Mathematisches Institut der Universität München
Sommersemester 2014

Daniel Rost
Lukas-Fabian Moser

Grundlagen der Mathematik II
Lösungsvorschlag zum 2. Tutoriumsblatt

Aufgabe 1.

a) Die Additions- und Multiplikationsoperationen in $\mathbb{Z}_7$ ererben sich von der üblichen Addition und Multiplikation in $\mathbb{Z}$; Restklassen werden also addiert bzw. multipliziert, indem man ihre (im Prinzip beliebig zu wählenden) Vertreter addiert bzw. multipliziert. Dies liefert zunächst die folgenden Verknüpfungstafeln:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$

und

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{12}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$	$\overline{15}$	$\overline{18}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{12}$	$\overline{16}$	$\overline{20}$	$\overline{24}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{12}$	$\overline{18}$	$\overline{24}$	$\overline{30}$	$\overline{36}$

Nun gilt aber $\overline{7} = \overline{0}$, $\overline{8} = \overline{1}$ usw. in $\mathbb{Z}_7$, und es ist sinnvoll, zur Benennung von Elementen von $\mathbb{Z}_7$ tatsächlich nur die sieben Bezeichnungen $\overline{0}, \overline{1}, \ldots, \overline{6}$ zu verwenden. Damit erhalten die oben angegebenen Verknüpfungstafeln die folgende Gestalt, die den Vorteil hat, daß die Einträge der Tabelle nur Symbole enthalten, die auch in den Zeilen- und Spaltenbeschriftungen auftauchen:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

und

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Erst an dieser Form der Verknüpfungstafeln kann man beispielsweise direkt ablesen, daß der Ring $\mathbb{Z}_7$ tatsächlich ein Körper ist (denn jede Zeile der Multiplikationstafel außer der Nullzeile enthält einmal $\overline{1}$).

Die Lösungen der weiteren Teilaufgaben kann man nun anhand der Multiplikationstafel von $\mathbb{Z}_7$ ablesen:

b) Das Element $\overline{a}^{-1}$ ist das eindeutig bestimmte Element mit $\overline{a} \cdot \overline{a}^{-1} = \overline{1}$; anhand der Multiplikationstafel ergibt sich:

$\overline{a}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{a}^{-1}$	$\overline{1}$	$\overline{4}$	$\overline{5}$	$\overline{2}$	$\overline{3}$	$\overline{6}$

(Es wurde also in der Zeile $\overline{a}$ die Position des Eintrags $\overline{1}$ gesucht; diese liefert den Wert von $\overline{a}^{-1}$.)

c) Dies funktioniert ähnlich wie in b) (wo wir ja im Prinzip die Gleichung $\overline{a} \cdot x = \overline{1}$ gelöst haben). Ein Blick in die Multiplikationstafel zeigt, daß $x = \overline{2}$ die einzige Lösung der Gleichung $\overline{5} \cdot x = \overline{3}$ ist. – Alternativ kann man auch die Gleichung auflösen und direkt rechnen:

$$\begin{aligned} & \overline{5} \cdot x = \overline{3} && \text{(Auflösen nach } x \ldots\text{)} \\ \iff\ & x = \overline{5}^{-1} \cdot \overline{3} && \text{(Nachschlagen unter b) } \ldots\text{)} \\ \iff\ & x = \overline{3} \cdot \overline{3} && \text{(Nachschlagen in der Multiplikationstafel } \ldots\text{)} \\ \iff\ & x = \overline{2}. \end{aligned}$$

Auf die gleiche Art ergibt sich für die Gleichung $\overline{4} \cdot x = \overline{2}$ in $\mathbb{Z}_7$ die einzige Lösung $x = \overline{4}$.

d) Die Quadrate in $\mathbb{Z}_7$ sind die Einträge auf der Hauptdiagonalen (also der von Nordwest nach Südost verlaufenden Diagonalen) der Multiplikationstafel. Hier tauchen nur die Werte $\overline{0}$, $\overline{1}$, $\overline{2}$ und $\overline{4}$ auf, und zwar gilt genauer:

- Die Gleichung $x^2 = \overline{0}$ hat nur die Lösung $x = \overline{0}$,
- die Gleichung $x^2 = \overline{1}$ hat die Lösungen $x_1 = \overline{1}$ und $x_2 = \overline{6}$,
- die Gleichung $x^2 = \overline{2}$ hat die Lösungen $x_1 = \overline{3}$ und $x_2 = \overline{4}$, und
- die Gleichung $x^2 = \overline{4}$ hat die Lösungen $x_1 = \overline{2}$ und $x_2 = \overline{5}$.

