TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften Fachrichtung Mathematik, Institut für Algebra

Prof. Dr. A. Fehm, Dr. C. Zschalig

Algebra und Zahlentheorie (Modul ALGZTH), Sommersemester 2017

1. Übungsblatt für die Übungen vom 3.4.-7.4.2017

Wiederholung: Gruppen, Ringe, Körper, Permutationen, Matrizenkalkül

Ziel dieser Übung ist es, dass Sie einige algebraische Konzepte, die Sie in der Vorlesung LAAG (und möglicherweise in anderen Lehrveranstaltungen) kennengelernt haben, wieder in ihr aktives Wissensreservoir transferieren. Bitte konsultieren Sie ggf. Ihre Vorlesungs- und Übungsskripte und versuchen Sie, die Aufgaben vor der Übung so weit wie möglich zu lösen.

Ü1. Eine Gruppe $G = (G, \circ)$ (wir identifizieren hier die Gruppe mit ihrer Grundmenge) besteht aus einer Grundmenge G und einer Verknüpfung $\circ : G \times G \to G$ (oft wird auch $+$ oder ein anderes Operationszeichen verwendet) mit folgenden Eigenschaften:
(1) $\circ$ operiert *assoziativ* auf G.
(2) Es gibt ein *neutrales Element* $e \in G$ (d.h. es gilt $\forall g \in G : e \circ g = g \circ e = g$).
(3) Zu jedem Element $g \in G$ existiert ein *Inverses* (d.h. $\forall g \in G \exists h \in G : g \circ h = h \circ g = e$), welches oft mit $-g$ oder g^{-1} bezeichnet wird. (siehe LAAG-Skript)

Es sei $(G, \circ)$ eine Gruppe und e das neutrale Element in G.

(a) Zeigen Sie, dass es in G nur ein neutrales Element geben kann.

(b) Zeigen Sie, dass zu einem Gruppenelement $g \in G$ höchstens ein Inverses g^{-1} existiert.

(c) Beweisen Sie die Kürzungsregeln:
$$\forall\, a, b, c \in G : \; a \circ b = a \circ c \implies b = c \quad \text{und} \quad b \circ a = c \circ a \implies b = c.$$

(d) Beweisen Sie, dass für beliebige Gruppenelemente $a, b \in G$ die Gleichungen $ax = b$ bzw. $ya = b$ jeweils eine eindeutige Lösung besitzen.

(e) Durch Ü1c und Ü1d ist gezeigt: Ist G endlich, dann tritt in der Verknüpfungstafel von G jedes Element von G in jeder Zeile und jeder Spalte genau einmal auf. Begründen Sie diese Aussage.

(f) Beweisen Sie die folgenden Formeln:
$$\text{(i) } e^{-1} = e, \quad \text{(ii) } \forall a, b \in G : \; (a \circ b)^{-1} = b^{-1} \circ a^{-1}, \quad \text{(iii) } \forall a \in G : \; (a^{-1})^{-1} = a.$$

Ü2. Füllen Sie die Verknüpfungstafeln so aus, dass eine Gruppe beschrieben wird.

Hinweise:

- Das Symbol 1 bezeichnet in (a) das neutrale Element
- Jede Zeile und jede Spalte muss jedes Element genau einmal enthalten (vgl. mit dem Spiel *sudoku*).
- Zusätzlich muss die Verknüpfung $\circ$ assoziativ sein.

(a)

$\circ$	1	2	3	4
1				
2		1		
3			1	
4				

(b)

$\circ$	a	b	c	d	e	f
a			a			
b		c		f		
c						
d		e		a		
e					c	
f						c

Ü3. Eine *Permutation* einer n-elementigen Menge ist ist eine bijektive Abbildung auf dieser Menge (siehe LAAG-Skript). Oft werden Permutationen in Zyklen- bzw. Zykelschreibweise dargestellt (siehe LAAG-Skript). Die symmetrische Gruppe S_n enthält alle Permutationen der Menge $\{1, \ldots, n\}$ zusammen mit der Hintereinanderausführung (üblicherweise von rechts nach links) als Verknüpfung (siehe LAAG-Skript).

(a) Geben Sie alle Elemente der symmetrischen Gruppe S_3 in Zyklen-/Zykelschreibweise an und stellen Sie die Verknüpfungstafel auf.

(b) Bestimmen Sie alle Untergruppen der S_3.

Ü4. Die Menge der invertierbaren 2×2-Matrizen über dem Körper $\mathbb{R}$ bildet zusammen mit der Matrizenmultiplikation eine Gruppe, die general linear group $GL(2, \mathbb{R})$ (siehe LAAG-Skript). Rekapitulieren Sie, dass das tatsächlich gilt, d.h. begründen Sie, dass $GL(2, \mathbb{R})$ wirklich die Eigenschaften einer Gruppe (Abgeschlossenheit, Assoziativität, neutrales Element, inverse Elemente) besitzt.

Zeigen Sie, dass die Potenzen der Matrix $D = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in GL(2, \mathbb{R})$ (beschreibt eine Drehung um $\frac{\pi}{2}$) eine Untergruppe U_1 von $GL(2, \mathbb{R})$ bilden. Wie viele Elemente hat diese Untergruppe?

Zeigen Sie, dass die Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

eine Untergruppe U_2 von $GL(2, \mathbb{R})$ bilden. Können Sie eine Begründung geben, dass U_1 und U_2 nicht isomorph sind?

Ü5. Für Zahlen $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ (üblicherweise ist $n \geq 2$) schreiben wir $a \equiv b \pmod{n}$, wenn a den selben Rest bei Division durch n lässt wie b bzw. wenn $\exists k \in \mathbb{Z} : a = b + kn$ (siehe LAAG-Skript). Für jedes n ist die Relation $\equiv$ eine Äquivalenz- und sogar Kongruenzrelation, die Klassen heißen Restklassen $\pmod{n}$ (siehe LAAG-Skript). Der Restklassenring $\mathbb{Z}_n$ besteht aus der Menge $\{0, \ldots, n-1\}$ zusammen mit der Addition und der Multiplikation $(\mathrm{mod}\ n)$ (siehe LAAG-Skript).

Stellen Sie für $n \in \{5, 6, 7\}$ die Tafeln für Addition $x + y := (x + y \mod n)$ und Multiplikation $x \cdot y := (x \cdot y \mod n)$ in $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ auf. Begründen Sie (ohne detaillierten Beweis), dass $(\mathbb{Z}_n, +, \cdot)$ für $n \in \{5, 7\}$ jeweils die Körpereigenschaften erfüllt.
Warum trifft das für $n = 6$ nicht zu?

Ü6. Es sei R ein Ring mit Nullelement 0 und Einselement 1 und

$$\mathcal{A} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in R \right\} \subseteq R^{3 \times 3}.$$

(a) Zeigen Sie für $R = \mathbb{Z}$, dass $(\mathcal{A}, \cdot)$ (mit der üblichen Matrizenmultiplikation $\cdot$ als Verknüpfung) eine Gruppe bildet.

(b) Geben Sie für $R = \mathbb{Z}_2$ die Verknüpfungstafel von $\mathcal{A}$ an.