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 $z_0 \equiv ... \equiv z_{p-1} \mod p$.

Lösung:

zu (a) Wir bezeichnen die Teilmenge $\{y_0 + y_1\zeta + ... + y_{p-2}\zeta^{p-2} \mid y_0, ..., y_{p-2} \in \mathbb{Z}\}$ von $\mathbb{C}$ mit M. Weil $\mathbb{Z}[\zeta]$ nach Definition der Durchschnitt aller Teilringe R von $\mathbb{C}$ mit $R \supseteq \mathbb{Z} \cup \{\zeta\}$ ist, müssen wir für den Beweis der Gleichung $Z[\zeta] = M$ zeigen:

(i) Die Menge M ist ein Teilring von $\mathbb{C}$ mit $M \supseteq \mathbb{Z} \cup \{\zeta\}$.

(ii) Ist R ein beliebiger Teilring von $\mathbb{C}$ mit $R \supseteq \mathbb{Z} \cup \{\zeta\}$, dann folgt $R \supseteq M$.

Denn aus (i) folgt, dass M den Durchschnitt all dieser Teilringe enthält, und aus (ii) folgt umgekehrt, dass M im Durchschnitt all dieser Teilringe enthalten ist.

zu (i) Für den Nachweis, dass M ein Teilring von $\mathbb{C}$ ist, stellen wir zunächst fest, dass $x_0 + x_1\zeta + ... + x_{p-2}\zeta^{p-2} = 1$ gilt, wenn wir $x_0 = 1$ und $x_k = 0$ für $1 \le k \le p-2$ setzen. Deshalb ist 1 in M enthalten. Seien nun $\alpha, \beta \in M$ vorgegeben. Zu zeigen ist $\alpha - \beta \in M$ und $\alpha\beta \in M$. Wegen $\alpha, \beta \in M$ gibt es $y_k, y'_k \in \mathbb{Z}$ für $0 \le k \le p-2$ mit $\alpha = y_0 + y_1\zeta + ... + y_{p-2}\zeta^{p-2}$ und $\beta = y'_0 + y'_1\zeta + ... + y'_{p-2}\zeta^{p-2}$. Es folgt

$$\alpha - \beta \quad = \quad (y_0 - y'_0) + (y_1 - y'_1)\zeta + ... + (y_{p-2} - y'_{p-2})\zeta^{p-2} \quad \in \quad \mathbb{Z}[\zeta]$$

wegen $y_k - y'_k \in \mathbb{Z}$ für $0 \le k \le p-2$.

Das Produkt von α und β ist gegeben durch

$$\alpha\beta \quad = \quad \left(\sum_{k=0}^{p-2} y_k\zeta^k\right)\left(\sum_{\ell=0}^{p-2} y'_\ell\zeta^\ell\right) \quad = \quad \sum_{r=0}^{2p-2}\left(\sum_{k+\ell=r} y_k y'_\ell\right)\zeta^r$$

wobei die innere Summe jeweils über alle Paare (k, ℓ) mit $k, \ell \in \{0, 1, ..., p-2\}$ und $k + \ell = r$ läuft. Es genügt nun zu zeigen, dass $\zeta^r \in M$ für $0 \le r \le 2p-2$ gilt. Denn wir haben bereits zeigt, dass $1 \in M$ gilt, und dass M unter der Verknüpfung $-$ abgeschlossen ist. Daraus folgt $0 = 1 - 1 \in M$, weiter $-\gamma = 0 - \gamma \in M$ für alle $\gamma \in M$ und schließlich $\gamma + \delta = \gamma - (-\delta) \in M$ für alle $\gamma, \delta \in M$. Dies zeigt, dass M jedenfalls eine Untergruppe von $(\mathbb{C}, +)$ ist. Daraus folgt $c\gamma \in M$ für alle $c \in \mathbb{Z}$ und $\gamma \in M$, denn die Bildung von $c\gamma$ kann als Potenzierung in der Gruppe $(\mathbb{C}, +)$ aufgefasst werden. Wenn also $\zeta^r \in M$ für alle $r \in \{0, 1, ..., p-2\}$ gezeigt ist, dann folgt daraus auch $\alpha\beta \in M$.

Wir zeigen nun, dass sogar $\zeta^r \in M$ für alle $r \in \mathbb{N}_0$ gilt, durch vollständige Induktion über r. Für $0 \le r \le p-2$ ist dies nach Definition von M klar (es ist $\zeta^r = \sum_{k=0}^{p-2} z_k\zeta^k$, wenn $z_r = 1$ und $z_k = 0$ für $k \ne r$ gesetzt wird). Sei nun $r \ge p-1$, und setzen wir $\zeta^s \in M$ für alle $s \in \mathbb{N}_0$ mit $s < r$ voraussetzen. Sei nun $\Phi_p = X^{p-1} + X^{p-2} + ... + X + 1 \in \mathbb{Z}[X]$, das p-te Kreisteilungspolynom. Aus der Vorlesung ist bekannt, dass Φ_p das Minimalpolynom von ζ über $\mathbb{Q}$ ist, weil es sich bei ζ um eine primitive p-te Einheitswurzel handelt. Insbesondere gilt $\Phi_p(\zeta) = 0$, also $\zeta^{p-1} + \zeta^{p-2} + ... + \zeta + 1 = 0$. Umstellen nach

ζ^{p-1} und Multiplikation der Gleichung mit ζ^{r-p+1} liefert $\zeta^r = -\zeta^{r-p+1} - \zeta^{r-p+2} - ... - \zeta^{r-1}$. Weil ζ^k für $r-p+1 \leq k \leq r-1$ nach Induktionsvoraussetzung in M liegt, und weil M unter Addition und Subtraktion abgeschlossen ist, folgt $\zeta^r \in M$. Damit ist der Nachweis von $\alpha\beta \in M$ abgeschlossen.

