Mathematisches Institut der Universität München
Sommersemester 2014

Daniel Rost
Lukas-Fabian Moser

Grundlagen der Mathematik II
Lösungsvorschlag zum 3. Übungsblatt

Aufgabe 1.

a) Die Einheiten in $\mathbb{Z}_{16}$ sind genau die Elemente $\overline{a}$ mit $0 \leq a < 16$ und $\mathrm{ggT}(a, 16) = 1$. Da der einzige Primfaktor von 16 die Primzahl 2 ist, ist eine ganze Zahl genau dann teilerfremd zu 16, wenn sie ungerade ist. Die Menge der Einheiten in $\mathbb{Z}_{16}$ ist also

$$\begin{aligned}(\mathbb{Z}_{16})^* &= \left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\right\} \\ &= \left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, -\overline{7}, -\overline{5}, -\overline{3}, -\overline{1}\right\} \\ &= \left\{\pm\overline{1}, \pm\overline{3}, \pm\overline{5}, \pm\overline{7}\right\}.\end{aligned}$$

Die Bestimmung der Inversen ist im Prinzip mit dem Euklidischen Algorithmus möglich; in diesem Fall kann man jedoch auch mit Probieren zum Ziel kommen und findet $\overline{1}^{-1} = \overline{1}$ (dies gilt stets), $\overline{3}^{-1} = \overline{11} = -\overline{5}$, $\overline{5}^{-1} = \overline{13} = -\overline{3}$ und $\overline{7}^{-1} = \overline{7}$. Da außerdem $(-\overline{a})^{-1} = -(\overline{a}^{-1})$ gilt, erhalten wir die folgende Tabelle:

$\overline{a}$	$\pm\overline{1}$	$\pm\overline{3}$	$\pm\overline{5}$	$\pm\overline{7}$
$\overline{a}^{-1}$	$\pm\overline{1}$	$\mp\overline{5}$	$\mp\overline{3}$	$\pm\overline{7}$

Man beachte, daß der Ring $\mathbb{Z}_{16}$ also mehr als zwei invertierbare Elemente mit $\overline{a}^{-1} = \overline{a}$ enthält, nämlich $\pm\overline{1}$ und $\pm\overline{7}$. In einem Körper würde das nicht passieren, siehe Aufgabe 4 c) vom 2. Übungsblatt!

b) Ein Element $\overline{a} \in \mathbb{Z}_{16}$ ist genau dann ein Nullteiler (d.h. es gibt ein $0 \neq \overline{b} \in \mathbb{Z}_{16}$ mit $\overline{a} \cdot \overline{b} = \overline{0}$), wenn $\overline{a}$ nicht invertierbar ist. (Dies gilt laut Vorlesung in jedem *endlichen* kommutativen Ring; bewiesen wurde es in Aufgabe 3 vom 2. Übungsblatt.) Da wir die invertierbaren Elemente schon in a) bestimmt haben, ist die Hälfte der Arbeit schon getan: Die Menge der Nullteiler von $\mathbb{Z}_{16}$ ist genau

$$\begin{aligned}\mathbb{Z}_{16} \setminus (\mathbb{Z}_{16})^* &= \left\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}\right\} \\ &= \left\{\overline{0}, \pm\overline{2}, \pm\overline{4}, \pm\overline{6}, \overline{8}\right\}.\end{aligned}$$

Durch Probieren (es ginge natürlich im Prinzip auch systematischer) findet man nun die folgenden Kombinationen aus $\overline{a}$ und $\overline{b}$ mit $\overline{a}, \overline{b} \neq \overline{0}$ und $\overline{a} \cdot \overline{b} = \overline{0}$:

$\overline{a}$	Mögliche Werte für $\overline{b}$
$\pm\overline{2}$	$\overline{8}$
$\pm\overline{4}$	$\pm\overline{4}, \overline{8}$
$\pm\overline{6}$	$\overline{8}$
$\overline{8}$	$\pm\overline{2}, \pm\overline{4}, \pm\overline{6}, \overline{8}$.

c) Das Kriterium aus der Vorlesung (8.17) beruht auf der Berechnung von $d = \mathrm{ggT}(16, 13)$; da $d = 1$ ist, besitzt die Gleichung genau eine Lösung.[1]

[1] Man beachte, daß das Kriterium eigentlich zweiteilig ist: *Wenn* die Gleichung lösbar ist, so ist d die Anzahl der Lösungen; wenn aber sogar $d = 1$ ist, so ist die Gleichung *in jedem Fall* lösbar – und die Lösung ist eindeutig.

