5. Übungsblatt - Lösungshinweise

1. *Die vom Erzeugendensystem $\{d^2, d^3s\}$ erzeugte Untergruppe der Diedergruppe D_6*

a) Bestimmen Sie gemäß Definition 2.2.2 die vom Erzeugendensystem $\{d^2, d^3s\}$ erzeugte Teilmenge $\langle d^2, d^3s\rangle$ von

$$D_6 = \{id, d, d^2, d^3, d^4, d^5, s, ds, d^2s, d^3s, d^4s, d^5s\}.$$

6 BE

Lösungshinweise zu Aufgabe 1a)

Im Folgenden werden die Schritte gemäß Definition 2.2.2 der Reihe nach ausgeführt.

Schritt 0:

$$A_0 = \{d^2, d^3s\}$$

Schritt 1:

- Alle Inverse zu den Elementen aus A_0 werden gebildet:
  - $(d^2)^{-1} = d^4$, da $d^2 \circ d^4 = id$.
    Wir haben ein neues Element gefunden, und beziehen es im nächsten Schritt mit ein.
  - $(d^3s)^{-1} = d^3s$, weil Achsenspiegelungen involutorisch, also selbstinvers sind.
  - Die Menge aller Inverser zu Elementen aus A_0 ist also:
    $(A_0)^{-1} := \{(d^2)^{-1}, (d^3s)^{-1}\} = \{d^4, d^3s\}$
- Alle Verknüpfungen der Elemente von A_0 bilden:
  - $d^2 \circ d^3s = (d^2 \circ d^3) \circ s = d^5 \circ s = d^5s$
    Wir haben ein neues Element gefunden, und beziehen es im nächsten Schritt mit ein.
  - $d^3s \circ d^2 = d^3 \circ (s \circ d^2) \overset{sd^{n-k}=d^ks}{\triangleq} d^3 \circ (d^4 \circ s) = (d^3 \circ d^4) \circ s = d \circ s = ds$
    Wir haben ein neues Element gefunden, und beziehen es im nächsten Schritt mit ein.
  - $d^2 \circ d^2 = d^4$
  - $d^3s \circ d^3s \overset{d^3s \text{ involutorisch}}{\triangleq} id$
    Wir haben ein neues Element gefunden, und beziehen es im nächsten Schritt mit ein.
  - $A_0 \circ A_0 := \{id, d^4, ds, d^5s\}$, die Menge der möglichen Verkettungen aus Elementen von A_0, die noch nicht in A_0 waren.
- $A_1 = A_0 \cup (A_0)^{-1} \cup (A_0 \circ A_0) = \{d^2, d^3s\} \circ \{d^4, d^3s\} \circ \{id, d^4, ds, d^5s\}$
  $= \{id, d^2, d^4, ds, d^3s, d^5s\}$

Schritt 2:

- Alle Inverse zu den Elementen aus A_1 werden gebildet:
  - $(d^4)^{-1} = d^2$, da $d^4 \circ d^2 = id$.
  - $(d^5s)^{-1} = d^5s$, weil Achsenspiegelungen involutorisch sind.
  - $(d \circ s)^{-1} = ds$, weil Achsenspiegelungen involutorisch sind.
  - $(id)^{-1} = id$, weil $id \circ id = id$.
  - Die Menge aller Inverser zu Elementen aus A_1 ist also:
    $(A_1)^{-1} := \{id^{-1}, (d^2)^{-1}, (d^4)^{-1}, (ds)^{-1}, (d^3s)^{-1}, (d^5s)^{-1}\} = \{id, d^2, d^4, ds, d^3s, d^5s\}$
    $= A_1$

- Alle Verknüpfungen der Elemente von A_1 bilden:

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

  - $A_1 \circ A_1 = A_1$, da keine neuen Elemente hinzukommen.
- $A_2 = A_1 \cup (A_1)^{-1} \cup (A_1 \circ A_1) = A_1$
- Da im Schritt 2 keine neuen Elemente dazugekommen sind, kann der Algorithmus hier abgebrochen werden.
  Also gilt: $\langle d^2, d^3s\rangle = A_0 \cup A_1 = \{id, d^2, d^4, ds, d^3s, d^5s\} \subset D_6$

b) Begründen Sie, warum $\left(\langle d^2, d^3s\rangle, \circ\right)$ eine Untergruppe von $(D_6, \circ)$ ist. ***2 BE***

Lösungshinweise zu Aufgabe 1b)

Nach den Untergruppenkriterien (vgl. Satz 2.2.1) ist wegen $\langle d^2, d^3s\rangle \subset D_6$ nur zu zeigen:

