SOLUZIONI DELL'ESAME DI ALGEBRA 3, 05/05/2014

Esercizio 1. Sia $F := \mathbb{Q}\left(\sqrt{\pm 2}, \sqrt{3}\right)$.

(1) Si calcoli $[F : \mathbb{Q}]$.
(2) Si mostri che $F/\mathbb{Q}$ è una estensione di Galois e si calcoli $G_{F/\mathbb{Q}}$.
(3) Detto $\mathcal{E}_{F/\mathbb{Q}}$ il reticolo dei sottocampi di F si calcoli
$$\#\left\{K \in \mathcal{E}_{F/\mathbb{Q}} : K \not\subseteq \mathbb{R}\right\}.$$
(4) Si calcoli $\mathcal{E}_{F/\mathbb{Q}}$, presentando ogni campo $K \in \mathcal{E}_{F/\mathbb{Q}} - \{\mathbb{Q}, F\}$ nella forma $K = \mathbb{Q}(\alpha)$ oppure $K = \mathbb{Q}(\alpha, \beta)$ con $\alpha, \beta \in F$
(5) Si calcoli $\mathbb{Q}(\alpha)$, dove $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{-2}$.

Soluzione: (1) Poniamo $F^+ := \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ e cominciamo con l'osservare che $[F^+ : \mathbb{Q}] = 4$. Infatti $\sqrt{2} \notin \mathbb{Q}\left(\sqrt{3}\right)$ (altrimenti $\sqrt{2} = a + b\sqrt{3}$ con $a, b \in \mathbb{Q}$ ed elevando al quadrato si deriva facilmente una contraddizione). D'altra parte $F = F^+\left(\sqrt{-2}\right)$ e $\sqrt{-2} \notin F^+ \subset \mathbb{R}$, da cui segue che $\left[F^+\left(\sqrt{-2}\right) : F^+\right] = 2$ e, quindi,
$$[F : \mathbb{Q}] = \left[F^+\left(\sqrt{-2}\right) : F^+\right]\left[F^+ : \mathbb{Q}\right] = 8.$$

(2) Poichè $F/\mathbb{Q}$ è l'estensione composta delle estensioni di Galois $\mathbb{Q}\left(\sqrt{d}\right)/\mathbb{Q}$ con $d \in \{\pm 2, 3\}$, segue che $F/\mathbb{Q}$ è di Galois; per lo stesso motivo anche $F^+/\mathbb{Q}$ è di Galois. Notiamo che, poichè $\sqrt{2} \notin \mathbb{Q}\left(\sqrt{3}\right)$, si ha $\mathbb{Q}\left(\sqrt{2}\right) \cap \mathbb{Q}\left(\sqrt{3}\right) = \mathbb{Q}$ e, pertanto, l'applicazione di restrizione da luogo ad un isomorfismo
$$G_{F^+/\mathbb{Q}} \to G_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} \times G_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}.$$
Similmente, poichè $\sqrt{-2} \notin F^+$, $F^+ \cap \mathbb{Q}\left(\sqrt{-2}\right) = \mathbb{Q}$ è l'applicazioen di restrizione è un isomorfismo
$$G_{F/\mathbb{Q}} \to G_{F^+/\mathbb{Q}} \times G_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}} \to G_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} \times G_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}} \times G_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}$$
Poichè $G_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} G_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}$ per $d \in \{\pm 2, 3\}$ si ha $G_{F/\mathbb{Q}} \simeq \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Sia $\sigma_d \in G_{F/\mathbb{Q}}$, con $d \in \{\pm 2, 3\}$, un sollevamento dell'elemento non banale di $G_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}$: si ha dunque che l'identificazione $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \to G_{F/\mathbb{Q}}$ è data da
$$(i, j, k) \mapsto \sigma_2^i \sigma_3^j \sigma_{-2}^k.$$

