Algebra I, WiSe 2011\2012 – Lösung Blatt 7

7.1. (i) Aussage falsch:

Sei $g = ([g_1], [g_2]) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, so folgt

$$4g = ([2(2g_1)], [4g_2]) = ([0],[0])$$

Also: $\forall g \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ gilt: $4g = 0$

↯ $\varphi: \mathbb{Z}/8\mathbb{Z} \to \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\right)$ ist Isomorphismus, dann:

$$\varphi([0]) = [0] \overset{\text{s.o.}}{=} 4 \cdot \varphi([1]) = \varphi(\underbrace{[4]}_{\neq [0] \text{ in } \mathbb{Z}/8\mathbb{Z}})$$

$\Rightarrow$ φ ist nicht injektiv ↯

(ii) Aussage falsch: (völlig analog)

$\forall g \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gilt: $2g = 0$ (wie eben)

↯ $\varphi: \mathbb{Z}/8\mathbb{Z} \to \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right)$ ist Isomorphismus, dann:

$$\varphi([0]) = 2 \cdot \varphi([1]) = \varphi(\underbrace{[2]}_{\neq [0] \text{ in } \mathbb{Z}/8\mathbb{Z}})$$

$\Rightarrow$ φ ist nicht injektiv ↯

(iii) Aussage falsch:

Wegen $ggT(2,3) = 1$ folgt mit Aufgabe 2 (ii):

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

$\nearrow$ $\mathfrak{S}_3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$\Rightarrow \mathfrak{S}_3 \cong \mathbb{Z}/6\mathbb{Z} = \langle [1] \rangle$

$\Rightarrow$ In $\mathfrak{S}_3$ gibt es ein Element der Ordnung 6.

Aber:

$\mathfrak{S}_3 = \{ (1), (12), (13), (23), (123), (132) \}$

Ordnung 1 Ordnung 2 Ordnung 3 $\lightning$

(iv) Aussage richtig:

Die Diedergruppe D_3 kann als Untergruppe von $\mathfrak{S}_3$ konstruiert werden: Setze

$$\alpha := (13) \in \mathfrak{S}_3$$
$$\beta := (123) \in \mathfrak{S}_3 \quad \overset{\text{rechnen}}{\Longrightarrow} \quad \alpha\beta = \beta^{-1}\alpha$$

$\overset{\operatorname{ord}\alpha=2,\ \operatorname{ord}\beta=3}{\Longrightarrow}$ Jedes „Wort" in α und β kann in der Form $\beta^k\alpha^l$ geschrieben werden, z.B.

$$\begin{aligned} \alpha\beta\alpha\alpha\beta &= \beta^{-1}\alpha\alpha\alpha\beta = \beta^{-1}\alpha\alpha\beta^{-1}\alpha = \beta^{-1}\alpha\beta\alpha\alpha \\ &= \beta^{-1}\beta^{-1}\alpha^3 \\ &= \beta^k\alpha^l \quad \text{für } k, l \text{ geeignet.} \end{aligned}$$

$$\Rightarrow \langle \{\alpha, \beta\} \rangle = \{ id, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2 \}$$

$$= \{ (1), (123), (132), (13), (12), (23) \}$$

$$= \mathfrak{S}_3$$

Also sicherlich $D_3 \cong \mathfrak{S}_3$ (hier sogar „="). $\blacksquare$

7.2. (i) Sei $\operatorname{ord} U_1 = n_1$, $\operatorname{ord} U_2 = n_2$.

- Zeigen: $U_1 \cap U_2 = \{e\}$.

  Ist $x \in U_1 \cap U_2$, dann:

$$\left.\begin{array}{l} x \in U_1 \overset{\text{Lagrange}}{\Longrightarrow} \operatorname{ord} x \mid n_1 \\ x \in U_2 \Longrightarrow \operatorname{ord} x \mid n_2 \end{array}\right\} \Rightarrow \operatorname{ord} x \mid \operatorname{ggT}(n_1, n_2) = 1$$

  $\Rightarrow \operatorname{ord} x = 1 \Rightarrow x = e$.

