Lösungsvorschläge zu Aufgabenblatt 11

(Untergruppen)

Aufgabe 11.1

1. Bestimmen Sie die Ordnungen der Elemente in der Gruppe $(\mathbb{Z}_7\backslash\{[0]_7\}, \otimes)$ sowie die von ihnen erzeugten Untergruppen.
2. Bestimmen Sie alle Untergruppen der Gruppe $(\mathbb{Z}_9, \oplus)$.
3. Bestimmen Sie alle Untergruppen der Gruppe $(\mathbb{Z}_9\backslash\{[0]_9, [3]_9, [6]_9\}, \otimes)$ (warum ist dies eine Gruppe?).
4. Bestimmen Sie alle Untergruppen der Gruppe $(\mathbb{Z}_{2017}, \oplus)$.

Lösung

Zur besseren Übersichtlichkeit notieren wir in den Lösungen anstelle der Restklassen nur ihre Repräsentanten.

(1)

g	ord(g)	$< g >$
1	1	$\{1\}$
2	3	$\{1, 2, 4\}$
3	6	$\{1, 2, 3, 4, 5, 6\}$
4	3	$\{1, 2, 4\}$
5	6	$\{1, 2, 3, 4, 5, 6\}$
6	2	$\{1, 6\}$.

(2) Die Untergruppen sind:

$$\begin{aligned} U_1 &= \{0\}, \\ U_2 &= \{0, 3, 6\}, \\ U_3 &= \mathbb{Z}_9. \end{aligned}$$

(3) Es handelt sich hierbei um die multiplikative Gruppe $\mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$. Die Untergruppen sind:

$$\begin{aligned} U_1 &= \{1\}, \\ U_2 &= \{1, 4, 7\}, \\ U_3 &= \{1, 8\}, \\ U_4 &= \mathbb{Z}_9^\times. \end{aligned}$$

(4) Da 2017 eine Primzahl ist und nach dem Satz von Lagrange die Ordnung jeder Untergruppe ein Teiler von $\text{ord}(\mathbb{Z}_{2017}) = 2017$ ist, hat $(\mathbb{Z}_{2017}, \oplus)$ nur die trivialen Untergruppen $\{0\}$ und $\mathbb{Z}_{2017}$.

Aufgabe 11.2

Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Zeigen Sie, dass $[a]_m$ genau dann ein Erzeuger der additiven Restklassengruppe $(\mathbb{Z}_m, \oplus)$ ist, wenn gilt $\mathrm{ggT}(m, a) = 1$.

Lösung

Beachte zunächst: Da die Verknüpfung in $(\mathbb{Z}_m, \oplus)$ additiv ist, gilt

$$\langle [a]_m \rangle = \{k \cdot [a]_m \mid k \in \mathbb{Z}\} = \{[k \cdot a]_m \mid k \in \mathbb{Z}\} = \{[a]_m \otimes [k]_m \mid k \in \mathbb{Z}\} = \{[a]_m \otimes x \mid x \in \mathbb{Z}_m\}.$$

„⇒“: Es sei $[a]_m$ ein Erzeuger der additiven Restklassengruppe $(\mathbb{Z}_m, \oplus)$, es gilt also $\langle [a]_m \rangle = \mathbb{Z}_m$. Wegen $[1]_m \in \mathbb{Z}_m$ gilt dann auch $[1]_m \in \langle [a]_m \rangle$, also gibt es ein $x \in \mathbb{Z}_m$ mit $[a]_m \cdot x = [1]_m$. Das bedeutet aber gerade, dass $[a]_m$ multiplikativ invertierbar ist, und dies ist nach Vorlesung äquivalent zu $\mathrm{ggT}(m, a) = 1$.

„⇒“: Es gelte $\mathrm{ggT}(m, a) = 1$. Nach Vorlesung ist dies äquivalent dazu, dass $[a]_m$ multiplikativ invertierbar ist. Wähle also $k \in \mathbb{Z}$ mit $[a]_m^{-1} = [k]_m$, dann folgt $[1]_m = [k]_m \otimes [a]_m = k \cdot [a]_m \in \langle [a]_m \rangle$. Da aber $[1]_m$ ein Erzeuger der ganzen Gruppe $(\mathbb{Z}_m, \oplus)$ ist, muss damit auch schon $\langle [a]_m \rangle = \mathbb{Z}_m$ sein.

