R. Herzog, G. Müller
Universität Heidelberg

Übung I - 5 (Lösung)

Ausgabedatum: 10. November 2025
Abgabedatum: 17. November 2025

Übungsaufgabe I-5.1. ((Abelsche) Gruppen)

(a) Entscheiden Sie, welche der Beispiele aus Übungsaufgabe I-4.3 Gruppen sind, und ob sie kommutativ sind. Begründen Sie Ihre Entscheidung.

(b) Gegeben seien eine nichtleere Indexmenge I und für jedes $i \in I$ eine Gruppe $(G_i, \star_i)$. Wir definieren auf $\bigtimes_{i\in I} G_i$ die Verknüpfung

$$\star_\times(a, b) \coloneqq (a_i \star_i b_i)_{i\in I}.$$

Zeigen Sie, dass $(\bigtimes_{i\in I} G_i, \star_\times)$ eine Gruppe ist. (Diese Gruppe wird **direktes Produkt** der Gruppen $(G_i, \star_i)$ genannt). Zeigen Sie weiterhin, dass $(\bigtimes_{i\in I} G_i, \star_\times)$ genau dann abelsch ist, wenn alle $(G_i, \star_i)$ abelsch sind.

Lösung.

(a) In Frage kommen nur die Monoide, also die Paare (i) und (iii).

(i): Für $(\mathbb{R}^X, \cdot)$ mit der konstanten Einsfunktion besitzt bspw. die konstante Nullfunktion kein Inverses, hier liegt also **keine Gruppe** vor.

(iii): Für $(\mathcal{P}(X), \cup)$ mit der leeren Menge als neutralem Element ist lediglich $\emptyset$ invertierbar, hier liegt also **keine Gruppe** vor.

(b) Entsprechend Definition 6.42 ist

$$\bigtimes_{i\in I} G_i \coloneqq \left\{ F\colon I \to \bigcup_{i\in I} G_i \;\middle|\; F(i) \in G_i \text{ für alle } i \in I \right\}.$$

Für a und b aus $\bigtimes_{i\in I} G_i$ sind die Auswertungen $a_i = a(i)$ und $b_i = b(i)$ also jeweils in G_i und nach Voraussetzung ist $\star_i$ eine Verknüpfung auf G_i, damit ist $a_i \times_i b_i \in G_i$, also ist $\star_\times$ zumindest schonmal wohldefiniert. Das war Teil der Aufgabenstellung, musste also nicht nachgeprüft werden, ebenso wie die Assoziativität, die aber ebenfalls einfach vererbt wird, denn es ist auf Grund der Assoziativität jeder Verknüpfung $\star_i$:

$$\begin{aligned}(a \star_\times b) \star_\times c &= (i \mapsto a_i \star_i b_i) \star_\times c \\ &= (i \mapsto (a_i \star_i b_i) \star_i c_i) \\ &= (i \mapsto a_i \star_i (b_i \star_i c_i)) \\ &= a \star_\times (i \mapsto b_i \star_i c_i) \\ &= a \star_\times (b \star_\times c).\end{aligned}$$

In jeder Gruppe G_i existiert ein neutrales Element e_i, und das Element $e_\times \coloneqq i \mapsto e_i$ ist dann neutral in $\bigtimes_{i\in I} G_i$, denn für jedes $b \in \bigtimes_{i\in I} G_i$ ist

$$e_\times \star_\times b = (i \mapsto (e_i \star_i b_i)) = (i \mapsto b_i) = b.$$

Außerdem ist jedes $b \in \bigtimes_{i\in I} G_i$ invertierbar mit inversem Element $b^{-1} \coloneqq i \mapsto b_i^{-1}$, denn

$$b^{-1} \star_\times b = (i \mapsto (b_i^{-1} \star_i b_i)) = (i \mapsto e_i) = e_\times.$$

Damit handelt es sich hier um eine Gruppe.

Sind alle Teilverknüpfungen kommutativ, dann gilt für $a, b \in \bigtimes_{i\in I} G_i$: $a \star_\times b = (a_i \star_i b_i)_{i\in I} = (b_i \star_i a_i)_{i\in I} = b \star_\times a$. Gibt es ein einziges $i_0 \in I$ für das Elemente a_{i_0}, b_{i_0} existieren, so dass $a_{i_0} \star_{i_0} b_{i_0} \neq b_{i_0} \star_{i_0} a_{i_0}$, dann ist für je beliebigen $a, b \in\in \bigtimes_{i\in I} G_i$ auch $a \star_\times b$ and Stelle i_0 verschieden von $b \star_\times a$ und damit $\star_\times$ nicht kommutativ.

Übungsaufgabe I-5.2. (Kommutativität in (Halb-)Gruppen)

Gegeben sei eine partiell geordnete, nichtleere Menge $(H, \preccurlyeq)$ mit der Eigenschaft, dass für je zwei Elemente x, y das Infimum $\inf(\{x, y\}) \in H$ existiert. Zeigen Sie, dass $(H, \inf(\{\cdot, \cdot\}))$ eine Halbgruppe ist, und untersuchen Sie, ob diese kommutativ ist, und in welchen Fällen es sich sogar um eine Gruppe handelt.

Lösung.

Per Definition ist das Infimum in H, damit bildet die Abbildung schonmal in die richtige Menge ab. Ebenfalls per Definition ist das Infimum einer Menge von zwei Elementen unabhängig von deren Reihenfolge, damit liegt Kommutativität vor.

Für die Assoziativität seien $a, b, c \in H$. Wir zeigen nun, dass $\inf(\{a, \inf(\{b,c\})\}) = \inf(\{a,b,c\})$ ist, dann folgt die Assoziativität sofort aus der Kommutativität. Wir setzen $i \coloneqq \inf(\{a, \inf(\{b,c\})\})$. Dann ist i eine untere Schranke an $\{a\}$ und an $\inf(\{b,c\})$. Auf Grund der Transitivität der Ordnungsrelation ist i auch untere Schranke an $\{b,c\}$ und damit auch eine untere Schranke an $\{a,b,c\}$. Ist nun s eine weitere untere Schranke an $\{a,b,c\}$, dann ist s auch untere Schranke an $\{a\}$ und an $\{b,c\}$. Per Definition des Infimums ist s damit auch untere Schranke an $\{a\}$ und $\{\inf(\{b,c\})\}$ und damit an $\{\{a\}, \inf(\{b,c\})\}$, woraus sofort $s \leqslant i$ folgt und damit, dass $i = \inf(\{a,b,c\})$.

Damit liegt eine kommutative Halbgruppe vor. Ein Element e ist genau dann neutral, wenn $\inf(\{e,a\}) = a$ für alle $a \in H$ gilt. Dies gilt genau dann, wenn $e \geqslant a$ für alle $a \in H$ und $e \in H$ ist, also wenn e ein Maximum in H ist. Das ist also der einzige Fall, in dem ein Monoid vorliegt.

Invertierbarkeit für jedes $a \in H$ bedeutet, dass jeweils ein a^{-1} existiert, so dass $\inf(a, a^{-1}) = e$ gilt, was genau dann der Fall ist, wenn $e \leqslant a \leqslant e$ für $a \in H$, also wenn H nur aus dem neutralen Element besteht.

