Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey

Übungsblatt 10

Aufgabe 1 Geben Sie die Verknüfungstabellen der folgenden Monoide an und bestimmen Sie, welches Monoid eine Gruppe ist:

1. S_3
2. $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$
3. $(\mathbb{Z}_4, \cdot)$

Lösung

1. Seien $e = (1)$, $d = (1,2,3)$, $d_2 = (1,3,2)$, $s_1 = (2,3)$, $s_2 = (1,3)$, $s_3 = (1,2)$. Hierbei steht d für ,,nach rechts drehen“ (d_2 für zwei mal nach rechts drehen) und s_i für ,,Spiegeln um i“ (die i-te Komponente wird festgehalten und die beiden anderen getauscht).

   Zeile $\circ$ Spalte:

	e	s_3	s_1	s_2	d_2	d
e	e	s_3	s_1	s_2	d_2	d
s_3	s_3	e	d_2	d	s_1	s_2
s_1	s_1	d	e	d_2	s_2	s_3
s_2	s_2	d_2	d	e	s_3	s_1
d_2	d_2	s_2	s_3	s_1	d	e
d	d	s_1	s_2	s_3	e	d_2

   S_3 ist eine Gruppe.

2.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

   $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ ist eine Gruppe, da 1 das neutrale Element ist und $2^{-1} = 3$, $3^{-1} = 2$ und $4^{-1} = 4$.

3.

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(\mathbb{Z}_4, \cdot)$ ist keine Gruppe, da 2^{-1} nicht definiert ist.

Aufgabe 2

1. Geben Sie alle Untergruppen der folgenden Gruppen an:
   (a) S_3
   (b) $(\mathbb{Z}_8, +)$
2. Finden Sie, falls möglich, zu den beiden Gruppen je zwei Untergruppen, deren Vereinigung keine Untergruppe ist.

Lösung

1. (a) Seien wieder $e = (1)$, $d = (1,2,3)$, $d_2 = (1,3,2)$, $s_1 = (2,3)$, $s_2 = (1,3)$ und $s_3 = (1,2)$. Idee: d und d_2 sind zueinander invers. Ebenso sind alle s_i $(i = 1, \ldots, 3)$ zu sich selbst invers. Die Untergruppen von S_3 sind also: $\{e\}$, S_3 selbst, $\{e, d, d_2\}$, $\{e, s_1\}$, $\{e, s_2\}$ und $\{e, s_3\}$.
   (b) Die Untergruppen von $(\mathbb{Z}_8, +_8)$ sind: $(\mathbb{Z}_8, +_8)$ selbst, $(\{0,2,4,6\}, +_8)$, $(\{0,4\}, +_8)$ und $(\{0\}, +_8)$. Diese Gruppen sind isomorph zu den Teilern von 8, also $(\mathbb{Z}_8, +_8)$, $(\mathbb{Z}_4, +_4)$, $(\mathbb{Z}_2, +_2)$ und $(\mathbb{Z}_1, +_1)$.
2. Es gilt $\{0\} \subseteq \{0,4\} \subseteq \{0,2,4,6\} \subseteq \{0, \ldots, 7\}$, also lassen sich keine zwei Untergruppen von $(\mathbb{Z}_8, +_8)$ finden, die vereinigt keine Gruppe sind. Hingegen ist $M = \{e, s_1\} \cup \{e, s_2\}$ keine Gruppe, da $s_2 \circ s_1 = d_2 \notin M$.

Aufgabe 3 Berechnen Sie:

1. $5^{40} \bmod 3$
2. $(77 \cdot 34) + (85 \cdot 44) \bmod 4$
3. $2^{3^4} \bmod 5$

Lösung

1.

$$\begin{aligned} 5^{40} \bmod 3 &= (5 \bmod 3)^{40} \bmod 3 \\ &= 2^{40} \bmod 3 \\ &= (2^2 \bmod 3)^{20} \bmod 3 \\ &= 1^{20} \bmod 3 \\ &= 1 \end{aligned}$$

2.

$$\begin{aligned} (77 \cdot 34) + (85 \cdot 44) \bmod 4 &= ((77 \cdot 34) \bmod 4 + (85 \cdot 44) \bmod 4) \bmod 4 \\ &= ((77 \cdot 34) \bmod 4 + (85 \bmod 4 \cdot 44 \bmod 4) \bmod 4) \bmod 4 \\ &= ((77 \cdot 34) \bmod 4 + (1 \cdot 0) \bmod 4) \bmod 4 \\ &= ((77 \cdot 34) \bmod 4) \bmod 4 \\ &= (77 \bmod 4 \cdot 34 \bmod 4) \bmod 4 \\ &= (1 \cdot 2) \bmod 4 \\ &= 2 \end{aligned}$$

3.

$$\begin{aligned} 2^{3^4} \bmod 5 &= (2^3 \bmod 5)^{3^3} \bmod 5 \\ &= 3^{3^3} \bmod 5 \\ &= (3^3 \bmod 5)^{3^2} \bmod 5 \\ &= 2^{3^2} \bmod 5 \\ &= 2^9 \bmod 5 \\ &= 2 \end{aligned}$$

Aufgabe 4 Beweisen Sie: Es ist $(a+b)^5 \equiv a^5 + b^5 \bmod 5$ für alle $a, b \in \mathbb{Z}$.

Lösung

$$
\begin{aligned}
(a+b)^5 \bmod 5 &= \left(\sum_{i=0}^{5} \binom{5}{i} a^i b^{5-i}\right) \bmod 5 \\
&= \left(\sum_{i=0}^{5} \binom{5}{i} a^i b^{5-i} \bmod 5\right) \bmod 5 \\
&= \left(\sum_{i=0}^{5} \frac{5!}{(5-i)!i!} a^i b^{5-i} \bmod 5\right) \bmod 5 \\
&= \left(a^5 \bmod 5 + b^5 \bmod 5 + \sum_{i=1}^{4} \frac{5!}{(5-i)!i!} a^i b^{5-i} \bmod 5\right) \bmod 5 \\
&= \left(a^5 \bmod 5 + b^5 \bmod 5 + \sum_{i=1}^{4} \frac{5^{\underline{i}}}{i!} a^i b^{5-i} \bmod 5\right) \bmod 5 \\
&= (a^5 + b^5) \bmod 5
\end{aligned}
$$

Aufgabe 5 Zeigen Sie, dass φ mit

$$\varphi : (\mathbb{Z}, +) \to (m\mathbb{Z}, +), \varphi(x) = mx$$

für $m \in \mathbb{N}$ ein Isomorphismus ist.

Lösung
φ ist injektiv, denn $\varphi(x) = \varphi(y) \Rightarrow mx = my \Rightarrow x = y$. Außerdem ist φ surjektiv, denn: Sei $b \in m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$, dann gibt es ein $a \in \mathbb{Z}$ mit $b = ma$ und somit $\varphi(a) = ma$. φ ist ein Homomorphismus, denn $\varphi(a+b) = m(a+b) = ma + mb = \varphi(a) + \varphi(b)$.