**ESAME DI ALGEBRA 3, 24/02/2014**

**Esercizio 1.** Si consideri il polinomio $f(X) := X^4 - 8X + 12 \in \mathbb{Q}[X]$.

(1) Si mostri che $f(X) \in \mathbb{Q}[X]$ è irriducibile.
(2) Si determini il gruppo di Galois del campo di spezzamento di $f(X)$ su $\mathbb{Q}$.

*Soluzione:* (1) Mostriamo, per cominciare, che $f(X) \in \mathbb{Q}[X]$ è irriducibile. Se per assurdo fosse riducibile, sarebbe il prodotto di due fattori irriducibili di grado due oppure ammetterebbe una radice $x \in \mathbb{Q}$. Ma in quest'ultimo caso il criterio della radice garantirebbe che $x \in \{\pm 1, \pm 2, \pm 4, \pm 6, \pm 12\}$ e, poichè $f(x) \neq 0$ in tutti questi casi, ciò non è possibile. Se $f(X)$ fosse il prodotto di due fattori irriducibili in $\mathbb{Q}[X]$ di grado 2, poichè $f(X) \in \mathbb{Z}[X]$ è primitivo, per il lemma di Gauss sarebbe anche il prodotto di due fattori irriducibili in $\mathbb{Z}[X]$ di grado due. In particolare, $f(X)$ $mod 5$ sarebbe il prodotto in $\mathbb{F}_5[X]$ di due polinomi di grado 2; mostriamo che ciò non è possibile.

Infatti osserviamo che $f(X) \equiv X^4 + 2X + 2 \in \mathbb{F}_5[X]$ e che 1 è la sola radice di $f(X) \in \mathbb{F}_5[X]$ in $\mathbb{F}_5$; segue che $f(X) \equiv (X-1)\, g(X) \in \mathbb{F}_5[X]$ e che la sola possibile radice di $g(X)$ in $\mathbb{F}_5$ è 1. Ma il polinomio derivato $f'(X) = 4X^3 + 2$ non ha 1 come radice q euindi 1 non è una radice doppia di $f(X)$. Segue che $g(X)$ è irriducibile, avendo grado 3 e non avendo radici, e che quindi $f(X)$ non può essere prodotto in $\mathbb{F}_5[X]$ di due polinomi di grado 2, da cui come notato l'irriducibilità di $f(X) \in \mathbb{Q}[X]$.

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

$$g_f(X) = X^3 - 48X - 64 \in \mathbb{Q}[X],$$

il cui discriminante è

$$\begin{aligned} D(g_f) &= -4 \cdot (-48)^3 - 27 \cdot (-64)^2 \\ &= 2^{14} \cdot 3^3 - 2^{12} \cdot 3^3 = 2^{12} \cdot 3^3 \cdot (4-1) \\ &= 2^{12} \cdot 3^4 \in \mathbb{Q}^{\times 2}. \end{aligned}$$

Mostriamo che $g_f(X) \in \mathbb{Q}[X]$ è irriducibile, da cui seguirà che $G_f \simeq A_4$. Si ha infatti $g_f(X) \equiv X^3 + 2X + 1 \in \mathbb{F}_5[X]$ e tale polinomio è irriducibile poichè ha grado 3 e non ammette radici.

**Esercizio 2.** Si consideri il polinomio $f(X) = X^{15} - 3 \in \mathbb{Q}[X]$ e sia $E/\mathbb{Q}$ il suo campo di spezzamento.

(1) Si calcoli $[E : \mathbb{Q}]$.
(2) Si mostri che $G_{E/\mathbb{Q}}$ può essere presentato come un prodotto semidiretto non diretto.
(3) Si trovi un elemento $\alpha \in E$ tale che $E = \mathbb{Q}(\alpha)$.
(4) Si mostri che $G_{E/\mathbb{Q}}$ è un prodotto semidiretto della forms

$$G_{E/\mathbb{Q}} = C_1 \rtimes (C_2 \times C_3)$$

con $C_i$ gruppi ciclici e se ne calcolino esplicitamente dei generatori.

