SOLUZIONI DEL COMPITO SCRITTO DEL 20/04/2016

Esercizio 1. Sia E il campo di spezzamento del polinomio $X^3-2\in\mathbb{Q}[X]$.

(1) Mostrare che $\exists!\sqrt[4]{2}\in\mathbb{R}_{\geq 0}$ (risp. $\exists!\sqrt[3]{2}\in\mathbb{R}_{\geq 0}$ ed $\exists!\sqrt{2}\in\mathbb{R}_{\geq 0}$) tale che $\left(\sqrt[4]{2}\right)^4=2$ (risp. $\left(\sqrt[3]{2}\right)^3=2$ e $\left(\sqrt{2}\right)^2=2$) e quindi calcolare $\left[E\left(\sqrt[4]{2}\right):\mathbb{Q}\right]$.

(2) Trovare una base di $E\left(\sqrt[4]{2}\right)/\mathbb{Q}$.

(3) Si determinino la chiusure normale $\widetilde{E'}/\mathbb{Q}$ ed il grado $\left[\widetilde{E'}:\mathbb{Q}\right]$ di $E':=E\left(\sqrt[4]{2}\right)$ scrivendo esplicitamente $\widetilde{E'}=\mathbb{Q}\left(\alpha_i:i\in I\right)$.

Soluzione: (1) Posto $f_k(X)=X^k-2\in\mathbb{Q}[X]$ con $k=2,3,4$, abbiamo $f_k'(X)=kX^{k-1}$ con $k-1>0$; dunque $f_k:\mathbb{R}\to\mathbb{R}$ è strettamente crescente per $x\geq 0$. Poichè $f_k(x)=-2<0$, deduciamo che $\exists!\sqrt[k]{2}\in\mathbb{R}_{\geq 0}$ tale che $\left(\sqrt[k]{2}\right)^k=2$. Notiamo anche che, posto $\zeta_k:=\exp\left(\frac{2\pi i}{k}\right)$, l'insieme delle radici di f_k è

$$R_{f_k}=\left\{\sqrt[k]{2}\zeta_k^i:i=0,...,k-1\right\}.$$

Deduciamo che, posto $E_k:=\mathbb{Q}(R_{f_k})$ (il campo di spezzamento di $f_k(X)\in\mathbb{Q}[X]$), abbiamo $E_k=\mathbb{Q}\left(\sqrt[k]{2},\zeta_k\right)$: infatti $\subset$ è ovvia dall espressione di R_{f_k} e, viceversa, $\sqrt[k]{2},\zeta_k=\frac{\sqrt[k]{2}\zeta_k}{\sqrt[k]{2}}\in E_k$. Poichè $f_k(X)\in\mathbb{Q}[X]$ è irriducibile (per il criterio di Eisenstein), sappiamo che $\left[\mathbb{Q}\left(\sqrt[k]{2}\right):\mathbb{Q}\right]=k$. Se $k=2$ abbiamo $\zeta_k=-1\in\mathbb{Q}$ e, dunque, $E_2=\mathbb{Q}\left(\sqrt{2}\right)$. Se $k=3$ notiamo che $[\mathbb{Q}(\zeta_k):\mathbb{Q}]=2$ (infatti ζ_k è radice del terzo polinomio ciclotomico, che ha grado 2): poichè

$$\left([\mathbb{Q}(\zeta_3):\mathbb{Q}],\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]\right)=(2,3)=1,$$

per moltiplicatività dei gradi,

$$[E_3:\mathbb{Q}]=[\mathbb{Q}(\zeta_3):\mathbb{Q}]\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=2\cdot 3=6.$$

Per calcolare $\left[E\left(\sqrt[4]{2}\right):\mathbb{Q}\right]$ notiamo che $E/\mathbb{Q}$ è di Galois e, dunque (abbiamo $E=E_3$),

$$\left[E\left(\sqrt[4]{2}\right):\mathbb{Q}\right]=\frac{[E:\mathbb{Q}]\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]}{\left[E\cap\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]}=\frac{6\cdot 4}{\left[E\cap\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]}.$$

Sappiamo anche che

$$\left[E\cap\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]\mid\left([E:\mathbb{Q}],\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]\right)=(6,4)=2.$$