Zum Berechnen der Lösung ist es am einfachsten, die Gleichung unter Verwendung der Invertierbarkeit von $\overline{13}$ direkt umzuformen: $\overline{13} \cdot x = \overline{9} \iff x = \overline{13}^{-1} \cdot \overline{9} = (-\overline{3})^{-1} \cdot \overline{9} = \overline{5} \cdot \overline{9} = \overline{45} = -\overline{3} = \overline{13}$. (Dabei haben wir auch gleich erneut mitbewiesen, daß die Lösung eindeutig ist.)

d) Wir verwenden das Kriterium der Vorlesung: $d := \mathrm{ggT}(16, 12) = 4$ ist kein Teiler von 9, also besitzt die Gleichung keine Lösung.

Aufgabe 2. Wir verwenden das Verfahren aus der Vorlesung (8.17). Die Gleichung lautet $\overline{b} \cdot x = \overline{a}$ in $\mathbb{Z}_n$ mit $a = 24$, $b = 40$, $n = 108$. Es gilt $d := \mathrm{ggT}(n, b) = \mathrm{ggT}(108, 40)$. Daß $d = 4$ ist, könnte man beispielsweise an den Primfaktorzerlegungen $40 = 2^3 \cdot 5$ und $108 = 2^2 \cdot 3^3$ sehen; da wir aber auch eine Darstellung von $\overline{d}$ als Vielfaches von $\overline{b}$ in $\mathbb{Z}_{108}$ benötigen werden, führen wir den Euklidischen Algorithmus dennoch durch:

$$\begin{aligned} 108 &= 2 \cdot 40 + 28 \\ 40 &= 1 \cdot 28 + 12 \\ 28 &= 2 \cdot 12 + \boxed{4} \\ 12 &= 3 \cdot 4 + 0. \end{aligned}$$

Da $d = 4$ ein Teiler von $a = 24$ ist, ist die Gleichung damit lösbar und besitzt $d = 4$ verschiedene Lösungen.
Eine spezielle (partikuläre) Lösung der Gleichung erhalten wir, indem wir zunächst $\overline{d} = \overline{4}$ als Vielfaches von $\overline{b} = \overline{40}$ darstellen und dann ausnutzen, daß $\overline{a} = \overline{6} \cdot \overline{d}$ gilt. Aus dem Euklidischen Algorithmus ergibt sich

$$\begin{aligned} 4 &= 28 - 2 \cdot 12 = 28 - 2 \cdot (40 - 28) \\ &= 3 \cdot 28 - 2 \cdot 40 = 3 \cdot (108 - 2 \cdot 40) - 2 \cdot 40 \\ &= 3 \cdot 108 - 8 \cdot 40. \end{aligned}$$

woraus in $\mathbb{Z}_{108}$ die Beziehung $\overline{4} = -\overline{8} \cdot \overline{40}$ folgt, und damit erhalten wir $\overline{24} = \overline{6} \cdot \overline{4} = \overline{6} \cdot (-\overline{8} \cdot \overline{40}) = -\overline{48} \cdot \overline{40}$. Also ist $x_p := -\overline{48} = \overline{60}$ eine partikuläre Lösung der Gleichung.
Die übrigen Lösungen ergeben sich aus der Lösung x_p durch Addition von Vielfachen von $\frac{n}{d} = \frac{108}{4} = 27$. Die Lösungen der Gleichung sind damit

$$\overline{60}, \quad \overline{60} + \overline{27} = \overline{87}, \quad \overline{60} + \overline{2} \cdot \overline{27} = \overline{114} = \overline{6}, \quad \overline{60} + \overline{3} \cdot \overline{27} = \overline{33},$$

und das bedeutet $L = \{\overline{6}, \overline{33}, \overline{60}, \overline{87}\}$.

Aufgabe 3. Wie im Hinweis empfohlen, gehen wir in mehreren Schritten vor:

a) **1. Schritt:** Lösung der ersten Gleichung $\overline{2} \cdot \overline{x} \stackrel{!}{=} \overline{0}$ in $\mathbb{Z}_4$.

