Lineare Algebra I
5. Tutorium
Die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Dr. Kollross
Dr. Le Roux
Dipl.-Math. Susanne Kürsten

WS 2010/2011
19. November 2010

Aufgaben

In diesem Tutrorium soll es um die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ und den Umgang mit ihnen gehen.
Um in einer ersten Schreibweise angeben zu können, was $\mathbb{Z}/n\mathbb{Z}$ ist, benötigt man die folgende Definition von Resten.
Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ für die

$$a = q \cdot n + r \text{ und } 0 \leq r < n$$

gilt. Die Zahl r heißt dann Rest von a bei der Dividion durch n oder auch Rest von a modulo n.

Aufgabe G1 (Beispiele und Nullteiler)
Wir betrachten die Menge $\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Dabei sei n eine natürliche Zahl. Für zwei Elemente $\overline{a}$ und $\overline{b}$ aus $\mathbb{Z}/n\mathbb{Z}$ wird wie folgt eine Multiplikation und eine Addition definiert:

$$\begin{aligned} \overline{a} +_n \overline{b} &:= \overline{r}, && \text{wobei } r \text{ der Rest von } a+b \text{ bei der Division durch } n \text{ ist,} \\ \overline{a} \cdot_n \overline{b} &:= \overline{r}, && \text{wobei } r \text{ der Rest von } a \cdot b \text{ bei der Division durch } n \text{ ist.} \end{aligned}$$

(a) Stellen Sie die Additions und Multiplikationstabellen für $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ auf.

(b) Welche Elemente der Mengen aus Aufgabenteil (a) haben Inverse bezüglich der Multiplikation, geben Sie diese Inversen Elemente an.
In Aufgabe G2 wird gezeigt, dass $\left(\mathbb{Z}/n\mathbb{Z}, +_n, \cdot_n, \overline{0}, \overline{1}\right)$ für alle natürlichen Zahlen $n \geq 2$ ein Ring mit Eins ist. Wenn Sie dies vorraussetzen, welche der Ringe aus Aufgabenteil (a) sind dann Körper und warum?

(c) Welche der Ringe aus Aufgabenteil (a) haben Nullteiler? Geben Sie alle Nullteiler an.

(d) Für welche natürlichen Zahlen n besitzt $\mathbb{Z}/n\mathbb{Z}$ Nullteiler? Kann in diesem Fall $\mathbb{Z}/n\mathbb{Z}$ ein Körper sein?

Aufgabe G2 (Restklassen und die Ringeigenschaft von $\mathbb{Z}/n\mathbb{Z}$)
Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$.
Man sagt a ist kongruent zu b modulo n und schreibt $a \equiv b \pmod{n}$, wenn a und b bei der Division durch n denselben Rest lassen.

(a) Zeige, dass die Relation $\equiv_n \subseteq \mathbb{Z} \times \mathbb{Z}$, die gegeben ist durch $(a, b) \in \equiv_n \Leftrightarrow a \equiv b \pmod{n}$ eine Äquivalenzrelation (siehe Tutoriumsblatt 1) ist.

(b) Zeige, dass die Äquivalenzklasse $\overline{a}$ dieser Relation, welche das Element a enthält die Gestalt

$$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\} =: a + n\mathbb{Z}$$

hat. Wie viele verschiedene solcher Äquivalenzklassen gibt es? Wann gilt $\overline{a} = \overline{b}$?

Diese Äquivalenzklassen heißen auch Restklassen modulo n. Sie bilden, wie bereits aus dem ersten Tutorium bekannt ist eine Partition von $\mathbb{Z}$. Betrachtet man die Restklasse $\overline{a}$, so wird a als Repräsentant von $\overline{a}$ bezeichnet.
Man kann nun $\mathbb{Z}/n\mathbb{Z}$ als die Menge der Restklassen modulo n mit den Operationen

$$\begin{aligned} +_n &: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} && (a + n\mathbb{Z}, b + n\mathbb{Z}) \mapsto a + b + n\mathbb{Z} \text{ und} \\ \cdot_n &: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} && (a + n\mathbb{Z}, b + n\mathbb{Z}) \mapsto a \cdot b + n\mathbb{Z} \end{aligned}$$

definieren. (Dabei bezeichnen $a + b$ und $a \cdot b$ die normale Addition bzw. Multiplikation in den ganzen Zahlen.)

(c) Zeigen Sie, dass diese Operationen wohldefiniert sind.
Wohldefiniert bedeutet hier: Das Ergebnis der Multiplikation und Addition in $\mathbb{Z}/n\mathbb{Z}$ hängt nicht von der Wahl der Repräsentanten ab.

(d) Zeigen Sie, dass diese Definition mit der aus Aufgabe G1 übereinstimmt.

(e) Für welche natürlichen Zahlen n stimmt in $\mathbb{Z}/n\mathbb{Z}$ das Nullelement mit dem Einselement überein?

