Matthias Hamann
Alexander Moch

Mannheim, den 30.11.2020

CS 301 Formale Grundlagen der Informatik, Herbstsemester 2020

Lösungsskizze zum Übungsblatt 10

AUFGABE 10.1:

Zeige, dass die Gruppe $(\mathbb{Z}_5, \cdot)^*$ die $[2]$ als erzeugendes Element besitzt. Zeige weiterhin, dass die Gruppe $(\mathbb{Z}_{12}, \cdot)^*$ kein erzeugendes Element besitzt.

Wir betrachten zuerst $(\mathbb{Z}_5, \cdot)^* = \{[1], [2], [3], [4]\}$*:* $[2]^1 = [2]$*,* $[2]^2 = [4]$*,* $[2]^3 = [3]$ *und* $[2]^4 = [1]$*.*

Für $(\mathbb{Z}_{12}, \cdot)^* = \{[1], [5], [7], [11]\}$ *müssen wir alle Möglichkeiten durchprobieren:*

- $[1]^1 = [1]^2 = [1]^3 = [1]^4 = [1]$
- $[5]^1 = [5], [5]^2 = [1], [5]^3 = [5], [5]^4 = [1]$
- $[7]^1 = [7], [7]^2 = [1], [7]^3 = [7], [7]^4 = [1]$
- $[11]^1 = 11, [11]^2 = [1], [11]^3 = [11], [11]^4 = [1]$

AUFGABE 10.2:

In dieser Aufgabe betrachten wir Permutationen in Zweizeilenform. Im konkreten Fall heißt das, die bijektive Abbildung $p : [6] \to [6]$ wird wie folgt notiert:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ p(1) & p(2) & p(3) & p(4) & p(5) & p(6) \end{pmatrix}.$$

Gegeben seien die beiden Permutationen $\sigma, \pi \in \mathcal{S}_6$, definiert durch:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix} \qquad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 1 & 4 & 2 \end{pmatrix}.$$

a) Bilde die Permutationen $\sigma\pi$, $\pi\sigma$, σ^{-1}, π^{-1}.

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 2 & 3 & 5 \end{pmatrix} \qquad \pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 6 & 2 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 3 & 2 & 6 \end{pmatrix} \qquad \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 5 & 3 & 1 \end{pmatrix}$$

b) Bestimme die Lösung $x \in \mathcal{S}_6$ der Gleichung $\sigma x = \pi$.

Es gilt: $\sigma x = \pi \Leftrightarrow \sigma^{-1}\sigma x = \sigma^{-1}\pi \Leftrightarrow x = \sigma^{-1}\pi$*, also*

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

c) Bestimme $\text{ord}_{\mathcal{S}_6}(\sigma)$. Bilde dazu σ^i für $i = 1, 2, \ldots,$ bis $\sigma^i = id$ gilt (id bezeichnet hier die Identitätsabbildung auf $\{1, \ldots, 6\}$).

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 4 & 2 & 6 \end{pmatrix} \qquad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix}$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 4 & 1 & 6 \end{pmatrix} \qquad \sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 3 & 2 & 6 \end{pmatrix}$$

Schließlich gilt $\sigma^6 = id$.

AUFGABE 10.3:

a) Bestimme alle Elemente und deren Ordnungen in $(\mathbb{Z}_{15}, \cdot)^*$.

$(\mathbb{Z}_{15}, \cdot)^*$	*[1]*	*[2]*	*[4]*	*[7]*	*[8]*	*[11]*	*[13]*	*[14]*
Ordnung	*1*	*4*	*2*	*4*	*4*	*2*	*4*	*2*

b) Setze die partielle Abbildung ϕ, gegeben durch

$$\phi([1]) = ([0], [0])$$
$$\phi([2]) = ([0], [1])$$
$$\phi([7]) = ([1], [1])$$

zu einem Gruppenisomorphismus $\phi : (\mathbb{Z}_{15}, \cdot)^* \to (\mathbb{Z}_2, +) \times (\mathbb{Z}_4, +)$ fort.

Da ϕ ein Gruppenhomomorphismus ist, gilt:

$$\phi(g^{-1}) = \phi(g)^{-1}.$$

Daher können wir sagen:

$$\phi([8]) = \phi([2]^{-1}) = \phi([2])^{-1} = ([0], [1])^{-1} = ([0], [3]),$$
$$\phi([13]) = \phi([7]^{-1}) = \phi([7])^{-1} = ([1], [1])^{-1} = ([1], [3]).$$

Es verbleiben die Elemente mit Ordnung 2. Hier gilt:

$$\phi([14]) = \phi([2] \circ [7]) = \phi([2]) \circ \phi([7]) = ([0], [1]) \circ ([1], [1]) = ([1], [2])$$
$$\phi([11]) = \phi([8] \circ [7]) = \phi([8]) \circ \phi([7]) = ([0], [3]) \circ ([1], [1]) = ([1], [0]).$$

Es bleibt noch $\phi([4]) = ([0], [2])$ übrig. Die gesamte Verknüpfungstabelle befindet sich unten. Die eckigen Klammern wurden in der Tabelle aus Lesbarkeitsgründen weggelassen.