(UG1) $\forall_{a,b\in U} a \circ b \in U$ (Abgeschlossenheit)

(UG2) $\forall_{a\in U}\, a^{-1} \in U$ (Inverse in U enthalten)

Wegen der Konstruktion von $\langle d^2, d^3s\rangle$ bei der alle möglichen Verknüpfungen und alle Inverse gebildet werden, ist $\langle d^2, d^3s\rangle$ bzgl. der Verkettung $\circ$ einerseits abgeschlossen (UG1) und enthält andererseits auch alle Inverse zu allen Elementen. Damit ist $(\langle d^2, d^3s\rangle, \circ)$ nach Satz 2.2.1 eine Untergruppe von $(D_6, \circ)$.

c) Ist $\left(\langle d^2, d^3s\rangle, \circ\right)$ kommutativ? Begründen Sie ihre Antwort. ***2 BE***

Lösungshinweise zu Aufgabe 1c)

$\left(\langle d^2, d^3s\rangle, \circ\right)$ ist nicht kommutativ, dies wird bereits in Teilaufgabe a) deutlich, denn:

$d^2 \in \langle d^2, d^3s\rangle$ und $d^3s \in \langle d^2, d^3s\rangle$, jedoch gilt:

$$d^2 \circ d^3s = (d^2 \circ d^3) \circ s = d^5 \circ s = d^5s$$

$$d^3s \circ d^2 = d^3 \circ (s \circ d^2) \overset{sd^{n-k}=d^ks}{\widehat{=}} d^3 \circ (d^4 \circ s) = (d^3 \circ d^4) \circ s = d \circ s = ds$$

und somit $d^2 \circ d^3s \neq d^3s \circ d^2$.

2. Verknüpfungstafel zu $(\{8\mathbb{Z}, 1+8\mathbb{Z}, 2+8\mathbb{Z}, 3+8\mathbb{Z}, 4+8\mathbb{Z}, 5+8\mathbb{Z}, 6+8\mathbb{Z}, 7+8\mathbb{Z}\}, \cdot)$

Erstellen Sie für $(\{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}, \cdot)$ die Verknüpfungstafel bzgl. der Multiplikation als Verknüpfung. *4 BE*

Lösungshinweise zu Aufgabe 2

$\cdot$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$
$[1]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[2]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$
$[3]_8$	$[0]_8$	$[3]_8$	$[6]_8$	$[1]_8$	$[4]_8$	$[7]_8$	$[2]_8$	$[5]_8$
$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$
$[5]_8$	$[0]_8$	$[5]_8$	$[2]_8$	$[7]_8$	$[4]_8$	$[1]_8$	$[6]_8$	$[3]_8$
$[6]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$
$[7]_8$	$[0]_8$	$[7]_8$	$[6]_8$	$[5]_8$	$[4]_8$	$[3]_8$	$[2]_8$	$[1]_8$

3. Nullteiler

Zeigen Sie: Wenn ein Element a eines Rings $(R, +, \cdot)$ ein Nullteiler ist, dann ist entweder $a+a$ ebenfalls ein Nullteiler, oder $a+a=0$. *4 BE*

Lösungshinweise zu Aufgabe 3

Sei $a \in R \setminus \{0\}$ Nullteiler. Dann gibt es ein $b \in R \setminus \{0\}$ mit $a \cdot b = 0$ $(*)$.

1. Fall: $a + a = 0$

Und damit ist der erste Fall schon abgeschlossen. Warum benötigen wir den ersten Fall?

In diesem Fall kann nach Nullteiler-Definition $a+a$ kein Nullteiler sein, weil dies voraussetzt, dass $a + a \neq 0$.

Beispiel für diesen Fall:

In $\mathbb{Z}_8$ ist $[4]_8$ ein Nullteiler, wegen $[4]_8 \cdot [2]_8 = [4 \cdot 2]_8 = [8]_8 = [0]_8$.

Andererseits gilt: $[4]_8 + [4]_8 = [4+4]_8 = [8]_8 = [0]_8$

2. Fall: $a + a \neq 0$

$$(a+a) \cdot b \overset{R \text{ ist distributiv}}{\triangleq} a \cdot b + a \cdot b \overset{(*)}{\triangleq} 0 + 0 \overset{0 \text{ ist Nullelement in } R}{\triangleq} 0$$

Das ist aber gerade die Definition eines Nullteilers.

