Übung 5 - Lösung

Ausgabedatum: 13. November 2023
Abgabedatum: 19. November 2023

Hausaufgabe 5.1 (Untergruppen) 5 Punkte

(i) Beweisen oder widerlegen Sie, dass

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

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

(ii) Es sei $(U, \star)$ eine Untergruppe der Gruppe $(G, \star)$. Zeigen Sie Lemma 7.32 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.

(iii) 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 7.35 des Skripts, also dass dann auch $\bigcap_{i \in I} U_i$ mit $\star$ eine Untergruppe von $(G, \star)$ ist.

(iv) 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.

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

(a) 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. (0.5 Punkte)

(b) 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. (0.5 Punkte)

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

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

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.

(ii) 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 (7.10b) des Skripts für die Gruppe $(G, \star)$ folgt dann $e = e_U$. (0.5 Punkte)

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 (aufgrund von den Rechenregeln für Inverse (7.11b)) also $a'_U = a'$. (0.5 Punkte)

(iii) 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 7.33 aus dem Skript an. Wegen Lemma 7.32 bzw. Punkt (ii) 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 7.32 bzw. Punkt (ii) 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 7.32 bzw. Punkt (ii) 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 7.32 bzw. Punkt (ii) 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.

(iv) „$\Leftarrow$": 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:

$$\forall u_1 \in U_1 \, \forall u_2 \in U_2 \; \big((u_1 \in U_1 \land u_2 \in U_1) \lor (u_1 \in U_2 \land u_2 \in U_2)\big)\,,$$

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

$$\forall u_1 \in U_1 \setminus U_2 \, \forall u_2 \in U_2 \setminus U_1 \; \underbrace{\big((u_1 \in U_1 \land u_2 \in U_1) \lor (u_1 \in U_2 \land u_2 \in U_2)\big)}_{\text{immer falsch auf der Grundmenge}}$$

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 5.2 (Erzeugung und Ordnung) 3 Punkte

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

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

(i) 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.

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

(iii) Die Menge $\{a \cdot b \cdot a^{-1} \cdot b^{-1} \mid a, b \in G\}$ der **Kommutatoren** aus G erzeugt die sogenannte **Kommutatorgruppe** $K(G) := \langle \{a \cdot b \cdot a^{-1} \cdot b^{-1} \mid a, b \in G\} \rangle$, 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.

(i) Die Darstellung in der Aussage ist exakt die Darstellung in Satz 7.37 des Skripts, also der Darstellung von erzeugten Untergruppen, wenn die erzeugende Menge nur ein Element beinhaltet. (0.5 Punkte)

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 $a^z = a^{z \mod \operatorname{ord}(a)}$, 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). (1 Punkt)

(ii) 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

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

(0.5 Punkte)

(iii) 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 $a \cdot b \cdot a^{-1} \cdot b^{-1} = 1$):

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

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

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

(0.5 Punkte)

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. (0.5 Punkte)

Hausaufgabe 5.3 (Nebenklassen) 2 Punkte

Es sei $(G, \star)$ eine Gruppe und $(U, \star)$ eine Untergruppe.

(i) Zeigen Sie Folgerung 7.41 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.

(ii) Zeigen Sie den Satz 7.43 von Lagrange, also dass, wenn $(G, \star)$ endlich ist, die Beziehung $\#U \mid \#G$ gilt, also, dass die Kardinalität der Untergruppe ein Teiler der Kardinalität der Gruppe ist.

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

Lösung.

(i) 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

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

(0.5 Punkte)

(ii) Nach Lemma 7.40 des Skripts sind alle Äquivalenzklassen $[\cdot]_{{}^U\!\sim}$ gleichmächtig zu U, also $\#[a]_{{}^U\!\sim} = \#U$ für alle $a \in G$ und nach Satz 5.19 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. (1.5 Punkte)

Hausaufgabe 5.4 (Homomorphismen, Bild und Kern) 6 Punkte

(i) Entscheiden Sie, welche der unten stehenden Abbildungen Homomorphismen, Endomorphismen, Isomorphismen bzw. Automorphismen sind. Begründen Sie Ihre Antwort. Bestimmen Sie für die Gruppenhomomorphismen außerdem Bild und Kern.

