Aufgabe H14T2A3 (4+8 Punkte)

(a) Es seien $p \geq 2$ eine natürliche Zahl, $m \in \mathbb{N}$, $n \in \mathbb{N}_0 = \{0, 1, 2, ...\}$ und $a_i \in \mathbb{N}_0$ für $1 \leq i \leq m$, so dass

$$p^n \quad = \quad \sum_{i=1}^{m} p^{a_i}$$

gilt. Zeigen Sie, dass $m - 1$ durch $p - 1$ teilbar ist.
Hinweis: Betrachten Sie Kongruenzen modulo $p - 1$.

(b) Für eine Primzahl p und $n \in \mathbb{N}$ sei G eine Gruppe der Ordnung p^n, und

$$Z(G) \quad = \quad \{g \in G \mid xg = gx \text{ für alle } x \in G\}$$

sei das Zentrum von G. Zeigen Sie, dass die Anzahl der Konjugationsklassen von G, die nicht in $Z(G)$ liegen, durch $p - 1$ teilbar ist.

Lösung:

zu (a) Wegen $p \equiv 1 \mod (p-1)$ erhalten wir für den Wert auf der linken Seite der Gleichung $p^n \equiv 1^n \equiv 1 \mod (p-1)$. Für die rechte Seite gilt

$$\sum_{i=1}^{m} p^{a_i} \equiv \sum_{i=1}^{m} 1^{a_i} \equiv \sum_{i=1}^{m} 1 \equiv m \mod (p-1).$$

Durch Vergleich von linker und rechter Seite erhalten wir $1 \equiv m \mod (p-1)$, also ist $m - 1$ durch $p - 1$ teilbar.

zu (b) Wir betrachten die Operation der Gruppe G auf sich selbst durch Konjugation. Aus der Vorlesung ist bekannt, dass die Fixpunkte dieser Operation genau die Elemente von $Z(G)$ und die Bahnen der Operation mit mehr als einem Element genau die nicht in $Z(G)$ enthaltenen Konjugationsklassen sind. Sei $g_2, ..., g_m$ ein Repräsentantensystem der Konjugationsklassen, die nicht in $Z(G)$ liegen. Zu zeigen ist, dass deren Anzahl $m - 1$ von $p - 1$ geteilt wird. Weil G die disjunkte Vereinigung aller (ein- und mehrelementigen) Bahnen ist, gilt

$$|G| \quad = \quad |Z(G)| + \sum_{k=2}^{m} |G(g_k)| \quad ,$$

wobei $G(g_k)$ jeweils die Konjugationsklasse von g_k bezeichnet. Aus der Vorlesung ist bekannt, dass die Bahnlängen einer Gruppenoperation stets die Gruppenordnung teilen (falls die Gruppe endlich ist). Mit $|G|$ ist also auch $|G(g_k)|$ eine p-Potenz für $2 \leq k \leq m$, d.h. es gibt jeweils ein $a_k \in \mathbb{N}$ mit $|G(g_k)| = p^{a_k}$. Weil $Z(G)$ eine Untergruppe von G ist, wird $|G|$ auch von $|Z(G)|$ geteilt, und folglich gibt es eine Zahl $a_1 \in \mathbb{N}_0$ mit $|Z(G)| = p^{a_1}$. Insgesamt erhalten wir

$$p^n \quad = \quad |G| \quad = \quad |Z(G)| + \sum_{k=2}^{m} |G(g_k)| \quad = \quad \sum_{k=1}^{m} p^{a_k}.$$

Aus Aufgabenteil (a) folgt, dass $m - 1$ durch $p - 1$ teilbar ist.