Übungsaufgabe I-5.3. (Symmetrische Gruppe)

Bestimmen Sie die Fehlstände, eine Zerlegung in Transpositionen und das Signum der Permutation

$$\sigma \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 4 & 1 & 7 & 3 & 8 & 2 \end{pmatrix}.$$

Lösung.

Die Fehlstände lesen wir ab, indem wir für jedes Indexpaar (i,j) mit $i < j$ prüfen, ob $\sigma(i) > \sigma(j)$ ist. Wir prüfen also für jeden Index i aus $[\![1,8]\!]$ und alle größeren Indizes, also die j aus $[\![i+1,8]\!]$, die Werte aus der Permutation (untere Reihe). Beispielsweise ist $(1,2)$ ein Fehlstand, denn $\sigma(1) = 6 > 5 = \sigma(2)$. Es ergeben sich die Fehlstände

$(1,j)$ für alle $j \in \{2,3,4,6,8\}$
$(2,j)$ für alle $j \in \{3,4,6,8\}$
$(3,j)$ für alle $j \in \{4,6,8\}$
$(4,j)$ für keine j
$(5,j)$ für alle $j \in \{6,8\}$
$(6,j)$ für alle $j \in \{8\}$
$(7,j)$ für alle $j \in \{8\}$.

Eine Zerlegung in Transpositionen können wir dadurch bestimmen, dass wir durch Transpositionen die Permutation σ zurück in die Identität überführen. Dabei gibt es mindestens 4 gleichwertige Möglichkeiten vorzugehen. Entweder führt man die Transpositionen im Bildbereich von σ (also nach/links der ursprünglichen Permutation) aus oder im Definitionsbereich von σ (also vor/rechts der ursprünglichen Permutation).

Tauscht man im Bildbereich, dann ergibt sich die folgende Kette von Umformungen:

$$
\begin{aligned}
\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 4 & 1 & 7 & 3 & 8 & 2 \end{pmatrix} \\
&= \tau(6,1) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 4 & 6 & 7 & 3 & 8 & 2 \end{pmatrix} \\
&= \tau(6,1) \circ \tau(5,2) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 6 & 7 & 3 & 8 & 5 \end{pmatrix} \\
&= \tau(6,1) \circ \tau(5,2) \circ \tau(4,3) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 6 & 7 & 4 & 8 & 5 \end{pmatrix} \\
&= \tau(6,1) \circ \tau(5,2) \circ \tau(4,3) \circ \tau(6,4) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 7 & 6 & 8 & 5 \end{pmatrix} \\
&= \tau(6,1) \circ \tau(5,2) \circ \tau(4,3) \circ \tau(6,4) \circ \tau(7,5) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 8 & 7 \end{pmatrix} \\
&= \tau(6,1) \circ \tau(5,2) \circ \tau(4,3) \circ \tau(6,4) \circ \tau(7,5) \circ \tau(8,7) \circ \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}}_{\mathrm{id}} \\
&= \tau(6,1) \circ \tau(5,2) \circ \tau(4,3) \circ \tau(6,4) \circ \tau(7,5) \circ \tau(8,7)
\end{aligned}
$$

Dabei fällt auf, dass wir uns wirklich in jedem Schritt merken müssen, wie die verbleibende Permutation aussieht, denn es können sich Transpositionen ergeben, die eine verbleibende Stelle mehrfach verwenden, in diesem Beispiel also der Tausch der 3 und der 4 jeweils aus der Stelle 6 heraus. Außerdem haben wir eine Transposition weniger ausführen müssen als höchstens erforderlich, denn die 6 hatten wir zufällig zwischendurch an die richtige Stelle getauscht und konnten nach der 5 gleich mit der 7 weitermachen. Schön zu sehen ist, wie die verbleibende Permutation einen immer weiter wachsenden Identitätsblock auf der linken Seite stehen hat, also zum Beispiel nach dem dritten Tauschschritt die Struktur

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 6 & 7 & 4 & 8 & 5 \end{pmatrix}$$

hat.

Tauscht man im Definitionsbereich (was etwas weniger übersichtlich ist), dann ergibt sich:

$$
\begin{aligned}
\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 4 & 1 & 7 & 3 & 8 & 2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 4 & 6 & 7 & 3 & 8 & 2 \end{pmatrix} \circ \tau(4,1) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 6 & 7 & 3 & 8 & 5 \end{pmatrix} \circ \tau(8,2) \circ \tau(4,1) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 6 & 7 & 4 & 8 & 5 \end{pmatrix} \circ \tau(6,3) \circ \tau(8,2) \circ \tau(4,1) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 7 & 6 & 8 & 5 \end{pmatrix} \circ \tau(6,4) \circ \tau(6,3) \circ \tau(8,2) \circ \tau(4,1) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 8 & 7 \end{pmatrix} \circ \tau(8,5) \circ \tau(6,4) \circ \tau(6,3) \circ \tau(8,2) \circ \tau(4,1) \\
&= \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}}_{\mathrm{id}} \circ \tau(8,7) \circ \tau(8,5) \circ \tau(6,4) \circ \tau(6,3) \circ \tau(8,2) \circ \tau(4,1) \\
&= \tau(8,7) \circ \tau(8,5) \circ \tau(6,4) \circ \tau(6,3) \circ \tau(8,2) \circ \tau(4,1)
\end{aligned}
$$

Tauscht man die größeren Zahlen zuerst, dann ergeben sich ganz analog Zerlegungen.

Wir können das Signum nun aus der Anzahl der Fehlstände $d = 16$ als $(-1)^d = (-1)^{16} = 1$ oder mit der Anzahl $r = 6$ der Transpositionen in einer Zerlegung von σ als $(-1)^r = (-1)^6 = 1$ ermitteln.

Übungsaufgabe I-5.4. (Untergruppen)

(a) Beweisen oder widerlegen Sie, dass

(*i*) $(m\mathbb{Z}, +)$ für $m \in \mathbb{N}$ eine Untergruppe von $(\mathbb{Z}, +)$ ist;
Beachte: Hier ist tatsächlich $m\mathbb{Z} \coloneqq \{mz \mid z \in \mathbb{Z}\}$ gemeint, keine Restklassen.

(*ii*) $\left(\left\{f \in \mathbb{R}^{\mathbb{R}} \,\middle|\, \forall x \in \mathbb{R}\ (f(x) \geqslant 0)\right\}, \circ\right)$ eine Untergruppe von $\left(\{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ bijektiv}\}, \circ\right)$ ist.

(b) Es sei $(U, \star)$ eine Untergruppe der Gruppe $(G, \star)$. Zeigen Sie Lemma 7.43 des Skripts, also die folgende Aussage: Das neutrale Element e_U von $(U, \star)$ ist gleich dem neutralen Element e von $(G, \star)$. Außerdem gilt für alle $a \in U$, dass das Inverse von a in U übereinstimmt mit dem Inversen von a in G.

Lösung.

(a) Hier kann man schon anfangen mit dem Untergruppenkriterium zu arbeiten. In diesem Lösungsvorschlag werden wir den Nachweis aber nochmal händisch führen.

