Matthias Hamann
Alexander Moch

Mannheim, den 23.11.2020

CS 301 Formale Grundlagen der Informatik, Herbstsemester 2020

Lösungsskizze zum Übungsblatt 9

AUFGABE 9.1:

In dieser Aufgabe sei $G = (M, \circ)$ eine Gruppe mit neutralem Element e_G. Weiterhin sei N eine nichtleere Teilmenge von M (d. h. $\emptyset \neq N \subseteq M$) und $U = (N, \circ)$.
U heißt Untergruppe von G (Notation: $U < G$), wenn U wieder eine Gruppe ist. Dies ist genau dann der Fall, wenn die folgenden Bedingungen erfüllt sind:

- U ist abgeschlossen (d. h. $\forall u, v \in N : u \circ v \in N$) und
- U besitzt ein neutrales Element e_U (d. h. $\exists e_U \in N : \forall u \in N : e_U \circ u = u \circ e_U = u$) und
- jedes Element von U besitzt ein Inverses in U (d. h. $\forall u \in N : \exists u' \in N : u \circ u' = u' \circ u = e_U$).

Zeige nun:

a) Ist $U < G$, so sind bzgl. U und G die neutralen Elemente identisch und außerdem (jeweils für $a \in N \subseteq M$) die inversen Elemente identisch.

$e_G \overset{(G)}{=} e_U \circ e_U^{-1} \overset{(U)}{=} (e_U \circ e_U) \circ e_U^{-1} \overset{(G)}{=} e_U \circ (e_U \circ e_U^{-1}) \overset{(G)}{=} e_U \circ e_G \overset{(G)}{=} e_U$.
Sei nun a' das inverse Element für ein $a \in N$ bzgl. U, also $a \circ a' = a' \circ a = e_U = e_G$. Es folgt, dass a' identisch ist zu a^{-1}, dem inversen Element zu a bzgl. G.

b) $U < G \Leftrightarrow \forall u, v \in N : u \circ v^{-1} \in N$. ($v^{-1}$ bezeichnet das inverse Element zu v bzgl. G.)

(⇒): Da U eine Gruppe ist, gibt es zu jedem $v \in N$ ein inverses Element $v^{-1} \in N$ bzgl. U (wegen (a) *auch bzgl. G); wegen Abgeschlossenheit von U ist auch $u \circ v^{-1} \in N$.*
(⇐): Da $N \neq \emptyset$, existiert ein $u \in N$. Aus der Annahme folgt, dass auch $u \circ u^{-1} \in N$, also $e_G \in N$. Als neutrales Element von G erfüllt e_G dabei (da $N \subseteq M$) offenbar insbesondere auch $\forall u \in N : e_G \circ u = u \circ e_G = u$, d. h., U besitzt mit e_G ein neutrales Element. Sei nun $v \in N$ beliebig. Aus der Annahme folgt, dass $e_G \circ v^{-1} \in N$, also $v^{-1} \in N$. Damit gilt aber auch für alle $u, v \in N$ nach der Annahme $u \circ (v^{-1})^{-1} \in N$, also $u \circ v \in N$, d. h., N ist bzgl. $\circ$ abgeschlossen. Damit erfüllt U alle Bedingungen in der Definition einer (Unter-)Gruppe.

c) Ist N endlich, so gilt: $U < G \Leftrightarrow \forall u, v \in N : u \circ v \in N$.

(⇒): Trivial. (siehe Definition des Begriffs der Untergruppe im Aufgabentext oben)
(⇐): Sei $v \in N$ beliebig, aber fixiert. Aus der Annahme folgt $\forall k \in \mathbb{N}^+ : v^k \in N$. Da N endlich ist, existieren $i, j \in \mathbb{N}^+$ mit $i < j$ und $v^i = v^j$.
Sei zuerst $j - i \neq 1$. Dann gilt (bzgl. G) $(v^{-1})^{i+1} v^i = (v^{-1})^{i+1} v^j$ und damit $v^{-1} = v^{j-i-1} \in N$ (da $j - i - 1 \in \mathbb{N}^+$).
Für den Spezialfall $j = i + 1$ gilt (wieder bzgl. G) $(v^{-1})^{i-1} v^i = (v^{-1})^{i-1} v^{i+1}$ und damit $v = v \circ v$. Daraus folgt $v \circ v^{-1} = v \circ v \circ v^{-1}$ bzw. $e_G = v$ und damit schließlich $v = e_G = e_G^{-1} = v^{-1} \in N$.
Aus der Annahme folgt nun $\forall u \in N : u \circ v^{-1} \in N$ und damit (da $v \in N$ beliebig fixiert wurde) $\forall u, v \in N : u \circ v^{-1} \in N$. Die Behauptung folgt nun direkt aus (b).

AUFGABE 9.2:

Es seien $(G_1, \otimes_1)$ und $(G_2, \otimes_2)$ Gruppen mit neutralen Elementen e_1 und e_2. Die Operation $\otimes$ auf $G_1 \times G_2$ sei definiert durch

$$(g_1, g_2) \otimes (g_1', g_2') = (g_1 \otimes_1 g_1', g_2 \otimes_2 g_2').$$

Zeige, dass $(G_1 \times G_2, \otimes)$ eine Gruppe ist.

- *Assoziativität:*

$$\begin{aligned}\big((g_1, g_2) \otimes (g_1', g_2')\big) \otimes (g_1'', g_2'') &= \big((g_1 \otimes_1 g_1') \otimes_1 g_1'', (g_2 \otimes_2 g_2') \otimes_2 g_2''\big) \\ &= \big(g_1 \otimes_1 (g_1' \otimes_1 g_1''), g_2 \otimes_2 (g_2' \otimes_2 g_2'')\big) \\ &= (g_1, g_2) \otimes \big((g_1', g_2') \otimes (g_1'', g_2'')\big)\end{aligned}$$

- *Neutrales Element:*

$$(g_1, g_2) \otimes (e_1, e_2) = (g_1 \otimes_1 e_1, g_2 \otimes_2 e_2) = (g_1, g_2)$$

- *Inverses Element:*

$$(g_1, g_2) \otimes (g_1^{-1}, g_2^{-1}) = (g_1 \otimes_1 g_1^{-1}, g_2 \otimes_2 g_2^{-1}) = (e_1, e_2)$$

AUFGABE 9.3:

a) Bestimme für 71 (genauer: für die Restklasse modulo 256, deren Standardrepräsentant die Zahl 71 ist), ob diese ein Inverses in $(\mathbb{Z}_{256}, \cdot)$ besitzt. Falls ja, so berechne dieses mittels des erweiterten euklidischen Algorithmus.

i	0	1	2	3	4	5	6	7	8
a_i	256	71	43	28	15	13	2	**1**	0
y_i	0	1	-3	4	-7	11	-18	**119**	-256
d_i		3	1	1	1	1	6	2	

Aus der Tabelle lesen wir ab, dass $ggT(71, 256) = 1$ *gilt und* 119 *(genauer: die Restklasse modulo 256, welche die Zahl* 119 *enthält) das gesuchte Inverse ist.*

b) Bestimme für 231, ob diese ein Inverses in $(\mathbb{Z}_{1012}, \cdot)$ besitzt. Falls ja, so berechne dieses mittels des erweiterten euklidischen Algorithmus.

i	0	1	2	3	4	5	6	7
a_i	1012	231	88	55	33	22	**11**	0
y_i	0	1	-4	9	-13	22	-35	92
d_i		4	2	1	1	1	2	

Aus der Tabelle lesen wir ab, dass $ggT(1012, 231) = 11$ *gilt, d.h.* 231 *besitzt kein Inverses in* $(\mathbb{Z}_{1012}, \cdot)$.

AUFGABE 9.4:

Zeige, dass für alle natürlichen Zahlen $k, n \in \mathbb{N}$ mit $0 < k < n$ gilt:

$$\mathrm{ord}_{(\mathbb{Z}_n,+)}([k]) = \frac{n}{\mathrm{ggT}(n,k)}.$$

Das Problem lässt sich umformulieren zu

$$ord_{(\mathbb{Z}_n,+)}([k]) = min\{x,\ sodass\ k \cdot x = n \cdot y,\ wobei\ x, y \in \mathbb{N}\}.$$

Gemäß dem Satz von Fermat-Lagrange gilt, dass $ord_{(\mathbb{Z}_n,+)}([k]) = x$ *ein Teiler von* n *sein muss. Somit existiert ein* $a \in \mathbb{N}$*, sodass gilt* $x = n/a$*. Entsprechend lässt sich die Bedingung umformulieren:*

$$k \cdot x = n \cdot y \Longleftrightarrow k \cdot \frac{n}{a} = n \cdot y \Longleftrightarrow \frac{k}{a} = y.$$

Da y *eine natürliche Zahl ist, muss* a *sowohl ein Teiler von* n*, als auch von* k *sein. Um* x *zu minimieren, muss* a *als größte solche Zahl gewählt werden. Es folgt* $a = ggT(n,k)$ *und* $x = \frac{n}{ggT(n,k)}$*.*

AUFGABE 9.5:

Sei G eine Gruppe und seien H und H' Untergruppen von G. Zeige, dass dann auch $H \cap H'$ eine Untergruppe von G ist.

Sind $a, b \in H, H'$*, so gilt auch, dass* $a \circ b \in H, H'$ *und somit folgt, dass* $a \circ b \in H \cap H'$*. Sei* e *das neutrale Element der Gruppe* G*. Es folgt aus der Definition der Untergruppe, dass* $e \in H, H'$*. Somit gilt auch* $e \in H \cap H'$*. Sei* $a \in H, H'$*, so ist auch sein Inverses* $a^{-1} \in H, H'$*. Folglich ist auch* $a \in H \cap H'$ *und* $a^{-1} \in H \cap H'$*.*