*Soluzione:* (1) Poichè $f'(X) = 15X^{14}$ e $f(\pm\infty) = \pm\infty$ esiste uno ed un solo $\sqrt[15]{3} \in \mathbb{R}$ tale che $f\left(\sqrt[15]{3}\right) = 0$. Se $\zeta$ è una radice primitiva 15-esima dell'unità, le radici di $f(X)$ sono

$$R_f = \left\{ \sqrt[15]{3}\zeta^i : i = 0, ..., 14 \right\}.$$

Per definizione $E = \mathbb{Q}(R_f)$ e si ha chiaramente $E \subset \mathbb{Q}\left(\sqrt[15]{3}, \zeta\right)$. Viceversa $\sqrt[15]{3} \in R_f \subset E$ e $\zeta = \frac{\sqrt[15]{3}\zeta}{\sqrt[15]{3}} \in \mathbb{Q}(R_f) = E$, da cui segue che $E = \mathbb{Q}\left(\sqrt[15]{3}, \zeta\right)$.

Poichè $f(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein applicato al primo 3, deduciamo che $\left[\mathbb{Q}\left(\sqrt[15]{3}\right) : \mathbb{Q}\right] = 15$. Inoltre sappiamo dalla teoria delle estensioni cicliche che $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois e che

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \#G_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \#\mathbb{Z}_{15}^{\times} = \varphi(15) = 8.$$

Poichè $\mathbb{Q}\left(\sqrt[15]{3}\right)/\mathbb{Q}$ e $\mathbb{Q}(\zeta)/\mathbb{Q}$ hanno indici coprimi segue che $\mathbb{Q}\left(\sqrt[15]{3}\right) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$,

$$\left[E : \mathbb{Q}\left(\sqrt[15]{3}\right)\right] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 8,\ [E : \mathbb{Q}(\zeta)] = \left[\mathbb{Q}\left(\sqrt[15]{3}\right) : \mathbb{Q}\right] = 15$$

e si ha

$$[E : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}]\left[\mathbb{Q}\left(\sqrt[15]{3}\right) : \mathbb{Q}\right] = 8 \cdot 15 = 120.$$

(2) Poichè $E/\mathbb{Q}$ è di Galois sappiamo che $E/\mathbb{Q}\left(\sqrt[15]{3}\right)$ ed $E/\mathbb{Q}(\zeta)$ sono di Galois; inoltre come notato $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois e, pertanto, $G_{E/\mathbb{Q}(\zeta)} \lhd G_{E/\mathbb{Q}}$. Segue che $G_{E/\mathbb{Q}(\zeta)}H \subset G_{E/\mathbb{Q}}$ è un sottogruppo per ogni $H \subset G_{E/\mathbb{Q}}$ sottogruppo. Poichè $\#G_{E/\mathbb{Q}(\zeta)} = 15$ e $\#G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)} = 8$ sono coprimi, $G_{E/\mathbb{Q}(\zeta)} \cap G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)} = 1$ e

$$\begin{aligned} \#\left(G_{E/\mathbb{Q}(\zeta)}G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)}\right) &= \frac{\#G_{E/\mathbb{Q}(\zeta)} \cdot \#G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)}}{\#\left(G_{E/\mathbb{Q}(\zeta)} \cap G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)}\right)} = 15 \cdot 8 \\ &= 120 = \#G_{E/\mathbb{Q}}. \end{aligned}$$

Dunque $G_{E/\mathbb{Q}(\zeta)}G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)} = G_{E/\mathbb{Q}}$ e si è mostrato che

$$G_{E/\mathbb{Q}} = G_{E/\mathbb{Q}(\zeta)} \rtimes G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)}.$$

Non si tratta di un prodotto diretto, perchè in questo caso si avrebbe $G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)} \lhd G_{E/\mathbb{Q}}$ ovvero $\mathbb{Q}\left(\sqrt[15]{3}\right)/\mathbb{Q}$ sarebbe una estensione normale e quindi $E = \mathbb{Q}\left(\sqrt[15]{3}\right)$.

