhält man $x = b^i a^j$ mit $i, j \ge 0$.[2] Nun gibt es $i' \in \{0,\dots,r-1\}$ und $j' \in \{0,\dots,s-1\}$ mit $a^i = a^{i'}$ und $b^j = b^{j'}$ (endliche Ordnungen von a und b, Division mit Rest), womit man

$$x = a^{i'} b^{j'} \in H$$

hat.

Aufgabe (P3). *Sei G eine kommutative Gruppe multiplikativ geschrieben. Betrachte*

$$\Phi : \ (\mathbb{Z},\cdot) \to \mathrm{Abb}(G,G), \qquad \Phi(z) = \tau_z$$

mit $\tau_z : \ a \mapsto a^z$.

Zeige: Φ ist ein Monoidmorphismus und Bild Φ *ist kommutativ. Gib Beispiele von Gruppen an, wo* Kern Φ *nicht trivial ist.*

Lösung. Seien $z, w \in \mathbb{Z}$. Dann gilt für alle $a \in G$

$$(\Phi(z)\Phi(w))(a) = \tau_z(\tau_w(a)) = \tau_z(a^w) = (a^w)^z = a^{wz} = a^{zw} = \tau_{zw}(a) = \Phi(zw)(a),$$

womit Φ ein Monoidmorphismus ist. Sind $\varphi, \psi \in$ Bild Φ (also $\varphi = \Phi(z)$ und $\psi = \Phi(w)$ für gewisse $z, w \in \mathbb{Z}$), so ist

$$\varphi\psi = \Phi(z)\Phi(w) = \Phi(zw) = \Phi(wz) = \Phi(w)\Phi(z) = \psi\varphi,$$

also ist Bild Φ kommutativ.

Als Beispiel für einen nichttrivialen Kern wähle $G = \mathbb{Z}_3^*$ (die Gruppe der Einheiten des Monoiden[3] $(\mathbb{Z}_3,\cdot)$). Hier gilt Kern $\Phi = 2\,\mathbb{Z}+1$. Für z aus $\mathbb{Z}$ gilt nämlich

$$\Phi(2z+1)(2) = 2^{2z+1} = 2\cdot 2^{2z} = 2\cdot(2^2)^z = 2\cdot 1^z = 2$$

[2] Mathematisch einwandfrei lässt sich dies durch Induktion über die Anzahl n der Faktoren a, b in einem Produkt zeigen. Für $n = 1$ ist die Aussage klar. Für $x_1\cdots x_n$ mit $x_\mu \in \{a,b\}$, $1 \le \mu \le n$ gibt es nach Induktionsvoraussetzung $i, j \in \mathbb{N}$ mit $b^i a^j = x_2\cdots x_n$. Ist $x_1 = b$ oder $i = 0$, sind wir fertig. Ansonsten ist $x_1\cdots x_n = b^t a x_3\cdots x_n$, wobei nun nach Induktionsvoraussetzung $\mu, \nu \in \mathbb{N}$ mit $b^\mu a^\nu = a x_3\cdots x_n$ gibt, so dass $x_1\cdots x_n = b^{t+\mu}a^\nu$ folgt.

[3] Es ist $\mathbb{Z}_3^* = \{1,2\}$ mit $1\cdot x = x = x\cdot 1$, $x \in \mathbb{Z}_3^*$ und $2\cdot 2 = 1$. Es ist $(\mathbb{Z}_3^*,\cdot)$ isomorph zu $(\mathbb{Z}_2,+)$.

und $\Phi(2z+1)(1) = 1^{2z+1} = 1$, also $\Phi(2z+1) = \mathrm{id}_G$. Da $\Phi(2z)(2) = 2^{2z} = (2^2)^z = 1^z = 1$, also $\Phi(2z+1) \neq \mathrm{id}_G$, folgt Kern $\Phi = 2\mathbb{Z}+1$.

