F12-T3-A2

Sei $p \neq 2$ eine Primzahl, $\zeta := \exp(2\pi i/p) \in \mathbb{C}$ und $\sqrt[p]{p} \in \mathbb{R}_{>0}$. Weiter sei L der Zerfällungskörper des Polynomes $f(X) = X^p - p \in \mathbb{C}$ und M der Zerfällungskörper des Polynomes $g(X) = X^{p^2} - 1$ in $\mathbb{C}$. Zeigen Sie:

a) $L = \mathbb{Q}(\zeta, \sqrt[p]{p})$.

b) $[L : \mathbb{Q}] = [M : \mathbb{Q}]$.

c) Die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ ist nicht abelsch.

d) Die Körper L und M sind nicht isomorph.

Lösungsvorschlag. Zu a). Wir nennen $\alpha := \sqrt[p]{p}$. Die Nullstellen von f sind gerade $\zeta^i\alpha$, $i = 0, \ldots, p-1$. Nach Definition ist damit $L = \mathbb{Q}(\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{p-1}\alpha)$. Offensichtlich ist damit $L \subset \mathbb{Q}(\zeta, \alpha)$. Für die umgekehrte Inklusion "$\supset$" ist noch zu zeigen, dass $\zeta \in L$. Das ist aber klar, da $\zeta = \zeta\alpha/\alpha \in L$.
Zu b). Da $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = p$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ sowie $\mathrm{ggT}(p, p-1) = 1$ folgt nach der Gradformel $[\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}] = p(p-1)$, vgl. folgendes Diagramm:

$$\begin{tikzcd} & \mathbb{Q}(\zeta,\alpha) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta) \arrow[dr, dash, "p-1"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash, "p"] \\ & \mathbb{Q} & \end{tikzcd}$$

Weiter ist $M = \mathbb{Q}(\zeta_{p^2}^i | i = 0, \ldots, p^2 - 1)$ die von den p^2-ten Einheitswurzeln erzeugte Erweiterung von $\mathbb{Q}$, also $M = \mathbb{Q}(\zeta_{p^2})$ für eine primitive p^2-te Einheitswurzel ζ_{p^2}. Damit ist bekanntlich $[M : \mathbb{Q}] = \phi(p^2) = p(p-1)$, für ϕ die Eulersche Phifunktion. Also $[M : \mathbb{Q}] = p(p-1) = [L : \mathbb{Q}]$.
Zu c). Da f irreduzibel ist, wirkt $\mathrm{Gal}(f)$ bekanntlich transitiv auf den Nullstellen von f. Insbesondere existiert ein $\sigma \in \mathrm{Gal}(f)$, so dass $\sigma(\alpha) = \zeta\alpha$. Sei weiter $\mathrm{Gal}(f) \ni \iota \colon L \to L,\ z \mapsto \overline{z}$ der komplexe $\mathbb{Q}$-Automorphismus von L, dann gilt $\iota(\zeta\alpha) = \overline{\zeta}\alpha = \zeta^{p-1}\alpha$ und also

$$\sigma\iota(\alpha) = \sigma(\alpha) = \zeta\alpha \neq \zeta^{p-1}\alpha = \iota\sigma(\alpha),$$

also $\sigma\iota \neq \iota\sigma$, womit gezeigt ist, dass $\mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbb{Q})$ nicht abelsch ist.
Zu d). Es ist bekannt, dass

$$\mathrm{Gal}(M/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}) \simeq (\mathbb{Z}/p^2\mathbb{Z})^\times$$

gilt (vgl. Übungen). Somit ist $\mathrm{Gal}(M/\mathbb{Q})$ insbesondere abelsch und folgt $M \not\simeq L$, wie behauptet (da $M \simeq L$ offensichtlich $\mathrm{Gal}(M/\mathbb{Q}) \simeq \mathrm{Gal}(L/\mathbb{Q})$ implizieren würde).