$(\mathbb{Z}_{15},\cdot)^*$ $\phi((\mathbb{Z}_{15},\cdot)^*)$	*1* *(0,0)*	*2* *(0,1)*	*4* *(0,2)*	*7* *(1,1)*	*8* *(0,3)*	*11* *(1,0)*	*13* *(1,3)*	*14* *(1,2)*
1 *(0,0)*	*1* *(0,0)*	*2* *(0,1)*	*4* *(0,2)*	*7* *(1,1)*	*8* *(0,3)*	*11* *(1,0)*	*13* *(1,3)*	*14* *(1,2)*
2 *(0,1)*	*2* *(0,1)*	*4* *(0,2)*	*8* *(0,3)*	*14* *(1,2)*	*1* *(0,0)*	*7* *(1,1)*	*11* *(1,0)*	*13* *(1,3)*
4 *(0,2)*	*4* *(0,2)*	*8* *(0,3)*	*1* *(0,0)*	*13* *(1,3)*	*2* *(0,1)*	*14* *(1,2)*	*7* *(1,1)*	*11* *(1,0)*
7 *(1,1)*	*7* *(1,1)*	*14* *(1,2)*	*13* *(1,3)*	*4* *(0,2)*	*11* *(1,0)*	*2* *(0,1)*	*1* *(0,0)*	*8* *(0,3)*
8 *(0,3)*	*8* *(0,3)*	*1* *(0,0)*	*2* *(0,1)*	*11* *(1,0)*	*4* *(0,2)*	*13* *(1,3)*	*14* *(1,2)*	*7* *(1,1)*
11 *(1,0)*	*11* *(1,0)*	*7* *(1,1)*	*14* *(1,2)*	*2* *(0,1)*	*13* *(1,3)*	*1* *(0,0)*	*8* *(0,3)*	*4* *(0,2)*
13 *(1,3)*	*13* *(1,3)*	*11* *(1,0)*	*7* *(1,1)*	*1* *(0,0)*	*14* *(1,2)*	*8* *(0,3)*	*4* *(0,2)*	*2* *(0,1)*
14 *(1,2)*	*14* *(1,2)*	*13* *(1,3)*	*11* *(1,0)*	*8* *(0,3)*	*7* *(1,1)*	*4* *(0,2)*	*2* *(0,1)*	*1* *(0,0)*

AUFGABE 10.4:

Es seien G und G' Gruppen und $f : G \to G'$ ein Gruppenhomomorphismus.

a) Zeige, dass für alle $g \in G$ gilt: $f(g^{-1}) = f(g)^{-1}$.

Sei e das neutrale Element in $G = (G, \circ)$ und sei e' das neutrale Element in $G' = (G', \bullet)$. Dann gilt:

$$f(g) \bullet f(g^{-1}) = f(g \oplus g^{-1}) = f(e) = e'.$$

Daraus folgt, dass $f(g^{-1}) = f(g)^{-1}$.

b) Zeige: falls f bijektiv ist, so gilt $\mathrm{ord}_G(g) = \mathrm{ord}_{G'}(f(g))$ für alle $g \in G$.

Sei $k = ord_G(g)$. Also ist k die kleinste Zahl, sodass $g^k = e$. Da f ein Gruppenhomomorphismus ist, gilt $f(g)^k = f(g^k) = f(e) = e'$, also ist k eine obere Schranke für $ord_{G'}(f(g))$. Angenommen, es existiert ein $\ell < k$, sodass $e' = f(g)^\ell$ gilt. Da f ein Homomorphismus ist, gilt $e' = f(g^\ell)$ und aufgrund der Bijektivität folgt $f^{-1}(e') = e = g^\ell$. Dies ist ein Widerspruch zu der Annahme, dass k die Ordnung von g ist.

AUFGABE 10.5:

Es seien $G = (G, \circ)$ eine Gruppe und $g \in G$ ein Gruppenelement mit Ordnung $\mathrm{ord}_G(g) = k$. Beweise die folgenden Behauptungen.

a) Die Funktion $f : (\mathbb{Z}_k, +) \to \langle g \rangle$ mit $f([j]) = g^j$ ist ein Gruppenisomorphismus.

Sei e das neutrale Element in $\langle g \rangle$. Es gilt $f([0]) = g^0 = e$. Weiterhin gilt $f([i] + [j]) = f([i + j]) = g^{i+j} = g^i \circ g^j = f([i]) \circ f([j])$. Es ist leicht zu sehen, dass $(\mathbb{Z}_k, +)$ vom Element $[1]$ erzeugt wird und es gilt $[1]^j = [j]$. Somit lässt sich auch sehen, dass $f([j]) = f([1]^j) = g^j$ bijektiv ist.

b) Falls $\mathrm{ord}_G(g) = \infty$, so ist $f : (\mathbb{Z}, +) \to \langle g \rangle$ mit $f(j) = g^j$ ein Gruppenisomorphismus.

Analog zu a).