Generell ist Kern Φ bei endlichen Gruppen G nicht trivial. Zum Beispiel ist dann $\Phi(|G|+1) = \Phi(1) = \mathrm{id}_G$.

Aufgabe (P4). *Zeige: Ein endliches Monoid mit einer Kürzungsregel (z.B. Links) ist eine Gruppe.*

Lösung. Sei M endliches Monoid, und es gelte für alle $a, b, c \in M$

$$ab = ac \Rightarrow b = c \qquad \text{(Linkskürzungsregel)}.$$

Sei nun $a \in M$ beliebig. Betrachte die Potenzen

$$a^0, a^1, a^2, \ldots.$$

Diese liegen alle in M und da M endlich ist, gibt es ein $i > j > 0$ mit $a^i = a^j$. Also gilt

$$a^j a^{i-j} = a^{j+(i-j)} = a^j = a^j \cdot 1,$$

woraus mit der Kürzungsregel

$$a^{i-j} = aa^{i-j-1} = a^{i-j-1}a = 1$$

folgt. Damit ist a invertierbar. Da a beliebig gewählt war, sind alle Elemente aus M invertierbar, also ist M eine Gruppe.

Aufgabe (P5). *$\mathbb{Z}_2 \times \mathbb{Z}_3$ ist eine Abelsche Gruppe bzgl. komponentenweiser Addition. Ist sie isomorph zu $\mathbb{Z}_6$?*

Lösung. Ja, sie ist isomorph: Es ist $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,0), (0,1) \rangle$. Weiterhin ist $(1,0) = (1,1) + (1,1) + (1,1)$, also $(1,0) \in \langle (1,1) \rangle$, und es ist $(0,1) = (1,1) - (1,0)$, also $(0,1) \in \langle (1,1) \rangle$. Damit folgt $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (0,1), (1,0) \rangle \subseteq \langle (1,1) \rangle \subseteq \mathbb{Z}_2 \times \mathbb{Z}_3$, also ist $\mathbb{Z}_2 \times \mathbb{Z}_3$ zyklisch mit dem Erzeuger $(1,1)$. Nun sind zwei zyklische Gruppen gleicher Ordnung isomorph, womit $\mathbb{Z}_2 \times \mathbb{Z}_3$ isomorph zu $\mathbb{Z}_6$ ist (vergleiche Satz 3(b) in § 3 der Vorlesung).

Aufgabe (P6). *Sei H eine Untergruppe von G. Gilt $[G : H] = 2$, so ist H ein Normalteiler.*

Lösung. Wir zeigen $aH = Ha$ für alle $a \in G$; daraus folgt mit Aufgabe 8(a) die Behauptung. Sei also $a \in G$ beliebig. Gilt $a \in H$, so ist $aH = H = Ha$.

Ist dagegen $a \notin H$, so ist $aH \neq H \neq Ha$, da mit dem neutralen Element $e \in H$ das Element a auch in aH und Ha liegt. Nun ist $[G : H] = 2$, womit es nur genau zwei Links- und zwei Rechtsnebenklassen von H gibt. Da H selber auch eine Links- und Rechtsnebenklasse von H ist, und G die Vereinigung aller Links- oder Rechtsnebenklassen ist, muss gelten $aH = G \setminus H$ und $Ha = G \setminus H$, also $aH = Ha$.

Aufgabe (P7). *Sei H ein Normalteiler von G. Gilt $ord(H) = 2$, so ist H im Zentrum $Z(G)$ enthalten.*

Lösung. Sei $H = \langle a \rangle$, also $a^2 = 1$, $a \neq 1$. Ist nun $x \in G$ beliebig, so gilt $\{x \cdot 1, x \cdot a\} = xH = Hx = \{1 \cdot x, a \cdot x\}$. Da beide Nebenklassen die Mächtigkeit 2 haben und $1 \cdot x = x \cdot 1$ ist, muss auch $ax = xa$ sein. Da $x \in G$ beliebig ist, folgt $a \in Z(G)$ und somit $H = \langle a \rangle \subseteq Z(G)$.