Innermathematische Beziehungen
Übungsveranstaltung

Fabian Grünig
gruenig@ph-heidelberg.de

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

Aufgabe 17 *(Die Einheitengruppe von $\mathbb{Z}_m$)*
Wir haben in Aufgabe 12 gesehen, dass $\mathbb{Z}_6 \setminus \{[0]_6\}$ keine Gruppe bezüglich der Multiplikation von Restklassen ist. Insbesondere ist die Existenz von Inversen Elementen nicht gesichert, da etwa $[2]_6 \cdot [x]_6 \neq [1]_6$ für alle möglichen $x \in \mathbb{Z}$ (siehe Verknüpfungstafel).
Wir definieren allgemein für $m \in \mathbb{Z}$

$$\mathbb{Z}_m^\times = \{[x]_m \in \mathbb{Z}_m \mid \text{Es existiert ein } [y]_m \in \mathbb{Z}_m \text{ mit } [x]_m \cdot [y]_m = [1]_m\}.$$

Wir nennen $\mathbb{Z}_m^\times$ die *Einheitengruppe* von $\mathbb{Z}_m$. Sie enthält alle Restklassen bezüglich m, die in $\mathbb{Z}_m$ ein multiplikatives Inverses besitzen.

(i) Bestimme $\mathbb{Z}_6^\times$ in Mengenschreibweise. Stelle die Verknüpfungstafel von $\mathbb{Z}_6^\times$ bezüglich der Multiplikation auf. Zeige, dass es sich bei $\mathbb{Z}_6^\times$ um eine Gruppe handelt.

(ii) Bestimme $\mathbb{Z}_7^\times$. Zeige: $\mathbb{Z}_7^\times = \mathbb{Z}_7 \setminus \{[0]_7\}$.

(iii) Zeige allgemein: Für $m \in \mathbb{Z}$ ist $\mathbb{Z}_m^\times$ eine Gruppe bezüglich der Multiplikation. Beachte:

- Die Assoziativität ergibt sich aus den Rechenregeln in den ganzen Zahlen.
- Die Wohldefiniertheit bzw. Abgeschlossenheit der Verknüpfung ist hier der springende Punkt. Zeige, dass für zwei invertierbare Restklassen $[x]_m$ und $[y]_m$ auch deren Produkt $([x]_m \cdot [y]_m)$ wieder invertierbar ist.
- Für die Existenz des Neutralelements muss nachgewiesen werden, dass $[1]_m \in \mathbb{Z}_m$.

Aufgabe 18 *(Zyklisch erzeugte Untergruppen)*
Es sei G eine Gruppe mit Verknüpfung $\star$ und neutralem Element $e \in G$. Analog zu Aufgabe 14 definieren wir für ein $g \in G$ und ein $k \in \mathbb{Z}$:

$$g^k := \begin{cases} e & \text{falls } k = 0 \\ \underbrace{g \star g \star \ldots \star g}_{k \text{ Faktoren}} & \text{falls } k > 0 \\ \underbrace{g^{-1} \star g^{-1} \star \ldots \star g^{-1}}_{k \text{ Faktoren}} & \text{falls } k < 0 \end{cases}$$

Ausgehend von dieser Definition definieren wir das *Erzeugnis* eines Elements $g \in G$ wie folgt.

$$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\}$$

(i) Es sei $g \in G$. Zeige, dass $\langle g \rangle$ eine Untergruppe von G ist.
Hinweis: Auch wenn wir diese nicht explizit nachgewiesen haben, kannst du folgende Rechenregel verwenden: Für $k, l \in \mathbb{Z}$ gilt $g^k \star g^l = g^{k+l}$.

(ii) Bestimme $\langle [x]_6 \rangle$ in $\mathbb{Z}_6$ für $x = 2$, $x = 3$ und $x = 4$ bezüglich der Addition.

(iii) Bestimme $\langle [x]_7 \rangle$ in $\mathbb{Z}_7$ für $x = 2$, $x = 3$ und $x = 4$. bezüglich der Addition.

(iv) Bestimme $\langle [1]_m \rangle$ in $\mathbb{Z}_m$. bezüglich der Addition.

(v) Bestimme $\langle 1 \rangle$ in $\mathbb{Z}$, $\langle 2 \rangle$ in $\mathbb{Z}$ und $\langle 3 \rangle$ in $\mathbb{Z}$ bezüglich der Addition.

(vi) Bestimme $\langle e \rangle$ in G bezüglich $\star$.

Aufgabe 19 *(Zyklische Gruppen)*
Es sei G eine Gruppe mit Verknüpfung $\star$ und neutralem Element $e \in G$. Wir nennen G eine *zyklische Gruppe*, falls es ein Element $g \in G$ gibt, mit der Eigenschaft $\langle g \rangle = G$. Wir nennen gegebenenfalls g einen *Erzeuger* von G. Eine Gruppe heißt demnach zyklisch, wenn sie von einem Element (zyklisch) erzeugt wird.

(i) Argumentiere, dass $\mathbb{Z}$ bezüglich der Addition eine zyklische Gruppe ist.

(ii) Argumentiere, dass $\mathbb{Z}_m$ bezüglich der Addition eine zyklische Gruppe ist.

(iii) Argumentiere, dass $\mathbb{Z}_6^\times$ bezüglich der Multiplikation eine zyklische Gruppe ist.

(iv) Argumentiere, dass $\mathbb{Z}_7^\times$ bezüglich der Multiplikation eine zyklische Gruppe ist.

(v) Finde alle Erzeuger von $\mathbb{Z}_6$ bezüglich der Addition.

(vi) Finde alle Erzeuger von $\mathbb{Z}_7$ bezüglich der Addition.

Zusammenfassung: Wir haben in dieser Übung den Begriff der Untergruppe kennengelernt (vgl. Aufgabe 16). Untergruppen sind Teilmengen von Gruppen, die mit der *geerbten* Gruppenverknüpfung selbst wieder Gruppen sind. Am einfachsten erhalten wir Untergruppen als (zyklische) Erzeugnisse eines ausgewählten Gruppenelements. Dazu starten wir mit einem Gruppenelement und fügen beliebige Potenzen (und Potenzen des inversen Elements) hinzu (vgl. Aufgabe 18). Es stellt sich die Frage, ob es Gruppen gibt, die selbst zyklisch erzeugt sind (vgl. Aufgabe 19) und ob diese darüber hinaus besondere Eigenschaften aufweisen.