Innermathematische Beziehungen
Übungsveranstaltung

Fabian Grünig
gruenig@ph-heidelberg.de

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

Wir betrachten für $m \in \mathbb{Z}$ die Restklassen in $\mathbb{Z}_m$. Wir haben in $\mathbb{Z}_m$ zwei Rechenoperationen (Addition und Multiplikation) kennengelernt. Für das mehrmalige Hintereinanderausführen dieser Operationen führen wir folgende Notation ein.

Es sei $k \in \mathbb{N}_0$ eine natürliche Zahl. Für eine Restklasse $[x]_m \in \mathbb{Z}_m$ mit Vertreter $x \in \mathbb{Z}$ definieren wir:

$$k \cdot [x]_m := \underbrace{[x]_m + [x]_m + \ldots + [x]_m}_{k \text{ Summanden}}$$

$$([x]_m)^k := \underbrace{[x]_m \cdot [x]_m \cdot \ldots \cdot [x]_m}_{k \text{ Faktoren}}$$

Für $k = 0$ definieren wir die Spezialfälle $0 \cdot [x]_m := [0]_m$ (leer Summe) und $([x]_m)^0 := [1]_m$ (leeres Produkt).

Aufgabe 13 *(Rechnen mit Restklassen, Vertiefung)*

(i) Berechne die folgenden Ausdrücke gemäß der obigen Definition:

$$2 \cdot [3]_4, \quad 3 \cdot [2]_4, \quad 3 \cdot [1]_3, \quad 3 \cdot [2]_3, \quad 3 \cdot [3]_3, \quad 4 \cdot [3]_{12}, \quad 6 \cdot [6]_{12},$$
$$([2]_5)^2, \quad ([2]_5)^7, \quad ([2]_5)^{12}, \quad ([2]_5)^{17}, \quad ([5]_6)^2, \quad ([5]_6)^{998}, \quad ([5]_6)^{999}$$

(ii) Zeige: Für $k, m \in \mathbb{N}$ und $x \in \mathbb{Z}$ gilt $k \cdot [x]_m = [k]_m \cdot [x]_m$.

(iii) Zeige: Für $m \in \mathbb{N}$ und $x \in \mathbb{Z}$ gilt $m \cdot [x]_m = [0]_m$

Aufgabe 14 *(Ordnung von Gruppenelementen 1)*
Es sei G eine Gruppe mit Verknüpfung $\star$ und neutralem Element $e \in G$. Für ein Element $x \in G$ definieren wir dessen *Ordnung* $\operatorname{ord}(g)$ als die kleinste natürliche Zahl $k \neq 0$, sodass

$$\underbrace{g \star g \star \ldots \star g}_{k \text{ mal}} = e$$

gilt. Existiert keine solche Zahl, dann setzen wir $\operatorname{ord}(k) = \infty$.

(i) Berechne die Ordnung der folgenden Elemente in $\mathbb{Z}_6$ bezüglich der Addition: $[1]_6, [5]_6, [8]_6, [-3]_6$.

(ii) Berechne die Ordnung der folgenden Elemente in $\mathbb{Z}_7$ bezüglich der Addition: $[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7$.

(iii) Was ist die Ordung von $[0]_m$ in $\mathbb{Z}_m$ bezüglich der Addition?

(iv) Was ist die Ordung von 0 in $\mathbb{Z}$ bezüglich der Addition? Was ist die Ordung von 1 in $\mathbb{Z}$ bezüglich der Addition? Was ist die Ordung von 5 in $\mathbb{Z}$ bezüglich der Addition?

(v) Es sei $[x]_m \in \mathbb{Z}_m$. Wie groß kann die Ordnung von $[x]_m$ bezüglich der Addition maximal sein?

Aufgabe 15 *(Ordnung von Gruppenelementen 2)*
In Aufgabe 12 haben wir gesehen, dass $\mathbb{Z}_7 \setminus \{[0]_7\}$ bezüglich der Multiplikation eine Gruppe ist.

(i) Berechne die Ordnung der folgenden Elemente in $\mathbb{Z}_7$ bezüglich der Multiplikation: $[2]_7, [3]_7, [4]_7, [5]_7$.

(ii) Berechne die Ordnung der folgenden Elemente in bezüglich der Multiplikation:
- $[2]_3 \in \mathbb{Z}_3 \setminus \{[0]_3\}$,
- $[4]_5 \in \mathbb{Z}_5 \setminus \{[0]_5\}$,
- $[6]_7 \in \mathbb{Z}_7 \setminus \{[0]_7\}$,
- $[12]_{13} \in \mathbb{Z}_{13} \setminus \{[0]_{13}\}$.

Aufgabe 16 *(Elementordnung teilt Gruppenordnung)*
Es sei G eine endliche Gruppe mit Verknüpfung $\star$ und neutralem Element $e \in G$. Ferner sei $x \in G$ ein beliebiges Element. Dann gilt:

$$\operatorname{ord}(x) \quad \text{teilt} \quad \#(G).$$

Beweise die obige Behauptung durch folgende Schritte.
Hinweis: Verwende dabei (ohne Beweis), dass $x^{\#(G)} = e$.

(i) Der Beweis erfolgt durch Widerspruch. Formuliere den Widerspruchsansatz.

(ii) Führe ausgehend von der Widerspruchsannahme eine Division mit Rest durch.

(iii) Ist r der Rest, der bei entsprechender Division übrig bleibt, dann berechne x^r.
Hinweis: Du darfst Potenzrechengesetze der Form $(x^p)^q = (x^q)^p$ verwenden[1].

(iv) Aus dem vorherigen Schritt ergibt sich ein Widerspruch zur Minimalitätseigenschaft von $\operatorname{ord}(x)$. Was bedeutet das?

Zusammenfassung: Wir haben in dieser Übung den Ordnungsbegriff für Gruppenelemente eingeführt. In diesem Begriff steckt die Frage: Wie oft müssen wir ein Element einer Gruppe mit sich selbst verknüpfen, bis wir das neutrale Element erhalten. In Aufgabe 16 haben wir eine erste Strukturaussage bewiesen. Die Ordnung eines Elements in einer endlichen Gruppe ist immer ein Teiler der Gruppenordnung.

[1] Wir schreiben die Gruppe *multiplikativ*, meinen also mit $x^p = x \star x \ldots \star x$ (p Faktoren)