Aufgabe H18T2A5 (12 Punkte)

Sei p eine ungerade Primzahl und sei ζ eine primitive p-te Einheitswurzel. Zeigen Sie:

(a) Die Körpererweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ hat genau einen Zwischenkörper Z vom Grad 2 über $\mathbb{Q}$.

(b) Komplexe Konjugation induziert ein Element der Ordnung 2 in der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$.

(c) Der Körper Z aus (a) ist genau dann ein Unterkörper von $\mathbb{R}$, wenn $p \equiv 1 \bmod 4$.

Lösung:

zu (a) Bei $\mathbb{Q}(\zeta)$ handelt es sich um den p-ten Kreisteilungskörper, und aus der Vorlesung ist bekannt, dass die Galoisgruppe $G = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ isomorph zur primen Restklassengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ ist. Da es sich bei p um eine Primzahl handelt, ist diese wiederum isomorph zu $\mathbb{Z}/(p-1)\mathbb{Z}$. Als zyklische Gruppe der Ordnung $p-1$ besitzt $\mathbb{Z}/(p-1)\mathbb{Z}$ für jeden Teiler $d \in \mathbb{N}$ von $p-1$ genau eine Untergruppe der Ordnung d. Weil p ungerade ist, ist $\frac{p-1}{2}$ ein ganzzahliger Teiler von $p-1$. Also gibt es in $\mathbb{Z}/(p-1)\mathbb{Z}$, und damit auch in G, genau eine Untergruppe der Ordnung $\frac{p-1}{2}$ bzw. genau eine Untergruppe vom Index 2. Nach dem Hauptsatz der Galoistheorie gibt es eine bijektive Korrespondenz zwischen den Untergruppen von G vom Index 2 und den Zwischenkörpern Z von $\mathbb{Q}(\zeta)|\mathbb{Q}$ mit $[Z : \mathbb{Q}] = 2$. Also gibt es in $\mathbb{Q}(\zeta)|\mathbb{Q}$ genau einen Zwischenkörper Z mit $[Z : \mathbb{Q}] = 2$.

zu (b) Durch Einschränkung der komplexen Konjugation $\iota : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ auf $\mathbb{Q}(\zeta)$ erhält man einen $\mathbb{Q}$-Homomorphismus $\iota|_{\mathbb{Q}(\zeta)} : \mathbb{Q}(\zeta) \to \mathbb{C}$. Laut Vorlesung ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ als Kreisteilungserweiterung galoissch, insbesondere normal. Weil $\mathbb{C}$ ein algebraisch abgeschlossener Erweiterungskörper von $\mathbb{Q}(\zeta)$ ist, gilt deshalb $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\zeta), \mathbb{C}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Also ist $\sigma = \iota|_{\mathbb{Q}(\zeta)}$ ein Element der Galoisgruppe G.

Nun zeigen wir noch, dass $\mathrm{ord}(\sigma) = 2$ gilt. Dazu bemerken wir zunächst, dass $\zeta \notin \mathbb{R}$ gilt. Denn weil ζ eine Einheitswurzel ist, gilt einerseits $|\zeta| = 1$, damit auch $\zeta\bar{\zeta} = |\zeta|^2 = 1$ und $\bar{\zeta} = \zeta^{-1}$. Andererseits gilt $\zeta^{-1} \neq \zeta$, denn ansonsten wäre $\zeta^2 = 1$, im Widerspruch dazu, dass ζ als primitive p-te Einheitswurzel in der multiplikativen Gruppe $\mathbb{C}^\times$ ein Element der Ordnung $p > 2$ ist. Insgesamt gilt also $\zeta \neq \bar{\zeta}$ und damit $\zeta \notin \mathbb{R}$. Daraus folgt nun $\sigma(\zeta) = \bar{\zeta} \neq \zeta$ und damit $\sigma \neq \mathrm{id}_{\mathbb{Q}(\zeta)}$. Andererseits ist $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\bar{\alpha}) = \bar{\bar{\alpha}} = \alpha$ für alle $\alpha \in \mathbb{Q}(\zeta)$, also $\sigma^2 = \mathrm{id}_{\mathbb{Q}(\zeta)}$. Aus $\sigma \neq \mathrm{id}_{\mathbb{Q}(\zeta)}$ und $\sigma^2 = \mathrm{id}_{\mathbb{Q}(\zeta)}$ folgt $\mathrm{ord}(\sigma) = 2$.