(i) Es sei $m \in \mathbb{N}$. Für jedes $a \in \mathbb{Z}$ ist $ma \in \mathbb{Z}$ und somit tatsächlich $m\mathbb{Z} \subseteq \mathbb{Z}$. Bezüglich der Addition ist diese **Teilmenge** auch **abgeschlossen**, denn für $a_1 = mz_1$ und $a_2 = mz_2$ aus $m\mathbb{Z}$ ist

$$a_1 + a_2 = mz_1 + mz_2 = m\underbrace{(z_1 + z_2)}_{\in\mathbb{Z}} \in m\mathbb{Z}.$$

Das neutrale Element in $(\mathbb{Z}, +)$ ist die 0, und da auch $m0 = 0$ ist, ist $0 \in m\mathbb{Z}$, diese Teilmenge ist bezüglich der Addition also abgeschlossen und enthält das **neutrale Element**, formt mit der Addition also schonmal ein **Monoid**.

Dass es sich bei $(m\mathbb{Z}, +)$ sogar um eine **Gruppe** handelt sieht man daran, dass jedes Element $a = mz$ das inverse Element $a' = m(-z) \in m\mathbb{Z}$ besitzt. Jedes Element aus $(m\mathbb{Z}, +)$ ist also invertierbar.

(ii) Es handelt sich hier nicht um eine Untergruppe, denn $\left\{f \in \mathbb{R}^{\mathbb{R}} \,\middle|\, \forall x \in \mathbb{R}\ (f(x) \geqslant 0)\right\}$ ist nichtmal eine Teilmenge von $\{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ bijektiv}\}$, wie bspw. die positive aber nicht invertierbare Funktion $f \equiv 1$ zeigt.

Es handelt sich aber bei $\{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ bijektiv}\}$ tatsächlich um eine Gruppe (die symmetrische Gruppe $S(\mathbb{R})$), wir können also (spaßeshalber) die Menge

$$U \coloneqq \left\{f \in \mathbb{R}^{\mathbb{R}} \,\middle|\, \forall x \in \mathbb{R}\ (f(x) \geqslant 0) \text{ und } f \text{ bijektiv}\right\},$$

die tatsächlich eine Teilmenge von $\{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ bijektiv}\}$ ist, untersuchen. In U existiert aber nichtmal ein neutrales Element, denn das müsste die Identität sein, welche bzgl. der Komposition in $\{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ bijektiv}\}$ auch auf der Teilmenge A das eindeutige neutrale Element ist. Die Identität nimmt aber auch negative Werte an und liegt daher nicht in U.

(b) Es gilt

$$\begin{aligned} e \star e_U &= e_U && (e \text{ neutral in G}) \\ &= e_U \star_U e_U && (e_U \text{ neutral in U}) \\ &= e_U \star e_U. && (\text{Einschränkung der Verknüpfung}) \end{aligned}$$

Mit der Kürzungsregel aus (7.8b) des Skripts für die Gruppe $(G, \star)$ folgt dann $e = e_U$.

Beachte: Wir haben die Gruppeneigenschaft von U hier nicht genutzt und damit eigentlich gezeigt, dass schon das neutrale Element jedes Untermonoid $(U, \star_U)$ dem neutralen Element der Gruppe $(G, \star)$ entspricht. Ein Beispiel für einen Untermonoid in einer Gruppe, der aber keine Teilgruppe ist, ist $(\mathbb{N}_0, +)$ mit dem neutralen Element 0 in $(\mathbb{Z}, +)$. Der Begriff des Untermonoids ist allerdings eher ungewöhnlich und daher nicht Teil der Vorlesung.

Es sei nun $a \in U$. Bezeichnen wir mit a'_U das Inverse von a in U (das ja in U enthalten ist) und mit a' das Inverse von a in G (das möglicherweise nicht in U enthalten ist). Dann ist

$$a'_U \star a = a'_U \star_U a = e_U = e$$

und damit wieder auf Grund der Kürzungsregeln also $a'_U = a'$.

Übungsaufgabe I-5.5. (Erzeugung und Ordnung)

Es sei $(G, \cdot)$ eine Gruppe.

Beachte: In dieser Aufgabe werden wir in multiplikativer Notation arbeiten.

(a) Zeigen Sie, dass $\langle a \rangle = \{a^z \mid z \in \mathbb{Z}\}$ für $a \in G$ ist, sowie, dass $\operatorname{ord}(a) = \#\langle a \rangle$, wenn $\operatorname{ord}(a)$ endlich ist, und ansonsten $\langle a \rangle$ abzählbar unendlich ist.

(b) Zeigen Sie, dass zyklische Untergruppen von $(G, \cdot)$ immer kommutativ sind.

Lösung.

Beachte: Die multiplikative Notation ist in dieser Aufgabe hauptsächlich für die erste Teilaufgabe gewählt, um eine explizite, abkürzende Darstellung der zyklischen Gruppen zu ermöglichen. Die Resultate sind, wie immer, von der Notation völlig unabhängig.

(a) Die Darstellung in der Aussage ist exakt die Darstellung in Satz 7.50 des Skripts, also der Darstellung von erzeugten Untergruppen, wenn die erzeugende Menge nur ein Element beinhaltet.

Für zwei natürliche Zahlen $n, m \in \mathbb{N}$ ist auf Grund der Kürzungsregeln außerdem $a^n = a^m$ genau dann, wenn $a^{n-m} = e = a^{m-n}$ und damit genau dann, wenn die Differenz $n - m$ ein Vielfaches der $\operatorname{ord} a$ ist.

Für a mit unendlicher Ordnung passiert das daher nie, insbesondere sind in diesem Fall die a^z für $z \in \mathbb{Z}$ in $\langle a \rangle$ alle von einander verschieden. Es gibt für die Menge $\langle a \rangle = \{a^z \mid z \in \mathbb{Z}\}$ also die naheliegende Bijektion $a^z \mapsto z$ in die abzählbar unendliche Menge $\mathbb{Z}$, womit $\langle a \rangle$ abzählbar unendlich ist.

Wenn a endliche Ordnung $\operatorname{ord}(a)$ hat, dann ist entsprechend $a^z = a^{z \bmod \operatorname{ord}(a)}$, es gibt in $\langle a \rangle$ also genau $\operatorname{ord}(a)$ verschiedene Elemente, nämlich die Elemente $a^0, \dots, a^{\operatorname{ord} a - 1}$ (für die wir die Bijektion $a^i \mapsto i+1$ nach $\{1, \dots, \operatorname{ord}(a)\}$ angeben können).

(b) Die zyklischen Untergruppen von $(G, \cdot)$ sind genau die Mengen $\langle a \rangle$ für a aus G, von denen wir gerade die Darstellung $\{a^z \mid z \in \mathbb{Z}\}$ gezeigt haben. Für $a_1 = a^{z_1}$ und $a_2 = a^{z_2}$ aus $\langle a \rangle$ ist dann

$$a_1 \cdot a_2 = a^{z_1} \cdot a^{z_2} = a^{z_1 + z_2} = a^{z_2} \cdot a^{z_1} = a_2 \cdot a_1.$$

Übungsaufgabe I-5.6. (Nebenklassen)

Es sei $(G, \star)$ eine Gruppe und $(U, \star)$ eine Untergruppe. Zeigen Sie Folgerung 7.57 des Skripts, also dass, wenn $(G, \star)$ abelsch ist, die Äquivalenzrelationen $\sim^U$ und ${}^U\!\sim$ identisch sind und entsprechend für alle $a \in G$ die Nebenklassen $a \star U$ und $U \star a$ übereinstimmen.

Lösung.