Supponiamo per assurdo che $E\cap\mathbb{Q}\left(\sqrt[4]{2}\right)$ sia una estensione quadratica di $\mathbb{Q}$. Sappiamo che $G_{E/\mathbb{Q}}$ ha ordine 6 e non può essere abeliano poichè $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ è una sua sottoestensione non normale (se lo fosse, avremmo $\sqrt[3]{2}\zeta_3^i\in\mathbb{Q}\left(\sqrt[3]{2}\right)$ e, quindi, $E=\mathbb{Q}\left(\sqrt[3]{2}\right)$ dovrebbe avere grado 3). Dunque $G_{E/\mathbb{Q}}\simeq S_3$ contiene un solo sottogruppo di indice due che corrisponde all'unica sottoestensione $K/\mathbb{Q}$ di grado 2 di $E/\mathbb{Q}$. Poichè $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ e $E\cap\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ sarebbero estensioni di questo tipo, dedurremmo la contraddizione

$$\zeta_3\in\mathbb{Q}(\zeta_3)=K=E\cap\mathbb{Q}\left(\sqrt[4]{2}\right)\subset\mathbb{Q}\left(\sqrt[4]{2}\right)\subset\mathbb{R}.$$

Dunque $\left[E\left(\sqrt[4]{2}\right):\mathbb{Q}\right]=24$.

(2) Una base di $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ (risp. $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ oppure $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$) è data da

$$\{1, \zeta_3\} \text{ (risp. } \left\{1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2\right\} \text{ oppure } \left\{1, \sqrt[4]{2}, \left(\sqrt[4]{2}\right)^2, \left(\sqrt[4]{2}\right)^3\right\}\text{)}.$$

Poichè abbiamo verificato che $[E:\mathbb{Q}] = [\mathbb{Q}(\zeta_3):\mathbb{Q}]\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]$, una base di $E/\mathbb{Q}$ si ottiene per prodotto:

$$\left\{1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2, \zeta_3, \zeta_3\sqrt[3]{2}, \zeta_3\left(\sqrt[3]{2}\right)^2\right\}.$$

Similmente, poichè abbiamo verificato che $\left[E\left(\sqrt[4]{2}\right):\mathbb{Q}\right] = [E:\mathbb{Q}]\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]$, una base di $E\left(\sqrt[4]{2}\right)/\mathbb{Q}$ si ottiene per prodotto:

$$\left\{\zeta_3^a\left(\sqrt[3]{2}\right)^b\left(\sqrt[4]{2}\right)^c : a=0,1; b=0,1,2; c=0,1,2,3\right\}.$$

(3) Abbiamo $E\left(\sqrt[3]{2}\right) = E$ (poichè $\sqrt[3]{2} \in E$) ed $E/\mathbb{Q}$ è normale per costruzione, dunque $\widetilde{E} = \widetilde{E\left(\sqrt[3]{2}\right)} = E = \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$ e $\left[\widetilde{E'}:\mathbb{Q}\right] = 6$. La chiusura normale di $E\left(\sqrt[4]{2}\right)/\mathbb{Q}$ contiene $\sqrt[3]{2}, \sqrt[4]{2} \in E\left(\sqrt[4]{2}\right)$, che sono radici di $f_3(X)$ e di $f_4(X)$; dunque contiene l'estensione composta dei rispettivi campi di spezzamento $E_3E_4 = E E_4$ che, d'altra parte, è normale su $\mathbb{Q}$, essendo composta di estensioni normali. Tenendo conto della uguaglianza $E_k = \mathbb{Q}\left(\sqrt[k]{2}, \zeta_k\right)$, deduciamo che

$$\widetilde{E\left(\sqrt[4]{2}\right)} = EE_4 = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}, \zeta_3, i\right) \text{ (abbiamo } \zeta_4 = i\text{)}.$$

Poichè $\mathbb{Q}(\zeta_3, i)/\mathbb{Q}$ è di Galois (essendo composta di estensioni normali), sappiamo che

$$\left[\widetilde{E\left(\sqrt[4]{2}\right)}:\mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}, \zeta_3, i\right):\mathbb{Q}\right] = \frac{\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right):\mathbb{Q}\right]\left[\mathbb{Q}(\zeta_3, i):\mathbb{Q}\right]}{\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right)\cap\mathbb{Q}(\zeta_3, i):\mathbb{Q}\right]}.$$

L'estensione $\mathbb{Q}(\zeta_3, i)/\mathbb{Q}$ è biquadratica (poichè si verifica facilmente che $\mathbb{Q}(\zeta_3) \neq \mathbb{Q}(i)$), mentre

