F18-T1-A3

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

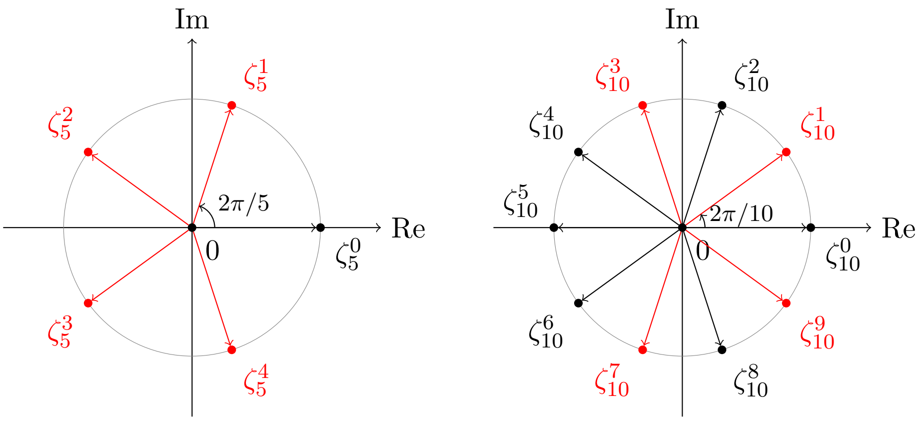
b) Sei $p \geq 3$ prim und $\zeta \in \mathbb{C}$. Zeigen Sie:

   i) Ist ζ eine 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.)

Lösungsvorschlag. Zu a).



5-te Einheitswurzeln, $\zeta_5 = e^{\frac{2\pi i}{5}}$ 10-te Einheitswurzeln, $\zeta_{10} = e^{\frac{2\pi i}{10}}$

Aufgabe a). Primitive Einheitswurzeln sind rot markiert.

Zu b), i). Wir bezeichnen mit $U_n \subset \mathbb{C}$ die Menge der n-ten Einheitswurzeln in $\mathbb{C}$ und zeigen, dass die Abbildung

$$\begin{aligned} f\colon U_2 \times U_p &\longrightarrow U_{2p}, \\ (\eta, \zeta) &\longmapsto \eta\zeta \end{aligned}$$

ein wohldefinierter Gruppenmorphismus ist. Die Wohldefiniertheit als Abbildung ist dabei klar, da für alle $\eta \in U_2$, $\zeta \in U_p$ offenbar gilt $(\eta\zeta)^{2p} = (\eta^2)^p(\zeta^p)^2 = 1$, also $\eta\zeta \in U_{2p}$. Weiter ist f ein Gruppenmorphismus, da

$$f((\eta, \zeta) \cdot (\eta', \zeta')) = f(\eta\eta', \zeta\zeta') = \eta\eta'\zeta\zeta' = \eta\zeta\eta'\zeta' = f((\eta, \zeta)) \cdot f((\eta', \zeta')).$$

Ist schließlich $1 = f((\eta, \zeta)) = \eta\zeta$, so folgt $\eta = \zeta^{-1} \in \mathbb{C}^\times$, wegen $\operatorname{ord}(\eta)|2 = |U_2|$, $\operatorname{ord}(\zeta)|p = |U_p|$ und $\operatorname{ggT}(2, p) = 1$ nach Voraussetzung impliziert dies aber bereits $\operatorname{ord}(\eta) = 1 = \operatorname{ord}(\zeta^{-1}) = \operatorname{ord}(\zeta)$, also $\eta = 1 = \zeta$, womit wir gezeigt haben, dass f injektiv ist. Wegen $|U_2 \times U_p| = 2p = |U_{2p}|$ ist f damit auch schon surjektiv und also bijektiv.

Insbesondere ist nun also für jedes $\zeta \in U_p$ wie gewünscht gezeigt $-\zeta = f(-1, \zeta) \in U_{2p}$.
Bemerkung: Diese Teilaufgabe wäre natürlich auch durch die einfache Beobachtung $(-\zeta)^{2p} = ((-1)^2)^p(\zeta^p)^2 = 1$ für alle $\zeta \in U_p$ bereits vollständig gelöst.
Zu b), ii). Mit Hilfe der zu Teil i) bewiesenen Beobachtung können wir folgern: Sei $\zeta \in U_n$ primitiv. Dann ist $\mathrm{ord}((-1, \zeta)) = \mathrm{kgV}(\mathrm{ord}(-1), \mathrm{ord}(\zeta)) = \mathrm{kgV}(2, p) = 2p$, das heißt $(-1, \zeta)$ ist ein Erzeuger von $U_2 \times U_p$. Da die Abbildung aus i) ein Gruppenisomorphismus ist, ist damit natürlich auch $f((-1, \zeta)) = -\zeta$ ein Erzeuger von U_{2p}, also eine primitive $2p$-te Einheitswurzel.
Zu b), iii). Nach Definition ist $\phi_{2p}(X) \in \mathbb{Z}[X]$ dasjenige Polynom, dessen Nullstellen gerade die primitiven $2p$-ten Einheitswurzeln sind. Nach Teil ii) ist damit jede Nullstelle von $\phi_p(-X)$ eine Nullstelle von $\phi_{2p}(X)$, also $\phi_p(-X)|\phi_{2p}(X)$. Wir wissen außerdem, dass gilt $\deg(\phi_{2p}) = \varphi(2p) = \varphi(2)\varphi(p) = \varphi(p) = \deg(\phi_p) = \deg(\phi_p(-X))$, wobei wie üblich $\varphi(\bullet)$ die Eulersche Phi-Funktion bezeichnet. Damit folgt also (beide Polynome sind normiert) $\phi_p(-X) = \phi_{2p}(X)$.