Aufgabe 11.3

Sei $(G, \cdot)$ eine kommutative Gruppe. Auf der Menge der Äquivalenzklassen bezüglich $\equiv_H$ definieren wir:

$$[g_1]_{\equiv_H} \circ [g_2]_{\equiv_H} := [g_1 g_2]_{\equiv_H}.$$

(a) Zeigen Sie, dass diese Definition unabhängig von der Wahl der Repräsentanten ist.

(b) Zeigen Sie, dass die Menge

$$G/H := G/{\equiv_H} = \{[g]_{\equiv_H} \mid g \in G\} = \{gH \mid g \in G\}$$

mit der Verknüpfung $\circ$ eine kommutative Gruppe ist.

Anmerkung zur Notation: *Verwendet man wie in dieser Aufgabe "$\cdot$" für die Gruppenverknüpfung, so ist es wie beim herkömmlichen Rechnen mit Zahlen üblich, verkürzt $gh := g \cdot h$ zu schreiben.*

Lösung

Wir erinnern zunächst daran, dass gemäß Vorlesung für alle $g \in G$ gilt $[g]_{\equiv_H} = gH$, also

$$g' \equiv_H g \Leftrightarrow g' \in [g]_{\equiv_H} \Leftrightarrow \exists\, h \in H :\ g' = gh.$$

(a) Seien $g_1, g_2, g_1', g_2' \in G$ mit $g_1' \equiv_H g_1$ und $g_2' \equiv_H g_2$.
Zu zeigen ist: $[g_1 \circ g_2]_{\equiv_H} = [g_1' \circ g_2']_{\equiv_H}$.

Nach der Vorbemerkung finden wir $h_1, h_2 \in H$ mit $g_1' = g_1 h_1$ und $g_2' = g_2 h_2$. Da G kommutativ ist, folgt

$$g_1' g_2' = g_1 h_1 \cdot g_2 h_2 = g_1 g_2 \cdot \underbrace{h_1 h_2}_{=:h \in H} = (g_1 g_2) \cdot h,$$

also gilt $g_1' g_2' \equiv_H g_1 g_2$ und damit $[g_1 g_2]_{\equiv_H} = [g_1' g_2']_{\equiv_H}$.

(b) Nach Teil (a) definiert $\circ$ eine Verknüpfung auf G/H. Die weiteren Gruppenaxiome übertragen sich von der Gruppe G auf die algebraische Struktur $(G/H, \circ)$:

Assoziativgesetz: Seien $g_1, g_2, g_3 \in G$, dann gilt:

$$\begin{aligned} ([g_1]_{\equiv_H} \circ [g_2]_{\equiv_H}) \circ [g_3]_{\equiv_H} &= [g_1 g_2]_{\equiv_H} \circ [g_3]_{\equiv_H} = [(g_1 g_2) g_3]_{\equiv_H} = [g_1 (g_2 g_3)]_{\equiv_H} \\ &= [g_1]_{\equiv_H} \circ [g_2 g_3]_{\equiv_H} = [g_1]_{\equiv_H} \circ ([g_2]_{\equiv_H} \circ [g_3]_{\equiv_H}). \end{aligned}$$

Existenz neutrales Element: Sei $e \in G$ das neutrale Element der Gruppe G. Dann gilt für alle $g \in G$:

$$[e]_{\equiv_H} \circ [g]_{\equiv_H} = [eg]_{\equiv_H} = [g]_{\equiv_H}.$$

Also ist $[e]_{\equiv_H}$ neutrales Element in G/H.

Existenz inverser Elemente: Sei $g \in G$, und sei $g^{-1} \in G$ das inverse Element von g in G, dann gilt:

$$[g^{-1}]_{\equiv_H} \circ [g]_{\equiv_H} = [g^{-1} g]_{\equiv_H} = [e]_{\equiv_H}.$$

Also ist $[g^{-1}]_{\equiv_H}$ inverses Element von $[g]_{\equiv_H}$ in G/H.

Kommutativgesetz: Seien $g_1, g_2 \in G$, dann gilt:

$$[g_1]_{\equiv_H} \circ [g_2]_{\equiv_H} = [g_1 g_2]_{\equiv_H} = [g_2 g_1]_{\equiv_H} = [g_2]_{\equiv_H} \circ [g_1]_{\equiv_H}.$$