Aufgabe F18T1A3 (12 Punkte)

(a) Zeichnen Sie alle 5-ten und alle 10-ten komplexen Einheitswurzeln in der komplexen Zahlenebene ein und markieren Sie jeweils die primitiven Einheitswurzeln.

(b) Sei $p \geq 3$ prim und $\zeta \in \mathbb{C}$. Zeigen Sie:

(i) Ist ζ eine primitive p-te Einheitswurzel, so ist $-\zeta$ eine $2p$-te Einheitswurzel.

(ii) Genau dann ist ζ eine primitive p-te Einheitswurzel, wenn $-\zeta$ eine primitive $2p$-te Einheitswurzel ist.

(iii) Es ist $\Phi_{2p}(x) = \Phi_p(-x)$. (Mit $\Phi_n \in \mathbb{Z}[x]$ bezeichnen wir das n-te Kreisteilungspolynom.)

Lösung:

zu (a) An Stelle einer Zeichnung geben wir hier nur eine Beschreibung an. Die 5-ten komplexen Einheitswurzeln liegen alle auf dem Einheitskreis um den Nullpunkt und bilden dort ein regelmäiges Fünfeck, wobei eine der Ecken auf dem Punkt 1 liegt. Es handelt sich um die komplexen Zahlen $\zeta_5^k = e^{2\pi ik/5}$ mit $0 \leq k < 4$, wobei die Elemente mit $k = 1, 2, 3, 4$ primitive 5-te Einheitswurzeln sind.

Die 10-ten komplexen Einheitswurzeln liegen ebenfalls alle auf dem Einheitskreis. Sie bilden ein regelmäßiges Zehneck, von dem eine Ecke mit 1 übereinstimmt. Insgesamt sind die zehn Ecken gegeben durch $\zeta_{10}^k = e^{2\pi ik/10}$ mit $0 \leq k < 10$, wobei die Werte $k = 1, 3, 7, 9$ den primitiven 10-ten Einheitswurzeln entsprechen. (Allgemein ist für $n \in \mathbb{N}$, $k \in \mathbb{Z}$ und $\zeta_n = e^{2\pi i/n}$ die Potenz ζ_n^k genau dann eine primitive n-te Einheitswurzel, wenn $\mathrm{ggT}(k, n) = 1$ gilt.)

zu (b)(i) Weil ζ eine p-te Einheitswurzel ist, gilt $\zeta^p = 1$. Daraus folgt $(-\zeta)^{2p} = (-1)^{2p}\zeta^{2p} = ((-1)^2)^p(\zeta^p)^2 = 1^p \cdot 1^2 = 1$. Dies zeigt, dass $-\zeta$ eine $2p$-te Einheitswurzel ist.

zu (b)(ii) „$\Rightarrow$“ Sei ζ eine primitive p-te Einheitswurzel. Zu zeigen ist, dass es sich bei $-\zeta$ um ein Element der Ordnung $2p$ in der multiplikative Gruppe $\mathbb{C}^\times$ handelt. Dazu überprüfen wir für ein beliebig vorgegebenes $k \in \mathbb{Z}$ die Äquivalenz $(-\zeta)^k = 1 \Leftrightarrow (2p) \mid k$. Aus Teil (i) wissen wir bereits, dass $(-\zeta)^{2p} = 1$ gilt. Ist nun $(2p) \mid k$, also $k = 2pm$ für ein $m \in \mathbb{Z}$, dann folgt $(-\zeta)^k = ((-\zeta)^{2p})^m = 1^m = 1$.

Setzen wir nun umgekehrt $(-\zeta)^k = 1$ voraus. Ist k ungerade, dann folgt $\zeta^k = -1$ und $\zeta^{2k} = (-1)^2 = 1$. Wegen $\mathrm{ord}(\zeta) = p$ folgt $p \mid 2k$, und weil p ungerade ist, sogar $p \mid k$. Aber dies bedeutet $\zeta^k = 1$ und führt zum Widerspruch $1 = (-1)^k\zeta^k = (-1) \cdot 1 = -1$. Also muss k gerade sein, und die Gleichung $(-1)^k\zeta^k = 1$ liefert $\zeta^k = 1$. Wiederum folgt $p \mid k$. Aus $2 \mid k$, $p \mid k$ und $\mathrm{ggT}(2, p) = 1$ folgt $(2p) \mid k$.

zu (b)(iii) Laut Vorlesung ist das Kreisteilungspolynom Φ_{2p} in $\mathbb{Q}[x]$ irreduzibel und wegen $\mathrm{char}(\mathbb{Q}) = 0$ somit auch separabel. Es zerfällt also über $\mathbb{C}$ in lauter verschiedene Linearfaktoren. Auch das Polynom $f(x) = \Phi_p(-x)$ ist irreduzibel. Denn ansonsten gäbe es eine Zerlegung $f = gh$ in zwei nicht-konstante Faktoren $g, h \in \mathbb{Q}[x]$, und durch $\Phi_p(x) = f(-x) = g(-x)h(-x)$ würde man eine Zerlegung von Φ_p in zwei nicht-konstante Faktoren aus $\mathbb{Q}[x]$ enthalten. Aber dies widerspricht der Irreduzibilität des Kreisteilungspolynoms Φ_p. Somit ist auch f separabel, zerfällt über $\mathbb{C}$ also ebenfalls in lauter verschiedene Linearfaktoren. Weil es jeweils nur einfache Nullstellen gibt, genügt es zu zeigen, dass die beiden Polynome f und Φ_{2p} dieselben komplexen Nullstellen besitzen.

Für ein beliebiges $\alpha \in \mathbb{C}$ gilt $f(-\alpha) = 0$ genau dann, wenn $\Phi_p(\alpha) = 0$ ist, also genau dann, wenn es sich bei α um eine primitive p-te Einheitswurzel handelt. Dies wiederum ist nach (iii) genau dann der Fall, wenn $-\alpha$ eine primitive $2p$-te Einheitswurzel ist, wenn also $\Phi_{2p}(-\alpha) = 0$ gilt. Damit ist gezeigt, dass f und Φ_{2p} tatsächlich dieselben Nullstellen in $\mathbb{C}$ haben.