Mathematisches Institut der Universität München | Daniel Rost
Sommersemester 2014 | Lukas-Fabian Moser

Grundlagen der Mathematik II – 2. Tutoriumsblatt

Aufgabe 1 (Rechnen in $\mathbb{Z}_7$). Man betrachte den Körper $(\mathbb{Z}_7, +, \cdot)$ mit $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

a) Man bestimme die Verknüpfungstafeln für $+$ und $\cdot$ in $\mathbb{Z}_7$.

b) Man bestimme $\overline{a}^{-1}$ für alle $\overline{a} \in \mathbb{Z}_7$ mit $\overline{a} \neq \overline{0}$.

c) Man löse die Gleichungen $\overline{5} \cdot x = \overline{3}$ und $\overline{4} \cdot x = \overline{2}$ in $\mathbb{Z}_7$.

d) Man bestimme in Abhängigkeit von $\overline{a} \in \mathbb{Z}_7$ die Lösungsmenge der quadratischen Gleichung $x^2 = \overline{a}$ in $\mathbb{Z}_7$.

Aufgabe 2 (Satz von Euler–Fermat). Es sei $(G, +)$ eine endliche abelsche Gruppe mit genau n Elementen – zur besseren Vorstellung hier zwei mögliche Beispiele für ihre Gruppentafel mit $n = 4$ bzw. $n = 6$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

oder

$+$	0	a	b	c	d	e
0	0	a	b	c	d	e
a	a	0	c	b	e	d
b	b	c	d	e	0	a
c	c	b	e	d	a	0
d	d	e	0	a	b	c
e	e	d	a	0	c	b

oder …

Wir schreiben 0 für das neutrale Element von $(G, +)$ (im ersten Beispiel wäre also $0 = \overline{0}$).
Der *Satz von Euler–Fermat* besagt: Für jedes $g \in G$ ist

$$\underbrace{g + g + \ldots + g}_{n \text{ Summanden}} = 0.$$

a) Man überprüfe die Aussage des Satzes an einigen Elementen der oben angegebenen (oder anderen) endlichen abelschen Gruppen.

b) Man begründe: Addiert man alle Einträge einer Zeile der Gruppentafel von $(G, +)$, so erhält man immer das gleiche Ergebnis, unabhängig davon, welche Zeile gewählt wurde.

c) Man wende b) auf die Zeile 0 und die Zeile des Elements g in der Gruppentafel von G an, um den Satz von Euler–Fermat zu beweisen.

(Um den Beweis zu formulieren, kann man die Elemente von G beispielsweise mit $a_1, \ldots, a_n$ bezeichnen.)

Aufgabe 3 (Körper mit vier Elementen). Es sei $(K, +, \cdot)$ ein Körper mit genau vier Elementen, und zwar sei $K = \{0, 1, a, b\}$ (wobei 0 wie üblich das neutrale Element der Addition in K bezeichnet und 1 das neutrale Element der Multiplikation).

a) Man berechne das Produkt $(1+1)\cdot(1+1)$ in K mit Hilfe des Distributivgesetzes und des Satzes von Euler-Fermat. (Für welche abelsche Gruppe wird hierbei der Satz von Euler-Fermat angewandt?)

b) Man folgere aus a), daß in K die Beziehung $1+1=0$ gelten muß.

c) Man fülle in der Verknüpfungstafel der Addition von K die 0- und die 1-Zeile und -Spalte aus.

d) Man beweise, daß $x+x=0$ für alle $x \in K$ gilt *(Hinweis: Distributivgesetz!)* und vervollständige die Verknüpfungstafel der Addition.

e) Man stelle die Verknüpfungstafel für die Multiplikation von K auf. *(Hinweis: Die* 0*- und die* 1*-Zeile sind unproblematisch. Für den Wert von* a^2 *müssen evtl. mehrere Möglichkeiten probiert werden.)*

Aufgabe 4 („Freshman's Dream"). Es sei p eine Primzahl. Man zeige: Im Körper $\mathbb{Z}_p$ gilt für alle $a, b \in \mathbb{Z}$ die Beziehung

$$(\overline{a}+\overline{b})^p = \overline{a}^p + \overline{b}^p.$$

(Hinweis: Aufgabe 2 c) vom 1. Übungsblatt!)

Die Aussage ist als „Freshman's Dream" – frei übersetzt: „der Traum eines jeden Erstsemesters" – bekannt, weil sie einen Fall beschreibt, in dem die falsche „Rechenregel" $(a+b)^n = a^n + b^n$ ausnahmsweise einmal *zutrifft*.

Dieses Blatt wird in den Tutorien im Zeitraum 28.–30. April 2014 behandelt.