## F25-T1-A4

Sei $G$ eine endliche Gruppe und $p$ eine Primzahl, die die Gruppenordnung $|G|$ teilt. Seien ferner $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit $p$ Elementen und $\mathbb{F}_p^\times$ die Einheitengruppe von $\mathbb{F}_p$. Wir definieren

$$M := \{g \in G \mid \operatorname{ord}(g) = p\}$$

als die Menge aller Gruppenelemente, deren Ordnung gleich $p$ ist.

a) Zeigen Sie, dass durch

$$\mathbb{F}_p^\times \times M \to M, \quad ([a], g) \mapsto g^a$$

eine Gruppenoperation definiert ist.

b) Sei $g \in M$ ein beliebiges Element. Zeigen Sie, dass der Stabilisator

$$(\mathbb{F}_p^\times)_g := \{[a] \in \mathbb{F}_p^\times \mid g^a = g\} \subseteq \mathbb{F}_p^\times$$

von $g \in M$ trivial ist, also $(\mathbb{F}_p^\times)_g = \{[1]\}$ gilt.

c) Folgern Sie, dass $|M|$ ein Vielfaches von $p-1$ ist.

**Lösung**

a) Wir weisen die Eigenschaften einer Gruppenoperation einzeln nach. Zu diesen Zweck seien $[a], [b] \in \mathbb{F}_p^\times$ und $g \in M$.

- $([1], g) \mapsto g^1 = g$;
- $([a], g^b) \mapsto (g^b)^a = g^{ab}, \quad ([ab], g) \mapsto g^{ab} \Rightarrow [a] \cdot g^b = [ab] \cdot g.$

Zudem sollte man verifizieren, dass die oben angegebene Gruppenoperation wohldefiniert ist, heißt für $[a] = [b]$ folgt $g^a = g^b$. Sei also $[a] = [b]$, das heißt es gibt ein $k \in \mathbb{Z}$ sodass $b = kp + a$. Wir berechnen $g^b = g^{kp+a} = g^{kp} g^a = (g^p)^k g^a = g^a$, da $g^p = e_G$, weil $g \in M$.

b) Offenbar ist $[1] \in (\mathbb{F}_p^\times)_g$ für $g \in M$. Sei also $[a] \in (\mathbb{F}_p^\times)_g$ für $g \in M$. Demnach ist $g^a = g$, also $g^{a-1} = e_G$. Da $g \in M$ gilt $\operatorname{ord}(g) = p$, also $p \mid a - 1$. Demnach ist $[a] = [1]$, denn $a \equiv 1 (\bmod p)$.

1. Wir bemühen die Bahnengleichung und erhalten

$$|M| = \sum_{g \in R} (\mathbb{F}_p^\times : (\mathbb{F}_p^\times)_g), \tag{0.1}$$

wobei $R$ ein Repräsentantensystem der Bahnen ist. Nach $B$ ist $(\mathbb{F}_p^\times)_g$ trivial für alle $g \in M$ und demnach $(\mathbb{F}_p^\times : (\mathbb{F}_p^\times)_g) = \left|\mathbb{F}_p^\times\right| = p - 1$. Sei nun $|R| = k$, dann erhält man mit (0.1), dass $|M| = k \cdot (p-1)$ gilt, was die Behauptung zeigt.