Es gilt $\mathbb{Z} \subseteq M$, denn für vorgegebenes $a \in Z$ ist $a = \sum_{k=0}^{p-2} x_k \zeta^k$, wenn wir $x_0 = a$ und $x_k = 0$ für $1 \leq k \leq p-2$ setzen. Außerdem ist ζ in M enthalten, denn es gilt $\zeta = \sum_{k=0}^{p-2} x_k \zeta^k$, wenn $x_1 = 1$ und $x_k = 0$ für $k \neq 1$ ist. Insgesamt gilt also $\mathbb{Z} \cup \{\zeta\} \subseteq M$.

zu (ii) Sei R ein beliebiger Teilring von $\mathbb{C}$ mit $\mathbb{Z} \cup \{\zeta\} \subseteq R$. Zu zeigen ist $M \subseteq R$. Sei dazu $\alpha \in M$ vorgegeben, $\alpha = x_0 + x_1\zeta + ... + x_{p-2}\zeta^{p-2}$ mit $x_0, x_1, ..., x_{p-2} \in \mathbb{Z}$. Dann ist $\alpha \in R$ zu zeigen. Wegen $\mathbb{Z} \subseteq R$ gilt $x_0, ..., x_{p-2} \in R$. Weil auch ζ in R liegt, und weil R als Teilring von $\mathbb{C}$ unter Multiplikation abgeschlossen ist, folgt $x_k\zeta^k \in R$ für $0 \leq k \leq p-2$. Weil R auch unter Addition abgeschlossen ist, folgt schließlich $\alpha = x_0 + x_1\zeta + ... + x_{p-2}\zeta^{p-2} \in R$.

Zum Schluss beweisen wir noch die Inklusion $M \subseteq \mathbb{Q}(\zeta)$. Sei $\alpha \in M$ vorgegeben, $\alpha = y_0 + y_1\zeta + ... + y_{p-2}\zeta^{p-2}$ mit $y_0, ..., y_{p-2} \in \mathbb{Z}$. Nach Definition ist $\mathbb{Q}(\zeta)$ ein Teilkörper von $\mathbb{C}$, der $\mathbb{Q} \cup \{\zeta\}$ enthält. Daraus folgt $y_0, ..., y_{p-2} \in \mathbb{Q}(\zeta)$ und $\zeta \in \mathbb{Q}(\zeta)$. Weil $\mathbb{Q}(\zeta)$ als Teilkörper insbesondere abgeschlossen unter Multiplikation ist, folgt $y_k\zeta^k$ für $0 \leq k \leq p-2$. Weil $\mathbb{Q}(\zeta)$ auch abgeschlossen unter Addition ist, erhalten wir schließlich $\alpha = y_0 + y_1\zeta + ... + y_{p-2}\zeta^{p-2} \in \mathbb{Q}(\zeta)$.

zu (b) Setzen wir $\frac{x}{p} \in \mathbb{Z}[\zeta]$ voraus, dann gibt es nach Teil (a) Elemente $y_0, y_1, ..., y_{p-2} \in \mathbb{Z}$ mit $\frac{x}{p} = y_0 + y_1\zeta + ... + y_{p-2}\zeta^{p-2}$. Es gilt also

$$z_0 + z_1\zeta + ... + z_{p-2}\zeta^{p-2} + z_{p-1}\zeta^{p-1} \quad = \quad py_0 + py_1\zeta + ... + py_{p-2}\zeta^{p-2}.$$

Da Φ_p das Minimalpolynom von ζ ist, gilt weiter

$$\Phi_p(\zeta) = 0 \quad \Leftrightarrow \quad \zeta^{p-1} + \zeta^{p-2} + ... + \zeta + 1 = 0 \quad \Leftrightarrow \quad \zeta^{p-1} = -1 - \zeta - ... - \zeta^{p-2}.$$

Setzen wir dies in die Gleichung von oben ein, so erhalten wir

$$\begin{aligned} & z_0 + z_1\zeta + ... + z_{p-2}\zeta^{p-2} + z_{p-1}(-1 - \zeta - ... - \zeta^{p-2}) = py_0 + py_1\zeta + ... + py_{p-2}\zeta^{p-2} \\ \Leftrightarrow \quad & (z_0 - z_{p-1}) + (z_1 - z_{p-1})\zeta + ... + (z_{p-2} - z_{p-1})\zeta^{p-2} \overset{(*)}{=} py_0 + py_1\zeta + ... + py_{p-2}\zeta^{p-2}. \end{aligned}$$

Weil das Minimalpolynom Φ_p von ζ vom Grad $p-1$ ist, handelt es sich bei $(1, \zeta, ..., \zeta^{p-2})$ laut Vorlesung um eine Basis von $\mathbb{Q}(\zeta)$ als $\mathbb{Q}$-Vektorraum. Dies bedeutet, dass jedes Element in $\mathbb{Q}(\zeta)$ auf eindeutige Weise als $\mathbb{Q}$-Linearkombination des Tupels $(1, \zeta, ..., \zeta^{p-2})$ darstellbar ist. Aus diesem Grund dürfen wir in der Gleichung (*) die Koeffizienten der Elemente $1, \zeta, ..., \zeta^{p-2}$ auf beiden Seiten vergleichen und erhalten $z_k - z_{p-1} = py_k$ für $0 \leq k \leq p-2$. Daraus folgt $z_k \equiv z_{p-1} \mod p$ für $0 \leq k \leq p-2$ und somit $z_0 \equiv z_1 \equiv ... \equiv z_{p-2} \equiv z_{p-1} \mod p$.