LA Zettel 5

Bearbeitet von Leon Krasniqi, Christian Krause, Silas Gaschler (Tutorium Gregor Teupke) ==
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:

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

(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: Aus der Surjektivität von ${}_a*$ und $\star_a$ folgt:

$$\forall a, x \in H, \exists y \in H, a * y = x \quad (i)$$

$$\forall a, x \in H, \exists y \in H, y * a = x \quad (ii)$$

Sei $a \in H$ beliebig aber fest. Es gibt ein $e \in H$, sodass $a * e = a$ (folgt aus (i)). Weiter gibt es für jedes $g \in H$ ein $y \in H$, sodass $y * a = g$ (folgt aus (ii)). Es gilt also

$$g * e = (y * a) * e = y * (a * e) = y * a = g$$

Da g beliebig gewählt war ist e Rechtsneutral zu allen Elementen von H.
Analog erhält man ein e', das Linksneutral zu allen Elementen von H ist, es gilt also

$$g * e = e' * g = g \quad \forall g \in H$$

Daraus folgt: $e = e' * e = e'$. Es gibt also ein Neutrales Element in H, das wir nun als e bezeichnen werden.
Um zu zeigen, dass $(H, \star)$ eine Gruppe ist, fehlt noch, dass es für jedes Element ein inverses gilt.
Aus (i) folgt, dass es für jedes $a \in H$, ein Element a' gibt, sodass $a * a' = e$. Aus (ii) folgt, dass es für jedes $a \in H$ ein Element a'' gibt, sodass $a'' * a = e$.

$$\begin{aligned} & a * a' = e \\ \Leftrightarrow\ & a'' * (a * a') = a'' \\ \Leftrightarrow\ & (a'' * a) * a' = a'' \\ \Leftrightarrow\ & e * a' = a'' \\ \Leftrightarrow\ & a' = a'' \end{aligned}$$

Es gibt also für jedes $a \in H$ ein inverses Element a', sodass $a * a' = a' * a = e$

∎

Aufgabe 2

Aufgabe 5.2

(i)

Das Tupel $(R^X, +)$ ist abelsch, denn:

$\forall f_1, f_2 \in R^X, \forall x_1, x_2 \in X : f_1(x_1) + f_2(x_2) = f_2(x_2) + f_1(x_1)$

Dies gilt, da Addition in R kommutativ ist.

(ii)
$(P(X), \cap)$ ist keine Gruppe.

(iii)
$(P(X), \Delta)$, wobei $A \Delta B = (A \setminus B) \cap (B \setminus A)$:

$A \Delta B = A \setminus B \cap B \setminus A = B \setminus A \cap A \setminus B = B \Delta A$

Daher: abelsche Gruppe.

(iv)
Keine Gruppe.

(v)
Keine Gruppe.

b)

Lemma 0.3: Jede Gruppe mit höchstens vier Elementen ist abelsch.

Proof:

Sei $(G, \star)$ eine Gruppe und e das neutrale Element.

Fall 1:

$$G = \{e\}$$

Einzig mögliche Verknüpfung:

$$e \star e = e$$

Elemente mit sich selber Verknüpft sind abelsch $\Rightarrow$ für Fall 1 ist $(G, \star)$ abelsch

Fall 2:

$$G = \{e, a\}$$

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

$\Rightarrow$ Gruppe ist abelsch.

Fall 3:

$$G = \{e, a, b\}$$

Angenommen:

$$a \star b \neq b \star a$$

Es gilt:

$$a \star a' = a' \star a \land b \star b' = b' \star b$$

$$\Rightarrow a' \neq b \land b' \neq a$$

Daraus folgt $a \star b \neq e \land b \star a \neq e$.

Somit:

$$a \star b \neq e \land a \star b \neq a \land a \star b \neq b$$

$$\Rightarrow a * b \notin G$$

$\Rightarrow$ Wiederspruch

Fall 4:

$$G = \{e, a, b, c\}$$

Annahme wie bei Fall 3:

Es gilt also weiterhin:

$$b \star a \neq e \land b \star a \neq a \land b \star a \neq b$$

$$a \star b \neq b \star a$$

Falls

$$b \star a = c \Rightarrow b \star a \notin G$$

Falls

$$a \star b = c \Rightarrow b \star a \notin G$$

$\Rightarrow$ Widerspruch $\Rightarrow$ Gruppe ist abelsch

$\Rightarrow$ Eine Gruppe mit maximal 4 Elementen ist abelsch

■

Nr.I-5.3

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

Fehlstände:

$$(2,5),(2,6),(2,7),(2,8),(3,5),(3,6),(3,7),(3,8),(4,5),(4,6),(4,7),(4,8),(5,8),(6,8),(7,8)$$

Signum:

$$sgn(\sigma) = (-1)^k$$

$$k = 15$$

$$\Rightarrow sgn(\sigma) = (-1)^{15} = -1$$

Transpositionen:

Proof:

$$\tau(8,6) \circ \tau(7,5) \circ \tau(8,4) \circ \tau(7,3) \circ \tau(6,2) \circ \sigma = \mathrm{id}$$

$$\Rightarrow \sigma = \mathrm{id} \circ \tau(6,2) \circ \tau(7,3) \circ \tau(8,4) \circ \tau(7,5) \circ \tau(8,6)$$

∎

Nr.I-5.4

(a) Sei X eine nichtleere Menge und $A \subset X$ sowie $n \in \mathbb{N}$, dann gelten:

Lemma 0.4: $(\mathcal{P}(A), \triangle)$ ist eine Untergruppe der Gruppe $(\mathcal{P}(X), \triangle)$

Proof:

1. $\mathcal{P}(A)$ ist nicht leer, da es mindestens das neutrale Element $e = \emptyset$ enthält
2. $$\forall a, b \in \mathcal{P}(A) : a \triangle b \in \mathcal{P}(A)$$
3. Es gilt $\forall a, b' \in \mathcal{P}(A)$, da für $\triangle$ alle Elemente selbstinvers sind und 2. gilt:

$$a \triangle a = (a \setminus a) \cap (a \setminus a) = \emptyset$$

∎

Lemma 0.5: $(A_n, \circ)$ mit $A_n = (\{\sigma \in S_n | sgn(\sigma) = 1\})$ ist eine Untergruppe der Gruppe $(S_N, \circ)$

Proof:

1. A_n ist nichtleer, da mindestens das neutrale Element id enthalten ist:

$$sgn(\text{id}) = (-1)^0 = 1$$

$$\Rightarrow \text{id} \in A_n$$

2. Seien $\sigma_a, \sigma'_b \in A_n$ mit

$$\sigma_a = \tau_{a_1} \circ \tau_{a_2} \circ \ldots \circ \tau_{a_n} \circ \text{id}$$

$$\sigma'_b = \tau_{b_k} \circ \tau_{b_{k-1}} \circ \ldots \circ \tau_{b_1} \circ \text{id}$$

wobei $n, k \in \mathbb{N}$ sind und gerade sind. Dann ist $sgn(\sigma_a \circ \sigma'_b) = 1$, da

$$\sigma_a \circ \sigma'_b = \tau_{a_1} \circ \ldots \tau_{a_n} \circ \text{id} \circ \tau_{b_k} \circ \ldots \circ \tau_{b_1} \circ \text{id}$$

$n + k$ Transpositionen, also eine gerade Anzahl an Transpositionen hat, und somit ist

$$\sigma_a \circ \sigma'_b \in A_n$$

■

(b) Sei $(G, \star)$ eine Gruppe mit neutralem Element e und $(U_i, \star)_{i \in I}$ eine Familie von Untergruppen, wobei I nicht die leere Menge ist, dann gilt:

Lemma 0.6: $(\bigcap_{i \in I} U_i, \star)$ ist eine Untergruppe von $(G, \star)$

Proof:

1. Neutrales Element: $\bigcap_{i \in I} U_i$ ist nicht leer, da nach Lemma 7.43 des Skripts in jeder Untergruppe das gleiche neutrale Element e enthalten ist.
2. Inverses: $\forall a \in \bigcap_{i \in I} U_i : \forall i \in I, a \in U_i \land a' \in U_i$

$$\Rightarrow a' \in \bigcap_{i \in I} U_i$$

3. Abgeschlossenheit: $\forall a, b \in \bigcap_{i \in I} U_i : \forall i \in I, a \in U_i \land b \in U_i$

$$\Rightarrow a \star b \in U_i$$

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

■

(c) Sei $(G, \star)$ eine Gruppe und $(U_1, \star), (U_2, \star)$ Untergruppen, dann gilt:

Lemma 0.7: $(U_1 \cup U_2, \star)$ ist genau dann eine Untergruppe von $(G, \star)$, wenn

$$U_1 \subset U_2 \lor U_2 \subset U_1$$

Proof: $(U_1 \cup U_2, \star)$ ist Untergruppe $\Rightarrow U_1 \subset U_2 \vee U_2 \subset U_1$
Kontraposition:

$$U_1 \not\subset U_2 \wedge U_2 \not\subset U_1$$

$$\Rightarrow \exists a \in U_1 : a \notin U_2 \wedge \exists b \in U_2 : b \notin U_1$$

$$\Rightarrow a \star b \in (U_1 \cup U_2, \star)$$

$$\Rightarrow a \star b \in U_1 \wedge a \star b \in U_2$$

$$1.\ \Rightarrow a' \star a \star b \in U_1$$

$$\Rightarrow b \in U_1$$

$$2.\ a \star b \star b' \in U_2$$

$$\Rightarrow a \in U_2$$

Das ist widersprüchlich zur Annahme, weshalb $U_1 \subset U_2 \vee U_2 \subset U_1$ gilt.
Die andere Rückrichtung ist trivial, da $U_1 \cup U_2 = U_1 \vee U_1 \cup U_2 = U_2$. ■

Aufgabe 5

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

Lemma 0.8: $\operatorname{ord}(a) = \operatorname{ord}(a^{-1})$

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

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

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 $(a^{-1})^m = 0$ und

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

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 $(a^{-1})^m = 1$ für ein $m \in \mathbb{N}$. Dann gilt für alle $n > m$:

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

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

Lemma 0.9:

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

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

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

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

Es gilt also:

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

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

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

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

■

Aufgabe 5.6

Lemma 0.10: $\#U \mid \#G$

Proof:

$$\forall a \in G : \exists a \star U$$

$\forall a, b \in G$ gilt $a \star U$ und $b \star U$ sind entweder gleich oder disjunkt

$$\Rightarrow [a_n] = \{a \in G | \ a \star U = a_n \star U\}$$

$$\Rightarrow \bigcup_n [a_n] = G$$

Es gilt:

$$\#A \cup B = \#A + \#B$$

$$\forall a \in G : \#(a * U) = \#U$$

$$\Rightarrow \#G = \# \bigcup_n [a_n] = \#([a_1] \cup [a_2] \cup ... \cup [a_n]) = \#[a_1] + \#[a_2] + ... + \#[a_n] = \#U + \#U + ... + \#U = n * \#U$$

$$\Rightarrow \#G = n * \#U \Rightarrow \#U \mid \#G$$

■