In abelschen Gruppen ist $a \star u = u \star a$ für alle $a, u \in G$, also ist

$$a \star U = \{a \star u \mid u \in U\} = \{u \star a \mid u \in U\} = U \star a$$

für jedes $a \in G$. Entsprechend ist

$$[a]_{\sim^U} = a \star U = U \star a = [a]_{{}^U\!\sim}.$$

Hausaufgabe I-5.1 (Gruppen) 2.5 + 1 + 3.5 = 7 Punkte

(a) Entscheiden Sie, welche der Beispiele aus Hausaufgabe I-4.4 Gruppen sind. Begründen Sie Ihre Entscheidung.

(b) Es sei G nichtleer und $(G, \star)$ eine Gruppe. Wir definieren auf $\mathcal{P}(G)$ die Abbildung $\tilde{\star}$ durch

$$A \,\tilde{\star}\, B \coloneqq \{a \star b \mid a \in A \wedge b \in B\} \quad \text{für } A, B \in \mathcal{P}(G).$$

Beweisen oder widerlegen Sie, dass $\left(\mathcal{P}(G), \tilde{\star}\right)$ eine Gruppe ist.

(c) Zeigen Sie Lemma 7.25 des Skripts, also die folgenden Aussagen:

(*i*) Ist $(G, \star)$ eine Gruppe, so sind die Links- und Rechtstranslationen $\star_a$ und ${}_a\star$ für alle $a \in G$ bijektive Abbildungen $G \longrightarrow G$.

(*ii*) Ist $(H, \star)$ eine nichtleere Halbgruppe und gilt für alle $a \in H$, dass die Links- und Rechtstranslationen $\star_a$ und ${}_a\star$ surjektive Abbildungen sind, dann ist $(H, \star)$ eine Gruppe.

Lösung.

(a) In Frage kommen nur die Monoide, also die Paare (i), (ii), (iii), (iv) und (v).

(i): Für $(\mathbb{R}^X, +)$ mit der konstanten Nullfunktion als neutrales Element vererbt sich die Invertierbarkeit jedes Funktionswerts und für jedes $f \in \mathbb{R}^X$ lässt sich $-f$ als Inverses Element angeben. Hier handelt es sich also um eine **Gruppe**. (0.5 Punkte)

(ii): Für $(\mathcal{P}(X), \cap)$ mit der gesamten Menge X als neutralem Element ist lediglich X selbst invertierbar, hier liegt also **keine Gruppe** vor. (0.5 Punkte)

(iii) : Für $(\mathcal{P}(X), \triangle)$ mit der leeren Menge als neutralem Element ist jedes Element selbstinvers, hier liegt also eine **Gruppe** vor. (0.5 Punkte)

(iv): Für $(X^X, \circ)$ mit der Identität als neutralem Element ist jede nicht bijektive Funktion nicht invertierbar, hier liegt also **keine Gruppe** vor, sobald mindestens zwei Elemente in X existieren. Anderenfalls handelt es sich um die triviale Gruppe. (0.5 Punkte)

(v): Für $(\mathbb{Z}^2, ((x_1, x_2), (y_1, y_2)) \mapsto (x_1 \cdot y_1, x_2 + y_2))$ mit dem neutralen Element $(1, 0)$ ist das Element $(0, 0)$ nicht invertierbar, da die ersten Komponente kein multiplikatives Inverses besitzt. (0.5 Punkte)

(b) Es handelt sich i. A. nicht um eine Gruppe, denn i. A. ist nicht jedes Element invertierbar. Das führen wir unten weiter aus, jetzt schauen wir aber erstmal, wie weit wir in der Strukturanalyse kommen. (1 Punkt)

Die definierte Abbildung ist tatsächlich eine Verknüpfung auf $\mathcal{P}(G)$, denn $a \star b$ für $a \in A,\ b \in B$ mit $A, B \in \mathcal{P}(X)$ liegt wieder in G, da $\star$ eine Verknüpfung auf G ist.

Auch assoziativ ist die Verknüpfung $\tilde{\star}$ (wieder eine vererbte Eigenschaft von $\star$), denn es ist

$$\begin{aligned} A \mathbin{\tilde{\star}} (B \mathbin{\tilde{\star}} C) &= A \mathbin{\tilde{\star}} \{b \star c \mid b \in B \wedge c \in C\} \\ &= \{a \star (b \star c) \mid a \in A \wedge (b \in B \wedge c \in C)\} \\ &= \{(a \star b) \star c \mid (a \in A \wedge b \in B) \wedge c \in C\} \\ &= \{a \star b \mid a \in A \wedge b \in B\} \mathbin{\tilde{\star}} C \\ &= (A \mathbin{\tilde{\star}} B) \mathbin{\tilde{\star}} C. \end{aligned}$$

Wir haben also schonmal eine **Halbgruppe**.

Ein neutrales Element gibt es in $(\mathcal{P}(G), \tilde{\star})$ ebenfalls, nämlich die Menge $E \coloneqq \{e\}$, die nur das neutrale Element e der Gruppe $(G, \star)$ enthält. Hier ist nämlich für jedes $A \in \mathcal{P}(G)$:

$$E \mathbin{\tilde{\star}} A = \{e \star a \mid a \in A\} = \{a \mid a \in A\} = A.$$

Wir haben also ein **Monoid**.

Invertierbarkeit können wir allerdings nur in Spezialfällen zeigen. Klar ist, dass einelementige Mengen $A = \{a\}$ für $a \in G$ in $\mathcal{P}(G)$ bzgl. $\tilde{\star}$ invertierbar sind (deren Inverse sind $A' \coloneqq \{a'\}$). Sobald mindestens zwei verschiedene Elemente in A liegen, also $A = \{a_1, a_2\}$ darf A' jedoch nur noch aus Inversen zu a_1 und a_2 **gleichzeitig** bestehen, was nur möglich ist, wenn diese übereinstimmen. Zudem gibt es ja da noch die leere Menge, für die kein Inverses existiert. Entsprechend ist $(\mathcal{P}(G), \tilde{\star})$ keine Gruppe.

(c) Aussage (i): Es sei $(G, \star)$ eine Gruppe und $a \in G$ beliebig. Wir betrachten die Rechtstranslation $\star_a \colon G \ni x \mapsto x \star a \in G$. Die Gleichung $x \star a = b$ hat für jedes $b \in G$ die Lösung $x = b \star a'$, d. h., $\star_a$ ist surjektiv. (1 Punkt)

Gilt andererseits $x_1 \star a = x_2 \star a$, so folgt aus der Kürzungsregel in (7.18), dass $x_1 = x_2$ gelten muss, also ist $\star_a$ auch injektiv. (1 Punkt)

Für die Linkstranslation argumentieren wir entsprechend.

Aussage (ii): Es sei $(H, \star)$ eine Halbgruppe. Zu zeigen ist, dass H ein neutrales Element besitzt und dass jedes $a \in H$ invertierbar ist.

Für beliebiges $a \in H$ sind nach Voraussetzung $\star_a$ und ${}_a\star$ surjektiv. Es gibt also zu jedem $a \in H$ und jedem $b \in H$ Lösungen $x, y \in H$ der Gleichungen $x \star a = b$ und $a \star y = b$.

