6. Übungsblatt - Lösungshinweise

1. *Rechengesetze in* $(\mathbb{Z}_n, +, \cdot)$

Beweisen Sie, dass in $(\mathbb{Z}_n, +, \cdot)$, bei einem festen $n \in \mathbb{N} \setminus \{0\}$, folgende Rechengesetze gelten:

a) $\forall_{[a]_n,[b]_n,[c]_n \in \mathbb{Z}_n}\ [a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$ ***2,5 BE***

Seien $[a]_n, [b]_n$ und $[c]_n$ beliebige Elemente aus $\mathbb{Z}_n$, dann sind $a, b, c \in \mathbb{Z}$ und es gilt:

$$\begin{aligned}
[a]_n \cdot ([b]_n + [c]_n) &\overset{\text{Definition 3.1.1}}{\triangleq} [a]_n \cdot [b+c]_n \overset{\text{Definition 3.1.1}}{\triangleq} [a \cdot (b+c)]_n \\
&\overset{\text{Distributivgesetz in } \mathbb{Z}}{\triangleq} [a \cdot b + a \cdot c]_n \overset{\text{Definition 3.1.1}}{\triangleq} [a \cdot b]_n + [a \cdot c]_n \\
&\overset{\text{Definition 3.1.1}}{\triangleq} [a]_n \cdot [b]_n + [a]_n \cdot [c]_n
\end{aligned}$$

∎

b) $\forall_{[a]_n,[b]_n,[c]_n \in \mathbb{Z}_n}\ ([a]_n + [b]_n) \cdot [c]_n = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n$ ***2,5 BE***

Seien $[a]_n, [b]_n$ und $[c]_n$ beliebige Elemente aus $\mathbb{Z}_n$, dann sind $a, b, c \in \mathbb{Z}$ und es gilt:

$$\begin{aligned}
([a]_n + [b]_n) \cdot [c]_n &\overset{\text{Definition 3.1.1}}{\triangleq} [a+b]_n \cdot [c]_n \overset{\text{Definition 3.1.1}}{\triangleq} [(a+b) \cdot c]_n \\
&\overset{\text{Distributivgesetz in } \mathbb{Z}}{\triangleq} [a \cdot c + b \cdot c]_n \overset{\text{Definition 3.1.1}}{\triangleq} [a \cdot c]_n + [b \cdot c]_n \\
&\overset{\text{Definition 3.1.1}}{\triangleq} [a]_n \cdot [c]_n + [b]_n \cdot [c]_n
\end{aligned}$$

∎

c) $\forall_{[a]_n,[b]_n,[c]_n \in \mathbb{Z}_n}\ ([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$ ***1 BE***

Seien $[a]_n, [b]_n$ und $[c]_n$ beliebige Elemente aus $\mathbb{Z}_n$, dann sind $a, b, c \in \mathbb{Z}$ und es gilt:

$$\begin{aligned}
([a]_n + [b]_n) + [c]_n &\overset{\text{Definition 3.1.1}}{\triangleq} [a+b]_n + [c]_n \overset{\text{Definition 3.1.1}}{\triangleq} [(a+b) + c]_n \\
&\overset{\text{Assoziativgesetz in } \mathbb{Z}}{\triangleq} [a + (b+c)]_n \overset{\text{Definition 3.1.1}}{\triangleq} [a]_n + [b+c]_n \\
&\overset{\text{Definition 3.1.1}}{\triangleq} [a]_n + ([b]_n + [c]_n)
\end{aligned}$$

∎

2. *Idee der Produktgruppen verstehen*

Diese Aufgabe soll ihnen helfen, die Idee der Produktgruppen (vgl. Definition 3.3.1) zu durchschauen. Dazu bilden wir aus der Diedergruppe $(D_3,\circ)$ mit der Verkettung $\circ$ von Deckabbildungen als Gruppenverknüpfung und der Gruppe $\mathbb{Z}_3 \setminus \{[0]_3, \cdot\}$ mit der Multiplikation $\cdot$von Restklassen als Gruppenverknüpfung wie folgt eine Produktgruppe $(D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\},*)$:

$$D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\} \coloneqq \{(\varphi, z) | \varphi \in D_3, z \in \mathbb{Z}_3 \setminus \{[0]_3\}\}$$
$$(\varphi_1, z_1) * (\varphi_2, z_2) \coloneqq (\varphi_1 \circ \varphi_2, z_1 \cdot z_2)$$

a) Zeigen Sie, dass gilt:

$$\forall_{\mathrm{a,b} \in D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\}}\ \mathrm{a} * \mathrm{b} \in D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\}$$