(3) Ovviamente (3) segue da (4), ma (3) può essere svolto in modo indipendente come segue. Sia c il coniugio complesso; allora $c_{|F} = \sigma_{-2}$. Segue che $F \cap \mathbb{R} = F^{\langle \sigma_{-2} \rangle}$ e dunque, se $K \in \mathcal{E}_{F/\mathbb{Q}}$, allora $K \subset \mathbb{R}$ se e solo se $K \subset F^{\langle \sigma_{-2} \rangle}$. Ma $F^+ \subset F^{\langle \sigma_{-2} \rangle}$ e, poichè
$$\left[F^{\langle \sigma_{-2} \rangle} : F\right] = \left[G_{F/\mathbb{Q}} : \langle \sigma_{-2} \rangle\right] = 4 = \left[F^+ : \mathbb{Q}\right],$$
deduciamo che $F^+ = F^{\langle \sigma_{-2} \rangle}$. Dunque
$$\#\left\{K \in \mathcal{E}_{F/\mathbb{Q}} : K \subset \mathbb{R}\right\} = \#\left\{K \in \mathcal{E}_{F/\mathbb{Q}} : K \subset F^+\right\} = 4.$$
Come notato all'inizio del punto (4) che segue, il numero totale dei sottogruppi di $G_{F/\mathbb{Q}}$ è 16. Deduciamo che
$$\#\left\{K \in \mathcal{E}_{F/\mathbb{Q}} : K \not\subseteq \mathbb{R}\right\} = 16 - 4 = 12.$$

(4) Poichè $G_{F/\mathbb{Q}} \simeq \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$, possiamo classificare i sottogruppi di $G_{F/\mathbb{Q}}$ a seconda della loro dimensione come $\mathbb{F}_2$-spazi vettoriali. Sia dunque $\mathcal{G}_n$, con $n \in \{0,1,2,3\}$, l'insieme dei sottogruppi di dimensione n. Si ha

$$\begin{aligned} \#\mathcal{G}_1 = &\quad \#\mathcal{G}_2 = \#\mathbf{P}^2(\mathbb{F}_2) = 2^2+2+1 = 7, \\ \#\mathcal{G}_0 = &\quad \#\mathcal{G}_3 = 1. \end{aligned}$$

Se $H \in \mathcal{G}_n$, si ha

$$\left[F^H : F^{G_{F/\mathbb{Q}}}\right] = \left[G_{F/\mathbb{Q}} : H\right] = 2^3/2^n = 2^{3-n}. \tag{1}$$

Mostriamo che possiamo scrivere F nella forma $F^H = \mathbb{Q}(\alpha)$ (rispettivamente $F^H = \mathbb{Q}(\alpha,\beta)$) quando $n = 2$ (rispettivamente $n = 1$) mostrando elementi tali che $\mathbb{Q}(\alpha) \subset F^H$ (rispettivamente $\mathbb{Q}(\alpha,\beta) \subset F^H$) e $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ (rispettivamente $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = 4$): l'uguaglianza seguirà dunque da (1). (Un approcio alternativo si ottiene scrivendo un elemento di F in termini di una $\mathbb{Q}$-base di F e quindi calcolando gli H-invarianti).

Per $n = 2$ si hanno le seguenti inclusioni $\mathbb{Q}\left(\sqrt{2}\right) \subset F^{\langle \sigma_3, \sigma_{-2}\rangle}$, $\mathbb{Q}\left(\sqrt{3}\right) \subset F^{\langle \sigma_2, \sigma_{-2}\rangle}$, $\mathbb{Q}\left(\sqrt{6}\right) \subset F^{\langle \sigma_2\sigma_3, \sigma_{-2}\rangle}$ (poichè $\sqrt{2}\sqrt{3} = \sqrt{6}$), $\mathbb{Q}\left(\sqrt{-2}\right) \subset F^{\langle \sigma_2, \sigma_3\rangle}$, $\mathbb{Q}\left(\sqrt{-1}\right) \subset F^{\langle \sigma_2\sigma_{-2}, \sigma_3\rangle}$ (poichè $\sqrt{2}\sqrt{-2} = 2\sqrt{-1}$), $\mathbb{Q}\left(\sqrt{-6}\right) \subset F^{\langle \sigma_{-2}\sigma_3, \sigma_2\rangle}$ (poichè $\sqrt{3}\sqrt{-2} = \sqrt{-6}$), $\mathbb{Q}\left(\sqrt{-3}\right) \subset F^{\langle \sigma_2\sigma_{-2}, \sigma_3\sigma_{-2}\rangle}$ (poichè $\sqrt{2}\sqrt{3}\sqrt{-2} = 2\sqrt{-3}$). Le uguaglianze seguono da quanto detto e si deduce anche che i gruppi H considerati sono tutti distinti (alternativamente basta notare che, nell'isomorfismo $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \to G_{F/\mathbb{Q}}$ fissato nel punto (2), i sottogruppi H considerati sono generati da due vettori indipendenti che generano spazi vettoriali distinti di dimension 2). Poichè come notato $\#\mathcal{G}_2 = 7$ abbiamo esaurito la nostra ricerca e, detto $\mathcal{E}_{F/\mathbb{Q},n}$ è l'insieme dei sottocampi di indice n su $\mathbb{Q}$, si ha

