R. Herzog, G. Müller
Universität Heidelberg

Lineare Algebra
Wintersemester 2023

Übung 4 - Lösung

Ausgabedatum: 6. November 2023
Abgabedatum: 12. November 2023

Hausaufgabe 4.1 (Halbgruppen und Monoide) 6 Punkte

(i) Es sei X eine nichtleere Menge. Entscheiden Sie, welche der folgenden Beispiele Halbgruppen bzw. Monoide sind. Begründen Sie Ihre Entscheidung. Geben Sie für Monoide das jeweilige neutrale Element an.

(a) $(\mathbb{R}^X, +)$	(b) $(\mathbb{R}^X, \cdot)$	(c) $\left(\mathbb{Z} \setminus \{0\}, (a, b) \mapsto \frac{a}{b}\right)$
(d) $(\mathcal{P}(X), \cap)$	(e) $(\mathcal{P}(X), \cup)$	(f) $(\mathcal{P}(X), \setminus)$
(g) $(\mathcal{P}(X), \triangle)$	(h) $(X^X, \circ)$	

(ii) Wir erweitern die Definition 7.6 des Skripts für eine Halbgruppe $(H, \star)$ wie folgt:
Ein Element $e_\ell \in H$ heißt **linksneutrales Element** von $(H, \star)$, wenn $e_\ell \star x = x \; \forall x \in H$ gilt.
Ein Element $e_r \in H$ heißt **rechtsneutrales Element** von $(H, \star)$, wenn $x \star e_r = x \; \forall x \in H$ gilt.

Zeigen Sie:

(a) I. A. sind linksneutrale Elemente nicht eindeutig. Das Gleiche gilt für rechtsneutrale Elemente.

(b) Wenn in einer Halbgruppe $(H, \star)$ ein linksneutrales Element e_ℓ und ein rechtsneutrales Element e_r existieren, dann stimmen beide überein und sind ein neutrales Element mit dem $(H, \star)$ ein Monoid ist.

Lösung.

(i) Für jedes Paar aus einer Menge und einer Abbildung ist für die Halbgruppeneigenschaft zu prüfen, ob die Abbildung eine Verknüpfung ist und ob diese assoziativ ist. Ob es sich bei einem

Paar um ein Monoid handelt, ist gleichbedeutend mit der Frage, ob ein neutrales Element bzgl. der angegebenen Verknüpfung existiert.

Die Angaben der Abbildungen müssen zu einem gewissen Grad aus dem Kontext interpretiert werden. Z. B. ist mit der „+“ Verknüpfung auf Funktionen die punktweise Addition gemeint, das kann man aber natürlich auch falsch verstehen und argumentieren, dass man in die reelle Addition keine Funktionen stecken kann. Wir versuchen hier immer den „best case“ zu untersuchen, also versuchen alles daran zu setzen, Halbgruppen zu erhalten.

(a) Das Paar $(\mathbb{R}^X, +)$ bezeichnet die Menge aller Funktionen aus der nichtleeren Menge X nach $\mathbb{R}$ wobei „+“ die punktweise Addition der Funktionen bzw. ihrer Funktionswerte ist. Für Funktionen f, g aus $\mathbb{R}^X$ liefert die Abbildung $(f, g) \mapsto f + g$ also wieder eine Funktion aus $\mathbb{R}^X$, die Abbildung „+“ ist also eine **Verknüpfung** auf $\mathbb{R}^X$. Sie erbt die **Assoziativität** von der Addition in den reellen Zahlen. Bei diesem Beispiel handelt es sich also um eine **Halbgruppe**. Die konstante Nullfunktion ist weiterhin ein **neutrales Element** bzgl. der punktweisen Addition, entsprechend handelt es sich sogar um ein **Monoid**. (0.5 Punkte)

(b) Bei dem Paar $(\mathbb{R}^X, \cdot)$ besteht die Grundmenge, wie im vorherigen Beispiel, aus der Menge aller Funktionen aus der nichtleeren Menge X nach $\mathbb{R}$ wobei „·“ die punktweise Multiplikation der Funktionen bzw. ihrer Funktionswerte ist. Für Funktionen f, g aus $\mathbb{R}^X$ liefert die Abbildung $(f, g) \mapsto f \cdot g$ also wieder eine Funktion aus $\mathbb{R}^X$, die Abbildung „·“ ist also eine **Verknüpfung** auf $\mathbb{R}^X$. Sie erbt die **Assoziativität** von der Multiplikation in den reellen Zahlen. Bei diesem Beispiel handelt es sich also um eine **Halbgruppe**. Die konstante Einsfunktion ist weiterhin ein **neutrales Element** bzgl. der punktweisen Multiplikation, entsprechend handelt es sich sogar um ein **Monoid**. (0.5 Punkte)

