Musterlösung Serie 11

Einige (Teil-)Aufgaben sind mit (∗) markiert. Versuchen Sie, wenigstens diese Aufgaben zu lösen.

0. **(∗) (Gruppenwirkung)** Diese Aufgabe haben wir in der Vorlesung im Beweis eines Satzes (Hausdorff-Paradox) verwendet. Sei G eine Gruppe. Wir definieren die *G-Wirkung auf sich selbst durch Linkstranslation* als die Abbildung

$$L_G : G \times G \to G, \qquad L_G(g, x) := g \circ x.$$

Zeigen Sie, dass das eine Gruppenwirkung ist.

Lösung: Seien $g, h \in G$ und $x \in X := G$. Es gilt

$$L_G(e, x) = e \circ x = x, \qquad L_G(h \circ g, x) = (h \circ g) \circ x = h \circ (g \circ x) = L_G\big(h, L_G(g, x)\big).$$

Daher ist L_G eine Gruppenwirkung.

1. **(∗) (Äquivalenzrelation, Zerlegung)** Diese Aufgabe werden wir in Aufgabe **2**. verwenden. Sei S eine Menge. Eine *Zerlegung* (oder *Partition*) von S ist eine Menge P nichtleerer disjunkter Teilmengen von S, die S überdecken, d. h. $\bigcup P = \bigcup_{X \in P} X = S$.

Eine *Äquivalenzrelation auf S* ist eine reflexive, symmetrische und transitive binäre Relation auf S. Seien R eine Äquivalenzrelation auf S und $x, y \in S$. Wir schreiben xRy g. d. w. $\langle x, y\rangle \in R$. Wir definieren die *Äquivalenzklasse von x bzgl. R* als die Menge

$$[x] := [x]_R := \big\{y \in S \,\big|\, xRy\big\}. \tag{1}$$

Wir definieren

$$P := P_R := \big\{[x]_R \,\big|\, x \in S\big\}. \tag{2}$$

Zeigen Sie:

Proposition 1 *Die Menge P_R aller Äquivalenzklassen bzgl. R ist eine Zerlegung von S.*

Hinweis: Verwenden Sie folgenden Hilfssatz.

Hilfssatz 2 *Seien $x, y \in S$ so, dass $[x] \cap [y] \neq \varnothing$. Dann gilt $[x] = [y]$.*

Um diesen Hilfssatz zu beweisen, verwenden Sie den folgenden Hilfssatz.

Hilfssatz 3 *Für jedes Paar $\langle x, y\rangle \in R$ gilt $[x] = [y]$.*

Lösung:

Beweis des Hilfssatzes 3: "$\subseteq$": Sei $z \in [x]$. Es gilt

$$xRz.$$

Aus unserer Annahme xRy und Symmetrie von R folgt, dass yRx. Da R transitiv ist, folgt, dass yRz. Daher gilt, dass $z \in [y]$. Das beweist "$\subseteq$". Indem wir die Rollen von x und y vertauschen, folgt daraus die umgekehrte Inklusion. Das beweist Hilfssatz 3. $\square$

Beweis des Hilfssatzes 2: Wir wählen $z \in [x] \cap [y]$. Es gilt xRz. Wegen Hilfssatz 3 gilt daher $[x] = [z]$. Analog folgt, dass $[y] = [z]$, also $[x] = [z] = [y]$. Das beweist Hilfssatz 2. $\square$

Beweis der Proposition 1:

- **(nichtleere Elemente)** Sei $X \in P$. Es gibt ein $x \in S$, sodass $X = [x]$. Es gilt $x \in [x] = X$. Daher ist X nicht leer.
- **(Disjunktheit)** Seien $X, Y \in P$ so, dass $X \neq Y$. Wir wählen $x, y \in S$, sodass $X = [x]$ und $Y = [y]$. Gemäss der Kontraposition des Hilfssatzes 2 gilt, dass $[x] \cap [y] = \varnothing$. Also sind $X = [x]$ und $Y = [y]$ disjunkt.
- **(Teilmengen von S)** Die Elemente von P sind Teilmengen von S.
- **(Überdeckung)** Für jedes $x \in S$ gilt $x \in [x] \in P$. Es folgt, dass $S \subseteq \bigcup P = \bigcup_{X \in P} X$.