$$\mathcal{E}_{F/\mathbb{Q},2} = \left\{\mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}\left(\sqrt{3}\right), \mathbb{Q}\left(\sqrt{6}\right), \mathbb{Q}\left(\sqrt{-2}\right), \mathbb{Q}\left(\sqrt{-1}\right), \mathbb{Q}\left(\sqrt{-6}\right), \mathbb{Q}\left(\sqrt{-3}\right)\right\}.$$

Sia ora $n = 1$ e notiamo le inclusioni $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \subset F^{\langle \sigma_{-2}\rangle}$, $\mathbb{Q}\left(\sqrt{2},\sqrt{-2}\right) \subset F^{\langle \sigma_3\rangle}$, $\mathbb{Q}\left(\sqrt{2},\sqrt{-6}\right) \subset F^{\langle \sigma_3\sigma_{-2}\rangle}$ (poichè $\sqrt{3}\sqrt{-2} = \sqrt{-6}$), $\mathbb{Q}\left(\sqrt{3},\sqrt{-2}\right) \subset F^{\langle \sigma_2\rangle}$, $\mathbb{Q}\left(\sqrt{3},\sqrt{-1}\right) \subset F^{\langle \sigma_2\sigma_{-2}\rangle}$ (poichè $\sqrt{2}\sqrt{-2} = 2\sqrt{-1}$), $\mathbb{Q}\left(\sqrt{6},\sqrt{-2}\right) \subset F^{\langle \sigma_2\sigma_3\rangle}$ (poichè $\sqrt{2}\sqrt{3} = \sqrt{6}$) e $\mathbb{Q}\left(\sqrt{6},\sqrt{-6}\right) \subset F^{\langle \sigma_2\sigma_3\sigma_{-2}\rangle}$ (poichè $\sqrt{2}\sqrt{3} = \sqrt{6}$ e $\sqrt{3}\sqrt{-2} = \sqrt{-6}$). Si concludono come prima le uguaglianza ed il fatto che i sottogruppi H considerati sono tutti e soli quelli di dimensione 1. Si ha pertanto:

$$\begin{aligned} \mathcal{E}_{F/\mathbb{Q},1} = &\left\{\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right), \mathbb{Q}\left(\sqrt{2},\sqrt{-2}\right), \mathbb{Q}\left(\sqrt{2},\sqrt{-6}\right), \mathbb{Q}\left(\sqrt{3},\sqrt{-2}\right),\right. \\ &\left.\mathbb{Q}\left(\sqrt{3},\sqrt{-1}\right), \mathbb{Q}\left(\sqrt{6},\sqrt{-2}\right), \mathbb{Q}\left(\sqrt{6},\sqrt{-6}\right)\right\}. \end{aligned}$$

Infine

$$\mathcal{E}_{F/\mathbb{Q}} = \{\mathbb{Q}\} \sqcup \mathcal{E}_{F/\mathbb{Q},1} \sqcup \mathcal{E}_{F/\mathbb{Q},2} \sqcup \{F\}.$$

per quanto notato e ciò conclude (3).