Wir wählen zunächst ein beliebiges, aber festes $a \in H$. Dann gibt es nach Voraussetzung $e_1, e_2 \in H$ mit $e_1 \star a = a$ und $a \star e_2 = a$. Es sei weiter $b \in H$ beliebig und x, y Lösungen

der Gleichungen $x \star a = b$ und $a \star y = b$. Dann haben wir

$$\begin{aligned} & e_1 \star b = e_1 \star (a \star y) = (e_1 \star a) \star y = a \star y = b \\ \text{und} \quad & b \star e_2 = (x \star a) \star e_2 = x \star (a \star e_2) = x \star a = b. \end{aligned}$$

(e_1 und e_2 sind also nicht nur für a, sondern für alle $b \in H$ links- bzw.. rechtsneutrale Elemente.) Aus Hausaufgabe I-4.4 wissen wir, dass dieses Element (wir nennen es ab jetzt e) eindeutig ist und ein neutrales Element für das Monoid. (1 Punkt)

Schließlich existieren für beliebiges $a \in H$ Lösungen x, y der Gleichungen $x \star a = e$ und $a \star y = e$. Wegen

$$x = x \star e = x \star (a \star y) = (x \star a) \star y = e \star y = y$$

ist $x = y$ das eindeutige Inverse zu a. (0.5 Punkte)

Hausaufgabe I-5.2 (Kommutativität in Gruppen) 1 + 3 = 4 Punkte

(a) Entscheiden Sie, welche Beispiele aus Hausaufgabe I-4.4 abelsche Gruppen sind. Begründen Sie Ihre Entscheidung.

(b) Zeigen Sie, dass jede Gruppe mit höchstens vier Elementen abelsch ist.

Lösung.

(a) In Frage kommen nur die Gruppen aus Übungsaufgabe I-5.1 , also $(\mathbb{R}^X, +)$ und $(\mathcal{P}(X), \triangle)$.

Wegen der vererbten Kommutativität der Addition in $\mathbb{R}$ handelt es sich bei $(\mathbb{R}^X, +)$ um eine abelsche Gruppe. (0.5 Punkte)

Bei $(\mathcal{P}(X), \triangle)$ handelt es sich ebenso um eine abelsche Gruppe, denn die Definition der symmetrischen Differenz ist natürlich symmetrisch. (0.5 Punkte)

(b) **Nachweisoption 1**: Jede einelementige Gruppe besteht nur aus dem neutralen Element und ist damit automatisch kommutativ. Für Gruppen mit zwei, drei und vier Elementen zeigen wir Kommutativität, indem wir nutzen, dass die Verknüpfung einer Gruppe genau dann kommutativ ist, wenn ihre Verknüpfungstabelle symmetrisch ist. Wichtige Zutaten in der folgenden Argumentation sind das Gruppenkriterium in Lemma 7.25 des Skripts und Satz 6.35, also die Aussage, dass Injektivität und Bijektivität auf endlichen Mengen übereinstimmen. Zusammengenommen sagen diese beiden Aussagen, dass in jeder Zeile und in jeder Spalte der Verknüpfungstabelle alle Elemente der Gruppe vorkommen müssen und das keines doppelt vorkommen darf. In der Verknüpfungstabelle sind die Spalte und

die Zeile zu dem neutralen Element schon vorgegeben und von da aus können wir ganz ähnlich wie bei der Lösung eines Sudoku argumentieren.

Im Folgenden nennen wir die Elemente, die in den Gruppen vorkommen können stellvertretend e, a, b, c, wobei e das neutrale Element bezeichnet. Wir müssen also die möglichen Verknüpfungen auf Mengen $\{e, a\}$, $\{e, a, b\}$ und $\{e, a, b, c\}$ darauf untersuchen, ob sie eine Gruppe liefern.

Im Fall von zwei Elementen, also für $\{e, a\}$, ist die Verknüpfungstabelle schon wie folgt durch das neutrale Element vorgegeben

$\star$	e	a
e	e	a
a	a	$\cdot$

wobei uns egal ist, was in dem letzten verbleibenden Platz steht, denn symmetrisch ist die Tabelle definitiv. Wir wissen, dass in der letzten Spalte und in der letzten Zeile noch das e fehlt, die volle Tabelle ergibt sich also zu

$\star$	e	a
e	e	a
a	a	e

(wobei man hier auch mit der Invertierbarkeit von a argumentieren könnte). (0.5 Punkte)

Im Fall von drei Elementen ist die Verknüpfungstabelle durch das neutrale Element vorgegeben als

$\star$	e	a	b
e	e	a	b
a	a	$\cdot$	$\cdot$
b	b	$\cdot$	$\cdot$

Wie bei einem Sudoku können wir jetzt direkt ablesen, dass in der mittleren Zeile das b nicht an die letzte Stelle kann (denn dann hätte die letzte Spalte zwei bs). Entsprechend für die letzte Zeile argumentiert erhalten wir die eindeutige Verknüpfungstabelle

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Wie schon zuvor brauchen wir hier garnicht nachweisen, dass es sich wirklich um eine Gruppe handelt (Assoziativität der Vernüpfung), denn wir wissen, dass jede mögliche Gruppe kommutativ ist. (1 Punkt)

Im Fall von vier Elementen in G ist die Tabelle vorgegeben als

$\star$	e	a	b	c
e	e	a	b	c
a	a	$\cdot$	$\cdot$	$\cdot$
b	b	$\cdot$	$\cdot$	$\cdot$
c	c	$\cdot$	$\cdot$	$\cdot$

Für den linken oberen Eintrag des verbleibenden $3x3$ Blocks haben wir die Möglichkeiten e, b oder c. Setzen wir hier b, dann ergibt sich, durch analoge Argumente zu den bisherigen, die folgende Tabelle

$\star$	e	a	b	c
e	e	a	b	c
a	a	b	$\cdot$	$\cdot$
b	b	$\cdot$	$\cdot$	$\cdot$
c	c	$\cdot$	$\cdot$	b

und damit als Folgerung für die Positionierung des Werts c in der Tabelle nur die Option

$\star$	e	a	b	c
e	e	a	b	c
a	a	b	c	$\cdot$
b	b	c	$\cdot$	$\cdot$
c	c	$\cdot$	$\cdot$	b

In der zweiten Zeile sowie Spalte bleibt nur das neutrale Element, wir haben also die Belegung

$\star$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	$\cdot$	$\cdot$
c	c	e	$\cdot$	b

und damit die letzte verbleibende Möglichkeit

$\star$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Analog argumentiert man, wenn c links oben im verbleibenden Block steht und erhält

$\star$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Alle verbleibenden Optionen haben eine symmetrische Tabelle.

Beginnt man links oben im verbleibenden Block mit e, dann hat man

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	$\cdot$	$\cdot$
b	b	$\cdot$	$\cdot$	$\cdot$
c	c	$\cdot$	$\cdot$	$\cdot$

vorgegeben. Die zweite Spalte und Zeile ergeben sich dann weiter zu

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	$\cdot$	$\cdot$
c	c	b	$\cdot$	$\cdot$

wobei wir den letzten verbleibenden $2x2$ Block auf zwei verschiede Weisen mit a und e belegen können, die möglichen Verknüpfungen sind also

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

und

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Beide sind symmetrisch. (1.5 Punkte) **Beachte:** Bei dieser Nachweisoption sieht man gleich, wieviele Gruppen es in der jeweiligen Größe maximal geben kann.

