5. Übungsblatt

Aufgabe 22. Gegeben sind einige Gleichungen über $\mathbb{Z}_n$, welche zu lösen sind:

$$\begin{aligned} 4x_1 &\equiv 3 \mod 7 \\ 6x_2 &\equiv 3 \mod 9 \\ 6x_3 &\equiv 4 \mod 9 \end{aligned}$$

Für x_1 suchen wir ein Vielfaches von 4, sodass $4x_1$ einen Modulo von 3 hat.

$$4 \cdot 6 = 24 \quad 24 \mod 7 = 3$$

Die Lösung für x_1 ist also $[6]_7$. Da $12 \mod 9 = 3$, ist $x_2 = [2]_9$. Da 6 immer Rest 3 oder Rest 6 hat, kann es kein $x_3 \in \mathbb{Z}$ geben, sodass die Gleichung erfüllt ist.

Aufgabe 23. Sei $(G, \circ)$ eine Gruppe. Zu zeigen ist, dass $f\colon G \to G$ mit $x \mapsto x^{-1}$ ein bijektiv ist, und ein Automorphismus, wenn $(G, \circ)$ abelsch ist.

Wenn f bijektiv ist, so muss $\forall x_1, x_2 \in G\colon x_1 = x_2 \Rightarrow x_1^{-1} = x_2^{-1}$ und $\forall x^{-1} \in G\colon \exists x \in G\colon x^{-1} = f(x)$ gelten. Da die inversen Element in einer Gruppe eindeutig sind, muss f injektiv sein. Wenn f nicht injektiv ist, dann folgt daraus, dass es nicht eindeutige Elemente gibt.

Proof. Sei $e, x_1, x_2 \in G$ mit $\forall x \in G\colon e \circ x = x = x \circ e$. Sei $x \in G$ mit $x^{-1} = x_1$ und $x^{-1} = x_2$.

$$x_1 = x_1 \circ e = x_1 \circ (x \circ x_2) = (x_1 \circ x) \circ x_2 = e \circ x_2 = x_2$$

□

Da eine Struktur $(G, \circ)$ nur dann eine Gruppe ist, wenn in dem darunterliegenden Monoid jedes Element invertierbar ist. In einer Gruppe gilt also:

$$\forall x \in G\colon \exists x^{-1} \in G\colon x \circ x^{-1} = e$$

Da $x = (x^{-1})^{-1}$ können wir auch schreiben:

$$\forall x^{-1} \in G\colon \exists x \in G\colon x^{-1} \circ x = e$$

Wir haben also gezeigt, dass f bijektiv ist. Damit ist f ein Isomorphismus auf $(G, \circ)$. Wenn $(G, \circ)$ abelsch ist, gilt dann (mit neutralem Element e). Sei $x, y \in G$:

$$f(x \circ y) = (x \circ y)^{-1} = y^{-1} \circ x^{-1} = x^{-1} \circ y^{-1} = f(x) \circ f(y)$$

Wenn f ein Automorphismus ist, dann muss $\forall x, y \in G\colon f(x \circ y) = f(x) \circ f(y)$ gelten.

$$\begin{aligned} &f(x \circ y) = f(x) \circ f(y) \\ \Leftrightarrow &y^{-1} \circ x^{-1} = x^{-1} \circ y^{-1} \end{aligned}$$

Wenn f ein Automorphismus ist, dann muss die Gleichung oben gültig sein. Das ist aber genau die Definition der Kommutativität, daher ist $(G, \circ)$ abelsch.

Aufgabe 24. Da $\circ$ über G abgeschlossen ist, liegt $g \circ x$ wieder in G. Seien $x, y \in G$:

$$\begin{aligned} \lambda_g(x) = g \circ x \quad \lambda_g(y) = g \circ y \\ x = y \Rightarrow \lambda_g(x) = \lambda_g(y) \Leftrightarrow g \circ x = g \circ y \\ \Leftrightarrow g^{-1} \circ g \circ x = g^{-1} \circ g \circ y \Leftrightarrow x = y \end{aligned}$$

Weiters zu zeigen: $\forall x \in G\colon \exists y \in G\colon \lambda_g(y) = x$

$$g \circ y = x$$

Wähle $y = g^{-1} \circ x$:

$$\lambda_g(y) = g \circ g^{-1} \circ x = x$$