Die Gleichungen $x^2 = \overline{3}$, $x^2 = \overline{5}$ und $x^2 = \overline{6}$ besitzen keine Lösungen.

Für Interessierte: Die Frage, welche Elemente des Körpers $\mathbb{Z}_p$ ($p > 2$ eine Primzahl) Quadrate sind und welche nicht, ist kompliziert, und sie hat die Mathematiker lange beschäftigt. Das Element $\overline{0}$ ist immer ein Quadrat (denn $\overline{0} = \overline{0}^2$); von den übrigen $p - 1$ Elementen sind stets genau die Hälfte Quadrate. Welche dies jedoch sind, ist schwieriger zu sagen; die Antwort liefert das berühmte *Quadratische Reziprozitätsgesetz* von Leonhard Euler (1707–1783) und Carl Friedrich Gauss (1777–1855).

Aufgabe 2.

a) In der angegebenen sechselementigen Gruppe ist beispielsweise

$$b + b + b + b + b + b = (b + b) + (b + b) + (b + b) = d + d + d = b + d = 0.$$

und

$$e + e + e + e + e + e = (e + e) + (e + e) + (e + e) = b + b + b = d + b = 0.$$

b) Da laut Vorlesung in jeder Zeile jedes Element der Gruppe genau einmal vorkommt, stehen in jeder Zeile der Gruppentafel genau die gleichen Elemente, nur in jeweils verschiedener Reihenfolge. Da wir in einer *abelschen* Gruppe arbeiten, ist die Summe all dieser Elemente also stets die gleiche. (Nebenbei: In einer nicht-abelschen Gruppe wäre nicht einmal klar, was mit „der Summe“ der Elemente gemeint sein soll.)

c) Wenn wir, wie vorgeschlagen, die Elemente von G mit $a_1, \ldots, a_n$ bezeichnen (wobei dann im übrigen eines dieser Elemente mit 0 und eines mit dem uns interessierenden Element g identisch sein wird), gilt nach b):

$$\begin{aligned} & \text{Summe der Elemente der } g\text{-Zeile} = \text{Summe der Elemente der } 0\text{-Zeile} \\ \iff\ & (g + a_1) + (g + a_2) + \ldots + (g + a_n) = a_1 + a_2 + \ldots + a_n \\ \iff\ & (a_1 + a_2 + \ldots + a_n) + \underbrace{g + g + \ldots + g}_{n \text{ Summanden}} = a_1 + a_2 + \ldots + a_n \\ \iff\ & \underbrace{g + g + \ldots + g}_{n \text{ Summanden}} = 0. \end{aligned}$$

Aufgabe 3.

a) Es ist $(1+1)\cdot(1+1) = 1\cdot(1+1)+1\cdot(1+1) = 1+1+1+1$, und der Satz von Euler-Fermat für die vierelementige abelsche Gruppe $(K,+)$ besagt, daß dieser Ausdruck den Wert 0 hat.

b) Wir haben in a) gezeigt, daß $(1+1)^2 = 0$ ist. In einem Körper folgt aber aus $x^2 = 0$ bereits $x = 0$, denn Körper sind nullteilerfrei (aus $x \cdot y = 0$ folgt, falls nicht schon $y = 0$ ist, $x = x \cdot y \cdot y^{-1} = 0 \cdot y^{-1} = 0$, also $x = 0$.) Also muß $1 + 1 = 0$ sein.

c) Da 0 das neutrale Element der Addition ist, und wir bereits $1 + 1 = 0$ bewiesen haben, erhalten wir folgendes Fragment einer Verknüpfungstafel:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	?	?
a	a	?		
b	b	?		

Um die Fragezeichen loszuwerden, verwenden wir, daß in jeder Zeile und jeder Spalte einer Gruppentafel (man beachte, daß $(K,+)$ eine Gruppe ist!) jedes Element der Gruppe genau einmal auftaucht. Die Fragezeichen müssen also jeweils für a bzw. b stehen. Wäre nun aber $a + 1 = a$, so würde $1 = 0$ folgen, und das kann nicht sein.[1] Also muß $a + 1 = b$ sein, und damit bleibt nur die folgende Möglichkeit:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b		
b	b	a		

d) Es ist $x + x = x \cdot 1 + x \cdot 1 = x \cdot (1 + 1) = x \cdot 0 = 0$ für alle $x \in K$. Damit können wir die Additionstafel um zwei Einträge ergänzen:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	?
b	b	a	?	0

Die beiden verbliebenen Fragezeichen ergeben sich nun wieder aus der Regel, daß jede Zeile und jede Spalte jedes Element des Körpers einmal enthält: Sie müssen also beide für 1 stehen, so daß sich die Additionstafel

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

ergibt.