Nachweisoption 2: Wir zeigen, dass jede nichtkommutative Gruppe mindestens 5 verschiedene Elemente besitzt. Mit sich selbst und dem neutralen Element kommutiert aber jedes Element einer Gruppe, wir wissen also, dass eine nichtkommutative Gruppe **mindestens drei** verschiedene Elemente $\{e, a, b\}$ besitzen muss, von denen e das neutrale

Element ist. Die einzige Verknüpfung von Elementen aus $\{e, a, b\}$, die nicht kommutiert, muss also die von a und b sein, also $a \star b \neq b \star a$.

Da inverse Elemente in einer Gruppe eindeutig sind und sowohl links- als auch rechtsinvers, kommutieren also alle Elemente mit ihren Inversen, es muss also $a \star b \neq e$ und $b \star a \neq e$ gelten.

Da neutrale Elemente in einer Gruppe eindeutig sind und sowohl links- als auch rechtsneutral sind muss außerdem $a \star b \neq a$ und $b \star a \neq a$ sowie $a \star b \neq b$ und $b \star a \neq b$ gelten.

Zusammengenommen ist keines der Elemente $a \star b$ und $b \star a$ also schon in $\{e, a, b\}$ vertreten, damit $\star$ eine Verknüpfung sein kann, muss die Gruppe mindestens die 5 verschiedenen Elemente $\{e, a, b, a \star b, b \star a\}$ enthalten.

Beachte: Bei dieser Nachweisoption sieht man schön, dass Nichtkommutativität zusätzliche Elemente generiert.

Es ist im Übrigen so, dass die kleinste nicht-abelsche Gruppe die S_3 ist, also eine Gruppe mit gerade $3! = 6$ Elementen. Dass keine Gruppe mit 5 Elementen nicht-abelsch sein kann (es gibt davon nur eine, nämlich $\mathbb{Z} / \overset{5}{\equiv}$), kann man sich noch wie folgt überlegen: Angenommen es würden zwei Elemente nicht kommutieren (o. B. d. A. seien das wie oben die Elemente a und b), also $a \star b \neq b \star a$, dann sind wir in dem Setting, das wir bisher auch für die Argumentation verwendet haben. Nun ist $a \star a \notin \{a \star b, b \star a, a\}$, auf Grund der Kürzungsregeln, denn sonst wäre $a \in \{b, e\}$, was nach Voraussetzung nicht gelten kann. Zudem kann nicht $a \star a = b$ gelten, denn dann wäre $a \star b = a \star a \star a = b \star a$ im Widerspruch zur Nichtkommutativität. Bleibt also nur, dass $a \star a = e$ sein muss. Betrachtet man nun $a \star b \star a$, findet man mit den Kürzungsregeln, dass $a \star b \star a \notin \{a \star b, b \star a, a\}$, indem man wie oben mit der Verschiedenheit der bisherigen Elemente argumentiert. Wäre $a \star b \star a = e$, dann wäre $b \star a = a' = a \star b$ (a' von links und rechts ranknüpfen) im Widerspruch zu Nichtkommutativität und wäre $a \star b \star a = b$, dann wäre $b \star a = a \star b$ (a von links ranknüpfen). Also ist jede Gruppe mit 5 Elementen abelsch.

Hausaufgabe I-5.3 (Symmetrische Gruppe) 3 Punkte

Bestimmen Sie die Fehlstände, eine Zerlegung in Transpositionen und das Signum der Permutation

$$\sigma \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 7 & 8 & 3 & 4 & 5 & 2 \end{pmatrix}.$$

Lösung.

Die Fehlstände lesen wir ab, indem wir für jedes Indexpaar (i, j) mit $i < j$ prüfen, ob $\sigma(i) > \sigma(j)$ ist. Wir prüfen also für jeden Index i aus $[\![1, 8]\!]$ und alle größeren Indizes, also die j aus $[\![i+1, 8]\!]$, die Werte aus der Permutation (untere Reihe). Beispielsweise ist $(4, 5)$ ein Fehlstand, denn $\sigma(4) = 8 > 3 = \sigma(5)$. Es ergeben sich die Fehlstände

$$
\begin{aligned}
&(2, j) \text{ für alle } j \in \{5, 6, 7, 8\}\\
&(3, j) \text{ für alle } j \in \{5, 6, 7, 8\}\\
&(4, j) \text{ für alle } j \in \{5, 6, 7, 8\}\\
&(5, j) \text{ für alle } j \in \{8\}\\
&(6, j) \text{ für alle } j \in \{8\}\\
&(7, j) \text{ für alle } j \in \{8\}.
\end{aligned}
$$

(1 Punkt)

Eine Zerlegung in Transpositionen können wir dadurch bestimmen, dass wir durch Transpositionen die Permutation σ zurück in die Identität überführen. Dabei gibt es mindestens 4 gleichwertige Möglichkeiten vorzugehen. Entweder führt man die Transpositionen im Bildbereich von σ (also nach/links der ursprünglichen Permutation) aus oder im Definitionsbereich von σ (also vor/rechts der ursprünglichen Permutation).

Tauscht man im Bildbereich (und beginnt mit den kleinen Urbildern), dann ergibt sich die folgende Kette von Umformungen:

$$
\begin{aligned}
\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 7 & 8 & 3 & 4 & 5 & 2 \end{pmatrix} \\
&= \tau(6,2) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 7 & 8 & 3 & 4 & 5 & 6 \end{pmatrix} \\
&= \tau(6,2) \circ \tau(7,3) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 8 & 7 & 4 & 5 & 6 \end{pmatrix} \\
&= \tau(6,2) \circ \tau(7,3) \circ \tau(8,4) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 7 & 8 & 5 & 6 \end{pmatrix} \\
&= \tau(6,2) \circ \tau(7,3) \circ \tau(8,4) \circ \tau(7,5) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 8 & 7 & 6 \end{pmatrix} \\
&= \tau(6,2) \circ \tau(7,3) \circ \tau(8,4) \circ \tau(7,5) \circ \tau(8,6) \circ \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}}_{\mathrm{id}} \\
&= \tau(6,2) \circ \tau(7,3) \circ \tau(8,4) \circ \tau(7,5) \circ \tau(8,6).
\end{aligned}
$$

Dabei fällt auf, dass wir uns wirklich in jedem Schritt merken müssen, wie die verbleibende Permutation aussieht, denn es können sich Transpositionen ergeben, die eine verbleibende Stelle mehrfach verwenden, in diesem Beispiel also der Tausch der 2 und der 6 jeweils aus der Stelle 8 heraus. Außerdem haben wir eine Transposition weniger ausführen müssen als höchstens erforderlich, denn die 7 hatten wir zufällig zwischendurch an die richtige Stelle getauscht und konnten nach der 6 aufhören. Schön zu sehen ist, wie die verbleibende Permutation einen immer weiter wachsenden Identitätsblock auf der linken Seite stehen hat, also zum Beispiel nach dem dritten Tauschschritt die Struktur

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 7 & 8 & 5 & 6 \end{pmatrix}$$

hat.

