SOLUZIONI DELL'ESAME DI ALGEBRA 3, 27/01/2014

Esercizio 1. Si calcoli il gruppo di Galois G_f su $\mathbb{Q}$ del polinomio $f(X) = X^4 + 10X^2 + 20 \in \mathbb{Q}[X]$.

Prima soluzione: Notiamo per cominciare che $f(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein applicato al primo 5. Osserviamo quindi che si ha la fattorizzazione

$$f(X) = \left(X^2 + 5 + \sqrt{5}\right)\left(X^2 + 5 - \sqrt{5}\right) \in \mathbb{Q}\left(\sqrt{5}\right)[X].$$

Il risolvente cubico di $f(X)$ è il polinomio

$$g_f(X) = X^3 - 10X^2 - 80X + 800 \in \mathbb{Q}[X],$$

che si fattorizza come segue:

$$g_f(X) = (X - 10)\left(X^2 - 80\right) \in \mathbb{Q}[X].$$

Deduciamo che, il campo di spezzamento di $g_f(X) \in \mathbb{Q}[X]$, è $E_{g_f} = \mathbb{Q}\left(\sqrt{80}\right) = \mathbb{Q}\left(\sqrt{5}\right)$ (poichè $80 = 5 \cdot 2^4$). La fattorizzazione di $f(X)$ mostra che $f(X) \in \mathbb{Q}\left(\sqrt{5}\right)[X] = E_{g_f}[X]$ è riducibile e la sola possibilità perchè ciò accada è che si abbia $G_f \simeq \mathbb{Z}/4\mathbb{Z}$.

Seconda soluzione: Segue dalla fattorizzazione del polinomio

$$f(X) = \left(X^2 + 5 + \sqrt{5}\right)\left(X^2 + 5 - \sqrt{5}\right) \in \mathbb{Q}\left(\sqrt{5}\right)[X].$$

che le radici di $f(X)$ sono $\pm\alpha$ e $\pm\beta$ con $\alpha = \sqrt{-5 - \sqrt{5}}$ e $\beta = \sqrt{-5 + \sqrt{5}}$. Allora $\alpha^2 = -5 - \sqrt{5}$ ovvero $\sqrt{5} \in \mathbb{Q}(\alpha)$ e $\alpha\beta = 2\sqrt{5}$ ovvero $\beta \in \mathbb{Q}(\alpha)$. Concludo quindi che il campo di spezzamento K di $f(X)$ coincide con $\mathbb{Q}(\alpha)$ che sappiamo avere grado 4 su $\mathbb{Q}$ in quanto $f(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein applicato al primo 5. Quindi il gruppo di Galois G_f di K su $\mathbb{Q}$ ha ordine 4 ed è necessariamente abeliano.

Visto che K è generato da α, ogni automorfismo di K risulta univocamente determinato dall'immagine di α e questa deve essere ancora una radice di $f(X)$. Segue che l'applicazione insiemistica $G_f \to \{\pm\alpha, \pm\beta\}$ che invia $\sigma \mapsto \sigma(\alpha)$ è iniettiva e dunque una biezione per ragioni di cardinalità. Sia γ l'unico automorfismo che invia $\alpha \mapsto \beta$. Allora

$$-5 - \gamma(\sqrt{5}) = \gamma(\alpha^2) = \beta^2 = -5 + \sqrt{5}$$

ovvero $\gamma(\sqrt{5}) = -\sqrt{5}$ e

$$-2\sqrt{5} = 2\gamma(\sqrt{5}) = \gamma(\alpha)\gamma(\beta) = \beta\gamma(\beta).$$

Concludo che $\gamma(\beta) = -\alpha$. Quindi γ^2 invia α in $-\alpha$ e non coincide con l'identità. L'elemento γ deve genera quindi G_f che risulta dunque essere un gruppo ciclico di ordine 4.

Esercizio 2. Si consideri il polinomio $f(X) := X^7 - 15 \in \mathbb{Q}[X]$.