1,5 BE

Da sowohl $(D_3,\circ)$ als auch $(\mathbb{Z}_3 \setminus \{[0]_3\},\cdot)$ Gruppen sind, sind sie bzgl. ihrer jeweiligen Gruppenoperationen $\circ$ bzw. $\cdot$ abgeschlossen. Es gilt also:

$$\forall_{\varphi_1,\varphi_2 \in D_3}\ \varphi_1 \circ \varphi_2 \in D_3 \qquad (i)$$

und

$$\forall_{z_1,z_2 \in \mathbb{Z}_3 \setminus \{[0]_3\}}\ z_1 \cdot z_2 \in \mathbb{Z}_3 \setminus \{[0]_3\} \qquad (ii)$$

Damit ergibt sich:

$$\forall_{(\varphi_1,z_1),(\varphi_2,z_2) \in D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\}}\ (\varphi_1, z_1) * (\varphi_2, z_2)$$
$$\overset{\text{Definition } *}{\triangleq} \left(\overbrace{\varphi_1 \circ \varphi_2}^{\in D_3\ (i)},\ \overbrace{z_1 \cdot z_2}^{\in \mathbb{Z}_3 \setminus \{[0]_3\}\ (ii)}\right) \in D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\}$$

■

b) Zeigen Sie, dass $(D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\},*)$ bzgl. der Verknüpfung * assoziativ ist.

2 BE

Da sowohl $(D_3,\circ)$ als auch $(\mathbb{Z}_3 \setminus \{[0]_3\},\cdot)$ bzgl. ihrer jeweiligen Gruppenoperationen $\circ$ bzw. $\cdot$ assoziativ sind, gilt:

$$\forall_{\varphi_1,\varphi_2,\varphi_3 \in D_3}\ \varphi_1 \circ (\varphi_2 \circ \varphi_3) = (\varphi_1 \circ \varphi_2) \circ \varphi_3 \qquad (\#)$$

und

$$\forall_{z_1,z_2,z_3 \in \mathbb{Z}_3 \setminus \{[0]_3\}}\ z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3 \qquad (\#\#)$$

Damit ergibt sich:

$$\forall_{(\varphi_1,z_1),(\varphi_2,z_2),(\varphi_3,z_3) \in D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\}}\ (\varphi_1, z_1) * \big((\varphi_2, z_2) * (\varphi_3, z_3)\big)$$
$$\overset{\text{Definition } *}{\triangleq} (\varphi_1, z_1) * (\varphi_2 \circ \varphi_3, z_2 \cdot z_3)$$
$$\overset{\text{Definition } *}{\triangleq} \big(\varphi_1 \circ (\varphi_2 \circ \varphi_3), z_1 \cdot (z_2 \cdot z_3)\big)$$
$$\overset{(\#)}{\triangleq} \big((\varphi_1 \circ \varphi_2) \circ \varphi_3, z_1 \cdot (z_2 \cdot z_3)\big)$$
$$\overset{(\#\#)}{\triangleq} \big((\varphi_1 \circ \varphi_2) \circ \varphi_3, (z_1 \cdot z_2) \cdot z_3\big)$$
$$\overset{\text{Definition } *}{\triangleq} (\varphi_1 \circ \varphi_2, z_1 \cdot z_2) * (\varphi_3, z_3)$$
$$\overset{\text{Definition } *}{\triangleq} \big((\varphi_1, z_1) * (\varphi_2, z_2)\big) * (\varphi_3, z_3)$$

■

c) Geben Sie das neutrale Element der Produktgruppe $(D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\},*)$ an und zeigen Sie, dass es das neutrale Element der Verknüpfung * ist. ***2 BE***

Behauptung:
Das neutrale Element der Produktgruppe $(D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\},*)$ bzgl. der Operation $*$ ist $(id,[1]_3)$.