  Also: $U_1 \cap U_2 = \{e\}$ (denn „$\supset$" ist Klar).

- Zeigen: $\forall u_1 \in U_1$, $\forall u_2 \in U_2$ gilt: $u_1 u_2 = u_2 u_1$.

  Betrachte $u_1 u_2 u_1^{-1} u_2^{-1}$:

$$u_1 u_2 u_1^{-1} u_2^{-1} = \underbrace{(u_1 u_2 u_1^{-1})}_{\substack{\in U_2 \text{ da} \\ \text{Normalteiler}}} u_2^{-1} \in U_2$$

$$u_1 u_2 u_1^{-1} u_2^{-1} = u_1 \underbrace{(u_2 u_1^{-1} u_2^{-1})}_{\substack{\in U_1 \text{ da} \\ \text{Normalteiler}}} \in U_1$$

$$\Rightarrow u_1 u_2 u_1^{-1} u_2^{-1} \in U_1 \cap U_2 = \{e\}$$

$$\Rightarrow u_1 u_2 u_1^{-1} u_2^{-1} = e$$

$$\Rightarrow u_1 u_2 = u_2 u_1.$$

- Zeigen: $U_1 \cdot U_2 = G$.

  Nach Vorlesung ist $U_1 \cdot U_2 \subset G$ Untergruppe. Da nach Voraussetzung $|G| = |U_1| \cdot |U_2| = n_1 n_2$ gilt, genügt es zu zeigen, dass $|U_1 \cdot U_2| = n_1 \cdot n_2$ gilt, d.h.

$$\left| \{ u_1 \cdot u_2 \mid u_1 \in U_1,\ u_2 \in U_2 \right| = n_1 n_2 .$$

Seien also $u_1, u_1' \in U_1$ und $u_2, u_2' \in U_2$ mit

$$u_1 u_2 = u_1' u_2'$$

Zu zeigen: $u_1 = u_1'$ und $u_2 = u_2'$ (genügt wegen $|U_1| = n_1$, $|U_2| = n_2$)

$$u_1 u_2 = u_1' u_2' \Rightarrow \underbrace{(u_1')^{-1} u_1}_{\in U_1} = \underbrace{u_2' u_2^{-1}}_{\in U_2}$$

$$\overset{U_1 \cap U_2 = \{e\}}{\Longrightarrow} (u_1')^{-1} u_1 = e = u_2' u_2^{-1}$$

$$\Rightarrow u_1 = u_1' \text{ und } u_2 = u_2' .$$

Also: $U_1 \cdot U_2 = G$.

Insgesamt folgt nach Definition: $G = U_1 \oplus U_2$.

(ii) n_1, n_2 teilerfremd $\Rightarrow ggT(n_1, n_2) = 1$.

Definiere $U_1 := \langle [n_2] \rangle \subset \mathbb{Z}/_{n_1 n_2 \mathbb{Z}}$ Normalteiler.

$U_2 := \langle [n_1] \rangle \subset \mathbb{Z}/_{n_1 n_2 \mathbb{Z}}$ Normalteiler.

$\Rightarrow$ $\text{ord}\, U_1 = n_1$ (wegen $n_1 \cdot [n_2] = [n_1 n_2] = [0]$ klar)

$\text{ord}\, U_2 = n_2$

Insbesondere haben wir $ggT(\text{ord}\, U_1, \text{ord}\, U_2) = 1$ und

$\text{ord}\, \mathbb{Z}/_{n_1 n_2 \mathbb{Z}} = n_1 n_2 = \text{ord}\, U_1 \cdot \text{ord}\, U_2$.

$$\overset{(i)}{\Rightarrow} \quad \mathbb{Z}/_{n_1 n_2 \mathbb{Z}} = U_1 \oplus U_2 \qquad (*)$$

Da nach Konstruktion U_1 und U_2 zyklisch sind, folgt

$$U_1 \cong \mathbb{Z}/_{n_1 \mathbb{Z}} \quad \text{und} \quad U_2 \cong \mathbb{Z}/_{n_2 \mathbb{Z}}$$

und damit aus $(*)$:

$$\mathbb{Z}/_{n_1 n_2 \mathbb{Z}} \cong \mathbb{Z}/_{n_1 \mathbb{Z}} \times \mathbb{Z}/_{n_2 \mathbb{Z}}.$$

$\blacksquare$

(Bemerkung: Aufgabe 1 (i), (ii) zeigt, dass $ggT(n_1, n_2) = 1$ wesentlich ist.)

