Mathematisches Institut der Universität München
Sommersemester 2014

Daniel Rost
Lukas-Fabian Moser

Grundlagen der Mathematik II
Lösungsvorschlag zum 2. Übungsblatt

Aufgabe 1.

a) Das Vorgehen bei der Bestimmung der Verknüpfungstafeln wurde schon im Lösungsvorschlag zum 2. Tutoriumsblatt, Aufgabe 1 a), erklärt. Ich gebe deshalb hier nur noch die Ergebnisse an:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{8}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$

und

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{3}$	$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{1}$	$\overline{6}$	$\overline{2}$	$\overline{7}$	$\overline{3}$	$\overline{8}$	$\overline{4}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

b) Laut Vorlesung besteht $(\mathbb{Z}_9)^*$ aus allen Klassen $\overline{a} \in \mathbb{Z}_9$, wobei $a \in \{0, 1, \ldots, 8\}$ ist mit $\mathrm{ggT}(a, 9) = 1$. Also ist $(\mathbb{Z}_9)^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$.

Alternativ kann man alle Zeilen bzw. Spalten der Multiplikationstabelle suchen, die den Eintrag $\overline{1}$ enthalten. Dies ist auch das einfachste Verfahren zur Bestimmung der Inversen (vgl. die Lösung zu Aufgabe 1 b) vom 2. Tutoriumsblatt):

$\overline{a}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$\overline{8}$
$\overline{a}^{-1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{2}$	$\overline{4}$	$\overline{8}$

c) Es gilt $\overline{5} \cdot x = \overline{3} \iff x = \overline{5}^{-1} \cdot \overline{3} = \overline{2} \cdot \overline{3} = \overline{6}$ sowie $\overline{4} \cdot x = \overline{2} \iff x = \overline{4}^{-1} \cdot \overline{2} = \overline{7} \cdot \overline{2} = \overline{5}$.

d) Wieder sind die Einträge auf der Hauptdiagonalen der Multiplikationstafel zu betrachten. An ihnen kann man ablesen:

- Die Gleichung $x^2 = \overline{0}$ hat die Lösungen $x_1 = \overline{0}$, $x_2 = \overline{3}$ und $x_3 = \overline{6}$,
- die Gleichung $x^2 = \overline{1}$ hat die Lösungen $x_1 = \overline{1}$ und $x_2 = \overline{8}$,
- die Gleichung $x^2 = \overline{4}$ hat die Lösungen $x_1 = \overline{2}$ und $x_2 = \overline{7}$, und
- die Gleichung $x^2 = \overline{7}$ hat die Lösungen $x_1 = \overline{4}$ und $x_2 = \overline{5}$.

Die Gleichungen $x^2 = \overline{2}$, $x^2 = \overline{3}$, $x^2 = \overline{5}$, $x^2 = \overline{6}$ und $x^2 = \overline{8}$ besitzen keine Lösungen.

Aufgabe 2. Die Kommutativität von G bedeutet, daß die Gruppentafel symmetrisch bezüglich Spiegelung an der Hauptdiagonalen (von „Nordwest“ nach „Südost“) ist. Damit kann man die gegebene Tabelle folgendermaßen auffüllen:

$+$	a	b	c	d	e
a		e	$\boxed{b}$		$\boxed{a}$
b	$\boxed{e}$			a	b
c	b				$\boxed{c}$
d		$\boxed{a}$			
e	a	$\boxed{b}$	c		e

Nun hilft die „Sudoku-Regel“, daß jede Zeile und jede Spalte einer Gruppentafel jedes Element der Gruppe enthält. Damit können wir die letzte Zeile und Spalte auffüllen:

$+$	a	b	c	d	e
a		e	b		a
b	e			a	b
c	b				c
d		a			$\boxed{d}$
e	a	b	c	$\boxed{d}$	e

Die beiden fehlenden Einträge in der ersten Zeile sind c und d. Da die d-Spalte bereits ein d enthält, bleibt nur die folgende Möglichkeit (wir ergänzen gleich symmetrisch die erste Spalte):

$+$	a	b	c	d	e
a	$\boxed{d}$	e	b	$\boxed{c}$	a
b	e			a	b
c	b				c
d	$\boxed{c}$	a			d
e	a	b	c	d	e

In der zweiten Zeile fehlen ebenfalls die Einträge c und d; da die c-Spalte aber bereits ein c enthält, ergibt sich zwangsläufig

