Prof. Dr. F. Schuricht
Dr. M. Herrich
F. Friedrich

6. Übung am 1. Oktober 2024 für die Gruppe „Lehramt Math Spezial“
Thema: Grundlagen der Gruppentheorie und Modulorechnung

Das sechste Übungsblatt beschäftigt sich mit den Grundlagen der Gruppentheorie und Modulorechnung. Wir verwenden wieder das Lehrbuch „Einführung in das mathematische Arbeiten“ von Hermann Schichl und Roland Steinbauer[1], speziell die Kapitel 5.1 und 5.2.

Übungsaufgaben Teil 1: Grundlagen der Gruppentheorie

Aufgabe 1

Lesen Sie die Definition 5.1.2. Überprüfen Sie anschließend in jeder der folgenden Teilaufgaben, ob die angegebene Operation $\circ$ zwischen zwei Elementen aus M eine Verknüpfung auf M, das heißt eine Abbildung $\circ : M \times M \to M$, begründet.

(a) $M := \{0, 1\}, \quad a \circ b := ab$

(b) $M := \{0, 1, 2\}, \quad a \circ b := ab$

(c) $M := \{\alpha, \beta, \gamma, \delta\}, \quad a \circ b := a$

(d) $M := \mathbb{Q}, \quad a \circ b := \sqrt{|ab|}$

(e) $M := \mathbb{R} \setminus \{0\}, \quad a \circ b := \dfrac{a}{b}$

(f) $M := \mathbb{Z} \setminus \{0\}, \quad a \circ b := \dfrac{a}{b}$

Aufgabe 2

Lesen Sie die Definition 5.2.2. In jeder der folgenden Teilaufgaben sind eine Menge M sowie eine Abbildung $\circ : M \times M \to M$ gegeben. Untersuchen Sie jeweils, ob $\circ$ eine assoziative Verknüpfung auf M ist. Handelt es sich bei $(M, \circ)$ demzufolge um eine Halbgruppe?

(a) $M := \mathbb{R}, \quad a \circ b := ab - 4$

(b) $M := \mathbb{Z}, \quad a \circ b := a + b - 8$

Aufgabe 3

Lesen Sie die Definition 5.2.10. Überprüfen Sie für jedes der folgenden Gruppoide, ob es ein neutrales Element besitzt. Falls ja, geben Sie dieses an.

(a) $(\mathbb{N}_0, +)$, $(\mathbb{N}, +)$, $(\mathbb{R}, +)$

(b) $(\mathbb{N}_0, \cdot)$, $(\mathbb{N}, \cdot)$, $(\mathbb{R}, \cdot)$

(c) $(M, \circ)$ mit $M := \mathbb{R} \setminus \{0\}$ und $a \circ b := ab - 4$

(d) $(M, \circ)$ mit $M := \mathbb{Z}$ und $a \circ b := a + b - 8$

[1] über die SLUB verfügbar unter `https://katalog.slub-dresden.de/id/0-1030104662`

Aufgabe 4

Lesen Sie die Definition 5.2.25. Untersuchen Sie für jedes der folgenden Gruppoide $(M, \circ)$, ob die Verknüpfung $\circ$ kommutativ ist.

(a) $M := \mathbb{R}, \quad a \circ b := ab - 4.$

(b) $M := \mathbb{Z}, \quad a \circ b := a + b - 8.$

(c) $M := \mathbb{R} \setminus \{0\}, \quad a \circ b := \dfrac{a}{b}$

(d) $M := \mathbb{R} \setminus \{0\}, \quad a \circ b := \dfrac{a(1 + \frac{b}{a})}{2}$

Aufgabe 5

Lesen Sie die Definition 5.2.29. Überprüfen Sie in jeder der folgenden Teilaufgaben, ob in den angegebenen Gruppoiden jedes Element ein zugehöriges inverses Element besitzt. Geben Sie dieses, wenn möglich, an.

(a) $(\mathbb{N}_0, +),\ (\mathbb{N}_0, \cdot)$

(b) $(\mathbb{Z}, +),\ (\mathbb{Z}, \cdot)$

(c) $(\mathbb{Q}, +),\ (\mathbb{Q}, \cdot)$

(d) $(\mathbb{R}, +),\ (\mathbb{R} \setminus \{0\}, \cdot)$

(e) $(M, \circ)$ mit $M := \mathbb{Z}$ und $a \circ b := a + b - 8$

Aufgabe 6

Lesen Sie die Definition 5.2.35. Bei welchen der Gruppoide aus den Aufgaben 2–5 handelt es sich um Gruppen?

Übungsaufgaben Teil 2: Modulorechnung

Wir definieren zunächst auf den ganzen Zahlen den Rest einer Zahl a bei Division durch b:

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann lässt sich a eindeutig darstellen als $a = q \cdot b + r$, wobei $q \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $r < |b|$. Die Zahl r wird als *Divisionsrest* oder einfach nur *Rest* bei Division von a durch b bezeichnet.
Beispiel: $7 = 2 \cdot 3 + 1$, d.h der Rest von 7 bei Division durch 3 ist 1.

Wir möchten uns nun der Modulorechnung widmen. Die exakte Einführung erfolgt über eine sogenannte Relation. Für unsere Zwecke reicht folgende Definition:

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann ist $a \equiv b \pmod{n}$ (Lies: „a kongruent zu b modulo n“) genau dann, wenn der Rest von a bei Division durch n mit dem Rest von b bei Division durch n übereinstimmt. Bezeichnet $r \in \{0, \ldots, n-1\}$ diesen gemeinsamen Divisionsrest, gilt im Falle $a \equiv b \pmod{n}$ dann insbesondere auch $a \equiv r \pmod{n}$ und $b \equiv r \pmod{n}$.
Beispiele:

- $7 = 2 \cdot 3 + 1$, also ist $7 \equiv 1 \pmod{3}$.
- $25 = 8 \cdot 3 + 1$, also ist auch $25 \equiv 1 \pmod{3}$.
- Da 7 und 25 bei Division durch 3 den gleichen Divisionsrest haben, gilt auch $7 \equiv 25 \pmod{3}$.

Aufgabe 7

(a) Bestimmen Sie für jede der folgenden Zahlen a_i, $i = 1, \ldots, 5$, diejenige Zahl $r \in \{0, \ldots, 4\}$, für die $a_i \equiv r \pmod 5$ gilt.

$$a_1 = 22, \quad a_2 = 41, \quad a_3 = 100, \quad a_4 = 2024, \quad a_5 = -7$$

(b) Bestimmen Sie für jede der folgenden Zahlen a_i, $i = 1, \ldots, 5$, diejenige Zahl $r \in \{0, \ldots, 5\}$, für die $a_i \equiv r \pmod 6$ gilt.

$$a_1 = 22, \quad a_2 = 41, \quad a_3 = 100, \quad a_4 = -7, \quad a_5 = -32$$

Aufgabe 8

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$. Es seien r der Rest von a bei Division durch n und s der Rest von b bei Division durch n. Beweisen Sie:

(a) $(a + b) \equiv (r + s) \pmod n$

(b) $(a \cdot b) \equiv (r \cdot s) \pmod n$

Mit Hilfe der Modulorechnung wollen wir nun, für jede Zahl $n \in \mathbb{N}$ mit $n \geq 2$, zwei spezielle Gruppoide $(\mathbb{Z}_n, \bigoplus)$ und $(\mathbb{Z}_n, \bigodot)$ definieren. Die Grundmenge $\mathbb{Z}_n$ beider Gruppoide ist dabei definiert durch

$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}.$$

Für zwei Elemente $a, b \in \mathbb{Z}_n$ definieren wir

- $a \bigoplus b$ als dasjenige Element r aus $\mathbb{Z}_n$, für das gilt: $a + b \equiv r \pmod n$,
- $a \bigodot b$ als dasjenige Element r aus $\mathbb{Z}_n$, für das gilt: $a \cdot b \equiv r \pmod n$.

Mit den nicht eingekreisten Operationen „+“ bzw. „·“ sind dabei die übliche Addition bzw. die übliche Multiplikation in den natürlichen Zahlen gemeint.

In den folgenden beiden Aufgaben wollen wir nun für die neu eingeführten Gruppoide Verknüpfungstabellen aufstellen und Eigenschaften untersuchen.

Aufgabe 9

Stellen Sie für $n = 2$, $n = 3$ und $n = 4$ jeweils die Verknüpfungstabellen für die Gruppoide $(\mathbb{Z}_n, \bigoplus)$ und $(\mathbb{Z}_n, \bigodot)$ auf.

Aufgabe 10

Lesen Sie aus den Tabellen der Aufgabe 9 jeweils das neutrale Element des Gruppoids ab. Geben Sie außerdem jeweils zu jedem Element das zugehörige inverse Element an, sofern dieses existiert. Bei welchen der Gruppoide aus Aufgae 9 handelt es sich um Gruppen?