(*a*) Si presenti il suo campo di spezzamento E (su $\mathbb{Q}$) nella forma $E = \mathbb{Q}(\alpha, \beta)$ per opportuni $\alpha, \beta \in \overline{\mathbb{Q}}$.
(*b*) Si calcoli $[E : \mathbb{Q}]$.
(*c*) Si mostri che $G_{E/\mathbb{Q}}$ è un prodotto semidiretto.
(*d*) Si fornisca una presentazione di $G_{E/\mathbb{Q}}$ come prodotto semidiretto.

Soluzione: (a) Il polinomio $f(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein applicato ai primi 3 o 5. Poichè $f'(X) = 7X^6$ esiste una ed una sola radice reale $\sqrt[7]{15} \in \mathbb{R}$ tale che $f\left(\sqrt[7]{15}\right) = 0$. Se ζ è una radice primitiva settima dell'unità le radici di $f(X)$ sono

$$R_f = \left\{ \sqrt[7]{15}\zeta^i : i = 0, \dots, 6 \right\}.$$

Dunque $\mathbb{Q}(R_f)$ il campo di spezzamento e chiaramente $\mathbb{Q}(R_f) \subset \mathbb{Q}\left(\sqrt[7]{15}, \zeta\right)$. Viceversa $\sqrt[7]{15}, \sqrt[7]{15}\zeta \in R_f \subset \mathbb{Q}(R_f)$, da cui $\zeta = \frac{\sqrt[7]{15}\zeta}{\sqrt[7]{15}} \in \mathbb{Q}(R_f)$ e, pertanto, $E := \mathbb{Q}(R_f) = \mathbb{Q}\left(\sqrt[7]{15}, \zeta\right)$.

(b) Si ha $\left[\mathbb{Q}\left(\sqrt[7]{15}\right) : \mathbb{Q}\right] = \deg(f) = 7$ e $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_7) = 6$, dove $\Phi_7(X) \in \mathbb{Q}[X]$ è il settimo polinomio ciclotomico. Segue dalla moltiplicatività dei gradi che, poichè $(7, 6) = 1$,

$$\begin{aligned} &[E : \mathbb{Q}] = 7 \cdot 6 = 42, \\ &\left[\mathbb{Q}\left(\sqrt[7]{15}\right) : \mathbb{Q}\right] = [E : \mathbb{Q}(\zeta)] = 7 \\ &\text{e } [\mathbb{Q}(\zeta) : \mathbb{Q}] = \left[E : \mathbb{Q}\left(\sqrt[7]{15}\right)\right] = 6. \end{aligned}$$

$(c-d)$ Poichè $E = F\left(\sqrt[7]{15}\right)$ con $\mu_7 \subset F = \mathbb{Q}(\zeta)$ e $[E : F] = 7$, dalla teoria delle estensioni cicliche sappiamo che $G_{E/\mathbb{Q}(\zeta)} \simeq \mu_7$, mediante l'applicazione $g \mapsto \zeta_g$, dove ζ_g è caratterizzato dall'equazione $\frac{g\left(\sqrt[7]{15}\right)}{\sqrt[7]{15}} = \zeta_g$. Sia dunque $\sigma \in G_{E/\mathbb{Q}(\zeta)}$ l'unico automorfismo tale che $\sigma\left(\sqrt[7]{15}\right) = \sqrt[7]{15}\zeta$: poichè ζ genera μ_7, $G_{E/\mathbb{Q}(\zeta)} = \langle\sigma\rangle \simeq \frac{\mathbb{Z}}{7\mathbb{Z}}$. Notiamo che, per induzione, si ha

$$\begin{aligned} \sigma^i\left(\sqrt[7]{15}\right) &= \sigma\left(\sigma^{i-1}\left(\sqrt[7]{15}\right)\right) = \sigma\left(\sqrt[7]{15}\zeta^{i-1}\right) \\ &= \sigma\left(\sqrt[7]{15}\right)\sigma(\zeta)^{i-1} = \sqrt[7]{15}\zeta\zeta^{i-1} = \sqrt[7]{15}\zeta^i. \end{aligned} \tag{1}$$

