Innermathematische Beziehungen
Übungsveranstaltung

Fabian Grünig
gruenig@ph-heidelberg.de

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

In Aufgabe 16 haben wir folgende Aussage (ohne einen zugehörigen Beweis) verwendet.

Satz *Es sei G eine endliche, abelsche Grupp mit Verknüpfung $*$ und Neutralelement $e \in G$. Es sei ferner $x \in G$ ein beliebiges Gruppenelement. Dann gilt*

$$x^{\#(G)} = e.$$

Hierbei bezeichnet $\#(G)$ die Anzahl der Elemente von G und $x^{\#(G)} = x * x * \cdots * x$ mit $\#(G)$ Faktoren.

Aufgabe 29 *(Element hoch Gruppenordnung ergibt Neutralelement)*
Vollziehe den folgenden Beweis des obigen Satzes nach und fülle die Argumentationslücken.

Beweis: Da G endlich ist können wir die Elemente in G durchnummerieren. Ist $\#(G) = n \in \mathbb{N}$, dann schreibe etwa

$$G = \{g_1, g_2, \dots, g_n\}.$$

Betrachten wir ein beliebiges Element der Gruppe $x \in G$ und die Menge

$$xG = \{(x * g_1), (x * g_2), \dots, (x * g_n)\}.$$

Die Menge G und xG enthalten die gleichen Elemente (i), also sind auch die folgenden Produkte gleich.

$$g_1 * g_2 * \cdots * g_n = (x * g_1) * (x * g_2) * \cdots * (x * g_n)$$

Durch Umstellen (ii) erhalten wir

$$g_1 * g_2 * \cdots * g_n = x^n * (g_1 * g_2 * \cdots * g_n),$$

woraus (iii) die Behauptung $x^n = e$ folgt. $\square$

(i) Warum beinhalten G und xG die selben Elemente? Kann es nicht passieren, dass $(x*g_i) = (x*g_j)$ für ein Paar $i \neq j$, die Menge xG also kleiner wird?

(ii) Wie erhält man die zweite Gleichung? Welche Eigenschaften der Gruppe werden ausgenutzt, welche Rechenregeln angewandt?

(iii) Wie folgt aus der zweiten Gleichung die Behauptung? Welche Rechenregel macht man sich hier zu Nutze?

Aufgabe 30 *(Der Satz von Euler)*
Es sei $m \in \mathbb{Z}$, dann definieren wir die sogenannte Euler'sche φ-Funktion[1]

$$\varphi(m) = \#\{1 \le k \le m \mid \mathrm{ggT}(k,m) = 1\},$$

die die zu m teilerfremden natürlichen Zahlen zählt, die kleiner als m sind.

(i) Bestimme $\varphi(2), \varphi(3), \varphi(4), \varphi(5), \varphi(6)$ und $\varphi(7)$.

(ii) Zeige mit Hilfe von Aufgabe 25 und Aufgabe 27, dass

$$\#(\mathbb{Z}_m^\times) = \#\{1 \le k < m \mid \mathrm{ggT}(k,m) = 1\}, \tag{1}$$

wir also mit $\varphi(m)$ die Größe der Einheitengruppe von $\mathbb{Z}_m$ beschreiben.

(iii) Es sei $x \in \mathbb{Z}$ eine zu m teilerfremde ganze Zahl. Zeige, dass in $\mathbb{Z}_m$ gilt:

$$\overline{x}^{\varphi(x)} = \overline{1}.$$

Hinweis: Interpretiere die Gleichung in der Gruppe $\mathbb{Z}_m^\times$.

(iv) Es sei $x \in \mathbb{Z}$ eine zu m teilerfremde ganze Zahl und $k \in \mathbb{N}$ eine beliebige natürlich Zahl. Ferner sei r der Rest, der beim Teilen von k durch $\varphi(m)$ bleibt. Zeige, dass in $\mathbb{Z}_m$ gilt

$$\overline{x}^k = \overline{x}^r.$$

Aufgabe 31 *(Potenzen in $\mathbb{Z}_m$ berechnen)*

(i) Berechne $\overline{4}^{12}, \overline{4}^{120}$ und $\overline{4}^{2730}$ in $\mathbb{Z}_7$.

(ii) Bereche $\overline{4}^{12}, \overline{4}^{120}$ und $\overline{4}^{2730}$ in $\mathbb{Z}_9$.

(iii) Bereche $\overline{4}^{9}, \overline{4}^{34}$ und $\overline{4}^{119}$ in $\mathbb{Z}_{12}$.

(iv) Was ist die letzte Ziffer (Einerstelle) von 7^{222} im Dezimalsystem?

[1] gelesen: Eulersche Phi-Funktion.