Zunächst ist diese Gleichung lösbar, denn 0 ist ein Vielfaches von $d := \mathrm{ggT}(2, 4) = 2$. Eine partikuläre Lösung ist hier offensichtlich $\overline{0}$. Alle weiteren Lösungen ergeben sich daraus durch Addition aller Klassen von Vielfachen von $\frac{4}{d} = 2$. Damit ergibt sich laut Vorlesung:

$$\begin{aligned} & x \in \mathbb{Z} \text{ ist eine Lösung von } \overline{2} \cdot \overline{x} \stackrel{!}{=} \overline{0} \text{ in } \mathbb{Z}_4 \\ \Big(\iff \quad & \overline{x} \in \{\overline{0},\ \overline{0} \pm \overline{2},\ \overline{0} \pm \overline{2} \cdot \overline{2},\ \dots\} \subset \mathbb{Z}_4 \Big) \\ \iff \quad & x \in \{0,\ 0 \pm 2,\ 0 \pm 2 \cdot 2,\ \dots\} \subset \mathbb{Z} \\ \iff \quad & x \in \{2k \mid k \in \mathbb{Z}\} = 2\mathbb{Z}. \end{aligned}$$

Dies hätte man mit weniger Aufwand ohne Rückgriff auf die Lösungsformel aus der Vorlesung einsehen können: Für eine ganze Zahl $x \in \mathbb{Z}$ gilt $\overline{2} \cdot \overline{x} = \overline{0}$ in $\mathbb{Z}_4 \iff 4 \mid 2x \iff 2 \mid x \iff x \in 2\mathbb{Z}$.

b) **2. Schritt:** Welche der gefunden Lösungen lösen auch die zweite Gleichung $\overline{3} \cdot \overline{x} \stackrel{!}{=} \overline{3}$ in $\mathbb{Z}_9$?

Wir nehmen eine allgemeine Lösung $x \in \mathbb{Z}$ der ersten Gleichung – also ist $x = 2k$ mit einem beliebigen $k \in \mathbb{Z}$ – und überprüfen, für welche Werte von k dieses x auch die zweite Gleichung löst. Wir möchten also

$$\overline{3} \stackrel{!}{=} \overline{3} \cdot \overline{x} = \overline{3} \cdot \overline{2k} = \overline{6} \cdot \overline{k} \quad \text{in } \mathbb{Z}_9.$$

Dies ist eine lineare Gleichung für die Zahl k, die mit dem schon verwendeten Verfahren zu lösen ist:

Sie ist lösbar, weil $\overline{3}$ ein Vielfaches von $d' := \mathrm{ggT}(9,6) = 3$ ist. Eine partikuläre Lösung können wir wieder raten: Wegen $\overline{6} = -\overline{3}$ sieht man, daß $\overline{-1}$ eine Lösung ist. Alle anderen Lösungen ergeben sich durch Addition von Vielfachen von $\frac{9}{d'} = 3$, so daß laut Vorlesung gilt:

$$\begin{aligned}
& k \in \mathbb{Z} \text{ ist eine Lösung von } \overline{6} \cdot \overline{k} \stackrel{!}{=} \overline{3} \text{ in } \mathbb{Z}_9 \\
\Big(\iff \quad & \overline{k} \in \left\{ \overline{-1},\ \overline{-1} \pm \overline{3},\ \overline{-1} \pm \overline{2} \cdot \overline{3},\ \dots \right\} \subset \mathbb{Z}_9 \Big) \\
\iff \quad & k \in \{-1,\ -1 \pm 3,\ -1 \pm 2 \cdot 3,\ \dots\} \subset \mathbb{Z} \\
\iff \quad & k \in \{-1 + 3\ell \mid \ell \in \mathbb{Z}\}\,.
\end{aligned}$$

c) **3. Schritt:** Zusammensetzen der Lösungen.

Insgesamt besagen die gewonnenen Erkenntnisse:

$$\begin{aligned}
& x \in \mathbb{Z} \text{ ist eine Lösung von } \overline{2} \cdot \overline{x} \stackrel{!}{=} \overline{0} \text{ in } \mathbb{Z}_0 \text{ und von } \overline{3} \cdot \overline{x} \stackrel{!}{=} \overline{3} \text{ in } \mathbb{Z}_9 \\
\iff \quad & x = 2k \quad \text{für ein } k \in \mathbb{Z}, \quad \text{und dabei ist } k = -1 + 3\ell \quad \text{für ein } \ell \in \mathbb{Z} \\
\iff \quad & x = 2 \cdot (-1 + 3\ell) \quad \text{für ein } \ell \in \mathbb{Z} \\
\iff \quad & x = -2 + 6\ell \quad \text{für ein } \ell \in \mathbb{Z}.
\end{aligned}$$

Die Lösungsmenge ist damit

$$L = \{6\ell - 2 \mid \ell \in \mathbb{Z}\}\,.$$

Aufgabe 4. Um zu zeigen, daß durch die angegebenen Vorschriften tatsächlich Abbildungen definiert werden, ist nachzuweisen, daß durch sie jedem Element der Quellmenge

a) ein eindeutig bestimmter Funktionswert zugewiesen wird,

b) und daß dieser tatsächlich in der Zielmenge enthalten ist.