(5) L'orbita di $\alpha^+ := \sqrt{2}+\sqrt{3}$ sotto l'azione di $G_{F^+/\mathbb{Q}}$ è data da $\left\{\pm\sqrt{2} \pm \sqrt{3}\right\}$, un insieme con quattro elementi. Segue che $F^+ = \mathbb{Q}(\alpha^+)$. Poichè $G_{F/\mathbb{Q}} \to G_{F^+/\mathbb{Q}} \times G_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}$, l'orbita di $\alpha = \alpha^+ + \sqrt{-2}$ è data da $\left\{\sigma(\alpha^+) \pm \sqrt{-2} : \sigma \in G_{F^+/\mathbb{Q}}\right\}$ e, pertanto, ha $4 \cdot 2 = 8$ elementi. Segue che

Esercizio 2. Si consideri il polinoamio $f(X) = X^4 - 2X^2 + \frac{1}{2} \in \mathbb{Q}[X]$ e sia F il suo campo di spezzamento.

(1) Si mostri che $f(X) \in \mathbb{Q}[X]$ è irriducibile.
(2) Si calcoli $G_{F/\mathbb{Q}}$.
(3) Si mostri $F(i)/\mathbb{Q}$ è di Galois e si calcoli $G_{F(i)/\mathbb{Q}}$.

Soluzione: (1) Posto $y = x^2$ si trova che $y = 1 \pm \frac{1}{\sqrt{2}}$ sono le radici del polinomio

$$f(X) = Y^2 - 2Y + \frac{1}{2}$$

e quindi $x = \pm\sqrt{1 \pm \frac{1}{\sqrt{2}}}$ sono le radici di f, ovvero

$$f(X) = \left(X - \sqrt{1 + \frac{1}{\sqrt{2}}}\right)\left(X + \sqrt{1 + \frac{1}{\sqrt{2}}}\right)\left(X - \sqrt{1 - \frac{1}{\sqrt{2}}}\right)\left(X + \sqrt{1 - \frac{1}{\sqrt{2}}}\right).$$

Da ciò (o anche da uno studio di funzione) si deduce che tutte le radici di f sono reali, osservazione che sarà utile per lo svolgimento di (3). Da questa espressione ed una considerazione dei possibili prodotti si deduce facilmente che $f(X) \in \mathbb{Q}[X]$ è irriducibile. Infatti possiamo sicuramente escludere fattorizzazioni che comportino una radice in $\mathbb{Q}[X]$ e pertanto, se $f(X)$ fosse riducibile, sarebbe della forma $f(X) = g(X)\,h(X)$ dove $g(X)$ è il prodotto di due fattori della forma $(X - x_i) \mid f(X)$ con $i = 1, 2$. Il fattore $\left(X - \sqrt{1 + \frac{1}{\sqrt{2}}}\right)$ si accoppierà con uno degli altri fattori e le possibilità tre possibilità per $g(X)$ sono le seguenti:

$$\left(X - \sqrt{1 + \frac{1}{\sqrt{2}}}\right)\left(X + \sqrt{1 + \frac{1}{\sqrt{2}}}\right),$$
$$\left(X - \sqrt{1 + \frac{1}{\sqrt{2}}}\right)\left(X - \sqrt{1 - \frac{1}{\sqrt{2}}}\right),$$
$$\left(X - \sqrt{1 + \frac{1}{\sqrt{2}}}\right)\left(X + \sqrt{1 - \frac{1}{\sqrt{2}}}\right).$$

Guardando al prodotto delle radici si dedurrebbe che $1 + \frac{1}{\sqrt{2}} \in \mathbb{Q}$ (nel primo caso) oppure

$$\pm\sqrt{1 + \frac{1}{\sqrt{2}}}\sqrt{1 - \frac{1}{\sqrt{2}}} = \pm\sqrt{1 - \frac{1}{2}} = \pm\sqrt{\frac{1}{2}} = \pm\frac{1}{\sqrt{2}}$$

(nel secondo e terzo caso). Ciò non è possibile.

