Universität Heidelberg
Institut für Informatik
Priv.-Doz. Dr. Wolfgang Merkle

1. Dezember 2023

Übungen zur Vorlesung

Mathematik für die Informatik 1

Blatt 7

Aufgabe 1 (6 Punkte)

Es sei d eine natürliche Zahl ungleich 0 und 1. In der Vorlesung wurde gezeigt, dass Addition und Multiplikation auf $\mathbb{Z}$ eine Addition $+$ beziehungsweise Multiplikation $\cdot$ auf der Menge $\mathbb{Z}_d$ der Restklassen modulo d induzieren. Diese Operationen können durch ihre VERKNÜPFUNGSTAFELN dargestellt werden. Die Restklasse werden dabei der Einfachheit halber durch ihren Repräsentanten in $\{0, \ldots, d-1\}$ dargestellt, wir schreiben also $0, \ldots, d-1$ für die Restklassen der Form $[m]_d$ in $\mathbb{Z}_d$. Für $d = 3$ ergeben sich damit beispielsweise folgende Verküpfungstafeln

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

und

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

a) Geben Sie für $d = 6$ und $d = 7$ die Verküpfungstafeln der Addition und Multipllikation auf $\mathbb{Z}_d$ an.

b) Betrachten Sie die Einschränkung der Multiplikation auf $\mathbb{Z}_d$ auf die Menge $\mathbb{Z}_d \setminus \{[0]_d\}$. Dies entspricht dem Übergang von der Funktion $\cdot$ von $\mathbb{Z}_d \times \mathbb{Z}_d$ nach $\mathbb{Z}_d$ zu einer ebenfalls als $\cdot$ geschriebenen Funktion mit Definitionsmenge $(\mathbb{Z}_d \setminus \{[0]_d\}) \times (\mathbb{Z}_d \setminus \{[0]_d\})$.

Leiten Sie aus der Verküpfungstafeln der Multiplikation ab, dass die Einschränkung für $d = 7$ eine Verküpfung auf $\mathbb{Z}_d \setminus \{[0]_d\}$ ist, dies für $d = 6$ aber nicht gilt.

c) Nach Teil b ist die Multiplikation $\cdot$ eine Verknüpfung auf $(\mathbb{Z}_7 \setminus \{[0]_7\}, +)$, deren Verknüpfungstafel ergibt sich aus der Verknüpfungstafel der Multiplikation auf $\mathbb{Z}_7$ indem die Spalte und Zeile für das Argument 0 gestrichen werden.

In der Vorlesung wurde gezeigt, dass $(\mathbb{Z}_p \setminus \{[0]_p, \cdot)$ für jede Primzahl p eine Gruppe ist. Leiten Sie ohne dieses Resultat zu benutzen direkt aus der Verknüpfungstafel der Multiplikation in $\mathbb{Z}_7 \setminus \{[0]_7\}$ ab, dass es in der Struktur $(\mathbb{Z}_7 \setminus \{[0]_7\}, \cdot)$ ein linksneutrales Element und zu jedem Element ein linksinverses Element gibt.

Aufgabe 2 (4 Punkte)

Bestimmen Sie nur mit Bleistift und Papier die natürliche Zahl $44444^{42} \mod 11$. Geben Sie dabei relevante Zwischenergebnisse an und beschreiben Sie Ihr Vorgehen in drei bis vier Sätzen.

Hinweis: Potenzen der Form $x, x^2, x^4, x^8, \ldots$ lassen sich durch sukzessives Quadrieren berechnen. Die Binärdarstellung der Zahl 42 ist 101010, eine Potenz der Form x^{42} lässt sich somit als $x^{32} \cdot x^8 \cdot x^2$ schreiben.