Tauscht man im Definitionsbereich (was etwas weniger übersichtlich ist), dann ergibt sich:

$$\begin{aligned}
\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 7 & 8 & 3 & 4 & 5 & 2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 7 & 8 & 3 & 4 & 5 & 6 \end{pmatrix} \circ \tau(2,8) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 8 & 7 & 4 & 5 & 6 \end{pmatrix} \circ \tau(3,5) \circ \tau(2,8) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 7 & 6 & 5 & 6 \end{pmatrix} \circ \tau(4,6) \circ \tau(3,5) \circ \tau(2,8) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 8 & 7 & 6 \end{pmatrix} \circ \tau(5,7) \circ \tau(4,6) \circ \tau(3,5) \circ \tau(2,8) \\
&= \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}}_{\mathrm{id}} \circ \tau(6,8) \circ \tau(5,7) \circ \tau(4,6) \circ \tau(3,5) \circ \tau(2,8) \\
&= \tau(6,8) \circ \tau(5,7) \circ \tau(4,6) \circ \tau(3,5) \circ \tau(2,8)
\end{aligned}$$

Tauscht man die größeren Zahlen zuerst ergibt sich ganz analog Zerlegungen. (1 Punkt)

Wir können das Signum nun aus der Anzahl der Fehlstände $d = 15$ als $(-1)^d = (-1)^{15} = -1$ oder mit der Anzahl $r = 5$ der Transpositionen in einer Zerlegung von σ als $(-1)^r = (-1)^5 = -1$ ermitteln. (1 Punkt)

Hausaufgabe I-5.4 (Untergruppen) 1 + 2 + 1 = 4 Punkte

(a) Es sei X eine nichtleere Menge und $A \subseteq X$ sowie $n \in \mathbb{N}$. Beweisen oder widerlegen Sie, dass

(*i*) $(\mathcal{P}(A), \triangle)$ eine Untergruppe von $(\mathcal{P}(X), \triangle)$ ist;

(*ii*) $(\{\sigma \in S_n \mid \operatorname{sgn}\sigma = 1\}, \circ)$ eine Untergruppe von $(S_n, \circ)$ ist.

(b) Es sei $(G, \star)$ eine Gruppe mit neutralem Element e und $(U_i, \star)_{i\in I}$ eine Familie von Untergruppen mit der nichtleeren Indexmenge I. Zeigen Sie Lemma 7.47 des Skripts, also dass dann auch $\bigcap_{i\in I} U_i$ mit $\star$ eine Untergruppe von $(G, \star)$ ist.

(c) Es seien $(G, \star)$ eine Gruppe und $(U_1, \star)$, $(U_2, \star)$ Untergruppen. Zeigen Sie, dass $(U_1 \cup U_2, \star)$ genau dann eine Untergruppe von $(G, \star)$ ist, wenn $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$ ist.

Lösung.

(a) Hier kann man schon anfangen mit dem Untergruppenkriterium zu arbeiten. In diesem Lösungsvorschlag werden wir den Nachweis aber nochmal händisch führen.

(*i*) Tatsächlich ist $\mathcal{P}(A) \subseteq \mathcal{P}(X)$ und für $B_1, B_2 \subseteq A$ ist $B_1 \triangle B_2 \subseteq B_1 \cup B_2 \subseteq A$, also ist $\mathcal{P}(A)$ bezüglich $\triangle$ abgeschlossen. Außerdem ist $\mathcal{P}(A)$ nichtleer, denn es enthält mindestens die leere Menge, also das neutrale Element bezüglich $\triangle$. Dass es sich um eine Gruppe handelt folgt aus den gleichen Überlegungen, wie für die Menge X selbst, also dass die Teilmengen jeweils selbstinvers sind. (0.5 Punkte)

(*ii*) Die angegebene Menge ist eine Untermenge der S_n, das neutrale Element ist außerdem darin enthalten. Die Abgeschlossenheit und die Existenz der Inversen folgt direkt aus der Eigenschaften des Signums in Satz 7.40 (0.5 Punkte)

(b) Da jedes der U_i eine Teilmenge von G ist, ist auch $\bigcap_{i\in I} U_i$ eine Teilmenge von G. (0.5 Punkte)

Alternative 1 für den Nachweis der Gruppeneigenschaft: Wir wenden das Untergruppenkriterium Satz 7.44 aus dem Skript an. Wegen Lemma 7.43 wissen wir, dass die neutralen Elemente der U_i alle mit e übereinstimmen, die Menge $\bigcap_{i\in I} U_i$ enthält also das Element e und ist nichtleer. (0.5 Punkte)

Es seien nun $a, b \in \bigcap_{i\in I} U_i$. Dann ist wegen der Gruppeneigenschaft jeder der U_i und auf Grund von Lemma 7.43 auch das Inverse b' zu b in jedem der U_i und damit in $\bigcap_{i\in I} U_i$. Wegen der Abgeschlossenheit aller U_i ist dann auch $a \star b'$ in U_i für alle $i \in I$ und damit in $\bigcap_{i\in I} U_i$. Nach dem Untergruppenkriterium handelt es sich dann bei $\bigcap_{i\in I} U_i$ mit $\star$ um eine Gruppe. (1 Punkt)

Alternative 2 für den Nachweis der Gruppeneigenschaft: Wir prüfen alle definierenden Eigenschaften. Weiterhin ist $\bigcap_{i\in I} U_i$ bezüglich $\star$ abgeschlossen, denn jedes der U_i ist bzgl.

$\star$ abgeschlossen, also ist für $a, b \in \bigcap_{i\in I} U_i$

$$a \star b \in U_i \; \forall i \in I$$

also $a \star b \in \bigcap_{i\in I} U_i$.

Wegen Lemma 7.43 wissen wir, dass die neutralen Elemente der U_i alle mit e übereinstimmen und die Neutralität überträgt sich direkt auf jedes Element in $\bigcap_{i\in I} U_i$. Hier sehen wir wieder, dass $\bigcap_{i\in I} U_i \neq \emptyset$.

Für $a \in U_i$ existiert jeweils ein U_i-inverses Element a'_{U_i}, die wieder auf Grund von Lemma 7.43 mit dem G-inversen Element a' übereinstimmen, entsprechend ist für $a \in \bigcap_{i\in I} U_i$ auch $a' \in \bigcap_{i\in I} U_i$, also alle Elemente invertierbar. Damit ist $\bigcap_{i\in I} U_i$ mit $\star$ eine Untergruppe.

