Esercizio 13.2.2

Sia K il campo di spezzamento di $x^5 - 3$ su $\mathbb{Q}$. Determinare il grado di K su $\mathbb{Q}$ e descrivere il gruppo di Galois $Aut(K/\mathbb{Q})$. Determinare i sottocampi F di K che hanno grado 5 su $\mathbb{Q}$.

Le radici del polinomio $x^5 - 3$ sono $\sqrt[5]{3}$ e $\sqrt[5]{3}\zeta_5^i$ con $i \in \{0,1,2,3,4\}$.
Il campo di spezzamento è dunque $\mathbb{Q}(\sqrt[5]{3}, \sqrt[5]{3}\zeta_5) = \mathbb{Q}(\sqrt[5]{3}, \zeta_5)$. Consideriamo le due torri $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{3}) \subseteq \mathbb{Q}(\sqrt[5]{3}, \zeta_5)$ e $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(\sqrt[5]{3}, \zeta_5)$. Cominciando ad analizzare la prima torre si vede che $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$, poichè ζ_5 è radice del polinomio ciclotomico (quindi irriducibile) $\phi_5(x) = x^4 + x^3 + x^2 + x + 1$ Dunque $4|[\mathbb{Q}(\sqrt[5]{3}, \zeta_5) : \mathbb{Q}]$. Per quanto riguarda la seconda torre, $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$, poichè $\sqrt[5]{3}$ è radice di $x^5 - 3$, irriducibile su $\mathbb{Q}$ per il criterio delle radici razionali, dunque $5||[\mathbb{Q}(\sqrt[5]{3}, \zeta_5) : \mathbb{Q}]$.
Inoltre $[\mathbb{Q}(\sqrt[5]{3}, \zeta_5) : \mathbb{Q}] \leq 4 \cdot 5 = 20$, da ciò si ricava che $[\mathbb{Q}(\sqrt[5]{3}, \zeta_5) : \mathbb{Q}] = 20$.
Dunque 20 è la cardinalità del gruppo di Galois G, $|G| = |Aut(^{\mathbb{Q}(\sqrt[5]{3},\zeta_5)}/_{\mathbb{Q}})| = 20$.
Consideriamo ora due sottogruppi di G, $Aut(^{\mathbb{Q}(\sqrt[5]{3},\zeta_5)}/_{\mathbb{Q}(\zeta_5)}) = H$ e $Aut(^{\mathbb{Q}(\sqrt[5]{3},\zeta_5)}/_{\mathbb{Q}(\sqrt[5]{3})}) = K$, poichè le corrispettive estensioni sono di Galois le cardinalità sono rispettivamente 5 e 4.
Ovviamente $H \simeq \mathbb{Z}_5 =< \sigma >$. Invece $K \simeq \mathbb{Z}_4 =< \tau >$, posso infatti esibire un automorfismo di K che abbia ordine 4, $\tau : \zeta_5 \to \zeta_5^2$, dunque $K =< \tau >$.
Notiamo inoltre l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5)$ è di Galois, poichè $\mathbb{Q}(\zeta_5)$ è campo di spezzamento del polinomio separabile $\phi_5(x)$, per il secondo teorema di Galois possiamo dunque affermare che $H \lhd G$. Inoltre $H \cap K = \{id\}$
Date queste ipotesi possiamo concludere che $G \simeq H \rtimes_c K \simeq \mathbb{Z}_5 \rtimes_c \mathbb{Z}_4$.
Per descrivere il gruppo basta descrivere il coniugio $c(\sigma) = \tau\sigma\tau^{-1}$, si nota che $c(\sigma) = \tau\sigma\tau^{-1} = \sigma^2$, infatti $c(\zeta_5) = \zeta_5$ e $c(\sqrt[5]{3}) = \sqrt[5]{3}\zeta_5^2$.
Per determinare i sottocampi $\mathbb{Q} \subseteq K$ di grado 5, occorre innanzitutto conoscerne il numero, che, per il primo teorema di Galois, è il numero dei sottogruppi di G di indice 5, ossia ordine 4, tali sottogruppi sono i 2-syolow di G, per i teoremi di Sylow e i teoremi sulle azioni sappiamo che $n_2|20$ e $n_2 \equiv 1(2)$, dunque $n_2 = 1 \vee n_2 = 5$.
Se $n_2 = 1$ avremmo che il 2-sylow, cioè K, è un sottogruppo normale, ma questo, per il secondo teorema di Galois, significherebbe che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{3})$ è di Galois, ciò è falso. Quindi $n_2 = 5$, ci sono 5 sottocampi di grado 5 su $\mathbb{Q}$, ossia quelli della forma $\mathbb{Q}(\sqrt[5]{3}\zeta_5^i)$ con $i \in \{0,1,2,3,4\}$.
Rimane da dimostrare che i 5 sottocampi sono tutti diversi fra loro.
Se esistessero $i, j \in \{0,1,2,3,4\}$ tali che $i \neq j$ e $\mathbb{Q}(\sqrt[5]{3}\zeta_5^i) = \mathbb{Q}(\sqrt[5]{3}\zeta_5^j)$, allora avremmo $\frac{\sqrt[5]{3}\zeta_5^i}{\sqrt[5]{3}\zeta_5^j} = \zeta_5^{i-j} \in \mathbb{Q}(\sqrt[5]{3}\zeta_5^i) \Rightarrow \zeta_5 \in \mathbb{Q}(\sqrt[5]{3}\zeta_5^i) \Rightarrow \mathbb{Q}(\zeta_5) \subset \mathbb{Q}(\sqrt[5]{3}\zeta_5^i)$, considerando i gradi dell'estensione avremmo quindi che $4|5$, ma questo è assurdo.