LA Zettel 5

Aufgabe 1

Entscheiden, ob die Beispiele aus Aufgabe 4. Gruppen sind.
(i): Der Monoid $(\mathbb{R}^X, +)$ ist eine Gruppe, das invers kann punktweise gebildet werden: Für alle $g \in \mathbb{R}^X$ gilt $g^{-1}(x) = -g(x)$ und damit $g(x) + g^{-1}(x) = g(x) - g(x) = 0$

(ii): Der Monoid $(\mathcal{P}(\mathcal{X}), \cap)$ ist keine Gruppe, weil alle Elemente (außer X) kein Inverses besitzen, da für alle $a, b \in \mathcal{P}(\mathcal{X})$ gilt:

$$a \cap b \Rightarrow a = b = X$$

TODO genauer
(iii): Der Monoid $(\mathcal{P}(\mathcal{X}), \triangle)$ ist eine Gruppe, da jedes Element invertierbar ist. Für alle $x \in \mathcal{P}(\mathcal{X})$ gilt $x^{-1} = x$, da

$$x \triangle x = (x \setminus x \cup x \setminus x) = \emptyset \cup \emptyset = \emptyset$$

(IV): Der Moniod $(X^X, \circ)$ ist im allgemeinen (für $\#X > 1$) keine Gruppe, da nicht alle Funktionen $f : X \to X$ invertierbar sind (Ein gutes Beispiel dafür sind konstante Funktionen) und damit nicht alle Elemente des Monoids ein inverses Element besitzen.

(V): Der Monoid $(\mathbb{Z}^2, ((x_1, x_2), (y_1, y_2)) \mapsto (x_1 \cdot y_1, x_2 + y_2)))$ ist keine Gruppe, da nicht alle Elemente invertierbar sind. Zum Beispiel das Element $(2, 2)$. Es müsste ein Element $(x_1, x_2) \in \mathbb{Z}^2$ geben, sodass $x_1 * 2 = 1$ und $x_2 + 2 = 0$. Ein solches x_1 gibt es allerdings nicht in $\mathbb{Z}$

b)

$(\mathcal{P}(\mathcal{G}), \tilde{\star})$ ist keine Gruppe. Sei G die gruppe der ganzen Zahlen $\mathbb{Z}$ mit der addition $+$. Die Menge $\{0\} \in \mathcal{P}(\mathbb{Z})$ wäre das Neutrale Element der Gruppe $(\mathcal{P}(\mathcal{G}), \tilde{\star})$, da

$$\{a + 0 \mid a \in A\} = A \quad \forall A \in \mathcal{P}(\mathbb{Z})$$

Es sind aber nicht alle Elemente der Gruppe $(\mathcal{P}(\mathbb{Z}), \tilde{+})$ invertierbar, da

$$a + b = a + c \Rightarrow b = c \quad \forall abc \in \mathbb{Z}$$

Wenn wir also eine Beliebige Menge $A \in \mathcal{P}(\mathbb{Z})$ mit $\#A > 1$ punktweise mit einer einelementigen Menge $\{c\}$ addieren, dann gilt $\#(A \tilde{+} \{c\}) = \#A$.
Für eine Menge $B \in \mathcal{P}(\mathbb{Z})$ mit $B = C \cup D$ gilt $A \tilde{+} B = A \tilde{+} C \cup A \tilde{+} D$. Daraus folgt, dass die Kardinalität von A durch die Punktweise Addition einer anderen Menge nur steigen kann:
Sei $B \in \mathcal{P}(\mathbb{Z})$ mit $B = \{c\} \cup D$:

$$\#(A \tilde{+} B) = \#(A \tilde{+} \{c\} \cup A \tilde{+} D) \geq \#(A \tilde{+} \{c\}) = \#A$$

Da das neutrale Element die Menge $\{0\}$ ist, gibt es für alle Mengen $A \in \mathcal{P}(\mathbb{Z})$ mit $\#A > 1$ kein inverses Element, da es dafür eine Menge $B \in \mathcal{P}(\mathbb{Z})$ geben müsste, sodass $\#(A \tilde{+} B) = 1$, was aber nicht möglich ist.

Notitz: Oben wurde angenommen, dass $\#B \geq 1$. Falls $B = \emptyset$ gilt $A \tilde{+} \emptyset = \emptyset$. Damit kann $\emptyset$ auch nicht das inverse Element von A sein. $\emptyset$ kann auch nicht das neutrale Element sein, da $A \tilde{+} \emptyset = \emptyset \neq A$

c)

Lemma 0.1: Ist $(G, \star)$ eine Gruppe, dann sind alle Links- und Rechtstranslationen ${}_a{*}$ und $\star_a$ bijektionen für alle $a \in G$.