(2) Il risolvente cubico di f è

$$\begin{aligned} g_f(X) &= X^3 + 2X^2 - 2X - 4 \\ &= (X + 2)\left(X^2 - 2\right). \end{aligned}$$

In particolare, il campo di spezzamento di g_f è $\mathbb{Q}\left(\sqrt{2}\right)$. Ma si ha

$$\begin{aligned} f(X) &= \left(X - \sqrt{1 + \frac{1}{\sqrt{2}}}\right)\left(X + \sqrt{1 + \frac{1}{\sqrt{2}}}\right)\left(X - \sqrt{1 - \frac{1}{\sqrt{2}}}\right)\left(X + \sqrt{1 - \frac{1}{\sqrt{2}}}\right) \\ &= \left(X^2 - \left(1 + \frac{1}{\sqrt{2}}\right)\right)\left(X^2 - \left(1 - \frac{1}{\sqrt{2}}\right)\right), \end{aligned}$$

da cui segue che f è riducibile nel campo di spezzamento $\mathbb{Q}\left(\sqrt{2}\right)$ di g_f. Poichè $f(X) \in \mathbb{Q}[X]$ è irriducibile la sola possibilità è che si abbia $G_{F/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$.

(3) Abbiamo notato che le radici di f sono tutte reali e, pertanto, $F \subset \mathbb{R}$ ed $F \cap \mathbb{Q}(i) = \mathbb{Q}$. Notiamo che $F(i)/\mathbb{Q}$ è l'estensione composta delle estensioni di Galois $F/\mathbb{Q}$ e $\mathbb{Q}(i)/\mathbb{Q}$. Poichè come notato $F \cap \mathbb{Q}(i) = \mathbb{Q}$, da ciò segue che l'applicazione di restrizione

$$G_{F(i)/\mathbb{Q}} \to G_{F/\mathbb{Q}} \times G_{\mathbb{Q}(i)/\mathbb{Q}}$$

è un isomorfismo. Poichè $G_{\mathbb{Q}(i)/\mathbb{Q}} \simeq \mathbb{F}_2$ deduciamo che $G_{F(i)/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{F}_2$.

Esercizio 3. Sia E/F una estensione di Galois tale che $[E:F]=p$ dove p è un primo diverso dalla caratteristica di F e si supponga che $\mu_p \subset F$ (dove μ_p è il gruppo delle radici p esime dell'unità). Si mostri che $E=F(\xi)$ per qualche elemento $\xi \in E$ tale che $\xi^p \in F$.

Soluzione: Vedere la Proposizione 1.2 del file "Note 5" all'indirizzo

"$https://sites.google.com/site/sevesomarco/courses$":

la dimostrazione in questo caso $n=p$ risulta notevolmente semplificata. Con le notazioni introdotte nella dimostrazione si ha $E_1=F$ e, se $0\neq x_0 \in E_{\zeta_0}$ e $\zeta_0 \neq 1$ (tale elemento esiste poichè altrimenti $E=E_1=F$), $E=F(x_0)$ ed $x_0^p \in F$: infatti ζ_0 è una radice primitiva e si applica direttamente l'argomentazione che compare nelle ultime righe della dimostrazione o più semplicemente, si osserva che $x_0^p \in F$ poichè $x_0 \in E_{\zeta_0}$ ed $E=F(x_0)$ poichè $F \subsetneqq F(x_0) \subsetneqq E$ ed $[E:F]=p$ con p primo.

Alternativamente, sia $G_{E/F}=\langle \sigma \rangle$ ed indichiamo con $P_\sigma(T)$ e con $\chi_\sigma(T)$ il polinomio minimo e rispettivamente il polinomio caratteristico di σ, che hanno gli stessi fattori riducibili in $F[T]$. Poichè σ soddisfa il polinomio

$$X^p-1=\prod_{\zeta\in\mu_p}(T-\zeta) \text{ (decomposizione in } F[T]),$$

deduciamo che $P_\sigma(T)=\prod_{\zeta\in S}(T-\zeta)$ in $F[T]$ per qualche $S\subset\mu_p$ e, dunque,

$$\chi_\sigma(T)=\prod_{\zeta\in S}(T-\zeta)^{e_\zeta} \text{ (decomposizione in } F[T]).$$

Se esiste $\zeta_0\neq 1$ tale che $\zeta_0\in S$, allora $\chi_\sigma(\zeta_0)=0$ e possiamo trovare un autovettore $0\neq x_0$ associato a ζ_0 e concludere come sopra. Se invece $S=\{1\}$, deduciamo che $P_\sigma(T)=T-1$; poichè σ soddisfa il suo polinomio minimo, ciò implica che $\sigma=1$, ovvero $F=E$, il che non è possibile.

