F25-T2-A2

Sei p eine Primzahl.

a) Sei q ein Primteiler von $2^p - 1$. Zeigen Sie: $q \equiv 1 (\bmod p)$.
Hinweis: Betrachten Sie die Ordnung von $2 \in (\mathbb{Z}/q\mathbb{Z})^\times$.

b) Zeigen Sie: Es gibt eine Galois-Erweiterung $\mathbb{Q} \subseteq K_p$ mit $\mathrm{Gal}(K_p|\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$.
Hinweis: Betrachten Sie Teilkörper von geeigeneten Kreisteilungskörpern.

Lösung

a) Dem Hinweis folgend berechnen wir die Ordnung von $2 \in (\mathbb{Z}/q\mathbb{Z})^\times$. Dafür führen wir die Notation $\mathrm{ord}_q(2)$ für jene Ordnung ein. Da $q \mid 2^p - 1$ gilt $2^p - 1 \equiv 0 (\bmod q) \iff 2^p \equiv 1 (\bmod q)$. Demnach gilt $\mathrm{ord}_q(2) | p$. Da p eine Primzahl ist, gilt $\mathrm{ord}_q(2) \in \{1, p\}$. Nach Lagrange gilt $\mathrm{ord}_q(2) \mid q - 1$. Im Fall $\mathrm{ord}_q(2) = p$ gilt demnach $p \mid q - 1 \iff q \equiv 1 (\bmod p)$. Den anderen Fall gilt es auszuschließen. Wäre $\mathrm{ord}_2(q) = 1$, dann würde $2 \equiv 1 (\bmod q)$ gelten. Das ist äquivalent zu $1 \equiv 0 (\bmod q)$. Ein Widerspruch.

b) Wir nutzen a) und den Hinweis. Wir betrachten $\zeta := \exp\left(\frac{2\pi i}{q}\right)$ und die zugehörige zyklotonische Körpererweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$. Bekanntermaßen gilt $\mathrm{Gal}(\mathbb{Q}(\zeta)\mathbb{Q}) \cong \mathbb{Z}/q - 1\mathbb{Z}$ (da q prim ist, gilt $(\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/q - 1\mathbb{Z}$). Da $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ zyklisch, also abelsch ist, sind alle Untergruppen Normalteiler. Zudem handelt es sich bei $\mathbb{Q}(\zeta)|\mathbb{Q}$ um eine endliche Galois-Erweiterung, weshalb wir den Hauptsatz der Galoistheorie verwenden können. Da $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ zyklisch ist, gibt es zu jedem Teiler von $q-1$ genau eine zyklische Untergruppe von $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ mit k Elementen, wobei $k \cdot p = q-1$. So ein k gibt es nach a), denn $q \equiv 1 (\bmod p) \Rightarrow p \mid q-1$. Nach dem Hauptsatz der Galoistheorie gibt es also ein K_p, sodass $\mathrm{Gal}(\mathbb{Q}(\zeta)|K_p) \cong \mathbb{Z}/k\mathbb{Z}$. Nach den obigen Ausführungen ist $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ ein Normalteiler von $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Nach dem Zusatz zum Hauptsatz der Galoistheorie gilt also $\mathrm{Gal}(K_p|\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta)|K_p) \cong \mathbb{Z}/q - 1\mathbb{Z}/\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$.