Aufgabe H18T2A4 (12 Punkte)

Es seien p eine Primzahl und $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Es sei $\mathbb{Z}[\zeta]$ der Durchschnitt aler Teilringe von $\mathbb{C}$, die $\mathbb{Z}$ und ζ enthalten. Weiter seien $z_0, z_1, ..., z_{p-1} \in \mathbb{Z}$ und $x = z_0 + z_1\zeta + ... + z_{p-1}\zeta^{p-1} \in \mathbb{Q}(\zeta)$. Zeigen Sie:

(a) $\mathbb{Z}[\zeta] = \{y_0 + y_1\zeta + ... + y_{p-2}\zeta^{p-2} \mid y_0, ..., y_{p-2} \in \mathbb{Z}\} \subseteq \mathbb{Q}(\zeta)$

(b) Ist $\frac{x}{p} \in \mathbb{Z}[\zeta]$, so gilt $z_0 \equiv ... \equiv z_{p-1} \bmod p$.

Hinweis/Kommentar:

In Teil (a) muss unter anderem gezeigt werden, dass die dort definierte Menge M ein Teilring von $\mathbb{C}$ ist. Der Nachweis der Abgeschlossenheit unter Multiplikation ist der mühsamste Teil der gesamten Aufgabe. Für die Durchführung gibt es (mindestens) zwei Möglichkeiten: Zum einen kann die Gleichung $\zeta^{p-1} = -1 - \zeta - ... - \zeta^{p-2}$ verwendet werden, um durch vollständige Induktion zu beweisen, dass ζ^k für jedes $k \in \mathbb{N}_0$ in M liegt. Weil das Produkt zweier Elemente aus M als $\mathbb{Z}$-Linearkombination von Elementen ζ^k mit $k \in \mathbb{N}_0$ geschrieben werden kann, hat man damit die Abgeschlossenheit unter Multiplikation bewiesen. Dabei folgt die Gleichung aus der Tatsache, dass ζ eine Nullstelle des p-ten Kreisteilungspolynoms ist.

Eine andere Möglichkeit besteht darin, dass man den Beweis des Satzes, dass ein Polynomring $K[x]$ über einem Körper K euklidisch ist, leicht modifiziert, um zu zeigen: Ist $f \in \mathbb{Z}[x]$ und $g \in \mathbb{Z}[x]$ ein normiertes Polynom, dann gibt es $q, r \in \mathbb{Z}[x]$ mit $f = qg + r$ mit $r = 0$ oder $\text{grad}(r) < \text{grad}(g)$. Damit kann man dann die Abgeschlossenheit unter Multiplikation ziemlich schnell zeigen (ähnlich wie beim Satz aus der Körpertheorie, dass $(1, \alpha, ..., \alpha^{n-1})$ eine Basis von $K(\alpha)$ als K-Vektorraum ist, wenn α ein Minimalpolynom vom Grad n besitzt).

In Teil (b) kann der besagte Satz aus der Körpertheorie angewendet werden: Nach Voraussetzung bzw. Teil (a) gibt es $y_0, y_1, ..., y_{p-1} \in \mathbb{Z}$ mit

$$\frac{1}{p}(z_0 + z_1\zeta + ... + z_{p-1}\zeta^{p-1}) \quad = \quad y_0 + y_1\zeta + ... + y_{p-2}\zeta^{p-2}.$$

Verwenden Sie nun, dass $(1, \zeta, ..., \zeta^{p-2})$ eine Basis von $\mathbb{Q}(\zeta)$ als $\mathbb{Q}$-Vektorraum ist, um einen Zusammenhang zwischen den y_k und den z_k herzustellen.