Esercizio 4. *[TeoNum]* Sia K un campo di numeri. Sia $\alpha\in\mathcal{O}_K$

i. Mostrare che la norma $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ è un elemento di $\mathbb{Z}$, nullo se e solo se α è nullo.
ii. Mostrare che l'elemento $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ appartiene a $\mathbb{Z}\cap(\alpha)$ dove (α) è l'ideale di $\mathcal{O}_K$ generato da α.
iii. Sia $\mathcal{P}\subset\mathcal{O}_K$ un ideale massimale. Mostrare che $\mathcal{P}\cap\mathbb{Z}\subset\mathbb{Z}$ è un ideale di $\mathbb{Z}$ generato da un numero primo non nullo.

Soluzione: Per il punto (i) vedere la Poposizione 3.3 delle note del collega Bertolini.

(ii) Considero $K\subset\mathbb{C}$ e sia $G=\mathrm{Hom}(K,\mathbb{C})$ l'insieme delle imemrsioni di K in $\mathbb{C}$. Osservo che $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)=\alpha\beta$ con $\beta=\prod_{\sigma\in G,\sigma\neq\mathrm{Id}}\sigma(\alpha)$ e $\beta\in\overline{\mathbb{Z}}\cap K=\mathcal{O}_K$. Concludo che $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)\in\alpha\mathcal{O}_K$.

(ii) Sia $P:=\mathcal{P}\cap\mathbb{Z}$. È un ideale di $\mathbb{Z}$ e per definizione l'applicazione composta $f\colon\mathbb{Z}\subset\mathcal{O}_K\to\mathcal{O}_K/\mathcal{P}$ ha P come nucleo. In particolare per il teorema di omomorfismo f fattorizza attraverso il quoziente $\mathbb{Z}/P\to\mathcal{O}_K/\mathcal{P}$ e tale applicazione è iniettiva. Ma $\mathcal{O}_K/\mathcal{P}$ è un campo e quindi $\mathbb{Z}/P$ è un dominio di integrità, ovvero P è un ideale primo. Per i punti (i) e (ii), dato un $\alpha\in\mathcal{P}$ non nullo, ho che $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ è un elemento non nullo di $\mathbb{Z}\cap(\alpha)\subset\mathbb{Z}\cap\mathcal{P}=P$. Quindi $P\neq 0$.

Esercizio 5. Sia $\zeta_9=\exp^{\frac{2\pi i}{9}}$ e sia $K=\mathbb{Q}(\zeta_9)$ il 9^o-campo ciclotomico.

i. Trovare una base intera per l'anello degli interi $\mathcal{O}_K$ e calcolare il discriminante di $\mathcal{O}_K$ (giustificando i conti).
ii. Determinare quali primi $p\in\mathbb{Z}$ ramificano in $\mathcal{O}_K$ e determinarne la decomposizione come prodotto di ideali primi di $\mathcal{O}_K$.
iii. Determinare la decomposizione di $2\mathbb{Z}$ in $\mathcal{O}_K$ [SUGG: scrivere $X^6+X^3+1=Y^2+Y+1$ con $Y=X^3$].