Das beweist Proposition 1.

2. **($*$) (Gruppenwirkung, Äquivalenzrelation, Menge der Bahnen)** Diese Aufgabe werden wir in der Vorlesung im Beweis einer Proposition verwenden (Paradoxität vererbt sich unter freier Gruppenwirkung). Diese Proposition haben wir im Beweis eines Satzes (Hausdorff-Paradox) verwendet.

Sei G eine Gruppe, X eine Menge und φ eine G-Wirkung auf S. Wir definieren

$$R := R_\varphi := \left\{ \langle x, y \rangle \in X \times X \,\middle|\, \exists g \in G\big(\varphi(g, x) = y\big) \right\}.$$

(a) Zeigen Sie, dass R eine Äquivalenzrelation auf X ist.

Lösung:

- **Reflexivität:** Sei $x \in X$. Es gilt $\varphi(e, x) = x$ und daher $\langle x, x \rangle \in R$. Daher ist R reflexiv.
- **Symmetrie:** Seien $x, y \in X$ so, dass $\langle x, y \rangle \in R$. Wir wählen ein $g \in G$, sodass $\varphi(g, x) = y$. Es gilt:

$$\begin{aligned} \varphi(g^{-1}, y) &= \varphi\big(g^{-1}, \varphi(g, x)\big) \\ &= \varphi\big(g^{-1} \circ g, x\big) \qquad \text{(da } \varphi \text{ eine } G\text{-Wirkung ist)} \\ &= \varphi(e, x) \\ &= x \qquad \text{(da } \varphi \text{ eine } G\text{-Wirkung ist).} \end{aligned}$$

Es folgt, dass $\langle y, x \rangle \in R$. Daher ist R symmetrisch.

- **Transitivität:** Seien $x, y, z \in X$ so, dass $\langle x, y\rangle, \langle y, z\rangle \in R$. Wir wählen $g, h \in G$, sodass $\varphi(g, x) = y$, $\varphi(h, y) = z$. Da φ eine G-Wirkung ist, gilt

$$\varphi\big(h \circ g, x\big) = \varphi\big(h, \varphi(g, x)\big) = \varphi(h, y) = z.$$

  Es folgt, dass $\langle x, z\rangle \in R$. Daher ist R transitiv.

Es folgt, dass R eine Äquivalenzrelation auf X ist.

(b) Sei $x \in X$. Die *φ-Bahn von x* ist die Menge

$$Gx := \big\{\varphi(g, x) \,\big|\, g \in G\big\}.$$

Zeigen Sie, dass

$$X/G := \big\{Gx \,\big|\, x \in X\big\},$$

die Menge der φ-Bahnen, eine Zerlegung von X ist.

Hinweis: Verwenden Sie **2**.a und **1**.

Lösung: Sei $x \in X$. Gemäss **2**.a ist $R := R_\varphi$ eine Äquivalenzrelation auf X. Daher ist die Äquivalenzklasse $[x]_R$, gegeben durch (1), wohldefiniert. Es gilt

$$Gx = [x]_R.$$

Wegen (2) folgt daraus, dass

$$X/G = P_R.$$

Gemäss **1**. ist das eine Zerlegung von X.

3. **(Kuratowski-Zorn-Lemma, Existenz einer maximalen Untergruppe)** Sei $(G, \circ)$ eine Gruppe. Wir schreiben e für das neutrale Element von G. Eine Teilmenge $H \subseteq G$ heisst *Untergruppe von G* g. d. w. $e \in H$ und für alle $h, h' \in H$ gilt, dass $h^{-1}, h'h \in H$. Eine *maximale Untergruppe von G* ist eine echte Untergruppe[1] $H \subsetneq G$, sodass für jede echte Untergruppe $K \subsetneq G$ gilt: Falls $H \subseteq K$, dann gilt $H = K$. Sei $S \subseteq G$. Wir definieren die *von S erzeugte Untergruppe von G* als die Menge

$$\langle S\rangle := \big\{g_n \cdots g_1 \,\big|\, n \in \omega,\ \forall i \in \{1, \dots, n\} :\ g_i \in S \vee g_i^{-1} \in S\big\}.$$

(g^{-1} ist das Inverse zu g.) Diese Menge ist eine Untergruppe von G. Die Menge S heisst *Erzeugendensystem von G* g. d. w. $\langle S\rangle = G$. Die Gruppe G heisst *endlich erzeugt*, falls sie ein endliches Erzeugendensystem besitzt. Zeigen Sie das folgende THEOREM.