(f) Zeigen Sie, dass $(\mathbb{Z}/n\mathbb{Z}, +_n, \cdot_n, 0+n\mathbb{Z}, 1+n\mathbb{Z})$ für jede natürliche Zahl $n \geq 2$ ein kommutativer Ring mit Eins ist.

Aufgabe G3 (Der größte gemeinsame Teiler und die Körpereigenschaft von $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p)
In der ganzen Aufgabe sei $n \geq 2$ eine natürliche Zahl.
Außerdem seien jetzt a und b natürliche Zahlen. Der größte gemeinsame Teiler von a und b wird mit Hilfe des euklidischen Algorithmus bestimmt. Bei diesem macht man im ersten Schritt eine Division mit Rest von a durch b. Der Rest sei r_1. Im nächsten Schritt macht man dasselbe mit b und r_1. Dies wird fortgeführt, bis ein Rest r_k Null ist. Dann gilt $\mathrm{ggT}(a,b) = r_{k-1}$.
Der allgemeine Verlauf des Euklidischen Algorithmus sieht also wie folgt aus.

$$\begin{aligned}
a &= q_1 \cdot b + r_1 \text{ mit } 0 \leq r_1 < b \\
b &= q_2 \cdot r_1 + r_2 \text{ mit } 0 \leq r_2 < r_1 \\
r_1 &= q_3 \cdot r_2 + r_3 \text{ mit } 0 \leq r_3 < r_2 \\
\vdots &\ \vdots\ \vdots \\
r_{k-4} &= q_{k-2} \cdot r_{k-3} + r_{k-2} \text{ mit } 0 \leq r_{k-2} < r_{k-3} \\
r_{k-3} &= q_{k-1} \cdot r_{k-2} + r_{k-1} \text{ mit } 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} &= q_k \cdot r_{k-1} + 0
\end{aligned}$$

Dabei sind alle vorkommenden Zahlen natürliche Zahlen und man erhält $\mathrm{ggT}(a,b) = r_{k-1}$.

(a) Bestimmen sie mit Hilfe des Euklidischen Algorithmus $\mathrm{ggT}(99,78)$ und $\mathrm{ggT}(34357,17017)$.

(b) Zeigen Sie, dass der beschriebene Euklidische Algorithmus immer endet.

(c) Zeigen Sie, dass der beschriebene Euklidische Algorithmus tatsächlich den größten gemeinsamen Teiler der beiden gegebenen Zahlen bestimmt.

Es gilt der Satz: Für $a, b, d \in \mathbb{N}$ mit $d = \mathrm{ggT}(a,b)$ existieren immer ganze Zahlen x und y mit

$$d = ax + by\ .$$

Die Zahlen x und y können dabei aus dem Euklidischen Algorithmus durch Rückwärtseinsetzen bestimmt werden. Mit den obigen Bezeichnungen hat man

$$\begin{aligned}
d &= r_{k-1} = r_{k-3} - q_{k-1} r_{k-2} = x_1 r_{k-3} + y_1 r_{k-2} \text{ mit } x_1 := 1, y_1 := -q_{k-1} \\
d &= x_1 r_{k-3} + y_1 (r_{k-4} - q_{k-2} r_{k-3}) = x_2 r_{k-4} + y_2 r_{k-3} \text{ mit } x_2 := y_1, y_2 := x_1 - y_1 q_{k-2} \text{ usw.}
\end{aligned}$$

Es ergibt sich also eine Gleichungskette

$$d = x_1 r_{k-3} + y_1 r_{k-2} = x_2 r_{k-4} + y_2 r_{k-3} = \cdots = x_{k-2} b + y_{k-2} r_1 = x_{k-1} a + y_{k-1} b,$$

wobei alle vorkommenden Zahlen ganze Zahlen und x_{k-1}, y_{k-1} die gesuchten Zahlen sind.
Auf diese Weise zeigt man den obigen Satz und kann im konkreten Beispiel die Zahlen x und y bestimmen.

(d) Bestimmen Sie auf die gerade beschriebene Weise ganze Zahlen x und y mit $\mathrm{ggT}(99,78) = 99x + 78y$.

(e) Bestimmen Sie ganze Zahlen x und y mit $\mathrm{ggT}(34357,17017) = 34357x + 17017y$.

(f) Sei $(\mathbb{Z}/n\mathbb{Z})^\times$ die Menge der bezüglich der Multiplikation invertierbaren Elemente in $(\mathbb{Z}/n\mathbb{Z})$. Zeigen Sie

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \mid \mathrm{ggT}(a,n) = 1\}\ .$$

Tipp: Zeigen Sie als ersten Schritt, dass ein Element $\overline{a}$ von $\mathbb{Z}/n\mathbb{Z}$ genau dann invertierbar ist, wenn es ganze Zahlen x und y gibt für die $ax + ny = 1$ gilt.

(g) Für welche n ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper?