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 $p \equiv 1 \bmod 4$.

Hinweis/Kommentar:

Für Teil (a) verwendet man neben dem Hauptsatz der Galoistheorie den aus der Vorlesung bekannten Isomorphismus $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, wobei $\zeta \in \mathbb{C}^\times$ eine primitive n-te Einheitswurzel bezeichnet. Die Struktur der primen Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ ist aus der Vorlesung ebenfalls für jedes $n \in \mathbb{N}$ bekannt.

In Teil (b) benötigt man die Eigenschaft *normal* der Erweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$, um zu zeigen, dass die komplexe Konjugation ein Element der Galoisgruppe definiert; im Allgemeinen kann es passieren, dass ein Zwischenkörper von $\mathbb{C}|\mathbb{Q}$ durch die komplexe Konjugation nicht in sich abgebildet wird. Beispielsweise gilt dies für den Körper $\mathbb{Q}(\zeta\sqrt[3]{2})$ der Fall, wenn $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ ist. Der Nachweis, dass das so erhalten Element von $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ Ordnung 2 hat, ist dagegen einfach.

In Teil (c) ist der entscheidende Ansatz die *Antitonie* der Galois-Korrespondenz: Ist $L|K$ eine Galois-Erweiterung, $G = \mathrm{Gal}(L|K)$ die zugehörige Galoisgruppe und $U, V \subseteq G$ Untergruppen, dann gilt die Äquivalenz $U \subseteq V \Leftrightarrow L^U \supseteq L^V$, wobei L^U, L^V die Fixkörper von U und V sind. Es kommt also darauf an, Z und $\mathbb{Q}(\zeta) \cap \mathbb{R}$ als Fixkörper geeigneter Untergruppen von $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ darzustellen, wobei man die Ergebnisse aus Teil (a) und (b) verwendet. Um einen Zusammenhang zwischen den beiden Untergruppen herzustellen, verwendet man, dass die Galoisgruppe zyklisch von Ordnung $p-1$ ist.