(3) Mostriamo che $E = \mathbb{Q}(\alpha)$ con $\alpha = \sqrt[15]{3} + \zeta$. Per farlo ricordiamo la seguente descrizione esplicita dei gruppi $G_{E/\mathbb{Q}(\zeta)}$ e $G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)}$. Poichè $\mu_{15} \subset \mathbb{Q}(\zeta)$ e $[E : \mathbb{Q}(\zeta)] = 15$, sappiamo dalla teoria delle estensioni cicliche che si ha un isomorfismo di gruppi $\mu_{15} \to G_{E/\mathbb{Q}(\zeta)}$, ottenuto mediante una associazione $\xi \mapsto \sigma_\xi$ tale che $\sigma_\xi$ è univocamente determinato da $\sigma_\xi(\alpha) = \alpha\xi$. Poichè $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois e $\mathbb{Q}\left(\sqrt[15]{3}\right) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$, sappiamo anche che l'applicazione di restrizione $G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è un isomorfismo e, dalla teoria delle estensioni cicliche, sappiamo che $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \mathbb{Z}_{15}^{\times}$. L'isomorfismo $\mathbb{Z}_{15}^{\times} \to G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)}$ è ottenuto mediante la regola $i \mapsto \rho_i$ dove $\rho_i$ è univocamente determinato da $\rho_i(\zeta) = \zeta^i$. Per mostrare che $E = \mathbb{Q}(\alpha)$ verifichiamo la condizione equivalente $g(\alpha) = \alpha \Rightarrow g = 1$ per ogni $g \in G_{E/\mathbb{Q}}$. Possiamo scrivere $g = \sigma_\xi\rho_i$ dove $(\xi, i) \in \mu_{15} \times \mathbb{Z}_{15}^{\times}$ e si ha

$$\begin{aligned} g(\alpha) &= \sigma_\xi\left(\rho_i\left(\sqrt[15]{3} + \zeta\right)\right) = \sigma_\xi\left(\rho_i\left(\sqrt[15]{3}\right) + \rho_i(\zeta)\right) \\ &= \sigma_\xi\left(\sqrt[15]{3} + \zeta^i\right) = \sigma_\xi\left(\sqrt[15]{3}\right) + \sigma_\xi(\zeta)^i \\ &= \sqrt[15]{3}\xi + \zeta^i. \end{aligned}$$

Dunque $g(\alpha) = \alpha$ se e solo se

$$\sqrt[15]{3} + \zeta = \sqrt[15]{3}\xi + \zeta^i \ \Leftrightarrow\ \sqrt[15]{3}(1 - \xi) = \zeta^i - \zeta.$$

Se $\xi \neq 1$ (rispettivamente $i \neq 1$) deduciamo $\sqrt[15]{3} = \frac{\zeta^i - \zeta}{1 - \xi} \in \mathbb{Q}\left(\sqrt[15]{3}\right) \cap \mathbb{Q}(\zeta)$ (rispettivamente $\frac{1}{\sqrt[15]{3}} = \frac{1-\xi}{\zeta^i - \zeta} \in \mathbb{Q}\left(\sqrt[15]{3}\right) \cap \mathbb{Q}(\zeta)$): poichè $\mathbb{Q}\left(\sqrt[15]{3}\right) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ si ottiene la contraddizione

$\sqrt[15]{3} \in \mathbb{Q}$ (rispettivamente $\frac{1}{\sqrt[15]{3}} \in \mathbb{Q}$, ovvero ancora $\sqrt[15]{3} \in \mathbb{Q}$). Dunque abbiamo mostrato che, se $g(\alpha) = \alpha$, non è possibile $(\xi, i) \neq (1,1)$ (ovvero $g \neq 1$); in altre parole $g = 1$.

(4) Per il teorema cinese dei resti si ha l'isomorfismo di anelli $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$ e dunque $\mathbb{Z}_{15}^\times \simeq \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times$. Poichè $\mathbb{Z}_3^\times$ (rispettivamente $\mathbb{Z}_5^\times$ o $\mu_{15}$) è un sottogruppo moltiplicativo finito di un campo, si ha che $\mathbb{Z}_3^\times \simeq \mathbb{Z}_2$ (rispettivamente $\mathbb{Z}_5^\times \simeq \mathbb{Z}_5$ o $\mu_{15} \simeq \mathbb{Z}_{15}$) è ciclico. Segue da quanto mostrato in (2) e (3) che

$$\begin{aligned} G_{E/\mathbb{Q}} &= G_{E/\mathbb{Q}(\zeta)} \rtimes G_{E/\mathbb{Q}\left(\sqrt[15]{3}\right)} \simeq \mu_{15} \rtimes \mathbb{Z}_{15}^\times \\ &\simeq \mathbb{Z}_{15} \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_4). \end{aligned}$$