(c) Das Paar $\big(\mathbb{Z} \setminus \{0\}, (a, b) \mapsto \frac{a}{b}\big)$ können wir nur sinnvoll interpretieren, wenn wir „$(a, b) \mapsto \frac{a}{b}$“ als Abbildung in die rationalen Zahlen bzw. die Menge aller Brüche verstehen, womit der Bildbereich der Abbildung die Grundmenge $\mathbb{Z} \setminus \{0\}$ verlässt, da z. B. $(1, 2) \mapsto \frac{1}{2} \notin \mathbb{Z} \setminus \{0\}$. Es handelt sich bei der Abbildung also um **keine Verknüpfung** und damit haben wir keine Halbgruppe und entsprechend kein Monoid vorliegen. (0.5 Punkte)

(d) In dem Paar $(\mathcal{P}(X), \cap)$ bildet der Mengenschnitt zwei Mengen aus $\mathcal{P}(X)$ wieder auf eine Menge in $\mathcal{P}(X)$ ab, es handelt sich also um eine **Verknüpfung** auf $\mathcal{P}(X)$. Dass die Schnittoperation für Mengen assoziativ ist, folgt sofort aus der Assoziativität des logischen $\wedge$ und ist in dieser Veranstaltung bereits mehrfach thematisiert worden, wir haben haben also eine **Halbgruppe** vorliegen. Das neutrale Element bzgl. des Schnitts auf $\mathcal{P}(X)$ ist die Menge X selbst, wir haben also sogar ein **Monoid**. (0.5 Punkte)

(e) In dem Paar $(\mathcal{P}(X), \cup)$ bildet die Mengenvereinigung zwei Mengen aus $\mathcal{P}(X)$ wieder auf eine Menge in $\mathcal{P}(X)$ ab, es handelt sich also um eine **Verknüpfung** auf $\mathcal{P}(X)$. Dass die Vereinigungsoperation für Mengen assoziativ ist folgt sofort aus der Assoziativität des logischen $\vee$ und ist in dieser Veranstaltung bereits mehrfach thematisiert worden, wir haben haben also eine **Halbgruppe** vorliegen. Das neutrale Element bzgl. der Vereinigung auf $\mathcal{P}(X)$ ist die leere Menge, wir haben also sogar ein **Monoid**. (0.5 Punkte)

(f) In dem Paar $(\mathcal{P}(X), \setminus)$ bildet die Mengendifferenz zwar zwei Mengen aus $\mathcal{P}(X)$ wieder auf eine Menge in $\mathcal{P}(X)$ ab und ist damit eine **Verknüpfung** auf $\mathcal{P}(X)$, dass diese Operation jedoch nicht assoziativ ist, wissen wir aus Hausaufgabe 2.2. Hier liegt also **keine Halbgruppe** vor. (0.5 Punkte)

(g) Bei dem Paar $(\mathcal{P}(X), \triangle)$ bildet die symmetrische Differenz Mengen aus $\mathcal{P}(X)$ auf eine Menge in $\mathcal{P}(X)$ ab, es handelt sich also um eine **Verknüpfung**. Die Verknüpfung ist sogar assoziativ, was wir bisher aber noch nicht gesehen haben, weshalb es hier noch kurz bewiesen wird.

Es seien dafür Mengen A, B, C gegeben. Zur Erinnerung, die symmetrische Differenz war definiert als $A \triangle B \coloneqq A \setminus B \cup B \setminus A$, was uns die folgende Gleichungskette liefert:

$$\begin{aligned}
(A \triangle B) \triangle C &= (A \setminus B \cup B \setminus A) \triangle C && \text{(Definition)}\\
&= (A \setminus B \cup B \setminus A) \setminus C \;\cup\; C \setminus (A \setminus B \cup B \setminus A) && \text{(Definition)}\\
&= A \setminus (B \cup C) \;\cup\; B \setminus (A \cup C) \;\cup\; C \setminus (A \cup B) && \text{(Split der A,B-Teile)}\\
&= A \setminus (B \setminus C \cup C \setminus B) \;\cup\; (B \setminus C \cup C \setminus B) \setminus A && \text{(Gruppieren der B,C Teile)}\\
&= A \setminus (B \triangle C) \;\cup\; (B \triangle C) \setminus A && \text{(Definition)}\\
&= A \triangle (B \triangle C). && \text{(Definition)}
\end{aligned}$$

Das zeigt, dass wir hier tatsächlich eine **Halbgruppe** vorliegen haben. Das neutrale Element ist hier wieder die leere Menge, wir haben also sogar ein **Monoid**. (0.5 Punkte)

(h) Das Paar $(X^X, \circ)$ beschreibt die Menge aller Funktionen $f : X \to X$ mit der Komposition, die eine **Verknüpfung** auf X^X darstellt. Die Assoziativität ist für die Verknüpfung klar, denn für $f, g, h \in X^X$ ist für alle $x \in X$:

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

hier liegt also wieder eine **Halbgruppe** vor und das neutrale Element $\mathrm{id} \in X^X$ zeigt, dass wir sogar ein **Monoid** haben. (0.5 Punkte)

(ii) (a) Für jede Menge X mit mindestens zwei Elementen können wir $\star : X \times X \to X$ durch $(x, y) \mapsto y$ (die „Rechtsauswahl") definieren. Diese ist eine Verknüpfung auf X und assoziativ, denn es ist für x, y, z aus X immer

$$(x \star y) \star z = y \star z = z = x \star z = x \star (y \star z).$$

Entsprechend ist das so definierte $(X, \star)$ eine Halbgruppe und da $x \star y = y \forall x, y \in X$ gilt ist jedes Element aus X linksneutral. Um zu zeigen, dass rechtsneutrale Elemente nicht eindeutig sind, definiert man analog die Linksauswahl und erhält, dass jedes Element rechtsneutral ist. (1 Punkt)

(b) Es seien $(H, \star)$ eine Halbgruppe, e_ℓ ein linksneutrales Element und e_r ein rechtsneutrales Element. Dann ist

$$e_\ell \overset{e_r \text{ rechtsneutral}}{=} e_\ell \star e_r \overset{e_\ell \text{ linksneutral}}{=} e_r.$$

Entsprechend ist $e := e_\ell = e_r$ ein links- und rechtsneutrales Element und damit ein neutrales Element – welches auf Grund von Lemma 7.7 des Skripts eindeutig ist – und $(H, \star)$ mit e ein Monoid. (1 Punkt)

Beachte: Dieser Punkt zeigt direkt, dass eine Halbgruppe keine Monoid sein kann, wenn mehrere links- bzw. rechtsinverse Elemente existieren.

Hausaufgabe 4.2 (Invertierbarkeit) 3 Punkte

Wir erweitern die Definition 7.11 des Skripts für eine Halbgruppe $(H, \star)$ mit neutralem Element e wie folgt:

Ein Element $a \in H$ heißt **linksinvertierbar**, wenn ein $b_\ell \in H$ existiert mit $b_\ell \star a = e$. In diesem Fall heißt b_ℓ ein **linksinverses Element** zu a.

Ein Element $a \in H$ heißt **rechtsinvertierbar**, wenn ein $b_r \in H$ existiert mit $a \star b_r = e$. In diesem Fall heißt b_r ein **rechtsinverses Element** zu a.

Es sei $(H, \star)$ eine Halbgruppe. Zeigen Sie:

(i) I. A. sind linksinverse Elemente nicht eindeutig. Das Gleiche gilt für rechtsinverse Elemente.

(ii) Wenn a aus H links- und rechtsinvertierbar ist, dann ist a invertierbar und jedes links- oder rechtsinverses Element zu a gleicht dem eindeutigen Inversen von a.

Lösung.

(i) Wir betrachten als Beispiel $(\mathbb{N}^\mathbb{N}, \circ)$, also die Halbgruppe der Funktionen von $\mathbb{N}$ nach $\mathbb{N}$ mit der Komposition. Diese bildet mit dem neutralen Element id ein Monoid, es ist aber nicht jedes Element invertierbar, denn nicht alle Elemente sind injektiv und surjektiv zugleich. Wir können für eine nicht injektive aber surjektive Funktion verschiedene Rechtsinverse konstruieren, z. B. besitzt die surjektive aber nicht injektive Funktion $f(n) := \max(1, n-1)$ die beiden Rechtsinversen

$$f_1^{-R}(n) := n+1 \qquad \text{und} \qquad f_2^{-R}(n) := \begin{cases} 1 & n = 1 \\ n+1 & n \neq 1 \end{cases}$$

mit $f \circ f_1^{-R} = f \circ f_2^{-R} = \mathrm{id}$.

Außerdem kann man für die nicht surjektive aber injektive Funktion $f(n) := n+1$ die abzählbar unendliche Familie von linksinversen Funktionen f_m^{-L} in Abhängigkeit vom Index $m \in \mathbb{N}$ angeben:

$$f_m^{-L}(n) := \begin{cases} m & n = 1 \\ n-1 & n \neq 1 \end{cases}.$$

(2 Punkte)

(ii) Es sei $a \in H$ links- sowie rechtsinvertierbar und $a^{-\ell}$ und a^{-r} ein linksinverses bzw. ein rechtsinverses Element für a. Dann ist

$$a^{-\ell} = a^{-\ell} \star \underbrace{e}_{a \star a^{-r}} = \underbrace{a^{-\ell} \star a}_{e} \star a^{-r} = a^{-r},$$

es stimmen also alle links- und alle rechtsinversen Elemente überein (Eindeutigkeit) und sind damit links- und rechtsinverse von a, also Inverse zu a. (1 Punkt)

Beachte: Der obige Beweis unterscheidet sich kaum vom Beweis von Lemma 7.12 des Skripts.

