Aufgabe 1

Sei $G = (G, \cdot, e)$ eine Gruppe. Auf der Potenzmenge $P(G)$ betrachten wir die Abbildung

$$(A, B) \mapsto A * B = \{a \cdot b | (a, b) \in A \times B\}.$$

Zeigen Sie, dass es sich um eine assoziative Verknüpfung handelt und ein eindeutiges (links- und rechts-)neutrales Element existiert. Zu welchen Teilmengen gibt es inverse Elemente? Ist $(P(G), *)$ jemals eine Gruppe?

Beweis. **Assoziativität:**

$$\begin{aligned}
(A * B) * C &= \{a \cdot b | (a, b) \in A \times B\} * C \\
&= \{(a \cdot b) \cdot c | ((a, b), c) \in (A \times B) \times C\} \\
&= \{(a \cdot b) \cdot c | (a, b) \in (A \times B) \wedge c \in C\} \\
&= \{(a \cdot b \cdot c) | a \in A, b \in B, c \in C\} \\
&= \{a \cdot (b \cdot c) | a \in A, (b, c) \in B \times C\} \\
&= \{a \cdot (b \cdot c) | (a, (b, c)) \in A \times (B \times C)\} \\
&= A * \{b \cdot c | (b, c) \in B \times C\} \\
&= A * (B * C)
\end{aligned}$$

Es existiert ein neutrales Element $E = \{e\}$.
Dann ist

$$E * A = \{x \cdot a | (x, a) \in E \times A\} = \{x \cdot a | x \in \{1\} \wedge a \in A\} = \{1 \cdot a | a \in A\} = A$$

und

$$A * E = \{a \cdot x | (a, x) \in A \times E\} = \{a \cdot x | a \in A \wedge x \in \{1\}\} = \{a \cdot 1 | a \in A\} = A.$$

Das neutrale Element ist eindeutig.
Seien E, E' zwei verschiedene neutrale Elemente. Daraus folgt aber

$$E = E * E' = E' \lightning.$$

Offensichtlich existiert also nur ein neutrales Element.

Es gibt nur zu einelementigen Teilmengen ein Inverses. Sei $A = \{a\}$ eine einelementige Teilmenge von $P(G)$. Dann ist $A^{-1} = \{a^{-1}\}$ das Inverse zu A, da

$$A * A^{-1} = \{x \cdot y | (x, y) \in A \times A^{-1}\} = \{x \cdot y | (x, y) \in \{a\} \times \{a^{-1}\}\} = \{a \cdot a^{-1}\} = \{e\}$$

Die leere Menge hat kein Inverses, da $A * \emptyset = \{x \cdot y | (x, y) \in A \times \emptyset\} = \{x \cdot y | (x, y) \in \emptyset\} = \emptyset$. Sei A eine Teilmenge von $P(G)$ mit mindestens zwei verschiedenen Elementen $x \in A \subset G$ und $y \in A \subset G$. Angenommen, es gäbe ein A^{-1} zu A. Dieses muss mindestens ein Element $z \in A^{-1} \subset G$ enthalten. Damit wissen wir aber, dass $\{x \cdot z, y \cdot z\} \subset A * A^{-1}$. Da G eine Gruppe ist und $x \neq y$ ist auch $x \cdot z \neq y \cdot z$. $A * A^{-1}$ enthält also mindestens zwei Elemente. Damit ist $A * A^{-1} \neq \{e\}$. Dies steht aber im Widerspruch dazu, dass das neutrale Element eindeutig ist. Unsere Annahme ist also falsch und es gibt kein Inverses A^{-1} zu A. $P(G)$ ist niemals eine Gruppe, da die leere Menge stets ein Element der Potenzmenge ist, es aber kein Inverses zur leeren Menge gibt. $\square$

Aufgabe 2

Es seien A, B und C Mengen und $f : A \to B$, $g : B \to C$ Abbildungen zwischen ihnen. Zeigen Sie:

a) Ist $g \circ f$ injektiv, so ist f injektiv.

Beweis. Wir zeigen die Kontraposition: f nicht injektiv $\implies$ $g \circ f$ nicht injektiv.
Da f nicht injektiv ist, wählen wir $x, x' \in A$ mit $f(x) = f(x') \in B$. Daraus folgt sofort, dass $g(f(x) = g(f(x'))$. Folglich ist auch $g \circ f$ nicht injektiv □

b) Ist $g \circ f$ surjektiv, so ist g surjektiv.