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right):\mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right] = 3\cdot 4 = 12,$$

essendo

$$\left(\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right], \left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]\right) = (3,4) = 1.$$

Infine

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right)\cap\mathbb{Q}(\zeta_3, i):\mathbb{Q}\right] \mid \left(\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right):\mathbb{Q}\right], \left[\mathbb{Q}(\zeta_3, i):\mathbb{Q}\right]\right) = (12,4) = 4.$$

Ma certamente l'indice non è 4, altrimenti avremmo

$$\mathbb{Q}(\zeta_3, i) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right)\cap\mathbb{Q}(\zeta_3, i) \subset \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right) \subset \mathbb{R}.$$

Non può nemmeno essere 2, poichè $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right)\cap\mathbb{Q}(\zeta_3, i)$ sarebbe una estensione quadratica reale in $\mathbb{Q}(\zeta_3, i)$; ma l'estensione biquadratica $\mathbb{Q}(\zeta_3, i)$ ha solamente tre sottoestensioni proprie, dunque $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(i)$ e $\mathbb{Q}(\zeta_3 i)$, delle quali nessuna è reale (abbiamo $\zeta_3 i = -\frac{1}{2}i - \frac{\sqrt{3}}{2}$). Necessariamente $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{2}\right)\cap\mathbb{Q}(\zeta_3, i) = \mathbb{Q}$ e, dunque,

$$\left[\widetilde{E\left(\sqrt[4]{2}\right)}:\mathbb{Q}\right] = \frac{12\cdot 4}{1} = 48.$$

Esercizio 2. Sia $\zeta := \exp\left(\frac{2\pi i}{8}\right)$ una radice primitiva ottava dell'unità.

(1) Si calcoli il polinomio minimo $\Phi_8(X) \in \mathbb{Q}[X]$ di ζ.
(2) Si mostri che $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois e si calcoli $G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$.

(3) Trovare tutti i sottocampi di $\mathbb{Q}(\zeta)/\mathbb{Q}$.

Soluzione: (1) Notiamo che ζ è radice del polinomio

$$\begin{aligned}\Phi_8(X) &: = (X-\zeta)(X+\zeta)\left(X-\overline{\zeta}\right)\left(X+\overline{\zeta}\right)\\ &= \left(X^2-\zeta^2\right)\left(X^2-\overline{\zeta}^2\right) = \left(X^2-i\right)\left(X^2-\overline{i}\right)\\ &= \left(X^2-i\right)\left(X^2+i\right) = X^4+1 \in \mathbb{Q}[X].\end{aligned}$$

Mostriamo che tale polinomio è irriducibile in $\mathbb{Q}[X]$. Non ha radici e se dunque fosse riducibile sarebbe prodotto di due polinomi di grado 2. Verifichiamo che tutti i possibili polinomi di grado 2 ottenuti da due fattori di $\Phi_8(X)$ non sono in $\mathbb{Q}[X]$. Il fattore $X-\zeta$ compare necessariamente in uno dei due polinomi di grado due che esprimono $\Phi_8(X)$ come il loro prodotto e può essere accoppiato con uno qualunque degli altri fattori. Occorre dunque calcolare

$$\begin{aligned}(X-\zeta)(X+\zeta) &= X^2-i \notin \mathbb{Q}[X]\\ (X-\zeta)\left(X-\overline{\zeta}\right) &= X^2-\left(\zeta+\overline{\zeta}\right)X+\zeta\overline{\zeta},\\ (X-\zeta)\left(X+\overline{\zeta}\right) &= X^2-\left(\zeta-\overline{\zeta}\right)X+\zeta\overline{\zeta}.\end{aligned}$$

Abbiamo $\zeta = \frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$ (che infatti soddisfa $\zeta^2=i$), da cui

$$\begin{aligned}\zeta+\overline{\zeta} &= \left(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)+\left(\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right) = \sqrt{2} \notin \mathbb{Q},\\ \zeta-\overline{\zeta} &= \left(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)-\left(\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right) = i\sqrt{2} \notin \mathbb{Q}.\end{aligned}$$

Dunque $\Phi_8(X)$ è irriducibile in $\mathbb{Q}[X]$ ed è dunque il polinomio minimo di ζ.