(a) $f\colon (\mathbb{R}, \cdot) \to (\mathbb{R}, +),\ f(x) := 2^x$ (b) $f\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot),\ f(x) := 2^x$

(c) $f\colon (\mathcal{P}(\mathbb{Z}), \cup) \to (\mathcal{P}(\mathbb{Z}), \cap),\ f(A) := \mathbb{Z} \setminus A$ (d) $f\colon (\mathbb{N}, \max(\cdot, \cdot)) \to (\mathbb{N}, +),\ f(n) := 2\,n$

(e)[1] $f\colon (\mathbb{Z}_m, +_m) \to (\mathbb{Z}_m, +_m),\ f(z) := m\,z$

(ii) Es sei f ein (Halbgruppen-, Monoid-, Gruppen-)isomorphismus von $(G_1, \star)$ nach $(G_2, \square)$. Zeigen Sie, dass dann auch f^{-1} ein solcher Isomorphismus von $(G_2, \square)$ nach $(G_1, \star)$ ist.

(iii) Es seien $(G_1, \star)$ und $(G_2, \square)$ zwei isomorphe Gruppen. Zeigen Sie, dass $(G_1, \star)$ genau dann abelsch ist, wenn $(G_2, \square)$ abelsch ist.

Lösung.

(i) (a) Die Beziehung

$$f(x \cdot y) = 2^{x \cdot y} = 2^x + 2^y = f(x) + f(y)$$

gilt nicht für beliebige $x, y \in \mathbb{R}$, denn z. B. für $x = 1$, $y = 2$ erhält man

$$f(1 \cdot 2) = 2^{1 \cdot 2} = 4 \neq 5 = 2^1 + 2^2 = f(1) + f(2).$$

Die multiplikative Struktur links und die additive Struktur rechts wird also von Exponentialfunktionen nicht erhalten. Diese Art von Struktur wird von den Logarithmusfunktionen erhalten (deren Umkehrfunktionen). Es handel sich also **nichtmal** um einen **Homomorphismus**. (0.5 Punkte)

(b) Die im Vergleich zu Beispiel (a) vertauschten Strukturen links und rechts sind mit der Exponentialfunktion wiederum verträglich, denn es gilt für alle $x, y \in \mathbb{R}$

$$f(x + y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y).$$

Da sowohl $(\mathbb{R}, +)$ als auch $(\mathbb{R}_{>0}, \cdot)$ Gruppen sind, handelt es sich also schonmal um einen **Gruppenhomomorphismus**. Da diese verschieden sind, liegt **kein Endomorphismus**

[1] Diese Teilaufgabe war ursprünglich unter Verwendung von Notation formuliert, die erst in der Woche 06 eingeführt wird. Ich habe Sie so angepasst, dass die Idee der Aufgabe erhalten bleibt aber schon bekannte Notation verwendet wird.[GM]

und damit kein Automorphismus vor. Da f auf Grund des eingeschränkten Bildbereichs bijektiv ist, handelt es sich allerdings um einen **Gruppenisomorphismus**. Der Bildbereich ist damit natürlich $\text{Bild}(f) = \mathbb{R}_{>0}$. Der Kern ist das Urbild des neutralen Elements in der Zielgruppe, also auf Grund der Bijektivität $\text{Kern}(f) = f^{-1}(\{1\}) = \{0\}$. (1 Punkt)

(c) Bei $(\mathcal{P}(\mathbb{Z}), \cup)$ und $(\mathcal{P}(\mathbb{Z}), \cap)$ handelt es sich um zwei verschiedene Monoide (mit den neutralen Elementen $\emptyset$ respektive $\mathbb{Z}$, jedoch nicht im Gruppen. Dass die Komplementbildung strukturerhaltend sind, also, dass

$$\mathbb{Z} \setminus (A \cup B) = (\mathbb{Z} \setminus A) \cap (\mathbb{Z} \setminus B),$$

ist genau die Aussage der de Morganschen Regeln in Lemma 4.5 des Skripts. Hier sehen wir sofort, dass es nicht ausschlaggebend ist, dass die Grundmenge für die Potenzmenge $\mathbb{Z}$ ist. Für Monoide fordern wir zusätzlich, dass die neutralen Elemente aufeinander abgebildet werden, bei den neutralen Elementen $\mathbb{Z}$ und $\emptyset$ unter Komplementbildung genau der Fall ist. Die Komplementbildung von der Potenzmenge in die Potenzmenge ist bijektiv (jede Teilmenge von $\mathbb{Z}$ ist eindeutig über ihr Komplement bestimmt), wir haben also einen **Monoidisomorphismus**. (1 Punkt)