Zu zeigen ist:

$$\forall_{(\varphi,z)\in D_3\times\mathbb{Z}_3\setminus\{[0]_3\}}\ (\varphi,z)*(id,[1]_3)=(\varphi,z)$$

Zunächst gilt:

- id ist das neutrale Element der Diedergruppe $(D_3,\circ)$, es gilt also:
  $$\forall_{\varphi\in D_3}\ \varphi\circ id=\varphi \qquad (\blacksquare)$$
- $[1]_3$ ist das neutrale Element der Gruppe $(\mathbb{Z}_3 \setminus \{[0]_3\},\cdot)$, es gilt also:
  $$\forall_{z\in\mathbb{Z}_3\setminus\{[0]_3\}}\ z\cdot[1]_3=z \qquad (\blacksquare\blacksquare)$$

Damit folgt:

$$\forall_{(\varphi,z)\in D_3\times\mathbb{Z}_3\setminus\{[0]_3\}}\ (\varphi,z)*(id,[1]_3) \overset{\text{Definition }*}{\triangleq} (\varphi\circ id, z\cdot[1]_3) \overset{(\blacksquare)}{\triangleq} (\varphi, z\cdot[1]_3) \overset{(\blacksquare\blacksquare)}{\triangleq} (\varphi,z)$$

$\blacksquare$

d) Zeigen Sie, dass $(D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\},*)$ eine Gruppe ist. ***5,5 BE***

Da in den Aufgaben ***a)*** bis ***c)*** die Gruppenbedingungen (G0), (G1) und (G2) gezeigt wurden, muss nur noch (G3) gezeigt werden, um insgesamt zu zeigen, dass $(D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\},*)$ eine Gruppe ist.

$$D_3\times\mathbb{Z}_3\setminus\{[0]_3\}=\{(id,[1]_3),(id,[2]_3),(d,[1]_3),(d,[2]_3),(d^2,[1]_3),(d^2,[2]_3),$$
$$(s,[1]_3),(s,[2]_3),(ds,[1]_3),(ds,[2]_3),(d^2s,[1]_3),(d^2s,[2]_3)\}$$

Zu jedem Element (φ,z) von $D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\}$ ist das jeweilige inverse Element gesucht, also das Element $(\varphi,z)^{-1}$, für das gilt:

$$(\varphi,z)*(\varphi,z)^{-1}=(id,[1]_3) \qquad (\Delta)$$

Da id das neutrale Element in $(D_3,\circ)$ und $[1]_3$ das neutrale Element in $(\mathbb{Z}_3 \setminus \{[0]_3\},\cdot)$ ist, folgt aus (Δ) zusammen mit der Definition von $*$:

$$(\varphi,z)^{-1}=(\varphi^{-1},z^{-1}) \qquad (\Delta\Delta)$$

Mit Hilfe der Gleichung $(\Delta\Delta)$ kann man Inverse identifizieren.

Es wird nun für jedes einzelne Element von $D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\}$ ein inverses Element angegeben und gezeigt, dass obige Bedingung (Δ) erfüllt ist:

$$(id,[1]_3)*\color{red}{(id,[1]_3)^{-1}}=(id,[1]_3)*\color{red}{(id,[1]_3)} \overset{\text{Definition }*}{\triangleq} (id\circ id,[1]_3\cdot[1]_3)$$
$$\overset{id\text{ ist neutrales Element bzgl.}\circ}{\triangleq} (id,[1]_3\cdot[1]_3) \overset{\text{Definition }\cdot}{\triangleq} (id,[1\cdot 1]_3)=(id,[1]_3)$$

$$(id,[2]_3)*\color{red}{(id,[2]_3)^{-1}}=(id,[2]_3)*\color{red}{(id,[2]_3)} \overset{\text{Definition }*}{\triangleq} (id\circ id,[2]_3\cdot[2]_3)$$
$$\overset{id\text{ neutr. Element bzgl.}\circ}{\triangleq} (id,[2]_3\cdot[2]_3) \overset{\text{Definition }\cdot}{\triangleq} (id,[2\cdot 2]_3)=(id,[4]_3)=(id,[1]_3)$$