Consideriamo quindi $G_{E/\mathbb{Q}\left(\sqrt[7]{15}\right)} \subset G_{E/\mathbb{Q}}$ e notiamo che $G_{E/\mathbb{Q}\left(\sqrt[7]{15}\right)} \cap G_{E/\mathbb{Q}(\zeta)} = 1$ poichè $E = \mathbb{Q}\left(\sqrt[7]{15}, \zeta\right)$. Segue che l'applicazione di restrizione $G_{E/\mathbb{Q}} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$, che ha nucleo $G_{E/\mathbb{Q}(\zeta)}$, da luogo ad un omomorfismo di gruppi iniettivo

$$G_{E/\mathbb{Q}\left(\sqrt[7]{15}\right)} \hookrightarrow G_{\mathbb{Q}(\zeta)/\mathbb{Q}},$$

dove infatti notiamo che $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois (e dunque l'applicazione ben definita). Ma

$$\#G_{E/\mathbb{Q}\left(\sqrt[7]{15}\right)} = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \left[E : \mathbb{Q}\left(\sqrt[7]{15}\right)\right] = \#G_{\mathbb{Q}(\zeta)/\mathbb{Q}},$$

da cui concludiamo che tale applicazione di restrizione è un isomorfismo. Dalla teoria delle estensioni ciclotomiche, sappiamo anche che $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times$ mediante l'applicazione $g \mapsto i_g$, dove i_g è caratterizzato dall'equazione $g(\zeta) = \zeta^{i_g}$. Sappiamo che $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times$ è un gruppo ciclico ed esplitamente è generato dalla moltiplicazione per 3 o dal suo inverso, ovvero la moltiplicazione per 5 . Dunque $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \langle\rho\rangle$, dove ρ è caratterizzato da $\rho(\zeta) = \zeta^3$ e, poichè la restrizione $G_{E/\mathbb{Q}\left(\sqrt[7]{15}\right)} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è un isomorfismo, si ha anche $G_{E/\mathbb{Q}\left(\sqrt[7]{15}\right)} = \langle\rho\rangle$.

Notiamo che $\sigma^i, \rho\sigma\rho^{-1} \in G_{E/\mathbb{Q}(\zeta)} \lhd G_{E/\mathbb{Q}}$ e, poichè $E = F\left(\sqrt[7]{15}\right)$ con $F = \mathbb{Q}(\zeta)$, entrambi questi elementi sono caratterizzato dalla loro azione su $\sqrt[7]{15}$. Abbiamo

$$\begin{aligned} \rho\left(\sigma\left(\rho^{-1}\left(\sqrt[7]{15}\right)\right)\right) &= \rho\left(\sigma\left(\sqrt[7]{15}\right)\right) = \rho\left(\sqrt[7]{15}\zeta\right) = \rho\left(\sqrt[7]{15}\right)\rho(\zeta) \\ &= \sqrt[7]{15}\rho(\zeta) = \sqrt[7]{15}\zeta^3 \end{aligned}$$

a dal confronto con (1) segue $\rho\sigma\rho^{-1} = \sigma^3$. Dunque

$$G_{E/\mathbb{Q}} = G_{E/\mathbb{Q}(\zeta)} \rtimes G_{E/\mathbb{Q}\left(\sqrt[7]{15}\right)} = \langle\sigma\rangle \rtimes \langle\rho\rangle \simeq \frac{\mathbb{Z}}{7\mathbb{Z}} \rtimes_\varphi \frac{\mathbb{Z}}{6\mathbb{Z}}$$

dove $\varphi : \langle\rho\rangle \to Aut(\langle\sigma\rangle)$ è caratterizzato da $\varphi(\rho)(\sigma) = \rho\sigma\rho^{-1} = \sigma^3$.

Esercizio 3. *[TeoGal]* Sia F un campo perfetto e si mostri che sono equivalenti le seguenti affermazioni, per un intero $n \geq 1$.

(1) Se $f(X) \in F[X]$ è tale che $\deg(f) = n$, allora $f(X) \in F[X]$ è riducibile.
(2) Non esistono estensioni finite E/F tali che $[E : F] = n$.