THEOREM 4 *In* ZFC *besitzt jede nichttriviale*[2] *endlich erzeugte Gruppe eine maximale Untergruppe.*

Hinweise:

[1] d. h. eine Untergruppe, die eine echte Teilmenge ist

[2] Eine Gruppe heisst *nichttrivial* g. d. w. sie aus mehr als einem Element besteht.

- Verwenden das Kuratowski-Zorn-Lemma. Sei G eine endlich erzeugte Gruppe. Wir wählen ein endliches Erzeugendensystem S_0 für G. Zeigen Sie, dass es eine Teilmenge $S \subseteq S_0$ und ein Element $g \in S_0$ gibt, sodass

$$\big\langle S \cup \{g\} \big\rangle = G, \qquad \langle S \rangle \neq G.$$

  Starten Sie dazu mit der leeren Menge und nehmen sie sukzessive Elemente aus S_0 hinzu.

- Wir definieren

$$P := \big\{ H \,\big|\, H \subseteq G \text{ Untergruppe}, \, S \subseteq H, \, g \notin H \big\}.$$

  Zeigen Sie, dass das Paar $\big(P, \leqslant := \subseteq\big)$ eine halbgeordnete Menge ist. Verwenden Sie dazu eine Aufgabe aus Übungsserie 10.

- Sei $C \subseteq P$ eine $\subseteq$-Kette. Zeigen Sie, dass C eine obere Schranke in P besitzt.
- Wenden Sie das Kuratowski-Zorn-Lemma an.
- Seien H ein maximales Element von P und $K \subsetneq G$ eine Untergruppe, sodass $H \subseteq K$. Zeigen Sie, dass $g \notin K$. Folgern Sie, dass $H = K$.

Lösung: Gemäss einem THEOREM aus der Vorlesung (Umformulierungen des Auswahlaxioms) impliziert in ZF das Auswahlaxiom AC das Kuratowski-Zorn-Lemma KZL. Da wir AC annehmen, gilt also KZL.

Sei G eine endlich erzeugte Gruppe. Wir wählen ein endliches Erzeugendensystem S_0 für G.

Behauptung 1 *Es gibt eine Teilmenge $S \subseteq S_0$ und ein Element $g \in S$, sodass*

$$\big\langle S \cup \{g\} \big\rangle = G, \tag{3}$$

$$\langle S \rangle \neq G. \tag{4}$$

Beweis der Behauptung 1: Wir wählen ein $n \in \omega$ und eine surjektive Abbildung $a : \mathrm{s}(n) = n \cup \{n\} \to S_0$. Wir schreiben $a_i := a(i)$ und definieren

$$A := \Big\{ k \leqslant n \,\Big|\, \big\langle \{ a_i \,|\, i \leqslant k \} \big\rangle = G \Big\}.$$

Da $\langle S_0 \rangle = G$, gilt $n \in A$ und daher $A \neq \varnothing$. Da $A \subseteq \omega$ und ω wohlgeordnet ist, besitzt A ein kleinstes Element m. Wir definieren

$$S := \big\{ a_i \,\big|\, i < m \big\}, \qquad g := a_m.$$

Da $m \in A$, gilt (3). Da m das kleinste Element von A ist und G nicht trivial ist, gilt (4).[3] Das beweist Behauptung 1. □

Wir wählen S, g wie in dieser Behauptung. Wir definieren

$$P := \big\{ H \,\big|\, H \subseteq G \text{ Untergruppe}, \, S \subseteq H, \, g \notin H \big\}.$$

[3] Im Fall $m = 0$ ist $S = \varnothing$ und daher $\langle S \rangle = \{e\} \neq G$.

Gemäss einer Aufgabe aus Übungsserie 10 (Halbordnung) ist $\subseteq$ [4] eine Halbordnung auf $\mathcal{P}(G)$. Daraus folgt, dass $\subseteq$ eine Halbordnung auf P ist.

Sei $C \subseteq P$ eine Kette. Wir zeigen, dass C eine obere Schranke besitzt.