zu (c) Wie wir bereits in Teil (a) festgestellt haben, ist G zyklisch von Ordung $p-1$. Sei τ ein erzeugendes Element von G. Dann ist τ^2 von Ordnung $\frac{1}{2}(p-1)$ und $\langle\tau^2\rangle$ somit die eindeutig bestimmte Untergruppe vom Index 2 von G. Nach dem Hauptsatz der Galoistheorie ist dann der Fixkörper $\mathbb{Q}(\zeta)^{\langle\tau^2\rangle}$ der eindeutig bestimmte Zwischenkörper mit $[\mathbb{Q}(\zeta)^{\langle\tau^2\rangle} : \mathbb{Q}] = 2$, es gilt also $Z = \mathbb{Q}(\zeta)^{\langle\tau^2\rangle}$ mit dem Zwischenkörper Z aus Teil (a). Weiter gilt $\mathbb{Q}(\zeta)^{\langle\sigma\rangle} = \mathbb{Q}(\zeta) \cap \mathbb{R}$, denn ein Element $\alpha \in \mathbb{Q}(\zeta)$ liegt genau dann im Fixkörper von $\langle\sigma\rangle = \{\mathrm{id}_{\mathbb{Q}(\zeta)}, \sigma\rangle\}$, wenn $\bar{\alpha} = \sigma(\alpha) = \alpha$ gilt, also genau dann, wenn α in $\mathbb{Q}(\zeta) \cap \mathbb{R}$ enthalten ist.

Weil G zyklisch von Ordnung $p-1$ ist, gibt es in G genau eine Untergruppe der Ordnung 2, und damit auch genau ein Element der Ordnung 2. Denn jedes Element $\rho \in G$ der Ordnung 2 ist genau in einer Untergruppe der Ordnung 2 enthalten (nämlich $\langle\rho\rangle$), und umgekehrt enthält jede Untergruppe der Ordnung 2 genau ein Element der Ordnung 2. Wegen $\mathrm{ord}(\tau^{(p-1)/2} = 2$ folgt daraus $\tau^{(p-1)/2} = \sigma$. Berücksichtigen wir nun noch, dass die Galois-Korrespondenz $U \mapsto \mathbb{Q}(\zeta)^U$ von Untergruppen zu Zwischenkörpern antiton ist, so erhalten wir insgesamt die Äquivalenz

$$Z \subseteq \mathbb{R} \quad \Leftrightarrow \quad Z \subseteq \mathbb{Q}(\zeta) \cap \mathbb{R} \quad \Leftrightarrow \quad \mathbb{Q}(\zeta)^{\langle \tau^2 \rangle} \subseteq \mathbb{Q}(\zeta)^{\langle \sigma \rangle} \quad \Leftrightarrow \quad \mathbb{Q}(\zeta)^{\langle \tau^2 \rangle} \subseteq \mathbb{Q}(\zeta)^{\langle \tau^{(p-1)/2} \rangle}$$

$$\Leftrightarrow \quad \langle \tau^2 \rangle \supseteq \langle \tau^{(p-1)/2} \rangle \quad \Leftrightarrow \quad \tau^{(p-1)/2} \in \langle \tau^2 \rangle \quad \Leftrightarrow \quad \exists\, r \in \mathbb{Z} : \tau^{(p-1)/2} = (\tau^2)^r$$

$$\Leftrightarrow \quad \exists\, r \in \mathbb{Z} : \tau^{(p-1)/2} = \tau^{2r} \quad \Leftrightarrow \quad \exists\, r \in \mathbb{Z} : \tau^{(p-1)/2-2r} = \mathrm{id}_{\mathbb{Q}(\zeta)}$$

$$\overset{\mathrm{ord}(\tau)=p-1}{\Leftrightarrow} \quad \exists\, r \in \mathbb{Z} : (p-1) \mid \tfrac{1}{2}(p-1) - 2r \quad \Leftrightarrow \quad \exists\, r, s \in \mathbb{Z} : s(p-1) = \tfrac{1}{2}(p-1) - 2r$$

$$\Leftrightarrow \quad \exists\, r, s \in \mathbb{Z} : 2s(p-1) = (p-1) - 4r \quad \Leftrightarrow \quad \exists\, s \in \mathbb{Z} : 4 \mid (2s-1)(p-1) \quad \Leftrightarrow \quad 4 \mid (p-1)$$

$$\Leftrightarrow \quad p \equiv 1 \bmod 4.$$