H18-T2-A4

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

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

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

Lösungsvorschlag. Zu a). Wir wollen uns kurz davon überzeugen, dass gilt:

$$\bigcap_{\substack{\zeta \in R, \mathbb{Z} \subset R \\ R \text{ Teilring von } \mathbb{C}}} R = \{q(\zeta) \mid q(x) \in \mathbb{Z}[X]\}.$$

„$\subseteq$“ Das ist trivialerweise erfüllt ist, da $\{q(\zeta) \mid q(x) \in \mathbb{Z}[X]\}$ als Bild des kanonischen Einsetzungsmorphismus von $\mathbb{Z}[X]$ ein Teilring von $\mathbb{C}$ ist, der offensichtlich ζ und $\mathbb{Z}$ enthält.
„$\supseteq$“ Sei $a_n\zeta^n + \ldots + a_1\zeta + a_0 \in \{q(\zeta) \mid q(x) \in \mathbb{Z}[X]\}$. Wegen der Abgeschlossenheit eines Rings bezüglich Addition und Multiplikation muss dieses Element in jedem Ring enthalten sein, der ζ und $\mathbb{Z}$ enthält, und es ist damit auch im Schnitt über all diese enthalten. Es ist also $\mathbb{Z}[\zeta] = \{q(\zeta) \mid q(x) \in \mathbb{Z}[X]\}$. Wir wollen zeigen, dass es ausreicht, die Polynome von höchstens Grad $p-2$ zu berücksichtigen.
Das Minimalpolynom von ζ ist bekanntlich gegeben durch das p-te Kreisteilungspolynom $\phi_p(X) = X^{p-1} + \ldots + X + 1 \in \mathbb{Z}[X]$.
Sei nun $q(\zeta) \in \mathbb{Z}[\zeta]$, dann wollen wir ein $r(X) \in \mathbb{Z}[X]$ finden mit $\deg(r) < p-1$ und $r(\zeta) = q(\zeta)$. Da der Leitkoeffizient von $\phi_p(X)$ eine Einheit ist in $\mathbb{Z}$, existieren $f(X), r(X) \in \mathbb{Z}[X]$ mit $\deg(r) < \deg(\phi_p) = p-1$ und

$$q(X) = f(X) \cdot \phi_p(X) + r(X)$$

(vgl. Übungsblatt 5, Aufgabe 5). Wegen $\phi_p(\zeta) = 0$ folgt sofort wie gefordert $q(\zeta) = r(\zeta)$.
Zu b). Sei $q(\zeta) = y_0 + y_1\zeta + \ldots + y_{p-2}\zeta^{p-2} \in \mathbb{Z}[\zeta]$ mit $\frac{x}{p} = q(\zeta)$. Wegen $\phi_p(\zeta) = 0$, bzw. $\zeta^{p-1} = -(\zeta^{p-2} + \ldots + \zeta + 1)$ folgt:

$$\begin{aligned}
\frac{x}{p} = q(\zeta) &\Leftrightarrow z_0 + z_1\zeta + \ldots + z_{p-2}\zeta^{p-2} + z_{p-1} \cdot (-(\zeta^{p-2} + \ldots + \zeta + 1)) = p \cdot q(\zeta) \\
&\Leftrightarrow (z_0 - z_{p-1}) + (z_1 - z_{p-1})\zeta + \ldots + (z_{p-2} - z_{p-1})\zeta^{p-2} = p \cdot q(\zeta) \\
&\Leftrightarrow (z_0 - z_{p-1}) + (z_1 - z_{p-1})\zeta + \ldots + (z_{p-2} - z_{p-1})\zeta^{p-2} - p(y_0 + y_1\zeta + \ldots + y_{p-2}\zeta^{p-2}) = 0 \\
&\Leftrightarrow \underbrace{(z_0 - z_{p-1} - py_0)}_{:=a_0} + \underbrace{(z_1 - z_{p-1} - py_1)}_{:=a_1}\zeta + \ldots + \underbrace{(z_{p-2} - z_{p-1} - py_{p-2})}_{:=a_{p-2}}\zeta^{p-2} = 0
\end{aligned}$$

Dann ist $a_0 = a_1 = \ldots = a_{p-2} = 0$. Ansonsten wäre $f(x) = a_{p-2}X^{p-2} + \ldots + a_1X + a_0 \neq 0$ ein Polynom in $\mathbb{Z}[X]$ mit $f(\zeta) = 0$ und $\deg(f) = p-2 < \deg(\phi_p)$, was ein Widerspruch dazu ist, dass $\phi_p(X)$ das Minimalpolynom von ζ ist.
Es gilt also für alle $i \in \{0, \ldots, p-2\}$:

$$a_i = z_i - z_{p-1} - py_i = 0 \Rightarrow z_i \equiv z_{p-1} \mod p.$$