Aufgabe H15T3A2 (15 Punkte)

Sei $n \geq 2$ eine natürliche Zahl. Es bezeichne $\varphi(n)$ den Wert der Eulerschen φ-Funktion bei n. Zeigen Sie, dass es genau $\varphi(n)$ verschiedene injektive Gruppenhomomorphismen $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ gibt.

Lösung:

Aus der Vorlesung ist folgendes bekannt: Sind G und H Gruppen und ist G zyklisch von Ordnung n, $g \in G$ ein Element mit $\mathrm{ord}(g) = n \in \mathbb{N}$, dann gibt es für jedes Element $h \in H$, dessen Ordnung ein Teiler von n ist, einen eindeutig bestimmten Gruppenhomomorphismus $f_h : G \to H$ mit $f_h(g) = h$. Der Homomorphismus f_h ist genau dann injektiv, wenn $\mathrm{ord}(h) = n$ gilt. Denn im Falle der Injektivität folgt für alle $m \in \mathbb{Z}$ aus $h^m = e_H$ jeweils $f_h(g^m) = f_h(g)^m = h^m = e_G$ und somit $g^m = e_G$, wegen $\mathrm{ord}(g) = n$ also $m|n$. Wegen $\mathrm{ord}(h)|n$ ist damit insgesamt $\mathrm{ord}(h) = n$ gezeigt. Setzen wir nun umgekehrt $\mathrm{ord}(h) = n$ voraus, und sei $g' \in G$ mit $f_h(g') = e_H$ vorgegeben. Wegen $G = \langle G \rangle$ gibt es ein $a \in \mathbb{Z}$ mit $g' = g^a$. Es gilt $h^a = f_h(g)^a = f_h(g^a) = f_h(g') = e_H$, wegen $\mathrm{ord}(h) = n$ also $n|a$ und wegen $\mathrm{ord}(g) = n$ schließlich $g' = g^a = e_G$. Damit ist die Injektivität von f_h nachgewiesen.

Wenden wir dies nun auf die Gruppen $G = \mathbb{Z}/n\mathbb{Z}$ und $H = \mathbb{Q}/\mathbb{Z}$ an, so kommen wir zu dem Ergebnis, dass für jedes $n \in \mathbb{N}$ die Anzahl der injektiven Gruppenhomomorphismen $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ gleich der Anzahl der Elemente der Ordnung n in $\mathbb{Q}/\mathbb{Z}$ ist. Bezeichnen wir die Teilmenge der Elemente der Ordnung n in dieser Gruppe mit A_n, dann ist also $|A_n| = \varphi(n)$ zu zeigen. Dazu beweisen wir die Gleichung

$$A_n \quad = \quad \{\tfrac{a}{n} + \mathbb{Z} \;\mid\; a \in \mathbb{Z}\ ,\ 0 \leq a < n\ ,\ \mathrm{ggT}(a,n) = 1\}.$$

Die Menge auf der rechten Seite enthält genau $\varphi(n)$ verschiedene Elemente. Sind nämlich $a, a' \in \mathbb{Z}$ mit $0 \leq a, a' < n$ und $\mathrm{ggT}(a,n) = \mathrm{ggT}(a',n) = 1$ vorgegeben und gilt $\frac{a}{n} + \mathbb{Z} = \frac{a'}{n} + \mathbb{Z}$, dann folgt $\frac{a'-a}{n} \in \mathbb{Z}$ und somit $n|(a'-a)$. Wegen $0 \leq a, a' < n$ ist andererseits $|a'-a| < n$, woraus $a = a'$ folgt. Die Anzahl aller $a \in \mathbb{Z}$ mit $0 \leq a < n$ und $\mathrm{ggT}(a,n) = 1$ ist aber genau $\varphi(n)$, nach Definition der Eulerschen φ-Funktion.

Kommen wir nun zum Beweis der Gleichung. „$\supseteq$“ Sei $\alpha = \frac{a}{n} + \mathbb{Z}$ mit $a \in \mathbb{Z}$, $0 \leq a < n$ und $\mathrm{ggT}(a,n) = 1$. Dann gilt $n\alpha = \frac{na}{n} + \mathbb{Z} = a + \mathbb{Z} = 0 + \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}$ und somit $\mathrm{ord}(\alpha)|n$. Sei nun $k \in \mathbb{Z}$ mit $k\alpha = 0_{\mathbb{Q}/\mathbb{Z}}$ vorgegeben. Dann folgt $\frac{ka}{n} + \mathbb{Z} = 0 + \mathbb{Z}$, also $\frac{ka}{n} \in \mathbb{Z}$ und $n|(ka)$. Wegen $\mathrm{ggT}(a,n) = 1$ folgt daraus wiederum $n|k$. Damit ist insgesamt $\mathrm{ord}(\alpha) = n$, also $\alpha \in A_n$ nachgewiesen.

„$\subseteq$“ Sei $\alpha \in A_n$, also $\alpha \in \mathbb{Q}/\mathbb{Z}$ mit $\mathrm{ord}(\alpha) = n$. Dann wird α durch eine rationale Zahl $\frac{c}{b} \in \mathbb{Q}$ repräsentiert, mit $c \in \mathbb{Z}$ und $b \in \mathbb{N}$. Wir dürfen annehmen, dass der Bruch gekürzt ist, also $\mathrm{ggT}(b,c) = 1$ gilt. Aus $n\alpha = 0_{\mathbb{Q}/\mathbb{Z}}$ folgt $\frac{nc}{b} + \mathbb{Z} = \mathbb{Z}$, also $\frac{nc}{b} \in \mathbb{Z}$ und $b|(nc)$. Wegen $\mathrm{ggT}(b,c) = 1$ folgt daraus $b|n$. Nehmen wir nun an, dass b ein echter Teiler von n ist. Wegen $b\alpha = \frac{bc}{c} + \mathbb{Z} = b + \mathbb{Z} = 0 + \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}$ würde dann $\mathrm{ord}(\alpha) \leq b < n$ folgen, im Widerspruch zu $\mathrm{ord}(\alpha) = n$. Also ist $b = n$. Dividieren wir c durch n mit Rest, so erhalten wir $q, a \in \mathbb{Z}$ mit $c = qn + a$ mit $0 \leq a < n$. Es folgt

$$\alpha \quad = \quad \tfrac{c}{n} + \mathbb{Z} \quad = \quad \tfrac{qn+a}{n} + \mathbb{Z} \quad = \quad q + \tfrac{a}{n} + \mathbb{Z} \quad = \quad \tfrac{a}{n} + \mathbb{Z}.$$

Wegen $\mathrm{ggT}(c,n) = 1$ und $c = qn + a$ gilt auch $\mathrm{ggT}(a,n) = 1$. Dies zeigt, dass das Element α in der Menge auf der rechten Seite der Gleichung enthalten ist.