Si ha che $\mathbb{Z}_3^\times$ è generato da 2, mentre $\mathbb{Z}_5^\times$ è generato da 2 (oppure 3). Poichè l'immagine di $11 \in \mathbb{Z}_{15}$ (rispettivamente $7 \in \mathbb{Z}_{15}$) in $\mathbb{Z}_3 \times \mathbb{Z}_5$ è $(2,1) \in \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times$ (rispettivamente $(1,2) \in \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times$), $\mathbb{Z}_{15}^\times = \langle 7 \rangle \times \langle 11 \rangle$; d'altra parte $\mu_{15} = \langle \zeta \rangle$. Segue dalla descrizione in (3) che

$$G_{E/\mathbb{Q}} = \langle \sigma_\xi \rangle \rtimes (\langle 7 \rangle \times \langle 11 \rangle).$$

**Esercizio 3.** Siano date estensioni di campi $F \subset E \subset \Omega$ e si supponga che $E/F$ sia una estensione finita.

(1) Si mostri che, se $0 \neq f(X) \in E[X]$ è irriducibile, esiste $0 \neq g(X) \in F[X]$ tale che $f(X) \mid g(X)$ in $E[X]$.
(2) Si mostri che sono equivalenti i fatti che seguono.
   - $\forall f(X) \in F[X]$ si ha che $f(X)$ spezza completamente in $\Omega[X]$.
   - $\forall f(X) \in E[X]$ si ha che $f(X)$ spezza completamente in $\Omega[X]$.
(3) È possibile segliere il polinomio $g(X)$ in (1) in modo tale che sia anche irriducibile?

*Soluzione:* Quanto asserito nell'esercizio è vero supponendo semplicemente che $E/F$ sia una estensione algebrica e per un arbitrario polinomio $0 \neq f(X) \in E[X]$, non necessariamente irriducibile, in (1). Mostriamo dunque questo risultato più generale.

(1) Consideriamo l'estensione di anelli $F[X] \subset E[X]$ e, posto $I_f := E[X] f(X) \subset E[X]$, l'ideale $I := I_f \cap F[X]$; notiamo che

$$E[X] I \subset E[X] I_f = I_f$$

da cui segue che, se $g(X) \in I$, allora $f(X) \mid g(X)$ in $E[X]$. Resta dunque da mostrare che $0 \neq I$, in modo tale che, se $0 \neq g(X) \in I$, allora $f(X) \mid g(X)$ in $E[X]$.

Per farlo notiamo che l'inclusione $F[X] \subset E[X]$ induce un'applicazione

$$F_f := \frac{F[X]}{I_f \cap F[X]} \to \frac{E[X]}{I_f} =: E_f$$

che è iniettiva. Possiamo dunque vedere $F_f$ come un sottoanello di $E_f$ e considerare l'elemento

$$\overline{X} := X + (I_f \cap F[X]) = X + I_f.$$

Poichè $0 \neq f(X)$ è irriducibile, $E_f$ è una estensione finita di $E$; segue che, poichè $E/F$ è algebrica, allora $E_f/F$ è algebrica. Ma allora $\overline{X} \in F_f \subset E_f$ è algebrico su $F$, cioè l'applicazione $\psi_{\overline{X}} : F[X] \to F_f \subset E_f$ tale che $\psi_{\overline{X}}(g) = g\left(\overline{X}\right)$ ha nucleo non banale. Ma si ha $g\left(\overline{X}\right) = g(X) + I_f$ se $g(X) \in F[X]$ e dunque

$$\ker\left(\psi_{\overline{X}}\right) = \left\{g(X) \in F[X] : g\left(\overline{X}\right) = 0\right\} = I_f \cap F[X]$$

che risulta non nullo. Equivalentemente, una volta notato che $\overline{X} \in F_f \subset E_f$ è algebrico su $F$, si può concludere osservando che, se $I_f \cap F[X] = 0$, allora $F[X] \simeq F\left[\overline{X}\right] \subset E_f$ e dunque $\overline{X}$ non sarebbe algebrico su $F$.

