Universität Siegen
Lehrstuhl Theoretische Informatik

Carl Philipp Reh
Daniel König

Diskrete Mathematik für Informatiker

WS 2016/2017

Übung 8

1. Beweisen Sie: Ist $(G, \circ)$ eine Gruppe und $a, b \in G$, so gibt es ein eindeutiges $c \in G$ mit $a \circ c = b$.

2. Beweisen oder widerlegen Sie die folgenden Aussagen: In jeder Gruppe $(G, \circ)$ mit neutralem Element e gilt für alle $a, b \in G$

   a) $a \circ a = a \circ b \Rightarrow a = b$

   b) $a \circ a = b \circ b \Rightarrow a = b$

   c) $a^5 = a \Rightarrow a^4 = a$

   d) $a^5 = e \wedge a^4 = e \Rightarrow a = e$

3. Zeigen Sie, dass es eine Gruppe G und Elemente $a, b \in G$ gibt, so dass die Gleichung $(ab)^{-1} = a^{-1}b^{-1}$ nicht erfüllt ist.

4. Geben Sie die Verknüpfungstabellen der folgenden Monoide an und bestimmen Sie, welches Monoid eine Gruppe ist:

   a) S_3

   b) $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$

   c) $(\mathbb{Z}_4, \cdot)$

5. Berechnen Sie:

   a) $5^{40} \bmod 3$

   b) $(77 \cdot 34) + (85 \cdot 44) \bmod 4$

   c) $2^{3^4} \bmod 5$

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

Lösung zu Übung 8

1. Zum Beweis der Existenz wählt man $c = a^{-1} \circ b$, denn es gilt

$$a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$$

Sei $c' \in G$ ein weiteres Element mit $a \circ c' = b$. Es muss also gelten, dass $a \circ c' = a \circ c$. Verknüpft man dies mit a^{-1}, so erhält man:

$$\begin{aligned} a^{-1} \circ (a \circ c') = (a^{-1} \circ a) \circ c' = e \circ c' = c' \\ = a^{-1} \circ (a \circ c) = (a^{-1} \circ a) \circ c = e \circ c = c \end{aligned}$$

2. a) $a \circ a = a \circ b \Rightarrow a^{-1} \circ a \circ a = a^{-1} \circ a \circ b \Rightarrow a = b$

   b) Gilt nicht in $(\mathbb{Z}_2, +_2)$, da $0 +_2 0 = 1 +_2 1 = 0$.

   c) Gilt nicht in $(\mathbb{Z}_4, +_4)$, da $1^5 = 1$, aber $1^4 = 0$.

   d) $a^5 = e \wedge a^4 = e \Rightarrow a^5 = a^4 \Rightarrow (a^{-1})^4 a^5 = (a^{-1})^4 a^4 \Rightarrow a = e$

3. Diese Gleichheit kann nur in nicht kommutativen Gruppen verletzt sein. Die einfachste solche Gruppe ist S_3. Ihre Elemente sind Permutationen (Bijektionen) auf $\{1, 2, 3\}$, die wir in Zykelschreibweise angeben. Z.B. bedeutet $f = (1, 2, 3)$, dass $f(1) = 2$, $f(2) = 3$ und $f(3) = 1$. Die Gruppenoperation ist die Funktionskomposition (Achtung: $(f \circ g)(x) = g(f(x))$), das neutrale Element die Identität und die inversen Elemente die Umkehrfunktionen. Betrachte $a = (2, 3)$ und $b = (1, 2, 3)$. Wir erhalten $a \circ b = (1, 2)$, $a^{-1} = a$, $b^{-1} = (1, 3, 2)$ und somit

$$(a \circ b)^{-1} = (1, 2) \neq a^{-1} \circ b^{-1} = (2, 3) \circ (1, 3, 2) = (1, 3)$$

4. a) Seien $e = \mathrm{id}$, $d = (1, 2, 3)$, $d_2 = (1, 3, 2)$, $s_1 = (2, 3)$, $s_2 = (1, 3)$, $s_3 = (1, 2)$. 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).
   Erst Spalte, dann Zeile (Spalte $\circ$ Zeile):

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

Für die Inversen erhalten wir $d^{-1} = d_2$ und $d_2^{-1} = d$. Die Spiegelungen sind selbstinvers, also $s_1^{-1} = s_1$, $s_2^{-1} = s_2$ und $s_3^{-1} = s_3$. Insgesamt ist S_3 also eine Gruppe.

b) Spalte $\circ$ Zeile:

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

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

c) Spalte $\circ$ Zeile:

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

1 ist das neutrale Element. $(\mathbb{Z}_4, \cdot)$ ist aber keine Gruppe, da 0^{-1} und 2^{-1} nicht definiert sind.

5. a)

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

b)

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

c)

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

6.

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