Beweis. Wir zeigen die Kontraposition: g nicht surjektiv *implies* $g \circ f$ nicht surjektiv.
Da g nicht surjektiv ist, wählen wir ein $c \in C$, sodass $g^{-1}(\{b\}) = \emptyset$. Es existiert also kein $b \in B$ mit $f(b) = c$. Gäbe es ein $a \in A$ mit $(g \circ f)(a) = c$, so wäre $f(b) = c$ mit $b = f(a)$. Da es aber kein solches b geben kann, gibt es auch kein $a \in A$ mit $(g \circ f)(a) = c$ und $(g \circ f)$ ist nicht surjektiv. □

c) Sind f und g bijektiv, so ist auch $g \circ f$ bijektiv und es gilt $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Beweis.
f bijektiv $\implies$ $\forall a \in A : \exists! b \in B$ mit $f(a) = b$.
g bijektiv $\implies$ $\forall b \in B : \exists! c \in C$ mit $f(b) = c$.
$\implies$ $\forall a \in A : \exists! c \in C$ mit $(g \circ f)(a) = c$ $\implies$ $(g \circ f)$ bijektiv.
$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ ist äquivalent zu der Aussage: $(g \circ f) \circ f^{-1} \circ g^{-1} = \mathrm{id}$. Diese ist leicht zu zeigen: $(g \circ f) \circ f^{-1} \circ g^{-1} = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ g^{-1} = \mathrm{id}$. □

Aufgabe 3

Sei $a \in \mathbb{N}_0$. Wir betrachten folgende Abbildung:

$$\begin{aligned} f : \mathbb{N}_0 &\to \mathbb{N}_0 \\ n &\mapsto \begin{cases} a & \text{falls } n \leq 1, \\ f(n-1) + f(n-2) & \text{sonst.} \end{cases} \end{aligned}$$

Zeigen Sie:

a) f ist weder injektiv noch surjektiv

Beweis. **Nicht injektiv:** $f(0) = f(1) = a$.
Nicht surjektiv: Dafür zeigen wir zuerst: $f(n+1) \geq f(n)$: $f(n+1) = f(n) + f(n-1) \geq f(n)$.
Behauptung: $f^{-1}(\{4a \in \mathbb{N}_0\}) = \emptyset$. Beweis: $f(0) = a, f(1) = a, f(2) = 2a, f(3) = 3a, f(4) = 5a$.
Wir haben gezeigt, dass $f(n+1) \geq f(n-1)$ und somit $\forall n \geq 4 : f(n) \geq f(4) \geq 5a > 4a$. Daher hat $4a$ kein Urbild unter f und f ist nicht surjektiv. □

b) $f(n)^2 = f(n-1)f(n+1) + (-1)^n \cdot a^2$ für alle $n \geq 1$.

Beweis.
Induktionsanfang: $n = 1$: $f(1)^2 = a^2 = a \cdot 2a - 1 \cdot a^2 = f(0)f(2) + (-1)^1 \cdot a^2$
$n = 2$: $f(2)^2 = (2a)^2 = a \cdot 3a + 1 \cdot a^2 = f(1)f(3) + (-1)^n \cdot a^2$
Induktionsannahme: Es sei $f(n)^2 = f(n-1)f(n+1) + (-1)^n \cdot a^2$
Induktionsschluss: $n \to n+1$:

$$\begin{aligned}
f(n+1)^2 &= (f(n-1) + f(n))^2 \\
&= f(n-1)^2 + 2f(n-1)f(n) + f(n)^2 \\
&\overset{I.A.}{=} f(n-2)f(n) + (-1)^{n-1}a^2 + 2f(n-1)f(n) + f(n)^2 \\
&= f(n)(f(n-2) + 2f(n-1)f(n)) + (-1)^{n+1}a^2 \\
&= f(n)(f(n) + f(n+1)) + (-1)^{n+1}a^2 \\
&= f(n)f(n+2) + (-1)^{n+1}a^2
\end{aligned}$$

□

Aufgabe 4

Sei $f : X \to Y$ eine Abbildung. Wir definieren die Relation

$$R = \{(x_1, x_2) \in X \times X | f(x_1) = f(x_2)\}.$$

Zeigen Sie:

a) R ist eine Äquivalenzrelation auf X.

Beweis. Wir zeigen alle Axiome einer Äquivalenzrelation.

Ä1) $x \sim_R x$, da $f(x) = f(x)$

Ä2) $(x_1 \sim_R x_2) \implies (f(x_1) = f(x_2)) \implies (f(x_2) = f(x_1)) \implies x_2 \sim_R x_1$

Ä3) $(x_1 \sim_R x_2$ und $x_2 \sim_R x_3) \Leftrightarrow (f(x_1) = f(x_2)$ und $f(x_2) = f(x_3)) \implies f(x_1) = f(x_3) \implies x_1 \sim_R x_3$

□

b) Es bezeichne p die kanonische Projektion $p : X \to X/R$ und

$$\operatorname{im} f = \{y \in Y | \exists x \in X : f(x) = y\} \subset Y$$

das Bild von f. Dann existiert eine eindeutige bijektive Abbildung $\overline{f} : X/R \to \operatorname{im} f$ mit der Eigenschaft, dass $\overline{f} \circ p = f$ gilt.