Alternativamente, la ineguaglianza $I_f \cap F[X] \neq 0$ può essere dedotta dal fatto che $F[X] \subset E[X]$ è una estensione intera di anelli e dunque, se $\mathfrak{p} \subset E[X]$ è un ideale primo, si ha che $\mathfrak{p} \cap F[X]$ è massimale in $F[X]$ se e solo se $\mathfrak{p}$ è massimale in $E[X]$.

(2) Chiaramente se ogni polinomio in $E[X]$ spezza completamente in $\Omega[X]$ lo stesso è vero per i polinomi in $F[X]$ $(\subset E[X])$. Viceversa sia $0 \neq f(X) \in E[X]$ e supponiamo che ogni polinomio in $F[X]$ spezzi completamente in $\Omega[X]$. Sappiamo per (1) che esiste $0 \neq g(X) \in F[X]$ tale che $f(X) \mid g(X)$ in $E[X]$, ovvero

$$0 \neq g(X) = f(X) h(X) \text{ in } E[X].$$

Poichè $0 \neq g(X) \in F[X]$, sappiamo che possiamo scrivere

$$g(X) = \omega (X - \omega_1) ... (X - \omega_n) \text{ in } \Omega[X]$$

dove $\omega, \omega_1, ..., \omega_n \in \Omega$. Dunque

$$f(X) h(X) = (X - \omega_1) ... (X - \omega_n) \text{ in } \Omega[X]$$

e, poichè i polinomi $X - \omega_i \in \Omega[X]$ sono irriducibili ed $\Omega[X]$ è un $UFD$, possiamo supporre a meno di riordinare gli indici che si abbia

$$f(X) = (X - \omega_1) ... (X - \omega_m) \text{ in } \Omega[X]$$

a meno di moltiplicazione per elementi in $\Omega[X]^\times = \Omega^\times$. Ciò significa che $f(X) \in E[X]$ spezza completamente in $\Omega[X]$.

(3) Siano le notazioni come in (1) nel caso in cui $0 \neq f(X) \in E[X]$ sia irriducibile. Poichè $E[X]$ è un $UFD$, se $f(X) \in E[X]$ è irriducibile $I_f$ è un ideale primo e segue che $I$ è primo; ma poichè $F[X]$ è $PID$ si ha che $0 \neq I = (g(X))$ e $g(X)$ è irriducibile.

**Esercizio 4.** *[TeoNum]* Sia $K$ un campo di numeri con $n = [K : \mathbb{Q}]$. Sia $\{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Q}$-base di $K$ composta di interi algebrici e sia $d = \Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z} \backslash \{0\}$ il discriminante di $\{\alpha_1, \ldots, \alpha_n\}$.

i. Mostrare che per ogni $\alpha \in \mathcal{O}_K$ esistono unici $a_1, \ldots, a_n \in \mathbb{Z}$ tali che $\alpha = \frac{a_1}{d}\alpha_1 + \cdots + \frac{a_n}{d}\alpha_n$.
ii. Sia $\beta \in K$ un intero algebrico tale che $\alpha_i = \beta^{i-1}$ per ogni $i = 1, \ldots, n$, sia $f_\beta(X)$ il polinomio minimo di $\beta$ su $\mathbb{Q}$ e sia $\gamma := f'_\beta(\beta)$ dove $f'_\beta(X)$ è il polinomio derivato. Mostrare che $f_\beta(X)$ ha grado $n$ e che $\gamma \in \mathcal{O}_K \backslash \{0\}$.

*Soluzione:* Per il punto (i) vedere la Poposizione 4.6 delle note del collega Bertolini.

(ii) Visto che $\beta \in \mathcal{O}_K$ so che $f_\beta(X) \in \mathbb{Z}[X]$. Quindi $f'_\beta(X) \in \mathbb{Z}[X]$. Siccome $\mathcal{O}_K$ è un anello che contiene $\mathbb{Z}$ e $\beta$, concludo che $f'_\beta(\beta) = \gamma \in \mathcal{O}_K$. Siccome $\mathbb{Q}$ è un campo perfetto e $f_\beta(X)$ è un polinomio irriducibile, tale polinomio non ha zeri multipli. In particolare, $\beta$ è una radice semplice di $f_\beta(X)$ e quindi $f'_\beta(\beta) \neq 0$.

.