Soluzione: (1) $\Rightarrow$ (2) Supponiamo per assurdo che E/F sia una estensione finita di grado $[E : F] = n$. Poichè F è perfetto tale estensione è separabile e dunque, per il teorema dell'elemento primitivo, sappiamo che $E = F(\xi)$ per qualche $\xi \in E$. Segue che $E \simeq \frac{F[X]}{(f_\xi(X))}$ dove $f_\xi(X) \in F[X]$, il polinomio minimo di ξ su F, è irriducibile e di grado

$$\deg(f_\xi) = [E : F] = n.$$

Ciò contraddice l'ipotesi (1).

(2) $\Rightarrow$ (1) Supponiamo per assurdo che esista un polinomio $f(X) \in F[X]$ tale che $\deg(f) = n$ ma che $f(X) \in F[X]$ sia irriducibile. Allora $E := \frac{F[X]}{(f(X))}/F$ è una estensione di grado $[E : F] = \deg(f) = n$ e ciò contraddice l'ipotesi (2).

Esercizio 4. *[TeoTN]* Sia K un campo di numeri di grado n su $\mathbb{Q}$ e sia $\mathcal{O}_K$ l'anello degli interi.

i. Siano $\alpha_1, \ldots, \alpha_n \in K$. Mostrare che il discriminante $\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ è un elemento di $\mathbb{Q}$.
ii. Se $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, mostrare che il discriminante $\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ è un elemento di $\mathbb{Z}$.
iii. Ricordare la definizione di base intera e mostrare che due basi intere di $\mathcal{O}_K$ hanno uguale discriminante.

Soluzione: Sia $\mathrm{Hom}(K, E) := \{\sigma_1, \ldots, \sigma_n \colon K \to E$ gli omomorfismi di campi da K verso la chiusura normale E in $\mathbb{C}$ di K su $\mathbb{Q}$. Il discriminante di elementi $\alpha_1, \ldots, \alpha_n \in K$ è definito da

$$\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) := \big(\det A(\alpha_1, \ldots, \alpha_n)\big)^2$$

con $A(\alpha_1, \ldots, \alpha_n) = \big(\sigma_i(\alpha_j)\big)_{i,j=1}^n$ matrice quadrata $n \times n$ a valori in E.

(i) Il gruppo di Galois G di E su $\mathbb{Q}$ agisce per composizione sull'insieme $\mathrm{Hom}(K, E)$:

$$G \times \mathrm{Hom}(K, E) \to \mathrm{Hom}(K, E), \qquad (\sigma, \alpha) \mapsto \sigma \circ \alpha.$$

In particolare per ogni $\sigma \in G$ abbiamo $\sigma\big(\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)\big) = \big(\det B(\alpha_1, \ldots, \alpha_n)\big)^2$ con $B(\alpha_1, \ldots, \alpha_n) = \big(\sigma \circ \sigma_i(\alpha_j)\big)_{i,j=1}^n$. In particolare $B(\alpha_1, \ldots, \alpha_n)$ è ottenuta da $A(\alpha_1, \ldots, \alpha_n)$ permutando le righe. Segue che $\det B(\alpha_1, \ldots, \alpha_n) = \pm \det A(\alpha_1, \ldots, \alpha_n)$ e $\sigma\big(\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)\big) = \Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$. Quindi $\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in E^G = \mathbb{Q}$.

(ii) Se $\alpha \in \mathcal{O}_K$, ovvero α è radice di un polinomio monico $f(X)$ a coefficienti in $\mathbb{Z}$, allora per ogni $i = 1, \ldots, n$ anche $\sigma_i(\alpha)$ è radice di $f(X)$ e quindi $\sigma_i(\alpha) \in \mathcal{Q}_E$. Segue che se $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ la matrice $A(\alpha_1, \ldots, \alpha_n)$ ha coefficienti in $\mathcal{O}_E$ e dunque il suo determinante è in $\mathcal{O}_E$. Quindi, essendo $\mathcal{O}_E$ un anello, $\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q} \cap \mathcal{O}_E = \mathbb{Z}$.

