SOLUZIONI DEL COMPITO DEL 24/02/2016

Esercizio 1. Sia E il campo di spezzamento del polinomio $X^3-6 \in \mathbb{Q}[X]$ e sia $F = \mathbb{Q}\left(i, \sqrt{3}\right)$.

(1) Si calcoli il grado $[EF : \mathbb{Q}]$ del campo composto EF.
(2) Si esibisca una $\mathbb{Q}$-base di EF.
(3) Si mostri che $\mathbb{Q} \subset EF$ è una estensione di Galois e si calcoli il gruppo $\mathrm{Gal}_{EF/\mathbb{Q}}$ come gruppo astratto.

Soluzione: (1) Il polinomio $f(X) = X^3-6 \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein applicato al primo 3. Posto $\zeta := \exp\left(\frac{2\pi i}{3}\right)$ ed indicata con $\sqrt[3]{6}$ l'unica radice reale di $f(X)$, l'insieme delle radici di $f(X)$ è

$$R_f = \left\{\sqrt[3]{6}, \sqrt[3]{6}\zeta, \sqrt[3]{6}\zeta^2\right\}.$$

Deduciamo che $E = \mathbb{Q}\left(\sqrt[3]{6}, \zeta\right)$: infatti $\subset$ è ovvia data l'espressione di R_f e, viceversa, $\sqrt[3]{6}, \zeta = \frac{\sqrt[3]{6}\zeta}{\sqrt[3]{6}} \in E$. Poichè $\left[\mathbb{Q}\left(\sqrt[3]{6}\right) : \mathbb{Q}\right] = 3$ e $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ (essendo $f(X)$ ed il terzo polinomio ciclotomico irriducibili su $\mathbb{Q}$), deduciamo che

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

Poichè $E/\mathbb{Q}$ è di Galois, sappiamo che

$$[EF : \mathbb{Q}] = \frac{[E : \mathbb{Q}][F : \mathbb{Q}]}{[E \cap F : \mathbb{Q}]}.$$

Abbiamo già notato che $[E : \mathbb{Q}] = \left[\mathbb{Q}\left(\sqrt[3]{4}, \zeta\right) : \mathbb{Q}\right] = 6$, mentre $[F : \mathbb{Q}] = 4$ essendo $F/\mathbb{Q}$ biquadratica (infatti si verifica facilmente che $\mathbb{Q}(i) \neq \mathbb{Q}\left(\sqrt{3}\right)$). Dunque $G_{F/\mathbb{Q}} \simeq \mathbb{F}_2 \times \mathbb{F}_2$.

L'estensione $\mathbb{Q}\left(\sqrt[3]{6}\right)/\mathbb{Q}$ non è normale (essendo reale ma avendo estensioni coniugate non reali) e dunque $G_{E/\mathbb{Q}} \simeq S_3$ (avendo ordine 6 ma non potendo essere abeliano). Notiamo che

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

Poichè $\mathbb{Q}(\zeta) = \mathbb{Q}\left(\sqrt{3}i\right) \subset E \cap F$ (essendo $\zeta = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$) deduciamo $E \cap F = \mathbb{Q}(\zeta) = \mathbb{Q}\left(\sqrt{3}i\right)$ e quindi $[E \cap F : \mathbb{Q}] = 2$. Ma allora

$$[EF : \mathbb{Q}] = \frac{6 \cdot 4}{2} = 12.$$

(2) Notiamo che $EF = \mathbb{Q}\left(\sqrt[3]{6}, \zeta, i, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt[3]{6}, \zeta, i\right)$: si ha ovviamente $\supset$ e, viceversa, $\sqrt{3} = \frac{\sqrt{3}i}{i} \in \mathbb{Q}\left(\sqrt[3]{6}, \zeta, i\right) = E(i)$ poichè abbiamo notato che $\sqrt{3}i \in \mathbb{Q}\left(\sqrt{3}i\right) = E \cap F \subset E(i)$, da cui segue l'altra inclusione. Poichè

$$\left[\mathbb{Q}\left(\sqrt[3]{6}, \zeta, i\right) : \mathbb{Q}\right] = [EF : \mathbb{Q}] = 12 = 6 \cdot 2 = \left[\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right) : \mathbb{Q}\right][\mathbb{Q}(i) : \mathbb{Q}],$$

sappiamo che una $\mathbb{Q}$-base di $EF = \mathbb{Q}\left(\sqrt[3]{6}, \zeta, i\right)$ si ottiene come prodotto di una di $\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right)/\mathbb{Q}$ ed una base di $\mathbb{Q}(i)/\mathbb{Q}$. Ma per gli stessi motivi una base di $\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right)/\mathbb{Q}$ si ottiene come prodotto di una base di $\mathbb{Q}\left(\sqrt[3]{6}\right)/\mathbb{Q}$ ed una base di $\mathbb{Q}(\zeta)/\mathbb{Q}$, come per esempio la base

$$\left\{1, \sqrt[3]{6}, \left(\sqrt[3]{6}\right)^2, \zeta, \sqrt[3]{6}\zeta, \left(\sqrt[3]{6}\right)^2\zeta\right\}.$$