**Esercizio 5.** Sia $\zeta_7 = \exp^{\frac{2\pi i}{7}}$ e sia $K = \mathbb{Q}(\zeta_7)$ il $7^o$-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 $\mathcal{O}_K$.
iii. Mostrare che $p\mathbb{Z}$ spezza completamente in $\mathcal{O}_K$ se e solo se $p \equiv 1$ modulo 7 (dire che $p$ spezza completamente in $\mathcal{O}_K$ significa richiedere che $p\mathcal{O}_K = \prod_{i=1}^n \mathcal{P}_i$ è il prodotto di $n = [K : \mathbb{Q}]$ ideali primi distinti).

*Soluzione:* (i) Sappiamo che $K$ è di Galois su $\mathbb{Q}$ con gruppo ciclico $G$ di ordine 6. Inoltre $\mathcal{O}_K = \mathbb{Z}\big[\zeta_7\big]$ e, visto che $[K:\mathbb{Q}] = 6$, una base intera è data da $\{1, \zeta_7, \zeta_7^2, \cdots, \zeta_{12}^5\}$. Il polinomio minimo di $\zeta_7$è $f(X) := (X^7-1)/(X-1) = X^6+X^5+X^4+X^3+X^2+X+1 = \prod_{\sigma\in G}\big(X-\sigma(\zeta_7)\big)$. Il discriminante è $-\mathrm{Norm}_{K/\mathbb{Q}}\big(f'(\zeta_7)\big)$ dove $f'(X)$ è il polinomio derivato.

Usando il fatto che $f(X)(X-1) = X^7-1$, segue dalla regola di Leibniz che $f'(X)(X-1)+f(X) = 7X^6$ e quindi $f'(\zeta_7)(\zeta_7-1) = 7\zeta_7^6$. La norma di 7 è $7^6$ e la norma di $\zeta_7$ è il coefficiente costante del polinomio minimo, ovvero $-1$. Infine la norma di $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta_7-1) = \mathrm{Norm}_{K/\mathbb{Q}}(-1(1-\zeta_7)) = \mathrm{Norm}_{K/\mathbb{Q}}(1-\zeta_7) = \prod_{\sigma\in G}\big(1-\sigma(\zeta_7)\big) = f(1) = 7$.

Visto che la norma è moltiplicativa, deduciamo che il discriminante cercato è $-\mathrm{Norm}_{K/\mathbb{Q}}\big(f'(\zeta_7)\big) = -7^5$.

(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, $\mathcal{P}_i = \big(p, \widetilde{g}_i(\zeta_7)\big)$ dove $\widetilde{g}_i(X) \in \mathbb{Z}[X]$ modulo $p$ è uguale a $g_i(X)$.

Il polinomio $X^7-1$ modulo un primo $p \neq 7$, ha tutti zeri distinti in quanto il m.c.d fra $g(X)$ ed il suo polinomio derivato $g'(X) = 7X^6$ è banale. Essendo $f(X)$ un fattore di $X^7-1$ 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 $p \neq 7$ non ramifica in $\mathcal{O}_K$.

Invece $f(X)$ modulo 7 è uguale a $(X-1)^6$ e quindi $p = \mathcal{P}^6$ con $\mathcal{P} = (7, \zeta_7-1) = (\zeta_7-1)$ (abbiamo visto che $7 = \mathrm{Norm}_{K/\mathbb{Q}}(\zeta_7-1)$ e quindi $7 \in (\zeta_7-1)$.

Supponiamo $p \neq 7$. Affermo che $p$ spezza completamente se e solo se $p \equiv 1$ modulo 7. Questo equivale a chiedere che $f(X)$ modulo $p$ spezzi completamente in $\mathbb{F}_p[X]$. Se $p \equiv 1$ modulo 7 allora $\mathbb{F}_p^*$, essendo un gruppo ciclico di ordine $p-1$, contiene tutte le radici dell'unità di ordine 7, ovvero $X^7-1$ e quindi $f(X)$ modulo $p$ si spezza completamente in $\mathbb{F}_p$. Viceversa se $f(X)$ modulo $p$ si spezza completamente in $\mathbb{F}_p$, allora $\mathbb{F}_p^*$ contiene un sottogrupo di ordine 7 e $p \equiv 1$ modulo 7.