(iii) Una base intera è un insieme di n-elementi $\mathcal{A} := \{\alpha_1, \ldots, \alpha_n\}$ che generano $\mathcal{O}_K$ come gruppo abeliano. Ogni elemento di $\mathcal{O}_K$ si scrive in modo unico come combinazione a coefficienti in $\mathbb{Z}$ di $\alpha_1, \ldots, \alpha_n$. In particolare date un' altra base $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ ho che ${}^t(\alpha_1, \ldots, \alpha_n) = M \ {}^t(\beta_1, \ldots, \beta_n)$ e ${}^t(\beta_1, \ldots, \beta_n) = N \ {}^t(\alpha_1, \ldots, \alpha_n)$ con M ed N matrici $n \times n$ a coefficienti in $\mathbb{Z}$. Inoltre $M \cdot N = N \cdot M = 1_n$. Quindi M è invertibile ovvero $\det M = \pm 1$.

Segue che $A(\alpha_1, \ldots, \alpha_n) = A(\beta_1, \ldots, \beta_n)^t M$, quindi

$$\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \det(M)^2 \Delta_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \Delta_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n).$$

Esercizio 5. Sia $\zeta_{12} = \exp^{\frac{2\pi i}{12}}$ e sia $K = \mathbb{Q}(\zeta_{12})$ il 12^o-campo ciclotomico.

i. Mostrare che K è il campo composto di $\mathbb{Q}(\sqrt{-1})$ e di $\mathbb{Q}(\sqrt{-3})$.
ii. Trovare una base intera per l'anello degli interi $\mathcal{O}_K$ e calcolare il discriminante di $\mathcal{O}_K$.
iii. Trovare $\alpha \in \mathcal{O}_K$ tale che $\mathcal{O}_K = \mathbb{Z}[\alpha]$ e trovarne il polinomio minimo.
iv. Determinare la decomposione dei primi $p = 2$ e $p = 3$ in $\mathcal{O}_K$.

Soluzione: (i) Sappiamo che $\zeta_3 = \zeta_{12}^4 \in K$ e $\zeta_4 = \zeta_{12}^3 \in K$. Inoltre $\zeta_4\zeta_3$ è una radice primitiva di ordine 12 dell' unità. Segue che $K = \mathbb{Q}(\zeta_3, \zeta_4)$. Visto che $\zeta_4 = \sqrt{-1}$ e $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ la conlcusione segue. Sappiamo inoltre che K è di Galois su $\mathbb{Q}$ di grado $\varphi(12) = \varphi(3)\varphi(4) = 4$ ($\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. Infatti, il gruppo di Galois è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ generato dagli automorfismi $\sigma_1 \colon \sqrt{-1} \mapsto -\sqrt{-1}, \sqrt{-3} \mapsto \sqrt{-3}$ e $\sigma_2 \colon \sqrt{-1} \mapsto \sqrt{-1}, \sqrt{-3} \mapsto -\sqrt{-3}$.

(ii)–(iii) Sappiamo che $\mathcal{O}_K = \mathbb{Z}\big[\zeta_{12}\big]$ e, visto che $[K : \mathbb{Q}] = 4$, una base intera è data da $\{1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3\}$. Il polinomio minimo di ζ_{12} è il dodicesimo polinomio ciclotomico ovvero $f(X) := (X^{12}-1)/\big((X^6-1)(X^2+1)\big) = X^4-X^2+1$. Il discriminante è dunque $\mathrm{Norm}_{K/\mathbb{Q}}\big(f'(\zeta_{12})\big)$ dove $f'(X) = 4X^3 - 2X = 2X(2X^2 - 1)$ è il polinomio derivato.