(d) Bei $(\mathbb{N}, \max(\cdot, \cdot))$ handelt es sich um eine Halbgruppe, denn die Maximumsbildung in den natürlichen Zahlen ist eine assoziative Verknüpfung. Das neutrale Element bezüglich der Maximumsbildung ist die 1, hier liegt also ein Monoid vor. $(\mathbb{N}, +)$ ist eine bekannte Halbgruppe ohne neutrales Element, uns bleibt also nur zu prüfen, ob wir es mit einem Halbgruppenhomomorphismus (oder -isomorphismus) zu tun haben. Da für alle $n, m \in \mathbb{N}$ gilt, dass

$$f(\max(n, m)) = 2\max(n, m) = \max(2n, 2m) \neq 2n + 2m = f(n) + f(m)$$

handelt es sich hier um **keinen Homomorphismus**. (0.5 Punkte)

(e) Definitions- und Zielbereich sind tatsächlich Gruppen und da auf Grund der Kommutativität der Moduloaddition

$$f(a +_m b) = m(a +_m b) = ma +_m mb = f(a) + f(b)$$

gilt, haben wir auch tatsächlich einen Gruppenhomomorphismus und auf Grund gleicher Definitions- und Zielmenge sogar einen **Endomorphismus** vorliegen. Allerdings ist wegen $mz = \underbrace{z +_m \cdots +_m z}_{m\text{-Mal}} = 0$ auch klar, dass alle Elemente auf das Element 0 abgebildet werden, der Kern ist also ganz Z_m, und das Bild besteht lediglich aus $\{0\}$. Damit liegt offensichtlich **kein Automorphismus** vor. (1 Punkt)

(ii) Jede bijektive Funktion $f\colon (G_1, \star) \to (G_2, \square)$ ist natürlich invertierbar und ihre Umkehrfunktion ist bijektiv. Wenn sowohl der Definitions- als auch der Zielbereich die Halbgruppen-, Monoid-oder Gruppenstruktur hat, dann gilt das auch für die Umkehrfunktion f^{-1}. Für $a, b \in G_2$ ist dann

$$\begin{aligned} f^{-1}(a \mathbin{\square} b) &= f^{-1}\big(f(f^{-1}(a)) \mathbin{\square} f(f^{-1}(b))\big) \\ &= f^{-1}\big(f(f^{-1}(a) \star f^{-1}(b))\big) \\ &= f^{-1}(a) \star f^{-1}(b). \end{aligned}$$

Für Monoide haben wir zusätzlich gefordert, dass die inversen Elemente aufeinander abgebildet werden, was f nach Voraussetzung erfüllt und f^{-1} auf Grund der Bijektivität ebenfalls. (1 Punkt)

(iii) Es sei $f\colon (G_1, \star) \to (G_2, \square)$ ein Isomorphismus und $(G_2, \square)$ abelsch. Es seien weiter $a, b \in (G_1, \star)$ gegeben. Dann ist

$$\begin{aligned} a \star b &= f^{-1}(f(a \star b)) && \text{(Invertierbarkeit von } f\text{)} \\ &= f^{-1}(f(a) \mathbin{\square} f(b)) && \text{(Strukturerhaltung von } f\text{)} \\ &= f^{-1}(f(b) \mathbin{\square} f(a)) && \text{(Kommutativität in } (G_2, \square)\text{)} \\ &= f^{-1}(f(b \star a)) && \text{(Strukturerhaltung von } f\text{)} \\ &= b \star a. \end{aligned}$$

Die Gegenrichtung, für kommutatives $(G_1, \star)$, folgt analog mit vertauschten Rollen von $(G_1, \star)$ und $(G_2, \square)$ für eine entsprechende Bijektion. (1 Punkt)

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