Beweis. Wir führen den Beweis in drei Schritten

1) **Es existiert eine Abbildung $\overline{f}$, sodass $\overline{f} \circ p = f$.**

Def. 1. Die Abbildung $g(M)$ ordne einer einelementigen Menge M das Element der Menge M zu.

$\overline{f} : A \in X/R \mapsto g(f(A)) \in Y$ erfüllt die Bedingungen. Z.Z.: Diese Funktion ist wohldefiniert, d.h. sie ordnet jeder Äquivalenzklasse $A \in X/R$ mit $x \in X$ genau ein $y \in Y$ zu.
Dafür genügt es zu zeigen, dass $\#f(A) = 1$. Wir wählen ein beliebiges $x_0 \in A$. Per Definition von R ist dann $\forall x \in A : f(x) = f(x_0)$. Daher enthält das Bild von A genau ein Element, nämlich $f(x_0) = g(f(A)) \in Y$. Z.Z.: $\overline{f} \circ p = f \Leftrightarrow \forall x \in X : \overline{f}(p(x)) = f(x)$
Wir setzen unsere oben definierte Funktion $\overline{f}$ ein: $\forall x \in X : g(f(p(x))) = f(x)$. Die kanonische Projektion eines Elements x entspricht der Menge $p(x) = \{a \in X | f(a) = f(x)\}$. Das Bild $f(p(x))$ ist also die Menge $\{f(a) | a \in p(x)\}$. Da aber $\forall a \in p(x) : f(a) = f(x)$ ist $f(p(x)) = \{f(x)\}$. Da offenbar $\#f(p(x)) = 1$ ist $g(f(p(x)))$ wohldefiniert und gleich $g(\{f(x)\}) = f(x)$.

2) **Es existiert höchstens eine Abbildung $\overline{f} : X/R \to \operatorname{im} f$, sodass $\overline{f} \circ p = f$**
Beweis durch Widerspruch: Wir nehmen an, es gäbe zwei verschiedene Abbildungen $\overline{f}, \overline{f}'$, die diese Bedingung erfüllen. Dann $\exists A \in X/R : \overline{f}'(A) \neq \overline{f}(A)$. Wir wählen nun x so, dass $p(x) = A$. Damit erhalten wir $\overline{f}' \circ p(x) \neq \overline{f} \circ p(x)$. Es gilt aber nach Voraussetzung $\overline{f} \circ p = f$ und natürlich auch $\overline{f}' \circ p = f$. Mit Einsetzen folgt unmittelbar $f(x) \neq f(x)$ ↯.

3) **$\overline{f}$ ist bijektiv.** Da $\overline{f}$ eindeutig ist, reicht es, die Bijektivität von $\overline{f} : A \in X/R \mapsto g(f(A)) \in Y$ zu zeigen. Z.Z.: $\overline{f}$ ist injektiv $\Leftrightarrow$ Für $A \neq A' \in X/R$ ist $g(f(A)) \neq g(f(A'))$. Wir wählen wieder ein beliebiges Element $x_0 \in A$. Es gilt $\forall x \in A : f(x) = f(x_0)$ und daher $f(A) = \{f(x_0)\} \implies g(f(A)) = g(\{f(x_0)\}) = f(x_0)$.
Analog erhalten wir für ein beliebiges Element $x_0' \in A'$ die Aussage $\forall x' \in A' : f(x') = f(x_0')$ und daher $f(A') = \{f(x_0')\} \implies g(f(A')) = g(\{f(x_0')\}) = f(x_0')$. Wäre nun $f(x_0) = f(x_0')$, so müsste $x_0' \in A$ sein. Da Äquivalenzklassen aber stets disjunkt sind, ist $f(x_0) \neq f(x_0')$.
Z.Z.: $\overline{f}$ ist surjektiv.
Aus der Definition von $\operatorname{im} f$ folgt $\forall y \in \operatorname{im} f : \exists x \in X$ mit $f(x) = y$. Wir wissen, dass $\overline{f}(p(x)) = f(x) \forall x \in X$. Damit erhalten wir $\forall y \in \operatorname{im} f : \exists x \in X$ mit $\overline{f}(p(x)) = y$. Nun setzen wir $A = p(x)$ und erhalten $\forall y \in \operatorname{im} f : \exists A = p(x)$ mit $x \in X$ und $\overline{f}(p(x)) = y$. Das ist äquivalent zu: $\forall y \in \operatorname{im} f : \exists A \in X/R$ mit $\overline{f}(A) = y$. $\overline{f}$ ist also surjektiv.
Aus Injektivität und Surjektivität folgt sofort Bijektivität.

□