4. Nullteiler von $(\{8\mathbb{Z}, 1+8\mathbb{Z}, 2+8\mathbb{Z}, 3+8\mathbb{Z}, 4+8\mathbb{Z}, 5+8\mathbb{Z}, 6+8\mathbb{Z}, 7+8\mathbb{Z}\}, \cdot)$

a) Geben Sie für jede der Restklassen $[0]_8$, $[1]_8$, $[2]_8$, $[3]_8$, $[4]_8, [5]_8, [6]_8, [7]_8$ modulo 8 an, ob sie Nullteiler in $(\{8\mathbb{Z}, 1+8\mathbb{Z}, 2+8\mathbb{Z}, 3+8\mathbb{Z}, 4+8\mathbb{Z}, 5+8\mathbb{Z}, 6+8\mathbb{Z}, 7+8\mathbb{Z}\}, \cdot)$ ist und begründen Sie dies. ***4 BE***

Lösungshinweise zu Aufgabe 4a)

- $[0]_8$ ist kein Nullteiler, weil die $[0]_8$ in jedem Produkt $[0]_8 \cdot [1]_8 = [0]_8$, das $[0]_8$, also das neutrale Element der Multiplikation, ergibt, bereits mindestens einmal als Faktor vorkommt.
- $[1]_8$ ist kein Nullteiler, weil ein Produkt, bei dem ein Faktor die $[1]_8$ ist, nur dann gleich $[0]_8$ werden kann, wenn der andere Faktor $[0]_8$ ist, wie etwa bei $[0]_8 \cdot [1]_8 = [0]_8$.
  $[2]_8$, $[4]_8$ und $[6]_8$ sind Nullteiler, weil folgende Produkte, bei denen kein Faktor die $[0]_8$ ist, trotzdem gleich $[0]_8$ ist:
  $[2]_8 \cdot [4]_8 = [8]_8 = [0]_8$, $[4]_8 \cdot [4]_8 = [16]_8 = [0]_8$ und $[6]_8 \cdot [4]_8 = [24]_8 = [0]_8$, …
- $[3]_8$ ist kein Nullteiler, weil ein Produkt, bei dem ein Faktor die $[3]_8$ ist, nur dann gleich $[0]_8$ werden kann, wenn der andere Faktor $[0]_8$ ist, wie etwa bei $[0]_8 \cdot [3]_8 = [0]_8$.
- $[5]_8$ ist kein Nullteiler, weil ein Produkt, bei dem ein Faktor die $[5]_8$ ist, nur dann gleich $[0]_8$ werden kann, wenn der andere Faktor $[0]_8$ ist, wie etwa bei $[0]_8 \cdot [5]_8 = [0]_8$.
- $[7]_8$ ist kein Nullteiler, weil ein Produkt, bei dem ein Faktor die $[7]_8$ ist, nur dann gleich $[0]_8$ werden kann, wenn der andere Faktor $[0]_8$ ist, wie etwa bei $[0]_8 \cdot [7]_8 = [0]_8$.

b) Ist $(\mathbb{Z}_8 \setminus \{[0]_8\}, \cdot)$ eine Gruppe? ***1 BE***

Lösungshinweise zu Aufgabe 4b)

$(\mathbb{Z}_8 \setminus \{[0]_8\}, \cdot)$ ist keine Gruppe.
Zum Beispiel ist $[2]_8$ nicht invertierbar bzgl. $\cdot$, denn $\forall_{x \in \mathbb{Z}_8 \setminus \{[0]_8\}}\ [2]_8 \cdot x \neq [1]_8$.
$\mathbb{Z}_8 \setminus \{[0]_8\}$ ist bzgl. $\cdot$ auch nicht abgeschlossen, denn $[2]_8 \cdot [4]_8 = [8]_8 = [0]_8 \notin \mathbb{Z}_8 \setminus \{[0]_8\}$ (Siehe Verknüpfungstafel).

c) Bestimmen Sie für folgenden Gleichungen jeweils die Lösungsmenge in $\mathbb{Z}_8$:

$$[3]_8 \cdot x = [7]_8$$
$$[4]_8 \cdot x = [0]_8$$
$$[6]_8 \cdot x = [3]_8$$
$$[2]_8 \cdot x = [4]_8$$

4 BE

Lösungshinweise zu Aufgabe 4c)

$$[3]_8 \cdot x = [7]_8 \Rightarrow \mathbb{L} = \{[5]_8\}$$
$$[4]_8 \cdot x = [0]_8 \Rightarrow \mathbb{L} = \{[0]_8, [2]_8, [4]_8, [6]_8\}$$
$$[6]_8 \cdot x = [3]_8 \Rightarrow \mathbb{L} = \{\}$$
$$[2]_8 \cdot x = [4]_8 \Rightarrow \mathbb{L} = \{[2]_8, [6]_8\}$$

Erreichbare Gesamtpunktzahl für dieses Übungsblatt: 27 BE