7.3. (i) und (ii)

Sei für $i \in I$ $\pi_i : G_i \to G_i/N_i$, $g_i \mapsto g_i \cdot N_i$

der kanonische Restklassenhomomorphismus.

Definiere

$$\varphi : \prod_{i \in I} G_i \longrightarrow \prod_{i \in I} \left(G_i/N_i \right)$$
$$(g_i)_{i \in I} \longmapsto (\pi_i(g_i))_{i \in I}$$

• φ ist Homomorphismus, denn

$$\varphi\left((g_i)_{i\in I} \cdot (h_i)_{i \in I} \right) = \varphi\left((g_i \cdot h_i)_{i \in I} \right)$$
$$= \left(\pi_i (g_i \cdot h_i) \right)_{i \in I} = \left(\pi_i(g_i) \cdot \pi_i(h_i) \right)_{i \in I}$$
$$= (\pi_i(g_i))_{i \in I} \cdot (\pi_i(h_i))_{i \in I}$$
$$= \varphi\left((g_i)_{i \in I} \right) \cdot \varphi\left((h_i)_{i \in I} \right).$$

• φ ist surjektiv, denn ist $g \in \prod_{i \in I} \left(G_i/N_i \right)$, dann

$$g = (g_i \cdot N_i)_{i \in I} \qquad (\text{für gewisse } g_i \in G_i \ \forall i \in I)$$

und für $(g_i)_{i \in I} \in \prod_{i \in I} G_i$ folgt

$$\varphi\left((g_i)_{i \in I} \right) = (\pi_i(g_i))_{i \in I} = (g_i \cdot N_i)_{i \in I} = g \qquad \text{ok.}$$

• Es ist

$$\operatorname{Kern} \varphi = \left\{ (g_i)_{i \in I} \mid \varphi\left((g_i)_{i \in I} \right) = (N_i)_{i \in I} \right\}$$
$$= \left\{ (g_i)_{i \in I} \mid g_i \in N_i \ \forall i \in I \right\} = \prod_{i \in I} N_i$$

$$\Rightarrow \prod_{i\in I} N_i \trianglelefteq \prod_{i\in I} G_i \quad \text{(als Kern), d.h. (i)}$$

und der Homomorphiesatz liefert:

$$\left(\prod_{i\in I} G_i\right) \Big/ \left(\prod_{i\in I} N_i\right) \cong \prod_{i\in I} \left(G_i / N_i\right) \quad \text{, d.h. (ii)}$$

$\blacksquare$

7.4. (i) Sei $\alpha \in \mathbb{Q}/\mathbb{Z}$. Zu zeigen: $\operatorname{ord} \alpha < \infty$.

$\alpha \in \mathbb{Q}/\mathbb{Z} \Rightarrow \exists\, m,n \in \mathbb{Z},\ n > 0$ mit $\alpha = \frac{m}{n} + \mathbb{Z}$

$\Rightarrow\ n \cdot \alpha = m + \mathbb{Z} = \mathbb{Z} = [0]$ (neutral in $\mathbb{Q}/\mathbb{Z}$).

$\Rightarrow\ \operatorname{ord} \alpha < \infty$.

(Also: Alle $\alpha \in \mathbb{Q}/\mathbb{Z}$ haben endliche Ordnung
$\Rightarrow \mathbb{Q}/\mathbb{Z}$ Torsionsgruppe.)

(ii) Sei $n \in \mathbb{N}$. Schreiben Restklassen als $\overline{q} = [q]$.