$$(d,[1]_3) * (d,[1]_3)^{-1} = (d,[1]_3) * (d^2,[1]_3) \overset{\text{Definition } *}{\triangleq} (d \circ d^2,[1]_3 \cdot [1]_3) = (d^3,[1]_3 \cdot [1]_3)$$
$$\overset{d^3=id}{\triangleq} (id,[1]_3 \cdot [1]_3) \overset{\text{Definition } \cdot}{\triangleq} (id,[1 \cdot 1]_3) = (id,[1]_3)$$

$$(d,[2]_3) * (d,[2]_3)^{-1} = (d,[2]_3) * (d^2,[2]_3) \overset{\text{Definition } *}{\triangleq} (d \circ d^2,[2]_3 \cdot [2]_3) = (d^3,[2]_3 \cdot [2]_3)$$
$$\overset{d^3=id}{\triangleq} (id,[2]_3 \cdot [2]_3) \overset{\text{Definition } \cdot}{\triangleq} (id,[2 \cdot 2]_3) = (id,[4]_3) = (id,[1]_3)$$

$$(d^2,[1]_3) * (d^2,[1]_3)^{-1} = (d^2,[1]_3) * (d,[1]_3) \overset{\text{Definition } *}{\triangleq} (d^2 \circ d,[1]_3 \cdot [1]_3)$$
$$= (d^3,[1]_3 \cdot [1]_3) \overset{d^3=id}{\triangleq} (id,[1]_3 \cdot [1]_3) = (id,[1 \cdot 1]_3) = (id,[1]_3)$$

$$(d^2,[2]_3) * (d^2,[2]_3)^{-1} = (d^2,[2]_3) * (d,[2]_3) \overset{\text{Definition } *}{\triangleq} (d^2 \circ d,[2]_3 \cdot [2]_3)$$
$$= (d^3,[2]_3 \cdot [2]_3) \overset{d^3=id}{\triangleq} (id,[2]_3 \cdot [2]_3) = (id,[2 \cdot 2]_3)$$
$$= (id,[4]_3) = (id,[1]_3)$$

$$(s,[1]_3) * (s,[1]_3)^{-1} = (s,[1]_3) * (s,[1]_3) \overset{\text{Definition } *}{\triangleq} (s \circ s,[1]_3 \cdot [1]_3)$$
$$\overset{s \text{ involutorisch}}{\triangleq} (id,[1]_3 \cdot [1]_3) = (id,[1 \cdot 1]_3) = (id,[1]_3)$$

$$(s,[2]_3) * (s,[2]_3)^{-1} = (s,[2]_3) * (s,[2]_3) \overset{\text{Definition } *}{\triangleq} (s \circ s,[2]_3 \cdot [2]_3)$$
$$\overset{s \text{ involutorisch}}{\triangleq} (id,[2]_3 \cdot [2]_3) = (id,[2 \cdot 2]_3) = (id,[4]_3) = (id,[1]_3)$$

$$(ds,[1]_3) * (ds,[1]_3)^{-1} = (ds,[1]_3) * (ds,[1]_3) \overset{\text{Definition } *}{\triangleq} (ds \circ ds,[1]_3 \cdot [1]_3)$$
$$\overset{ds \text{ involutorisch}}{\triangleq} (id,[1]_3 \cdot [1]_3) = (id,[1 \cdot 1]_3) = (id,[1]_3)$$

$$(ds,[2]_3) * (ds,[2]_3)^{-1} = (ds,[2]_3) * (ds,[2]_3) \overset{\text{Definition } *}{\triangleq} (ds \circ ds,[2]_3 \cdot [2]_3)$$
$$\overset{ds \text{ involutorisch}}{\triangleq} (id,[2]_3 \cdot [2]_3) = (id,[2 \cdot 2]_3) = (id,[4]_3) = (id,[1]_3)$$

$$(d^2s,[1]_3) * (d^2s,[1]_3)^{-1} = (d^2s,[1]_3) * (d^2s,[1]_3) \overset{\text{Definition } *}{\triangleq} (d^2s \circ d^2s,[1]_3 \cdot [1]_3)$$
$$\overset{d^2s \text{ involutorisch}}{\triangleq} (id,[1]_3 \cdot [1]_3) = (id,[1 \cdot 1]_3) = (id,[1]_3)$$