[1] Alternative Begründung: Wäre $a + 1 = a$, so müßte das verbleibende Fragezeichen in der zweiten Zeile bzw. Spalte mit b gefüllt werden, und das würde $b + 0 = b + 1$ implizieren, was nicht sein kann.

Man beachte, daß sich diese Additionstafel von derjenigen des Ringes $\mathbb{Z}_4$ unterscheidet! Es lohnt sich erfahrungsgemäß, klarzustellen: Es gibt einen Körper mit vier Elementen – und wir erarbeiten in dieser Aufgabe, wie er aussehen muß –, er hat jedoch nichts mit dem ebenfalls vierelementigen Ring $\mathbb{Z}_4$ zu tun!.

e) Da in der Vorlesung bewiesen (und auch in diesen Lösungsskizzen schon mehrfach verwendet) wurde, daß in jedem Körper $0 \cdot x = 0$ für jedes x gilt, und 1 das neutrale Element der Multiplikation ist, kann man das folgende Fragment der Multiplikationstafel unmittelbar anschreiben:

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

Zum Vervollständigen hilft die Tatsache, daß $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe sein muß: Vergessen wir die 0-Zeile und -Spalte, so muß also jedes der drei Elemente $1, a, b$ in jeder der verbleibenden Zeilen und Spalten einmal auftauchen. Wir müssen also nur klären, ob $a^2 = 1$ oder $a^2 = b$ ist. Im ersten Fall würde sich dann aber zwangsläufig das folgende Bild ergeben:

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	1	b
b	0	b	b	

Dies kann nicht richtig sein, weil sich damit in der letzten Zeile/Spalte doppelte Einträge (und gleichzeitig damit zwangsläufig fehlende Elemente) ergeben. Also muß $a^2 = b$ sein, und es ergibt sich die Multiplikationstafel

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Bemerkung. In dieser Aufgabe haben wir *nicht* bewiesen, daß es einen Körper mit vier Elementen *gibt*! Stattdessen haben wir gezeigt: *Wenn* es einen solchen Körper gibt, *dann* sehen seine Additions- und Multiplikationstafeln aus wie angegeben.

Zum Nachweis der Existenz eines vierelementigen Körpers müßte man nun noch verifizieren, daß durch die angegebenen Additions- und Multiplikationstafeln eine Struktur definiert wird, die alle Axiome eines Körpers erfüllt. Insbesondere wäre also die Gültigkeit des Distributivitätsgesetzes zu zeigen, und wir haben schon im letzten (5. Tutoriums- und 5. Übungsblatt) gesehen, wie mühevoll das ist.

Zum Glück gibt es abstrakte Verfahren, um die Existenz eines vierelementigen Körpers mit weniger Rechenaufwand nachzuweisen (die jedoch in unserer Vorlesung keine Rolle spielen werden). Das definitive Resultat, das im Wesentlichen von Evariste Galois, 1811–1832, stammt, lautet: Es gibt genau dann einen Körper mit n Elementen, wenn n eine Potenz einer Primzahl ist, und die Verknüpfungstafeln dieses Körpers sind dann (bis auf eventuelle Umnumerierung der Elemente) schon eindeutig bestimmt.

Aufgabe 4. Die binomische Formel liefert

$$(a+b)^p = \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n}.$$

Nun haben wir in Aufgabe 2 c) vom 1. Übungsblatt gezeigt, daß die Binomialkoeffizienten $\binom{p}{n}$ für $1 \leq n < p$ allesamt durch p teilbar sind. Wir zerlegen die Summe in den (großen) Teil, der von dieser Regel erfaßt wird, und einen (kleinen) Restteil:

$$(a+b)^p = a^p + b^p + \sum_{n=1}^{p-1} \binom{p}{n} a^n b^{p-n}.$$

Wenn wir nun von dieser Gleichung ganzer Zahlen zu Restklassen in $\mathbb{Z}_p$ übergehen (also „Querstriche über alles setzen“), fällt das gesamte Summenzeichen weg, denn jeder seiner Summanden enthält einen Faktor p, der also in $\mathbb{Z}_p$ zu null wird, und das bedeutet

$$(\overline{a}+\overline{b})^p = \overline{a}^p + \overline{b}^p + \sum_{n=1}^{p-1} \overline{\binom{p}{n}} \overline{a}^n \overline{b}^{p-n} = \overline{a}^p + \overline{b}^p,$$

wie behauptet.