Hausaufgabe 4.3 (Gruppen) 10 Punkte

(i) Entscheiden Sie, welche der Beispiele aus Hausaufgabe 4.1 Teil (i) Gruppen sind. Begründen Sie Ihre Entscheidung.

(ii) Es sei $(H, \star)$ ein Monoid. Zeigen Sie, dass die Einheitengruppe

$$E(H, \star) := \{a \in H \mid a \text{ ist invertierbar}\} \tag{7.7}$$

von $(H, \star)$ mit der Verknüpfung $\star$ tatsächlich eine Gruppe ist.

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

$$A \mathbin{\tilde{\star}} B := \{a \star b \mid a \in A \land b \in B\} \quad \text{für } A, B \in \mathcal{P}(G).$$

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

(iv) Zeigen Sie die folgenden Aussagen (Lemma 7.18 des Skripts):

(a) Ist $(G, \star)$ eine Gruppe und ist $a \in G$ beliebig, so sind die Rechts- und Linkstranslation $\star_a$ und ${}_a\star$ bijektive Abbildungen $G \to G$.

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

Lösung.

(i) In Frage kommen nur die Monoide, also die Paare (a), (b), (d), (e), (g) und (h).

(a): 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)

(b): Für $(\mathbb{R}^X, \cdot)$ mit der konstanten Einsfunktion besitzt bspw. die konstante Nullfunktion kein Inverses, hier liegt also **keine Gruppe** vor. (0.5 Punkte)

(d): 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)

(e): Für $(\mathcal{P}(X), \cup)$ mit der leeren Menge als neutralem Element ist lediglich $\emptyset$ invertierbar, hier liegt also **keine Gruppe** vor. (0.5 Punkte)

(g) : 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)

(h): Für $(X^X, \circ)$ mit der Identität als neutralem Element ist jede nicht bijektive Funktion nicht invertierbar, hier liegt also **keine Gruppe** vor. (0.5 Punkte)

(ii) Die Operation $\star$ ist auf $E(H, \star)$ tatsächlich eine Verknüpfung, denn für $a, b \in E(H, \star)$ ist auch $a \star b$ invertierbar (mit inversem Element $(a \star b)' = b' \star a'$).

Die Verknüpfung bleibt natürlich assoziativ auf $E(H, \star)$, damit ist $E(H, \star)$ mit $\star$ schonmal eine Halbgruppe. (0.5 Punkte)

Wir bezeichnen das neutrale Element des Monoids wieder mit e. Da e selbstinvers ist, ist auch $e \in E(H, \star)$ und dort auch neutral. Damit liegt schonmal ein Monoid vor. (0.5 Punkte)

Jedes Element a aus $E(H, \star)$ besitzt nun ein $\star$-inverses Element a' in H. Da dieses a' auch ein Inverses in H besitzt (nämlich a) ist auch a' in $E(H, \star)$ und somit ist jedes a aus $E(H, \star)$ auch in $E(H, \star)$ bzgl. $\star$ invertierbar. Somit liegt eine Gruppe vor. (0.5 Punkte)

(iii) 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

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

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 $A \in \mathcal{P}(G)$:

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

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.

(iv) Aussage (a): 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 (7.10b), dass $x_1 = x_2$ gelten muss, also ist $\star_a$ auch injektiv. (1 Punkt)

Für die Linkstranslation argumentieren wir entsprechend.

Aussage (b): 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 4.1 wissen wir, dass dieses Element (wir nennen es ab jetzt e) eindeutig ist und ein neutrales Element für den Monoid. (1.5 Punkte)

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 Inverse zu a, das nach Lemma 7.12 des Skripts eindeutig ist. (1 Punkt)

Hausaufgabe 4.4 (Kommutativität) 4 Punkte

(i) Entscheiden Sie, welche Beispiele aus Hausaufgabe 4.1 Teil (i) abelsche Gruppen sind. Begründen Sie Ihre Entscheidung.

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

Lösung.

(i) In Frage kommen nur die Gruppen aus Hausaufgabe 4.3, 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)

(ii) **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 7.18 des Skripts und Satz 6.27, 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 $\star a$ 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 $a \star b \neq b \star a$, dan 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 4.5 (Symmetrische Gruppe) 3 Punkte

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

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

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

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

(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, dann ergibt sich die folgende Kette von Umformungen:

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

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

$$= \tau(6,1) \circ \tau(5,2) \circ \tau(4,3) \circ \tau(6,4) \circ \tau(7,5) \circ \tau(8,7)$$

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:

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

Tauscht man die größeren Zahlen zuerst ergibt sich ganz analog Zerlegungen. (1.5 Punkte)

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. (0.5 Punkte)

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