Alternativ lassen sich Potenzen von Restklassen modulo 11 wie folgt berechnen. In der Vorlesung wurde gezeigt, dass $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ für jede Primzahl p eine Gruppe ist, diese hat Ordnung $p-1$. Sei nun allgemein $(G, \cdot)$ eine endliche Gruppe G mit neutralem Element e. Es lässt sich dann zeigen, dass für alle a in G gilt $a^{|G|} = e$, dabei steht $|G|$ für die Größe oder Ordnung der Gruppe G, und die n-te POTENZ a^n eines Gruppenelements a ist induktiv durch $a^0 = e$ und $a^{n+1} = a \cdot a^n$ definiert. Für alle natürlichen Zahlen t und r gilt somit

$$a^{t \cdot |G| + r} = a^{t \cdot |G|} \cdot a^r = (a^{|G|})^t \cdot a^r = e^t \cdot a^r = a^r.$$

Bitte wenden!

Aufgabe 3 (4 Punkte)

Es sei p eine Primzahl. In der Vorlesung wurde gezeigt, dass $(\mathbb{Z}_p, +)$ undd $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ Gruppen sind.

a) Zeigen Sie, dass die Gruppe $(\mathbb{Z}_p, +)$ neben den trivialen Untergruppen $\{[0]_p\}$ und $\mathbb{Z}_p$ keine weiteren Untergruppen hat.

b) Geben Sie eine nichttriviale Untergruppe der Gruppe $(\mathbb{Z}_5 \setminus \{[0]_5\}, \cdot)$ an, das heißt, eine Untergruppe, die verschieden von der Einermenge des neutralen Elements und von der Gruppe selbst ist.

Aufgabe 4 (6 Punkte)

Die Menge $V = R^3$ wird zu einem reellen Vektorraum $(V, +)$, indem die Vektoraddition $+$ und skalare Multiplikation $\cdot$ wie folgt komponentenweise definiert werden

$$(x, y, z) + (x', y', z') \;=\; (x + x', y + y', z + z') \qquad \text{und} \qquad a \cdot (x, y, z) \;=\; (ax, ay, az). \tag{1}$$

Ist für die drei folgenden Paare von Körpern K und K' jeweils $U = K^3$ ein K'-Vektorraum, falls Vektoraddition und skalare Multiplikation gleich den Einschränkungen der entsprechenden Operationen auf V sind, also wie für den Vektorraum V komponentenweise durch (1) definiert sind?

a) Ist $U = \mathbb{R}^3$ ein $\mathbb{Q}$-Vektorraum?

b) ist $U = \mathbb{Q}^3$ ein $\mathbb{R}$-Vektorraum?

c) Ist $U = \mathbb{Q}^3$ ein $\mathbb{Q}$-Vektorraum?

Geben Sie eine kurze anschauliche Begründung für Ihre Antworten.

Hinweis: Untersuchen Sie zunächst, ob die betrachteten Menge U unter der Vektoraddition eine Gruppe bilden. Für $U = \mathbb{R}^3$ wurde das in der Vorlesung gezeigt, für $U = \mathbb{Q}^3 \subseteq \mathbb{R}^3$ bietet es sich an, das Untergruppenkriterium anwenden. Weiter ist zu prüfen, ob die betrachteten Menge U unter skalarer Multiplikation abgeschlossen sind. Ob die Vektorraumgesetze gelten, muss nicht geprüft werden, diese vererben sich jeweils vom reellen Vektorraum $\mathbb{R}^3$, ähnlich wie beim Beweis der Korrektheit des Untervektorraumkriteriums in der Vorlesung.

Abgabe: Bis Freitag, den 8. Dezember 2023, 20:00 Uhr.

Die Übungsblätter müssen in Zweiergruppen bearbeitet und abgegeben werden.

Biete laden Sie Ihre Lösung bis zum Abgabetermin als eine PDF-Datei in Moodle hoch.

Die Übungsblattpartner sind in Moodle nicht hinterlegt. Bitte nennen Sie auf Ihrer Lösung beide Namen. Stellen Sie sicher, dass pro Paar höchstens eine Datei hochgeladen wird, wer von beiden dies tut, können Sie sich aussuchen.