(2) Consideriamo l'applicazione

$$\begin{aligned}G_{\mathbb{Q}(\zeta)/\mathbb{Q}} &\xrightarrow{\sim} Aut(\mu_8) = \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^{\times}\\ \sigma &\mapsto \sigma_{|\mu_8}.\end{aligned}$$

Poichè $\mathbb{Q}(\zeta) = \mathbb{Q}(\mu_8)$ è iniettiva. Notiamo che $(x,8)=1$ se e solo se $\exists a,b \in \mathbb{Z}$ tali che $ax+8y=1$, ovvero se e solo se $x \in \frac{\mathbb{Z}}{8\mathbb{Z}}$ è invertibile. Poichè $(x,8)=1$ se e solo se $(x,2)=1$, vediamo che

$$\#\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^{\times} = 4 = \deg(\Phi_8(X)) = [\mathbb{Q}(\zeta):\mathbb{Q}] = \#G_{\mathbb{Q}(\zeta)/\mathbb{Q}}.$$

Dunque $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^{\times}$, che ha ordine 4, e possiamo avere che questo gruppo è $\simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$ oppure $\simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$. Abbiamo

$$\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^{\times} = \{1,3,5,7\},\ 3^2 = 9 \equiv 1 \text{ e } 5^2 = 25 \equiv 1 \bmod(8).$$

Dunque

$$G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

Alternativamente, poichè

$$i = \zeta^2 \in \mathbb{Q}(\zeta) \text{ e } \sqrt{2} = \zeta+\overline{\zeta} = \zeta+\zeta^{-1} \in \mathbb{Q}(\zeta),$$

sappiamo che $\mathbb{Q}(\zeta)$ contiene le due estensioni quadratiche $\mathbb{Q}(i)$ e $\mathbb{Q}\left(\sqrt{2}\right)$, che sono distinte. Da ciò si deduce che l'opzione $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$ non è possibile perchè altrimenti esisterebbe una sola estensione quadratica in $\mathbb{Q}(\zeta)$ che corrisponde all'unico sottogruppo di $\frac{\mathbb{Z}}{4\mathbb{Z}}$ di indice 2.

(3) Come notato, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ e dunque anche $\mathbb{Q}(i\sqrt{2})$ sono sottocampi di $\mathbb{Q}(\zeta)$. Sono distinti e, dunque, sono tutti i sottocampi propri di $\mathbb{Q}(\zeta)$, dovendo questi corrispondere ai sottogruppi propri di $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, che sono tre.

Esercizio 3. [Teo. Gal.] Supponiamo che E/F e K/F siano estensioni finite e che E/F sia di Galois.

(1) Si mostri che EK/K ed $E/E\cap K$ sono di Galois e che
$$G_{EK/K} \simeq G_{E/E\cap K}.$$
(2) Si mostri che, se $EK/E\cap K$ è di Galois, allora
$$G_{EK/E\cap K} \simeq G_{EK/E} \rtimes G_{E/E\cap K}$$
(3) Si mostri che, se EK/F è di Galois e se $([E:F],[K:F]) = 1$, allora
$$G_{EK/F} \simeq G_{EK/E} \rtimes G_{E/F}.$$

Soluzione: (1) Si veda "J. S. Milne, Fields and Galois theory, Proposition 3.18".
(2) Per (1) sappiamo che, poichè E/F è di Galois, EK/K ed $E/E\cap K$ sono di Galois e che
$$G_{EK/K} \simeq G_{E/E\cap K}.$$
Notiamo che, poichè $EK/E\cap K$ è di Galois, anche EK/E è di Galois. Possiamo dunque considerare l'applicazione di moltiplicazione
$$m : G_{EK/E} \times G_{EK/K} \to G_{EK/E\cap K}.$$
Si tratta di una applicazione iniettiva poichè ciò significa che $G_{EK/E} \cap G_{EK/K} = \{1\}$; ma se $\sigma \in G_{EK/E} \cap G_{EK/K}$, allora $\sigma_{|K} = 1_K$ e $\sigma_{|E} = 1_E$ da cui deduciamo che $\sigma_{|EK} = 1_{EK}$. Ma poichè
$$\begin{aligned}\#G_{EK/E\cap K} &= [EK : E\cap K] = [EK:E]\,[E:E\cap K]\\ &\overset{(1)}{=} [EK:E]\,[EK:K] = \#G_{EK/E}\#G_{EK/K},\end{aligned}$$
deduciamo che m è una biiezione. Infine notiamo che $G_{EK/E} \lhd G_{EK/E\cap K}$ poichè $E/E\cap K$ è normale. Dunque
$$G_{EK/F} = G_{EK/E} \rtimes G_{EK/K} \simeq G_{EK/E} \rtimes G_{E/E\cap K}.$$
(3) Basta notare che
$$[E\cap K : F] \mid ([E:F],[K:F]) = 1,$$
pertanto $E\cap K = F$ e possiamo applicare (2).

