F24-T1-A2

a) Bestimmen Sie alle $n \in \{1, 2, 3, \ldots\}$, für die die Gruppe $\mathbb{Z}/n\mathbb{Z}$ außer der Identität keinen weiteren Gruppenautomorphismus besitzt.

Sei G eine endliche Gruppe der Ordnung ≥ 2 mit der Eigenschaft, dass die Identität der einzige Gruppenautomorphismus ist.

b) Zeigen Sie, dass G eine abelsche Gruppe ist.

c) Zeigen Sie, dass $G \cong \mathbb{Z}/2\mathbb{Z}$ ist.

Lösung

a) Wir wissen, dass $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ gilt. Wir wollen also die Anzahl der Einheiten in $\mathbb{Z}/n\mathbb{Z}$ bestimmen. Dazu benutzen wir die eulersche Phi-Funktion, wir wollen also $\phi_{\text{euler}}(n)$ bestimmen. Für $n = 1$ und $n = 2$ gilt $\phi_{\text{euler}}(n) = 1$. Sei nun $n \geq 3$ wir betrachten die eindeutige Primfaktorzerlegung von $n = \prod_{i=1}^{k} p_i^{\eta_i}$, $\eta_i \geq 1$ für alle i. Jetzt gilt nach den Rechenregeln der eulerschen Phi-Funktion, dass $\phi_{\text{euler}}(n) = \prod_{i=1}^{k} \phi_{\text{euler}}(p_i^{\eta_i}) = \prod_{i=1}^{k}(p_i^{\eta_i} - p_i^{\eta_i - 1})$ gilt. Jetzt gilt entweder, dass es ein $p_i > 2$ gibt oder alle $p_i = 2$. Im ersren Fall setzen wir dieses $p_i := p$. Dann hat man $p^\eta - p^{\eta-1} = p^{\eta_i - 1}(p-1) \geq 1 \cdot 2 = 2$. Im anderen Fall gilt also $n = 2^k$ mit $k > 1$. Demnach gilt $\phi_{\text{euler}} n = 2^{k-1}(2-1) \geq 2 \cdot 1 = 2$. Und damit folgt für alle $n \geq 3$ gilt, dass $\phi_{\text{euler}}(n) \geq 2$ und damit auch die Anzahl der Automorphismen von $\mathbb{Z}/n\mathbb{Z}$. Die Antwort auf die Frage ist daher $n \in \{1, 2\}$.

b) Wir betrachten die Operation durch Konjugation von G auf sich selbst

$$G \times G \to G, \quad (x, y) \mapsto yxy^{-1}.$$

Dieser induziert uns einen Gruppenhomomorphismus

$$\Phi : G \to \mathrm{Aut}(G) \quad y \mapsto (\phi_y : G \to G, \quad x \mapsto yxy^{-1}).$$

Überlegen wir uns noch kurz, wieso wir tatsächlich in $\mathrm{Aut}(G)$ landen und nicht nur in $S(G)$. Dazu prüfen wir nach, dass ϕ_y ein Automorphismus auf G ist. $\phi_y(ab) = y(ab)y^{-1} = ya(y^{-1}y)by^{-1} = (yay^{-1})(yby^{-1}) = \phi_y(a)\phi_y(b)$. Das dieser bijektiv ist folgt ja schon aus der Gruppenoperation (Inverses ist $\phi_{y^{-1}}$). Jetzt gilt $\ker(\Phi) = G$ (nach Voraussetzung ist $\mathrm{Aut}(G) = \mathrm{id}_G$), also gilt für alle $z \in G$, dass $yzy^{-1} = z$ und das gilt für alle y, daher ist G abelsch.

c) Nach b) kann man den Hauptsatz über endliche abelsche Gruppen anweden und daher ist G von folgender Form:

$$G \cong \prod_{i=1}^{n} \mathbb{Z}/p_i\mathbb{Z},$$

wobei p_i Primzahlen sind (nicht unbedingt verschieden). Nach a) gilt $p_i = 2$ für alle $i \in \{1, \dots, n\}$ da es sonst mehr als einen Gruppenautomorphismus gäbe, denn existiert ein $i_0 \in \{1, \dots, n\}$ mit $p_{i_0} \neq 2$ so gibt es ein $\mathrm{id} \neq \phi_{i_0} : \mathbb{Z}/i_0\mathbb{Z} \to \mathbb{Z}/i_0\mathbb{Z}$ (Gruppenautomorphismus) und demnach wäre $\Phi : \prod_{i=1}^{n} \mathbb{Z}/p_i\mathbb{Z} \to \prod_{i=1}^{n} \mathbb{Z}/p_i\mathbb{Z}, (z_1, \dots, z_{i_0-1}, z_{i_0}, z_{i_0+1}, \dots, z_n) \mapsto (z_1, \dots, z_{i_0-1}, \phi_{i_0}(z_{i_0}), z_{i_0+1}, \dots, z_n)$ ein Gruppenautomorphismus der nicht die Identität ist. Folglich erhalten wir $G \cong (\mathbb{Z}/2\mathbb{Z})^k$ für $k \in \mathbb{N}_{>0}$. Angenommen $k > 1$, dann gibt es auch hier einen nicht trivialen Gruppenautomorphismus. Wir bezeichnen hierzu mit e_i die „Basisvektoren“ von $(\mathbb{Z}/2\mathbb{Z})^k$, also z.B. $e_1 = (1, 0, \dots, 0)$. Für $k > 1$ wird durch $(e_1 \mapsto e_2, e_2 \mapsto e_1, e_l \mapsto e_l \quad \forall l > 2)$ ein solcher nichttrivialer Gruppenhomomorphismus gegeben. Demnach folgt $G \cong \mathbb{Z}/2\mathbb{Z}$.