$+$	a	b	c	d	e
a	d	e	b	c	a
b	e	$\boxed{c}$	$\boxed{d}$	a	b
c	b	$\boxed{d}$			c
d	c	a			d
e	a	b	c	d	e

In der dritten Zeile fehlen a und e; ein Blick in die d-Spalte verrät, daß nur die folgende Lösung möglich ist:

$+$	a	b	c	d	e
a	d	e	b	c	a
b	e	c	d	a	b
c	b	d	$\boxed{a}$	$\boxed{e}$	c
d	c	a	$\boxed{e}$		d
e	a	b	c	d	e

In der vierten Zeile fehlt nun noch ein b, und die Lösung lautet damit

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

Daß es keine andere Möglichkeit der Vervollständigung gibt, folgt einfach daraus, daß in jedem Schritt die eingetragenen Werte aufgrund der „Sudoku-Bedingung“ alternativlos waren.

In dieser Aufgabe wurde nicht bewiesen, daß es eine fünfelementige Gruppe mit der angegebenen fragmentarischen Gruppentafel *gibt*. Stattdessen haben wir nur gezeigt: *Wenn* es eine solche Gruppe gibt, *dann* sieht ihre Gruppentafel aus wie angegeben.

Um nachzuweisen, daß durch die angegebene Gruppentafel wirklich eine Gruppe definiert wird, müßte man nachprüfen, daß die durch diese Gruppentafel definierte Struktur alle Axiome einer Gruppe erfüllt. Die Existenz eines neutralen Elementes (hier e) ist unmittelbar an der Tafel abzulesen (letzte Zeile und Spalte); ebenso die Existenz von Inversen. Die *Assoziativität* ist aber anhand der Gruppentafel nur höchst mühsam nachzuprüfen (im Prinzip müssen $5 \cdot 5 \cdot 5 = 125$ Gleichungen überprüft werden).

Stattdessen kann man beobachten (aber auch darauf muß man erst einmal kommen!), daß wir eine Gruppe mit der angegebenen Gruppentafel eigentlich schon kennen: Man muß nur a durch $\overline{1}$, b durch $\overline{4}$, c durch $\overline{3}$, d durch $\overline{2}$ und e durch $\overline{0}$ ersetzen, um zu sehen, daß wir hier die Gruppentafel von $(\mathbb{Z}_5, +)$ nachgebaut haben – und die Existenz dieser Gruppe ist uns schon lange bekannt:

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

Warum das funktioniert, wird aber nur mit etwas mehr abstrakter Gruppentheorie sichtbar, als wir zur Verfügung haben.

Aufgabe 3.

a) Jede Zeile der Multiplikationstafel enthält so viele Einträge, wie der Ring Elemente hat. Taucht nun irgendein Element (also etwa die 1) in der Zeile nicht auf, so muß notwendig ein anderes Element mindestens doppelt vorkommen.

Dieses Argument ist im wesentlichen das sogenannte *Schubfachprinzip von Dirichlet*, das besagt: Verteilt man k Objekte auf n Schubfächer, und gilt $k > n$, so landen in mindestens einem Schubfach mindestens zwei Elemente. In unserem Fall sind die „Elemente“ die Plätze in einer festen Zeile der Multiplikationstabelle, die „Schubfächer“ sind die Elemente des Rings R.

Eine andere Formulierung des gleichen Argumentes wäre die folgende: Eine Zeile der Multiplikationstabelle von R kann man auffassen als Wertetabelle einer Abbildung $R \to R$ (und zwar handelt es sich genauer um die Abbildung mit $x \mapsto ax$, wenn wir die Zeile des Elements $a \in R$ betrachten). Die Annahme, daß ein Element des Rings in dieser Zeile *nicht* auftaucht, bedeutet genau, daß diese Abbildung nicht surjektiv ist. Da für Abbildungen zwischen gleich großen endlichen Mengen jedoch Injektivität und Surjektivität äquivalent sind, ist die Abbildung damit auch nicht injektiv, d.h. sie trifft mindestens einen Wert mindestens doppelt.

b) Nehmen wir an, wir betrachten die Zeile des Elements $a \in R$. Wir haben in a) gezeigt, daß unter der gemachten Voraussetzung in der Zeile a ein Eintrag doppelt vorkommt. Das bedeutet genau, daß es $b, c \in R$ gibt mit $b \neq c$, aber $ab = ac$. Daraus folgt aber $0 = ab - ac = a(b - c)$. Wegen $b \neq c$ ist $b - c \neq 0$, und damit ist gezeigt, daß neben der zum Produkt $a \cdot 0 = 0$ gehörigen Null in der Zeile a noch eine weitere Null, nämlich zum Produkt $a \cdot (b - c) = 0$, in der Zeile a steht.