Fall $C = \varnothing$: Aus (3,4) folgt, dass $H_0 := \langle S \rangle \in P$. Es folgt, dass H_0 eine obere Schranke für C ist.

Fall $C \neq \varnothing$: Wir definieren

$$H_0 := \bigcup C = \bigcup_{H \in C} H.$$

Behauptung 1 *H_0 ist eine Untergruppe von G.*

Beweis der Behauptung 1: Sei $h \in H_0$. Wir wählen ein $H \in C$, sodass $h \in H$. Da H eine Untergruppe von G ist, folgt, dass $h^{-1} \in H \subseteq H_0$.

Seien $h, h' \in H_0$. Da $H_0 = \bigcup C$, gibt es $H, H' \in C$, sodass $h \in H$, $h' \in H'$.

Fall $H \subseteq H'$: Dann gilt $h, h' \in H'$. Da H' eine Untergruppe von G ist, folgt, dass $h'h \in H' \subseteq H_0$.

Fall $H' \subseteq H$: In diesem Fall folgt analog, dass $h'h \in H \subseteq H_0$.

Da C eine Kette ist, decken diese zwei Fälle alle Möglichkeiten ab. Daher gilt in jedem Fall, dass $h'h \in H_0$.

Das beweist Behauptung 1. $\square$

Gemäss unserer Annahme $C \neq \varnothing$ gibt es ein $H \in C$. Da $C \subseteq P$, gilt

$$S \subseteq H \subseteq \bigcup C = H_0. \tag{5}$$

Sei $H \in C$. Da $C \subseteq P$, gilt $g \notin H$. Daraus folgt, dass

$$g \notin \bigcup C = H_0. \tag{6}$$

Aus Behauptung 1 und (5,6) folgt, dass

$$H_0 \in P.$$

Für jedes $H \in C$ gilt $H \subseteq \bigcup C = H_0$. Es folgt, dass H_0 eine obere Schranke für C in P ist.

Die Kette C besitzt also in jedem Fall eine obere Schranke. Aus dem Kuratowski-Zorn-Lemma folgt daher, dass P ein maximales Element H besitzt. Da $H \in P$, gilt $g \notin H$ und daher

$$H \neq G.$$

Sei $K \subsetneq G$ eine Untergruppe, sodass $H \subseteq K$.

Behauptung 2 *Es gilt $H = K$.*

[4] genauer gesagt die Einschränkung von $\subseteq$ auf $\mathcal{P}(G)$

Beweis der Behauptung 2: Da $H \in P$, gilt $S \subseteq H$. Da $H \subseteq K$, folgt, dass

$$S \subseteq K.$$

Aus $S \subseteq K$, $K \neq G$ und (3) folgt, dass $g \notin K$. (Überprüfen Sie das!) Da K eine Untergruppe von G ist, folgt, dass $K \in P$. Da H ein maximales Element von P ist und $H \subseteq K$, folgt, dass $H = K$. Das beweist Behauptung 2. $\square$

Aus dieser Behauptung folgt, dass H eine maximale Untergruppe von G ist.

4. **(Gleichmächtigkeit von natürlichen Zahlen)** Zwei Mengen A und B heissen *gleichmächtig* g. d. w. es eine Bijektion zwischen A und B gibt. Zeigen Sie:

Proposition 5 *Zwei natürliche Zahlen genau dann gleichmächtig sind, falls sie gleich sind.*

Hinweise für die Implikation "$\rightarrow$":

- **Hilfssatz 6** *(a) (Transitivität einer natürlichen Zahl) Für jedes $n \in \omega$ und jedes $m \in n$ gilt $m \subseteq n$.*
  (b) (injektiv impliziert surjektiv) Sei $n \in \omega$. Jede injektive Abbildung von n nach n ist surjektiv.
  (c) ($\in$-Vergleichbarkeit) Für alle $m, n \in \omega$ gilt $m \in n$ oder $m = n$ oder $n \in m$.

  Beweis: **(a):** Hilfssatz in der Musterlösung zu einer Aufgabe aus Übungsserie 9 (ω und jede natürliche Zahl sind Ordinalzahlen), (a), (Je zwei Elemente von ω sind $\in$-vergleichbar.)