• Existenz einer Untergruppe der Ordnung n:

Betrachte $\left\langle \overline{\frac{1}{n}} \right\rangle \subset \mathbb{Q}/\mathbb{Z}$ Untergruppe.

Klar: $\operatorname{ord} \left\langle \overline{\frac{1}{n}} \right\rangle = n$ denn $n \cdot \overline{\frac{1}{n}} = \overline{1} = \overline{0}$

und für $1 \leq k < n$: $k \cdot \overline{\frac{1}{n}} = \overline{\frac{k}{n}} \neq \overline{0}$ da $\frac{k}{n} \notin \mathbb{Z}$.

Also existiert eine Untergruppe der Ordnung n, welche zu

$$\mathbb{Z}/n\mathbb{Z}$$

isomorph ist.

• Eindeutigkeit.

Sei $U \subset \mathbb{Q}/\mathbb{Z}$ Untergruppe der Ordnung n. Wir zeigen:

$$U = \left\langle \overline{\frac{1}{n}} \right\rangle = \left\{ \overline{\frac{0}{n}}, \overline{\frac{1}{n}}, \ldots, \overline{\frac{n-1}{n}} \right\}.$$

Sei dazu $U = \left\{ \overline{\frac{a_1}{b_1}}, \ldots, \overline{\frac{a_n}{b_n}} \right\}$ mit gewissen

$a_1, \ldots, a_n \in \mathbb{Z}$, $b_1, \ldots, b_n \in \mathbb{N}$.

Wegen ord $U = n$ gilt

$$n \cdot \overline{\frac{a_k}{b_k}} = \overline{0} \qquad \forall\ 1 \leq k \leq n \qquad \text{(Klar? siehe unten)}$$

also $$n \cdot \frac{a_k}{b_k} \in \mathbb{Z} \qquad \forall\ 1 \leq k \leq n.$$

$$\Rightarrow b_k \mid n \qquad \forall\ 1 \leq k \leq n$$

Wir Können die Brüche $\frac{a_k}{b_k}$ also derart erweitern, dass wir annehmen Können

$$U = \left\{ \overline{\frac{a_1}{n}}, \ldots, \overline{\frac{a_n}{n}} \right\}.$$

Indem wir die $\frac{a_k}{n}$ modulo $\mathbb{Z}$ reduzieren $\left(\text{z.B. } \overline{\frac{5}{4}} = \overline{\frac{1}{4} + 1} = \overline{\frac{1}{4}} \right)$ Können wir außerdem annehmen, dass

$$a_1, \ldots, a_n \in \{0, \ldots, n-1\}$$

gilt. Wegen ord $U = n$ müssen die a_k aber verschieden sein, so dass aus $\# \{0, \ldots, n-1\} = n = \# \{a_1, \ldots, a_n\}$ folgt:

$$U = \left\{ \overline{\frac{0}{n}}, \overline{\frac{1}{n}}, \ldots, \overline{\frac{n-1}{n}} \right\} = \left\langle \overline{\frac{1}{n}} \right\rangle$$

$\Rightarrow$ Insgesamt folgt: Zu jedem $n \in \mathbb{N}$ gibt es genau eine Untergruppe der Ordnung n in $\mathbb{Q}/\mathbb{Z}$, nämlich

$$\left\langle \overline{\frac{1}{n}} \right\rangle \cong \mathbb{Z}/n\mathbb{Z}$$

$\blacksquare$

Proposition:

Ist G endliche Gruppe, so gilt $\forall g \in G$:

$$g^{\operatorname{ord} G} = e \qquad (\text{bzw. additiv } (\operatorname{ord} G) \cdot g = 0 \ldots)$$

Beweis:

Nach Definition gilt offensichtlich

$$g^{\operatorname{ord} g} = e$$

Nach Lagrange ist $\operatorname{ord} G = K \cdot \operatorname{ord} g$ für ein $K \in \mathbb{N}$.

Also:

$$g^{\operatorname{ord} G} = g^{K \cdot \operatorname{ord} g} = \left(g^{\operatorname{ord} g}\right)^K = e^K = e$$

$\blacksquare$