(c) „$\Leftarrow$“: Wenn $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$ ist, dann ist $U_1 \cup U_2 = U_1$ oder $U_1 \cup U_2 = U_2$, und damit $(U_1 \cup U_2, \star) = (U_1, \star)$ oder $(U_1 \cup U_2, \star) = (U_2, \star)$, was beides Gruppen sind. (0.5 Punkte)

„$\Rightarrow$“: Vorausgesetzt $U_1 \cup U_2$ ist mit $\star$ eine Gruppe, dann wählen wir $u_1 \in U_1$ und $u_2 \in U_2$ beliebig. Wegen der Abgeschlossenheit von $U_1 \cup U_2$ unter $\star$ ist $u_1 \star u_2 \in U_1 \cup U_2$. Ist $u_1 \star u_2 \in U_1$, dann ist auch das zu u_1 inverse Element u'_1 in U_1 und somit $u'_1 \star u_1 \star u_2 = u_2 \in U_1$. Analog erhält man, dass wenn $u_1 \star u_2 \in U_2$ auch $u_1 \in U_2$ ist. Wir haben also gezeigt, dass die folgende Aussage wahr ist:

$$\forall u_1 \in U_1 \, \forall u_2 \in U_2 \; \left((u_1 \in U_1 \wedge u_2 \in U_1) \vee (u_1 \in U_2 \wedge u_2 \in U_2)\right),$$

also insbesondere (denn wir schränken nur die Grundmenge ein, für welche die Aussageform in den Klammern ausgewertet wird)

$$\forall u_1 \in U_1 \setminus U_2 \, \forall u_2 \in U_2 \setminus U_1 \; \underbrace{\left((u_1 \in U_1 \wedge u_2 \in U_1) \vee (u_1 \in U_2 \wedge u_2 \in U_2)\right)}_{\text{immer falsch auf der Grundmenge}}$$

Also muss eine der beiden Differenzmengen leer sein, was genau dann der Fall ist, wenn eine der Mengen eine Teilmenge der anderen ist. (0.5 Punkte)

Alternative 2 für den Beweis der Hinrichtung per Widerspruch: Wenn weder $U_1 \subseteq U_2$ noch $U_2 \subseteq U_1$ gilt, dann gibt es Elemente $u_1 \in U_1 \setminus U_2$ und $u_2 \in U_2 \setminus U_1$. Wäre $U_1 \cup U_2$ eine Untergruppe, dann muss $u_1 \star u_2 \in U_1 \cup U_2$ sein. Ist $u_1 \star u_2 \in U_1$ (wo auch u'_1 liegt), dann ist $u'_1 \star u_1 \star u_2 = u_2 \in U_1$ im Widerspruch zur Annahme. Ist $u_1 \star u_2 \in U_2$ (wo auch u'_2 liegt), dann ist $u_1 \star u_2 \star u'_2 = u_1 \in U_2$ im Widerspruch zur Annahme.

Hausaufgabe I-5.5 (Erzeugung und Ordnung) 1 + 2 = 3 Punkte

Es sei $(G, \cdot)$ eine Gruppe.

Beachte: In dieser Aufgabe werden wir in multiplikativer Notation arbeiten.

(a) Zeigen Sie, dass $\operatorname{ord}(a) = \operatorname{ord}(a^{-1})$.

(b) Die Menge $\{a \cdot b \cdot a^{-1} \cdot b^{-1} \mid a, b \in G\}$ der **Kommutatoren** aus G erzeugt die sogenannte **Kommutatorgruppe** $K(G) \coloneqq \langle \{a \cdot b \cdot a^{-1} \cdot b^{-1} \mid a, b \in G\} \rangle$, eine Untergruppe von $(G, \cdot)$. Zeigen Sie, dass genau dann $(K(G), \cdot) = (\{1\}, \cdot)$ ist, wenn $(G, \cdot)$ abelsch ist.

Lösung.

Beachte: Die multiplikative Notation ist in dieser Aufgabe hauptsächlich für die erste Teilaufgabe gewählt, um eine explizite, abkürzende Darstellung der zyklischen Gruppen zu ermöglichen. Die Resultate sind, wie immer, von der Notation völlig unabhängig.

(a) Ist $\operatorname{ord}(a)$ endlich, dann gibt es also ein $n \in \mathbb{N}$, so dass $e = a^n$. Diese Gleichung kann man nun n-fach mit a^{-1} von links verknüpfen, dann ergibt sich $\left(a^{-1}\right)^n = e$, also $\operatorname{ord}(a^{-1}) \leqslant \operatorname{ord}(a)$. Das gleiche Argument mit vertauschen Rollen liefert die Gleichheit.

Ist $\operatorname{ord}(a)$ nicht endlich, dann kann $\operatorname{ord}(a^{-1})$ nicht endlich sein, denn sonst könnte man mit der obigen Argumentation das Gleiche von $\operatorname{ord}(a)$ zeigen, im Widerspruch zur Annahme.

(1 Punkt)

(b) Wir zeigen erstmal, warum diese Objekte „Kommutatoren“ heißen, nämlich dass für $a, b \in G$ genau dann der Kommutator $a \cdot b \cdot a^{-1} \cdot b^{-1} = 1$ ist, wenn a und b kommutieren, also $a \cdot b = b \cdot a$ ist.

„$\Rightarrow$“: Es seien $a, b \in G$ mit $a \cdot b \cdot a^{-1} \cdot b^{-1} = 1$ gegeben. Dann ist (wir multiplizieren $b \cdot a$ von links mit dem Kommutator $a \cdot b \cdot a^{-1} \cdot b^{-1} = 1$):

$$b \cdot a = \overbrace{a \cdot b \cdot \underbrace{a^{-1} \cdot b^{-1} \cdot b \cdot a}_{1}}^{1} = a \cdot b,$$

„$\Leftarrow$“: Kommutieren a und b, dann ist der Kommutator

$$a \cdot b \cdot a^{-1} \cdot b^{-1} = b \cdot \underbrace{a \cdot a^{-1}}_{1} \cdot b^{-1} = b \cdot 1 \cdot b^{-1} = 1.$$

(1 Punkt)

Den obigen Schritt kann man auch direkt in den verbleibenden Beweis einbauen, dann sieht man aber den Grund für den Begriff Kommutator nicht so schön. Der Rest ergibt sich nun schnell:

„$\Rightarrow$“: Wenn $(K(G), \cdot) = (\{1\}, \cdot)$ ist, dann gilt insbesondere für die Kommutatoren

$$a \cdot b \cdot a^{-1} \cdot b^{-1} = 1 \quad \forall a, b \in G,$$

es kommutieren also alle a und b aus G also ist $(G, \cdot)$ abelsch.

„$\Leftarrow$“: Ist $(G, \cdot)$ abelsch, dann stimmen alle Kommutatoren mit dem neutralen Element überein und die Kommutatorengruppe die zyklische, vom neutralen Element erzeugte Untergruppe von $(G, \cdot)$. Sie besteht damit nur aus dem neutralen Element. (1 Punkt)

Hausaufgabe I-5.6 (Nebenklassen) 2 Punkte

Es sei $(G, \star)$ eine Gruppe und $(U, \star)$ eine Untergruppe. Zeigen Sie den Satz 7.60 von Lagrange, also dass, wenn $(G, \star)$ endlich ist, die Beziehung $\#U \mid \#G$ gilt.

Hinweis: Sie dürfen ohne Beweis verwenden, dass $\#A \cup B = \#A + \#B$ für endliche, disjunkte Mengen A, B gilt.

Lösung.

Nach Folgerung 7.57 des Skripts sind alle Äquivalenzklassen $[\cdot]_{U_\sim}$ gleichmächtig zu U, also $\#[a]_{U_\sim} = \#U$ für alle $a \in G$ und nach Satz 5.25 induziert die Äquivalenzrelation eine Partition von G, G ist also die disjunkte Vereinigung von endlich vielen Teilmengen (den Äquivalenzklassen), die alle die Mächtigkeit $\#U$ haben. Bei der disjunkten Vereinigung addieren sich die Kardinalitäten, daher muss $\#G$ von $\#U$ geteilt werden. Genauer entspricht $\frac{\#G}{\#U}$ genau der Anzahl der Äquivalenzklassen. (2 Punkte)

Bitte reichen Sie Ihre Lösungen der Hausaufgaben als ein PDF auf Mampf ein.