  (b): Zeigen Sie das mittels Induktion. Induktionsschritt: Sei $n \in \omega$ so, dass die Aussage für n gilt. Sei $f : \mathrm{s}(n) \rightarrow \mathrm{s}(n)$ eine injektive Abbildung. Wählen Sie eine Bijektion $\varphi : \mathrm{s}(n) \rightarrow \mathrm{s}(n)$, sodass $\varphi(f(n)) = n$. Betrachten Sie die Einschränkung der verknüpften Abbildung $\varphi \circ f$ auf n.

  (c): Übungsserie 9 (ω und jede natürliche Zahl sind Ordinalzahlen), (a)
- Seien $m, n \in \omega$. Unterscheiden Sie die Fälle $m \in n$, $m = n$ und $n \in m$. Verwenden Sie Hilfssatz 6.

Lösung: "$\rightarrow$":

Beweis von Teil (b) des Hilfssatzes 6: Für $n \in \omega$ betrachten wir die Aussage

$P(n)$: "Jede injektive Abbildung von n nach n ist surjektiv."

Wir zeigen mittels Induktion, dass $\forall n \in \omega\, P(n)$ gilt.

Induktionsverankerung: $P(0)$ gilt, da die einzige Abbildung von $0 = \varnothing$ nach 0 die leere Abbildung ist und diese Abbildung surjektiv ist.

Induktionsschritt: Sei $n \in \omega$ so, dass $P(n)$ gilt. Sei $f : \mathrm{s}(n) = n \cup \{n\} \rightarrow \mathrm{s}(n)$ eine injektive Abbildung. Wir wählen eine Bijektion $\varphi : \mathrm{s}(n) \rightarrow \mathrm{s}(n)$, sodass

$$\varphi(f(n)) = n. \tag{7}$$

(Wir können zum Beispiel die Abbildung φ nehmen, die $f(n)$ und n vertauscht und die anderen Elemente von $\mathrm{s}(n)$ festlässt.) Da f und φ injektiv sind, ist die Verknüpfung $\varphi \circ f : \mathrm{s}(n) \to \mathrm{s}(n)$ injektiv. Wegen (7) folgt daraus, dass $\varphi \circ f[n] \subseteq n$. Daher ist die folgende Abbildung wohldefiniert:

$$g : n \to n, \qquad g(m) := \varphi \circ f(m). \tag{8}$$

Diese Abbildung ist ebenfalls injektiv. Gemäss unserer Induktionsannahme $P(n)$ ist g daher surjektiv, d. h.

$$n \subseteq g[n]. \tag{9}$$

Es gilt:

$$\begin{aligned} \mathrm{s}(n) \backslash \{f(n)\} &= \varphi^{-1}[n] \qquad \text{(wegen (7))} \\ &\subseteq \varphi^{-1}[g[n]] \qquad \text{(wegen (9))} \\ &= \varphi^{-1} \circ g[n] \\ &= f[n] \qquad \text{(wegen (8))}. \end{aligned}$$

Da $\mathrm{s}(n) = n \cup \{n\}$, folgt, dass $\mathrm{s}(n) \subseteq f[\mathrm{s}(n)]$. Daher ist f surjektiv. Daher gilt $P(\mathrm{s}(n))$. Das zeigt den Induktionsschritt.

Mittels Induktion folgt, dass $P(n)$ für jedes $n \in \omega$ gilt. Das beweist Teil (b) des Hilfssatzes 6. □

Seien jetzt $m, n \in \omega$ gleichmächtige Zahlen.

Fall $m \in n$**:** Gemäss Hilfssatz 6(a) gilt dann

$$m \subseteq n.$$

Da m und n gleichmächtig sind, gibt es eine Bijektion $\varphi : n \to m$. Mittels Hilfssatz 6(b) folgt, dass $m = n$. (Warum?)

Im **Fall** $n \in m$ zeigt ein analoges Argument, dass $n = m$.

Gemäss Hilfssatz 6(c) decken die drei Fälle $m \in n$, $m = n$ und $n \in m$ alle Möglichkeiten ab. Es folgt, dass $m = n$ in jedem Fall gilt. Das beweist die Implikation "$\rightarrow$" in Proposition 5.

Die Implikation "$\leftarrow$" gilt, da für jedes $n \in \omega$ die Identität $\mathrm{id} : n \to n$ eine Bijektion ist.