**Aufgabe H12T2A3** (6 Punkte)

Seien $p$ eine Primzahl und $\zeta$ eine primitive $p$-te Einheitswurzel in $\mathbb{C}$. Sei $R = \mathbb{Z}[\zeta]$ der von $\zeta$ erzeugte Unterring von $\mathbb{C}$. Sei $a \in \mathbb{Z}$ eine ganze Zahl. Zeigen Sie, dass

$$\mathbb{Z}/\left(\sum_{\ell=0}^{p-1} a^\ell\right) \longrightarrow R/(a-\zeta) \quad , \quad n + \left(\sum_{\ell=0}^{p-1} a^\ell\right) \mapsto n + (a-\zeta)$$

ein wohldefinierter Ringisomorphismus ist und folgern Sie daraus, dass $2-\zeta$ genau dann ein Primelement in $R$ ist, wenn $2^p - 1$ eine Primzahl ist.

*Lösung:*

Wir beweisen die Wohldefiniertheit und die Ringisomorphismus-Eigenschaft der angegebenen Abbildung, indem wir den Homomorphiesatz für Ringe auf die Abbildung

$$\phi : \mathbb{Z} \longrightarrow R/(a-\zeta) \quad , \quad n \mapsto n + (a-\zeta)$$

anwenden. Als Komposition der Inklusionsabbildung $\mathbb{Z} \to R$ und des kanonischen Epimorphismus $R \to R/(a-\zeta)$, $\alpha \mapsto \alpha + (a-\zeta)$ ist $\phi$ ein Homomorphismus für Ringe. Für müssen nun noch zeigen, dass $\phi$ surjektiv und $(\sum_{\ell=0}^{p-1} a^\ell)$ der Kern von $\phi$ ist. Zum Nachweis der Surjektivität sei $\alpha + (a-\zeta) \in R/(a-\zeta)$ vorgegeben, mit $\alpha \in R$. Das Element $\alpha$ hat die Form $\alpha = g(\zeta)$ für ein geeignetes Polynom $g \in \mathbb{Z}[x]$, $g = \sum_{k=0}^{m} c_k x^k$ mit $m \in \mathbb{N}_0$ und $c_0, ..., c_m \in \mathbb{Z}$. Nun gilt

$$\phi(a) \quad = \quad a + (a-\zeta) \quad = \quad a - (a-\zeta) + (a-\zeta) \quad = \quad \zeta + (a-\zeta).$$

Weil $\phi$ ein Ringhomomorphismus ist, folgt

$$\begin{aligned} \phi(g(a)) \quad = \quad \phi\left(\sum_{k=0}^{m} c_k a^k\right) \quad = \quad \sum_{k=0}^{m} c_k \phi(a)^k \quad = \quad \sum_{k=0}^{m} c_k \zeta^k + (a-\zeta) \\ = \quad g(\zeta) + (a-\zeta) \quad = \quad \alpha + (a-\zeta). \end{aligned}$$

Damit ist die Surjektivität nachgewiesen. Der Kern von $\phi$ ist offenbar gegeben durch $Z \cap (a-\zeta)$, denn ein Element $c \in \mathbb{Z}$ liegt genau dann in $\ker(\phi)$, wenn $c + (a-\zeta) = \phi(c) = 0 + (a-\zeta)$ gilt, was zu $c \in (a-\zeta)$ äquivalent ist. Zu zeigen ist also

$$(\Phi_p(a)) \quad = \quad \mathbb{Z} \cap (a-\zeta)$$

wobei $\Phi_p = x^{p-1} + x^{p-2} + ... + x + 1 \in \mathbb{Z}[x]$ das $p$-te Kreisteilungspolynom bezeichnet. Für die Inklusion „$\subseteq$“ genügt es $\Phi_p(a) \in (a-\zeta)$ zu zeigen, und dies erhält man wegen $a + (a-\zeta) = \zeta + (a-\zeta)$ und $\Phi_p(\zeta) = 0$ durch die Rechnung

$$\Phi_p(a) + (a-\zeta) \quad = \quad \Phi_p(\zeta) + (a-\zeta) \quad = \quad 0 + (a-\zeta).$$

Für den Nachweis von „$\supseteq$“ sei $b \in \mathbb{Z} \cap (a-\zeta)$ vorgegeben. Dann gilt $b = (a-\zeta)\alpha$ für ein $\alpha \in \mathbb{Z}[\zeta]$, es gibt also ein $g \in \mathbb{Z}[x]$ mit $\alpha = g(\zeta)$. Setzen wir $h = (a-x)g - b$, dann gilt $h(\zeta) = (a-\zeta)g(\zeta) - b = (a-\zeta)\alpha - b = 0$. Weil $\Phi_p$ das Minimalpolynom von $\zeta$ über $\mathbb{Q}$ ist, folgt aus $h(\zeta) = 0$, dass $\Phi_p$ ein Teiler von $h$ in $\mathbb{Q}[x]$ ist. Da das Polynom $\Phi_p \in \mathbb{Z}[x]$ als normiertes Polynom insbesondere primitiv ist, ist $\Phi_p$ sogar ein Teiler von $h$ im Ring $\mathbb{Z}[x]$. Es gibt also ein Polynom $u \in \mathbb{Z}[x]$ mit $h = u\Phi_p$. Es folgt nun

$$u(a)\Phi_p(a) \quad = \quad h(a) \quad = \quad (a-a)g(a) - b \quad = \quad -b \quad ,$$

und wegen $u(a) \in \mathbb{Z}$ ist damit $b \in (\Phi_p(a))$ nachgewiesen. Der Beweis von $\mathbb{Z}/(\Phi_p(a)) \cong R/(a-\zeta)$ ist damit abgeschlossen.

Nun beweisen wir noch die angegebene Äquivalenz. Laut Vorlesung ist $2-\zeta$ genau dann ein Primelement in $R$, wenn das Hauptideal $(2-\zeta)$ in $R$ ein Primideal ist. Dies wiederum ist genau dann der Fall, wenn der Faktorring $R/(2-\zeta) \cong \mathbb{Z}/(\Phi_p(2))$ ein Integritätsbereich ist. Dies wiederum ist gleichbedeutend damit, dass es sich bei $\Phi_p(2)$ um ein Primelement des Rings $\mathbb{Z}$ handelt. Wegen $\Phi_p(2) = \sum_{k=0}^{p-1} 2^k = 2^p - 1 \in \mathbb{N}$ ist dies genau dann der Fall, wenn $2^p - 1$ eine Primzahl ist, denn die Primelemente von $\mathbb{Z}$ sind gegeben durch $\pm q$, wobei $q$ die Primzahlen durchläuft.