Osservo che $\zeta_{12}^2 = \zeta_6 = \frac{1+\sqrt{-3}}{2}$ e quindi $2\zeta_{12}^2 - 1 = \sqrt{-3}$. La norma di ζ_{12} è il coefficiente costante del polinomio caratteristico di ζ_{12}, che coincide con il polinomio minimo ed è uguale ad 1. La norma di $\sqrt{-3}$ è 3^2, ad esempio usando al descrizione di $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$ e del suo gruppo di galois su $\mathbb{Q}$. Visto che la norma è moltiplicativa e la norma di un elemento $\alpha \in \mathbb{Q}$ è α^4, concludiamo che il discriminante cercato è $\mathrm{Norm}_{K/\mathbb{Q}}\big(2\zeta_{12}(2\zeta_{12}^2 - 1)\big) = 2^4 3^2$.

Alternativamente, visto che $-1 \equiv 3$ modulo 4 l' anello degli interi di $L_1 = \mathbb{Q}(\sqrt{-1})$ è $\mathbb{Z}[\sqrt{-1}]$ ed L_1 ha discriminante 2. Analogamente, $-3 \equiv 1$ modulo 4 e quindi l' anello degli interi di $L_2 = \mathbb{Q}(\sqrt{-3})$ è $\mathbb{Z}\big[\frac{1+\sqrt{-3}}{2}\big]$ ed L_2 ha discriminante -3. In particolare L_1 ed L_2 hanno discriminanti coprimi e $\mathcal{O}_K = \mathcal{O}_{L_1}\mathcal{O}_{L_2}$. Una base intera è quindi data da $\{1, \sqrt{-1}, \frac{1+\sqrt{-3}}{2}, \frac{\sqrt{-1}+\sqrt{3}}{2}\}$. È possibile calcolare il discriminante utilizzando tale base, come il quadrato del determinante della matrice

$$\begin{pmatrix} 1 & \sqrt{-1} & \frac{1+\sqrt{-3}}{2} & \frac{\sqrt{-1}+\sqrt{3}}{2} \\ 1 & -\sqrt{-1} & \frac{1+\sqrt{-3}}{2} & \frac{-\sqrt{-1}-\sqrt{3}}{2} \\ 1 & \sqrt{-1} & \frac{1-\sqrt{-3}}{2} & \frac{\sqrt{-1}-\sqrt{3}}{2} \\ 1 & -\sqrt{-1} & \frac{1-\sqrt{-3}}{2} & \frac{-\sqrt{-1}+\sqrt{3}}{2} \end{pmatrix}$$

che per riduzione per righe risulta equivalente a

$$\begin{pmatrix} 1 & \sqrt{-1} & \frac{1+\sqrt{-3}}{2} & \frac{\sqrt{-1}+\sqrt{3}}{2} \\ 0 & -2\sqrt{-1} & 0 & -\sqrt{-1} - \sqrt{3} \\ 0 & 0 & -\sqrt{-3} & -\sqrt{3} \\ 0 & -2\sqrt{-1} & -\sqrt{-3} & -\sqrt{-1} \end{pmatrix}$$

ovvero a

$$\begin{pmatrix} 1 & \sqrt{-1} & \frac{1+\sqrt{-3}}{2} & \frac{\sqrt{-1}+\sqrt{3}}{2} \\ 0 & -2\sqrt{-1} & 0 & -\sqrt{-1} - \sqrt{3} \\ 0 & 0 & -\sqrt{-3} & -\sqrt{3} \\ 0 & 0 & -\sqrt{-3} & \sqrt{3} \end{pmatrix}$$

il cui determinante è $4\sqrt{-1}\sqrt{3}\sqrt{-3} = -2^2 3$. Il discriminate cercato risulta essere $2^4 3^2$.

(iv) Il polinomio $X^4 - X^2 + 1$ modulo 2 si scrive come $(X^2 + X + 1)^2$ con $X^2 + X + 1$ irriducibile. Quindi $2\mathcal{O}_K = \mathcal{P}^2$ con $\mathcal{P} = \big(2, \zeta_{12}^2 + \zeta_{12} + 1\big)$.

Il polinomio $X^4 - X^2 + 1$ modulo 3 si scrive come $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ con $X^2 + 1$ irriducibile. Quindi $3\mathcal{O}_K = \mathcal{Q}^2$ con $\mathcal{Q} = \big(2, \zeta_{12}^2 + 1\big)$.