Proof: Für alle $a \in G$ ist zu zeigen:
Die Funktion ${}_a{*} : G \to G := x \mapsto a \star x$ ist invertierbar.
Die inverse Funktion von ${}_a{*}$ ist gegeben durch ${}_{a^{-1}}{*}$, da: $a \star (a^{-1} \star x) = x$ und $a^{-1} \star (a \star x) = x$ für alle $x \in G$ gilt und a^{-1} aufgrund der Gruppenstruktur exsitiert.
Das selbe gilt für die Rechtstranslation: Das Inverse der Funktion $\star_a$ ist gegeben durch $\star_{a^{-1}}$, da $(x * a) * a^{-1} = x$ und $(x * a^{-1}) * a = x$ für alle $x \in G$. ■

Lemma 0.2: Sei $(H, \star)$ eine nichtleere Halbgruppe. Wenn für alle $a \in H$, die Links- und Rechtstranslationen ${}_a{*}$ und $\star_a$ surjektive Abbildungen sind, dann ist $(H, \star)$ eine Gruppe.

Proof:

Aufgrund der Surjektivität der Links- und Rechtstranslationen wissen wir:

$$\forall a, x \in H, \exists y \in H, a * y = x$$

$$\forall a, x \in H, \exists y \in H, y * a = x$$

Zu zeigen $\exists e \in H, \star_e = {}_e{\star} = \mathrm{id}_H$ test −−

■

Aufgabe 4

Es sei $(G, *)$ eine Gruppe.

Lemma 0.3: $\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$

Proof: Fall 1: $\operatorname{ord}(a)$ ist endlich: Sei $n = \operatorname{ord}(a)$. Es gilt $a^n = 1$.
Außerdem gilt

$$1 = a^n * \left(a^{-1}\right)^n = 1 * \left(a^{-1}\right)^n = \left(a^{-1}\right)^n$$

Daraus folgt, dass $\operatorname{ord}(a^{-1})$ maximal n ist. Im Folgenden zeigen wir, dass $\operatorname{ord}(a^{-1})$ mindestens n ist.

Sei also $\operatorname{ord}(a^{-1}) = m$ für ein $m < n$. Dann gilt $\left(a^{-1}\right)^m = 0$ und

$$1 = a^m * \left(a^{-1}\right)^m = a^m * 1 = a^m$$

Da $\operatorname{ord}(a) > m$ ist dies ein Widerspruch.

Fall 2: $\operatorname{ord}(a)$ ist unendlich, d.h. es gibt kein $n \in \mathbb{N}$, sodass $a^n = 1$.
Wir zeigen nun durch einen Widerspruch, dass $\operatorname{ord}(a^{-1})$ auch unendlich sein muss.
Sei also $\left(a^{-1}\right)^m = 1$ für ein $m \in \mathbb{N}$. Dann gilt für alle $n > m$:

$$1 = a^n * \left(a^{-1}\right)^n = a^n * \left(a^{-1}\right)^{n-m} = a^m$$

Das ist ein Widerspruch, da $\operatorname{ord}(a)$ unendlich ist, es kann also kein m geben, sodass $a^m = 1$. ■

Lemma 0.4:

$$[(K(G), *) = (\{1\}, *)] \Leftrightarrow (G, *) \text{ ist abelsch}$$

Proof: $\Longrightarrow$: Aus $[(K(G), *) = (\{1\}, *)]$ folgt, dass

$$\left\{a * b * a^{-1} * b^{-1} \mid a, b \in G\right\} = \{1\}$$

da die Erzeugermenge der Gruppe $(\{1\}, *)$ die Menge mit ausschließlich dem leeren Element ist.

Es gilt also:

$$\begin{gathered} a * b * a^{-1} * b^{-1} = 1 \quad \forall a, b \in G \\ \Leftrightarrow a * b * a^{-1} * b^{-1} * b * a = b * a \quad \forall a, b \in G \\ \Leftrightarrow a * b = b * a \quad \forall a, b \in G \end{gathered}$$

Das ist genau die Bedingung, die G zu einer abelschen Gruppe macht.
$\Longleftarrow$: In einer abelschen Gruppe gilt $a * b * a^{-1} * b^{-1} = 1$ für alle $a, b \in G$. Damit ist

$$K(G) = \left\langle\left\{a * b * a^{-1} * b^{-1} \mid a, b \in G\right\}\right\rangle = \langle\{1 \mid a, b \in G\}\rangle = \langle\{1\}\rangle = \{1\}$$

da die von $\{1\}$ erzeugte Untergruppe von G: $(\{1\}, *)$ ist.

■