Aufgabe 4.

a) Im Ring $\mathbb{Z}_n$ (und allgemein in jedem kommutativen Ring) ist ein Produkt $x_1 \cdot \ldots \cdot x_n$ genau dann invertierbar, wenn jeder seiner Faktoren invertierbar ist: Denn das Produkt invertierbarer Elemente ist wieder invertierbar, und aus einer Gleichung $x_1 \cdot \ldots \cdot x_n \cdot y = 1$ folgt auch sofort die Invertierbarkeit jedes der x_i (durch Zusammenklammern aller übrigen Faktoren).

Damit ergibt sich die folgende Kette von Äquivalenzen:

$$\begin{aligned}
\overline{(n-1)!} \text{ ist in } \mathbb{Z}_n \text{ invertierbar} &\iff \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{n-1} \text{ ist in } \mathbb{Z}_n \text{ invertierbar} \\
&\iff \overline{1}, \overline{2}, \ldots, \overline{n-1} \text{ sind in } \mathbb{Z}_n \text{ alle invertierbar} \\
&\iff \text{alle Elemente außer } \overline{0} \text{ in } \mathbb{Z}_n \text{ sind invertierbar} \\
&\iff \mathbb{Z}_n \text{ ist ein Körper} \\
&\iff n \text{ ist eine Primzahl.}
\end{aligned}$$

(Die letzte Äquivalenz ist dabei Satz 8.14 aus der Vorlesung.)

b) Es gilt

$$\begin{aligned}
x^2 = 1 &\iff 0 = x^2 - 1 = (x+1)(x-1) \\
&\overset{(*)}{\iff} (x+1=0) \ \vee \ (x-1=0) \\
&\iff (x=-1) \ \vee \ (x=1) \\
&\iff x = \pm 1.
\end{aligned}$$

Im mit $(*)$ markierten Schritt wurde dabei verwendet, daß in einem Körper ein Produkt $a \cdot b$ genau dann den Wert 0 hat, wenn (mindestens) einer der Faktoren a und b den Wert 0 hat.

c) Für $x \in K^*$ gilt $x^{-1} = x \iff 1 = x^2 \iff x = \pm 1$ nach Aufgabe b).

d) „$\Longrightarrow$“. Ist $\overline{(n-1)!} = \overline{-1}$ in $\mathbb{Z}_n$, so ist $\overline{(n-1)!}$ insbesondere invertierbar (es ist ja $\overline{-1} \cdot \overline{-1} = 1$), und nach a) folgt, daß n eine Primzahl ist.

„$\Longleftarrow$“. Im Produkt $\overline{(n-1)!} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{n-1}$ fassen wir jeweils ein Element mit seinem Inversen zu einem Paar zusammen; dies funktioniert, weil ja $(x^{-1})^{-1} = x$ ist. Das Produkt der beiden Elemente eines jeden Paares ist dann $\overline{1}$, und wir können diesen Faktor im Produkt fortlassen.

Nun bilden x und x^{-1} nur dann wirklich ein Paar, wenn nicht zufällig $x = x^{-1}$ ist – dies ist aber nach c) nur für $x = \pm\overline{1}$ der Fall. Damit folgt aber $\overline{(n-1)!} = \overline{1} \cdot \overline{-1} = \overline{-1}$, was zu beweisen war.

Zur Veranschaulichung spielen wir das Argument für $n = 11$ durch: Hier gilt in $\mathbb{Z}_{11}$

$$\begin{aligned}
\overline{(n-1)!} &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{7} \cdot \overline{8} \cdot \overline{9} \cdot \overline{10} \\
&= \overline{1} \cdot (\overline{2} \cdot \overline{6}) \cdot (\overline{3} \cdot 4) \cdot (\overline{5} \cdot \overline{9}) \cdot (\overline{7} \cdot \overline{8}) \cdot \overline{10} \\
&= \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{-1} \\
&= \overline{-1}.
\end{aligned}$$