Mathe für die Informatik I – WiSe 2017
Dr. Samuel Hetterich

Blatt 4 — Abgabe: Mo 20.11.2017, 10:00 Uhr

Hinweis:
▶ Denken Sie an den OMB+ Kurs (`https://www.ombplus.de`) - dort absolvieren Sie bitte die Lektion II (Gleichungen in einer Unbekannten) und die Lektion IV (Lineare Gleichungssysteme). In Ihrer Übungsstunde der 5. Vorlesungswoche (13.-17.11) werden Sie einen Test über die Inhalte dieser Lektionen schreiben. Mit Hilfe dieses Testes können Sie Zusatzpunkte erwerben - diese Punkte werden Ihnen als Hausaufgabenpunkte angerechnet, aber nicht auf die zu erreichende Gesamthausaufgabenpunktzahl dazugezählt.

Aufgabe 4.1 — 6 Punkte

a) Sei

- ▶ $G := \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} : x_1, x_2, x_3 \in \mathbb{R} \right\}$ (der gewöhnliche $\mathbb{R}^3$)
- ▶ für $\vec{x}, \vec{y} \in G$ mit $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ und $\vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$ die Addition definiert als $\vec{x} \oplus \vec{y} := \begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ x_3+y_3 \end{pmatrix}$

Zeigen Sie, dass das Paar $(G, \oplus)$ eine abelsche Gruppe ist.

Hinweis: Sie dürfen als bereits bewiesen voraussetzen, dass $(\mathbb{R}, +)$ eine abelsche Gruppe ist.

b) Zeigen Sie, dass das Paar $(\{1, 2, 3, 4, 5, 6\}, \odot_7)$ eine abelsche Gruppe ist.

c) Für welche $n \in \mathbb{N}$ ist $(\{1, 2, \ldots, n-1\}, \odot_n)$ eine Gruppe? Beweisen Sie Ihre Antwort.
Hinweis: Sie dürfen als bereits bewiesen voraussetzen, dass die Verknüpfungen $\odot_n$ assoziativ sind.

Aufgabe 4.2 — 4 Punkte

Beweisen Sie, dass die Gleichung $s \cdot a + t \cdot b = c$ genau dann eine Lösung $s, t \in \mathbb{Z}$ hat, wenn c ein Vielfaches von $\mathrm{ggT}(a, b)$ ist.

Aufgabe 4.3 — 4 Punkte

Es sei $G := \{a, b, c, d, g, h\}$ und $\circ : G \times G \to G$ eine Verknüpfung mit der folgenden Verknüpfungstabelle:

$\alpha \circ \beta$	$\beta =$ a	b	c	d	g	h
$\alpha =$ a	c	g	b	a	h	d
b	g	d	h	b	a	c
c	b	h	g	c	d	a
d	a	b	c	d	g	h
g	h	a	d	g	c	b
h	d	c	a	h	b	g

Das Paar $(G, \circ)$ bildet eine Gruppe (dies muss/soll nicht bewiesen werden).

a) Nennen Sie das neutrale Element e in $(G, \circ)$.

b) Bestimmen Sie für alle Elemente in G jeweils das Inverse Element.

c) Ist $(G, \circ)$ eine abelsche Gruppe? (Geben Sie eine Begründung!)

d) Zeigen Sie, dass das Assoziativgesetz für die Elemente a, b, c (das sind keine Variablen - also beliebige Gruppenelemente - sondern speziell die Gruppenelemente a, b, c) gilt, d.h. zeigen Sie $(a \circ b) \circ c = a \circ (b \circ c)$.

Aufgabe 4.4 **7 Punkte**

a) Berechnen Sie die Eulersche φ-Funktion für $n_1 = 17, n_2 = 204$ und $n_3 = 540$.

b) Berechnen Sie $\mathsf{Rest}(2^{167}, 83)$.

c) Berechnen Sie $\mathsf{Rest}(3^{167}, 17)$.

d) Berechnen Sie das inverse Element zur 7 in der Gruppe $(Z_{30}^*, \odot_{30})$.

e) Berechnen Sie das inverse Element zur 11 in der Gruppe $(Z_{41}^*, \odot_{41})$.

f) Hat 12 ein inverses Element modulo 15 (d.h. es gibt ein $s \in \mathbb{Z}$ mit $12 \cdot s \equiv 1 \pmod{15}$)? (Beweisen Sie Ihre Ausssage.)

g) Sei $n \in \mathbb{N}$, $n \geq 2$. Beweisen Sie, dass eine ganze Zahl $a \in \mathbb{Z}$ genau dann ein inverses Element modulo n besitzt (d.h. es gibt ein $s \in \mathbb{Z}$ mit $a \cdot s \equiv 1 \pmod{n}$), wenn $\mathrm{ggT}(a, n) = 1$?

Tipp: Hilft Ihnen die Aussage aus Aufgabe 4.2?

Zusatzaufgabe 4.5 **Für alle, Spaß dran haben!**

Es sei $(G := \{a, b, c, d, g, h\}$ und $\circ : G \times G \to G$ eine Verknüpfung, sodass das Paar $(G, \circ)$ eine Gruppe bildet. Vervollständigen Sie die folgende Verknüpfungstabelle:

$\alpha \circ \beta$		$\beta = a$	b	c	d	g	h
$\alpha =$	a					c	b
	b		d	h			
	c		g				
	d				d		
	g						
	h		a			d	