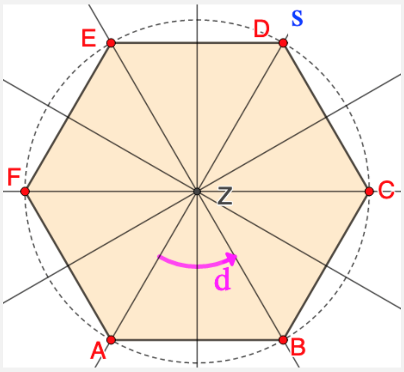
$$(d^2s,[2]_3) * (d^2s,[2]_3)^{-1} = (d^2s,[2]_3) * (d^2s,[2]_3) \overset{\text{Definition } *}{\triangleq} (d^2s \circ d^2s,[2]_3 \cdot [2]_3)$$
$$\overset{d^2s \text{ involutorisch}}{\triangleq} (id,[2]_3 \cdot [2]_3) = (id,[2 \cdot 2]_3) = (id,[4]_3) = (id,[1]_3)$$

■

Alle Gruppenaxiome sind erfüllt, somit handelt es sich bei $(D_3 \times \mathbb{Z}_3 \setminus \{[0]_3\},*)$ um eine Gruppe.

3. Diedergruppe D_6 mit Hilfe von Permutationen notiert

Die Abbildung zeigt ein reguläres Sechseck, bei dem alle Symmetrieachsen (unter anderem die Achse s) und eine Deckdrehung $d := d_{Z,60°}$, abgebildet sind. Mit Hilfe von Achsenspiegelungen und Drehungen lässt sich die Diedergruppe wie folgt darstellen:



$$\{id, d, d^2, d^3, d^4, d^5, s, ds, d^2s, d^3s, d^4s, d^5s\}$$

Diese Menge lässt sich aber auch durch Permutationen in Zykel-Schreibweise darstellen.

a) Geben Sie für jedes Element von D_6 die entsprechende Zykel-Schreibweise an.
Beispiel: $\boldsymbol{d^2} = (\boldsymbol{ACE})(\boldsymbol{BDF})$ *5 BE*

$id = (A)$
$d = (ABCDEF)$
$d^2 = (ACE)(BDF)$
$d^3 = (AD)(BE)(CF)$
$d^4 = (AEC)(BFD)$
$d^5 = (AFEDCB)$

$s = (A)(D)(BF)(CE) = (BF)(CE)$ **Bemerkung:** Die Eckpunkte A und D sind Fixpunkte
$ds = (AB)(CF)(DE)$
$d^2s = (AC)(B)(DF)(E) = (AC)(DF)$ **Bemerkung:** Die Eckpunkte B und E sind Fixpunkte
$d^3s = (AD)(BC)(EF)$
$d^4s = (AE)(BD)(C)(F) = (AE)(BD)$ **Bemerkung:** Die Eckpunkte C und F sind Fixpunkte
$d^5s = (AF)(BE)(CD)$

b) Berechnen Sie das Ergebnis der Verkettung nebenstehender Abbildungen, in der Zykel-Schreibweise und geben Sie jeweils auch an, welche Deckabbildung (Drehung bzw. Achsenspiegelung) des regulären Sechsecks sich als Ergebnis der Verkettung ergibt.

$(ABCDEF) \circ (AD)(BC)(EF)$
$(BF)(CE) \circ (AE)(BD)$
$(AEC)(BFD) \circ (AC)(DF)$
$(ABCDEF) \circ (AEC)(BFD)$

4 BE

i) $(ABCDEF) \circ (AD)(EF)(BC) = (AE)(BD)$

Spiegelung an der Symmetrieachse durch die Eckpunkte C und F

ii) $(BF)(CE) \circ (AE)(BD) = (ACE)(BDF)$

Drehung $d_{Z,120°}$ um 120° um den Mittelpunkt Z

iii) $(AEC)(BFD) \circ (AC)(DF) = (BF)(CE)$

Spiegelung an der Symmetrieachse durch die Eckpunkte A und D

iv) $(ABCDEF) \circ (AEC)(BFD) = (AFEDCB)$
Drehung $d_{Z,300°}$ um 300° um den Mittelpunkt Z