Esercizio 4. [Teo. Num.] Sia $K \subset L$ una estensione di campi di numeri di grado n e sia $\alpha \in L$.

(1) Definire il polinomio caractteristico $f^{\alpha}_{L/K}(X)$ di α relativamente a K
(2) Dimostrare che ponendo $f^{\alpha}_{L/K}(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ allora $a_{n-1} = -\mathrm{Tr}_{L/K}(\alpha)$ e $a_0 = (-1)^n \mathrm{Nm}_{L/K}(\alpha)$.
(3) Dimostrare che se $g_\alpha(X) \in K[X]$ è il polinomio minimo di α su K, allora $f^{\alpha}_{L/K}(X) = g_\alpha(X)^m$ con $m = [L : K(\alpha)]$.

Soluzione: Per (1) e (2) vedere la definizione 3.5 e la proposizione 3.7 delle note. (3) segue dalla porposizione 3.7 delle note che $f^{\alpha}_{L/K}(X) = \prod_{i=1}^{n}\big(X - \sigma_i(\alpha)\big)$ con $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_K(L, \mathbb{C})$. Inoltre $g_\alpha(X) = \prod_{j=1}^{d}(X - \beta_i)$ con $\{\beta_1, \ldots, \beta_d\} = \{\sigma_i(\alpha) | i = 1, \ldots, n\}$. Basta quindi dmostrare che per ogni j esistono m-omomorfismi fra i σ_i tali che $\sigma_i(\alpha) = \beta_j$. Dare un β_j equivale a dare una immersione $K(\alpha) \subset \mathbb{C}$ (il K-omomorfismo che invia α in β_j). L'asserzione segue dal fatto che la cardianlità dei σ_i tali che $\sigma_i(\alpha) = \beta_j$ è la cardinalità dell'insieme $\mathrm{Hom}_{K(\alpha)}(L, \mathbb{C})$ ovvero $[L : K(\alpha)] = m = n/d$.

Esercizio 5. Sia K l'8^o-campo ciclotomico.

(1) Determinare il grado $[K : \mathbb{Q}]$ ed esibire $\mathcal{O}_K = \mathbb{Z}[\zeta]$.
(2) Determinare la decomposizione dell' ideale $2\mathcal{O}_K$ come prodotto di ideali primi distinti.
(2) Determinare la decomposizione dell' ideale $5\mathcal{O}_K$ come prodotto di ideali primi distinti.

Soluzione: Abbiamo $\mathcal{O}_K = \mathbb{Z}[\zeta]$ e $K = \mathbb{Q}[\zeta]$ con ζ radice primitiva ottava del'unità. Il polinomio minimo di ζsu $\mathbb{Q}$ è $\Phi_8(X) = X^4 + 1$ (vedere eserizio 2). Quindi $[K : \mathbb{Q}] = 4$.

Inoltre $X^4 + 1 = (X + 1)^4$ in $\mathbb{F}_2[X]$ e quindi $2\mathcal{O}_K = Q^4$ con $Q = (\zeta + 1, 2)$.

Osserviamo che $\mathbb{F}_{25}^*$ è un gruppo ciclico di ordine 24. In particolare se δ è un generatore allora δ^{3i} per $i = 1$, 3, 5 e 7 sono radici del polinomio $X^4 + 1 = 0$. Quindi $X^4 + 1 \in \mathbb{F}_5[X]$ spezza completamente su $\mathbb{F}_{25}$ e quindi non è un polinomio irriducibile. Altrimenti $\mathbb{F}_{25} \cong \mathbb{F}_5[X]/(X^4 + 1)$ (tramite l'applicazione che invia $X \mapsto \delta^3$) il che è impossibile per ragioni di gradi. Il polinomio $X^4 + 1$ non ha radici in $\mathbb{F}_5$ in quanto $\mathbb{F}_5^*$ è ciclico di ordine 4. Segue che $X^4 + 1$ è il prodotto di due polinomi irriducibili di grado 2, coprimi fra loro in quanto $\mathrm{mcd}(X^4 + 1, 4X^3) = 1$. Concludiamo che $5\mathcal{O}_K = P_1 \cdot P_2$ è il prodotto di due ideali primi, coprimi fra loro, con indice di inerzia 2.