Soluzione: (i) Sappiamo che K è di Galois su $\mathbb{Q}$ con gruppo ciclico G isomorfo a $(\mathbb{Z}/9\mathbb{Z})^*$ e quindi ciclico di ordine 6. Inoltre $\mathcal{O}_K = \mathbb{Z}\big[\zeta_9\big]$ e, visto che $[K:\mathbb{Q}] = 6$, una base intera è data da $\{1, \zeta_9, \zeta_9^2, \cdots, \zeta_9^5\}$. Il polinomio minimo di ζ_9è $f(X) := (X^9-1)/(X^3-1) = X^6+X^3+1 = \prod_{\sigma\in G}\big(X - \sigma(\zeta_9)\big)$. Questo implica che $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta_9^2) = \prod_{\sigma\in G}\sigma(\zeta_9) = 1$. Il discriminante Δ_K è $-\mathrm{Norm}_{K/\mathbb{Q}}\big(f'(\zeta_9)\big)$ dove $f'(X) = 6X^5 + 3X^2 = 3X^2(2X^3+1)$ è il polinomio derivato. Quindi $f'(\zeta_9) = 3\zeta_9^2(2\zeta_9^3+1)$. Ma $\zeta_9^3 = \zeta_3$ e quindi $2\zeta_9^3 + 1 = \sqrt{-3}$ e $\mathrm{Norm}_{K/\mathbb{Q}}(\sqrt{-3}) = 3^3$. Quindi, usando la moltiplicatività della norma, ottengo

$$\Delta_K = -\mathrm{Norm}_{K/\mathbb{Q}}(3\zeta_9^2)\mathrm{Norm}_{K/\mathbb{Q}}(2\zeta_9^3+1) = -3^6\mathrm{Norm}_{K/\mathbb{Q}}(\zeta_9)^2 = -3^6 3^3 = -3^9.$$

(ii)–(iii) Utilizziamo il fatto che la decomposizione $p\mathcal{O}_K = \prod_{i=1}^s \mathcal{P}_i^{a_i}$ in fattori primi è univocamente determinata dalla decomposizoone di $f(X)$ modulo p in fattori irriducibili $\prod_{i=1}^s g_i^{a_i}$ in $\mathbb{F}_p[X]$. Infatti, $\mathcal{P}_i = \big(p, \widetilde{g}_i(\zeta_9)\big)$ dove $\widetilde{g}_i(X) \in \mathbb{Z}[X]$ modulo p è uguale a $g_i(X)$.

Il polinomio $X^9 - 1$ modulo un primo $p \neq 3$, ha tutti zeri distinti in quanto il m.c.d fra $g(X)$ ed il suo polinomio derivato $g'(X) = 9X^8$ è banale. Essendo $f(X)$ un fattore di $X^9 - 1$ segue che $f(X)$ modulo p ha anch'esso tutti zeri distinti e quindi i fattori irriducibili nella decomposizione in $\mathbb{F}_p[X]$ hanno molteplicità 1. Segue che $p \neq 3$ non ramifica in $\mathcal{O}_K$.

Invece $f(X)$ modulo 3 è uguale a $(X-1)^6$ e quindi $p\mathcal{O}_K = \mathcal{P}^6$ con $\mathcal{P} = (3, \zeta_9 - 1)$.

Infine affermo che $f(X)$ modulo 2 è un polinomio irriducibile di $\mathbb{F}_2[X]$. Se questo è vero segue che $2\mathcal{O}_K$ è un ideale primo di $\mathcal{O}_K$. Infatti $\mathbb{F}_2[X]/(X^6+X^3+1) \cong \mathbb{F}_2[Y,X]/(Y^2+Y+1, X^3-Y)$ e mi basta mostrare che quest'ultimo è un campo. Ma $\mathbb{F}_2[Y]/(Y^2+Y+1) \cong \mathbb{F}_4$, in quanto $Y^2+Y+1 \in \mathbb{F}_2[Y]$ è irriducibile. Oserviamo che l'isomorfismo è determinato da dove invio Y che può essere un qualsiasi elemento diverso da 0 ed 1. Poichè $\mathbb{F}_4^*$ è un gruppo ciclico di ordine 3, ogni elemento non nullo z di $\mathbb{F}_4$ soddisfa $z^3 = 1$. Segue quindi che il polinomio $X^3 - Y \in \mathbb{F}_2[Y]/(Y^2+Y+1)[X]$ non ha radici ovvero è irriducibile. Quindi $\mathbb{F}_2[Y,X]/(Y^2+Y+1, X^3-Y) \cong \mathbb{F}_2[X]/(X^6+X^3+1)$ è un campo.