Problematisch ist hier nur der Punkt a).

Das mögliche Problem zeigt sich, wenn man die Abbildungsvorschrift von f in Worten ausdrückt: Um das Bild $f(\overline{x})$ einer Klasse $\overline{x} \in \mathbb{Z}_{12}$ zu bestimmen, nehme man einen Repräsentanten $x \in \mathbb{Z}$ der Klasse, versehe ihn mit einem negativen Vorzeichen und nehme dann die Klasse von $-x$ in $\mathbb{Z}_4$. Daß ein auf diese Art gewonnenes Objekt tatsächlich in der Zielmenge $\mathbb{Z}_4$ liegt, ist klar. Ein Problem gibt es aber beim ersten Schritt, in dem *ein* Repräsentant x der Klasse $\overline{x}$ genommen wird: Wenn man zufällig einen anderen Repräsentanten $y \in \mathbb{Z}$ der gleichen Klasse erwischt hat (also $\overline{x} = \overline{y}$ in $\mathbb{Z}_{12}$) und mit diesem weiterarbeitet, erhält man dann den gleichen Funktionswert?

Wir müssen (für die Abbildung f) nachweisen: Sind $x, y \in \mathbb{Z}$ mit $\overline{x} = \overline{y}$ in $\mathbb{Z}_{12}$, so gilt auch $\overline{-x} = \overline{-y}$ in $\mathbb{Z}_4$. Dies erfolgt durch eine kurze Rechnung: Die Voraussetzung $\overline{x} = \overline{y}$ in $\mathbb{Z}_{12}$ bedeutet genau $12 \mid x - y$. Dann ist aber $(-x) - (-y) = y - x$ ebenfalls durch 12 und damit auch durch 4 teilbar, und das bedeutet $\overline{-x} = \overline{-y}$ in $\mathbb{Z}_4$. Dies beweist, daß f tatsächlich als Abbildung definiert ist.

Für die Abbildung g ist das gleiche zu überprüfen: Sind $x, y \in \mathbb{Z}$ mit $\overline{x} = \overline{y}$ in $\mathbb{Z}_4$, so gilt auch $\overline{3x} = \overline{3y}$ in $\mathbb{Z}_{12}$. Aber die Voraussetzung bedeutet $4 \mid x - y$, und durch Multiplikation mit 3 folgt $12 \mid 3(x - y) = 3x - 3y$, also $\overline{3x} = \overline{3y}$ in $\mathbb{Z}_{12}$.

Die Abbildung f ist surjektiv, denn für jedes $x \in \mathbb{Z}$ ist $f(\overline{-x}) = \overline{x}$, also wird jede Klasse in $\mathbb{Z}_4$ getroffen. Sie ist nicht injektiv, denn beispielsweise ist $f(\overline{4}) = \overline{0} = f(\overline{0})$, jedoch $\overline{4} \neq \overline{0}$ in $\mathbb{Z}_{12}$.
Die Abbildung g ist injektiv, denn ihre Werte $g(\overline{0}) = \overline{0}$, $g(\overline{1}) = \overline{3}$, $g(\overline{2}) = \overline{6}$ und $g(\overline{3}) = \overline{9}$ sind in $\mathbb{Z}_{12}$ paarweise verschieden. Sie ist jedoch nicht surjektiv, denn beispielsweise gibt es kein $x \in \mathbb{Z}$ mit $g(\overline{x}) = \overline{1}$: Dies würde nämlich $\overline{1} = \overline{3x} = \overline{3} \cdot \overline{x}$ in $\mathbb{Z}_{12}$ bedeuten, d.h. $\overline{3}$ wäre invertierbar in $\mathbb{Z}_{12}$, und dies ist laut Vorlesung nicht der Fall wegen $\mathrm{ggT}(12, 3) = 3 \neq 1$.