Innermathematische Beziehungen
Übungsveranstaltung

Fabian Grünig
gruenig@ph-heidelberg.de

Wintersemester 2017/18
Mittwoch, 10:00 Uhr, A206

Es sei $m \in \mathbb{Z}$. Wir bezeichnen die Menge aller Restklassen (vgl. Aufgabe 6) bezüglich m mit $\mathbb{Z}_m$. Wählen wir für diese Restklassen jeweils den kleinsten positiven – den sogenannten *kanonischen* – Vertreter zwischen 0 und $(m-1)$ ergibt sich folgende Darstellung.

$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \dots, [m-2]_m, [m-1]_m\}$$

Auf der Menge $\mathbb{Z}_m$ lassen sich die folgenden Verknüpfungen definieren (vgl. Aufgabe 7), wobei mit der Addition und Multiplikation der Vertreter die gewöhnlichen Verknüpfungen der ganzen Zahlen $\mathbb{Z}$ gemeint ist.

$$[x]_m + [y]_m := [x+y]_m \qquad \text{(Addition von Restklassen)}$$
$$[x]_m \cdot [y]_m := [x \cdot y]_m \qquad \text{(Multiplikation von Restklassen)}$$

Aufgabe 10 *(Kleinste Gruppen)*
Wir betrachten $\mathbb{Z}_m$ für die Zahlen $m \in \{1, 2, 3\}$. Wir erhalten für die Addition die folgenden Verknüpfungstafeln.

$+$	$[0]_1$
$[0]_1$	$[0]_1$

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

(i) Begründe, warum $\mathbb{Z}_1$ nur aus einem Element besteht. Welche Zahlen enthält $[0]_1$?

(ii) Begründe, warum $\mathbb{Z}_2$ nur aus zwei Elementen besteht. Welche Zahlen enthält $[0]_2$; welche Zahlen enthält $[1]_2$?

(iii) Begründe anhand der Verknüpfungstafeln, dass es sich bei $\mathbb{Z}_1$, $\mathbb{Z}_2$ und $\mathbb{Z}_3$ um Gruppen bzgl. der Addition von Restklassen handelt. Prüfe dazu die Gruppenaxiome nach.

- Assoziativität
  Rechne für alle alle $x, y, z \in \mathbb{Z}_m$ nach, dass $(x+y)+z = x+(y+z)$ gilt.
  Hinweis: Für $\mathbb{Z}_2$ sind 8 Rechnungen notwendig. Für $\mathbb{Z}_3$ wären 27 Rechnungen notwendig; beschränkt Euch hier auf einige Beispielrechnungen.
- Existenz eines neutralen Elementes
  Findet jeweils ein Element $e \in \mathbb{Z}_m$, für das $x+e = e+x = x$ für alle $x \in \mathbb{Z}_m$ gilt.
- Existenz von inversen Elementen
  Findet für jedes Element $x \in \mathbb{Z}_m$ ein Element $y \in \mathbb{Z}_1$, sodass $x+y = y+x = e$ gilt.

(iv) Argumentiere anhand der Verknüpfungstafeln, dass es sich bei $\mathbb{Z}_1$, $\mathbb{Z}_2$ und $\mathbb{Z}_3$ sogar um abelsche (kommutative) Gruppen handelt.

Aufgabe 11 *(Einfache zahlentheoretische Beweise)*
Eine häufige Übungsaufgabe zur Vorlesung *Zahlentheorie* ist der Beweis der Aussage

„Die Summe zweier ungerader Zahlen ist gerade.“.

Eine mögliche Lösung ist die Folgende.

Beweis: Es seien $a, b \in \mathbb{Z}$ zwei ungerade Zahlen. Da a, b ungerade sind, existieren zwei Zahlen $s, t \in \mathbb{Z}$, sodass $x = 2 \cdot s + 1$ und $y = 2 \cdot t + 1$. Damit berechnen wir die Summe aus a und b wie folgt.

$$a + b = (2 \cdot s + 1) + (2 \cdot t + 1) = 2 \cdot s + 2 \cdot t + 2 = 2 \cdot (s + t + 1)$$

Demnach ist $(a + b)$ gerade. □

(i) Vollziehe den Beweis nach: Warum gibt es die Zahlen s, t? Was passiert in den jeweiligen Schritten der Rechnung? Was ist schlussendlich das Argument, dass $(a + b)$ gerade ist?

(ii) Verwende eine Rechnung in $\mathbb{Z}_2$, um einen alternativen Beweis für obige Aussage zu finden.

(iii) Zeige: „Die Summe zweier gerader Zahlen ist gerade.“

(iv) Zeige: „Die Summe einer geraden und einer ungeraden Zahl ist ungerade.“

(v) Zeige: „Die Summer dreier aufeinanderfolgender Zahlen ist durch 3 teilbar“.

Aufgabe 12 *(Gruppen bzgl. der Multiplikation?)*
Wir betrachten $\mathbb{Z}_m \setminus \{[0]_m\}$ (Wir entfernen die Nullrestklasse) für die Zahlen $m \in \{2, 3, 4, 6, 7\}$. Wir erhalten für die Multiplikation die folgenden Verknüpfungstafeln.

$\cdot$	$[1]_2$
$[1]_2$	$[1]_2$

$\cdot$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[2]_3$	$[1]_3$

$\cdot$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[3]_4$	$[2]_4$	$[1]_4$

$\cdot$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

$\cdot$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[1]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[2]_7$	$[2]_7$	$[4]_7$	$[6]_7$	$[1]_7$	$[3]_7$	$[5]_7$
$[3]_7$	$[3]_7$	$[6]_7$	$[2]_7$	$[5]_7$	$[1]_7$	$[4]_7$
$[4]_7$	$[4]_7$	$[1]_7$	$[5]_7$	$[2]_7$	$[6]_7$	$[3]_7$
$[5]_7$	$[5]_7$	$[3]_7$	$[1]_7$	$[6]_7$	$[4]_7$	$[2]_7$
$[6]_7$	$[6]_7$	$[5]_7$	$[4]_7$	$[3]_7$	$[2]_7$	$[1]_7$

Entscheide anhand der Verknüpfungstafeln, ob es sich bei $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$ oder $\mathbb{Z}_7$ um Gruppen bzgl. der Multiplikation von Restklassen handelt. Handelt es sich gegebenenfalls um abelsche Gruppen?
Hinweis: Die Assoziativität muss nicht überprüft werden.

Zusammenfassung: Wir haben in dieser Übung gesehen, dass es sich bei der Menge der Restklassen bezüglich einer Zahl $m \in \mathbb{Z}$ mit der Addition um Gruppen handelt. Betrachtet man jedoch die Multiplikation von Restklassen, so erhalten wir nicht immer eine Gruppe. Ein Problem scheint zu sein, dass bei der Multiplikation die Nullrestklasse entstehen kann. (Ein Exkurs in die Zahlentheorie hat uns gezeigt, dass das Rechnen mit Restklassen durchaus lohnenswert ist. So lassen sich Aussagen über Teilbarkeiten oft einfacher begründen, wenn man sie in Aussagen über Restklassen formuliert.)