Matthias Hamann
Alexander Moch

Mannheim, den 23.11.2020

CS 301 Formale Grundlagen der Informatik, Herbstsemester 2020

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.

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.)

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

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.

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.

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

AUFGABE 9.4:

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

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

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.