Poichè una base di $\mathbb{Q}(i)/\mathbb{Q}$ è $\{1,i\}$, deduciamo che una $\mathbb{Q}$-base di EF è

$$\left\{1, \sqrt[3]{6}, \left(\sqrt[3]{6}\right)^2, \zeta, \sqrt[3]{6}\zeta, \left(\sqrt[3]{6}\right)^2\zeta, i, \sqrt[3]{6}i, \left(\sqrt[3]{6}\right)^2 i, \zeta i, \sqrt[3]{6}\zeta i, \left(\sqrt[3]{6}\right)^2\zeta i\right\}.$$

(3) Abbiamo già notato che $EF = \mathbb{Q}\left(\sqrt[3]{6}, \zeta, i\right)$; poichè $E = \mathbb{Q}\left(\sqrt[3]{6}, \zeta\right)/\mathbb{Q}$ e $\mathbb{Q}(i)/\mathbb{Q}$ sono di Galois, se mostriamo che $\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right) \cap \mathbb{Q}(i) = \mathbb{Q}$ segue che

$$G_{EF/\mathbb{Q}} \simeq G_{E/\mathbb{Q}} \times G_{\mathbb{Q}(i)/\mathbb{Q}} \simeq S_3 \times \mathbb{F}_2.$$

Ma poichè $\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right)/\mathbb{Q}$ è di Galois,

$$\left[\mathbb{Q}\left(\sqrt[3]{6}, \zeta, i\right) : \mathbb{Q}\right] = \frac{\left[\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right) : \mathbb{Q}\right]\left[\mathbb{Q}(i) : \mathbb{Q}\right]}{\left[\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right) \cap \mathbb{Q}(i) : \mathbb{Q}\right]} = \frac{6 \cdot 2}{\left[\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right) \cap \mathbb{Q}(i) : \mathbb{Q}\right]}.$$

Avendo già notato che $\left[\mathbb{Q}\left(\sqrt[3]{6}, \zeta, i\right) : \mathbb{Q}\right] = 12$, deduciamo che $\left[\mathbb{Q}\left(\sqrt[3]{6}, \zeta\right) \cap \mathbb{Q}(i) : \mathbb{Q}\right] = 1$ come si voleva.

Esercizio 2. Si consideri il polinomio $f(X) = X^5 - 7 \in \mathbb{Q}[X]$ e sia E il suo campo di spezzamento.

(1) Mostrare che $\mathbb{Q} \subset E$ è una estensione di Galois ed esibire una base di E come $\mathbb{Q}$-spazio vettoriale.
(2) Descrivere tutti gli elementi del gruppo $\mathrm{Gal}_{E/\mathbb{Q}}$.
(3) Trovare $\eta \in E$ tale che $E = \mathbb{Q}(\eta)$.

Soluzione: Indicata con α una radice di $f(X)$ e con ζ una radice primitiva 5 dell'unità, si ha $E = \mathbb{Q}(\alpha, \zeta)$. Infatti

$$R_f = \left\{\alpha\zeta^i : i = 0, ..., 4\right\},$$

per cui certamente $E \subset \mathbb{Q}(\alpha, \zeta)$ e viceversa, essendo $\zeta = \frac{\alpha\zeta}{\alpha} \in E$. Abbiamo che $f(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein, per cui

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5.$$

D'altra parte $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. Poichè i gradi sono coprimi, deduciamo che

$$\#G_{E/\mathbb{Q}} = [E : \mathbb{Q}] = 4 \cdot 5 = 20.$$

(1) Una base di $\mathbb{Q}(\alpha)/\mathbb{Q}$ (risp. $\mathbb{Q}(\zeta)/\mathbb{Q}$) è

$$\{\alpha^r : r = 0, ..., 4\} \text{ (risp. } \{\zeta^s : s = 0, ..., 3\}\text{)}.$$

Poichè

$$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 20 = 5 \cdot 4 = [\mathbb{Q}(\alpha) : \mathbb{Q}]\left[\mathbb{Q}(\zeta) : \mathbb{Q}\right],$$

sappiamo che una base di $E/\mathbb{Q}$ è

$$\mathcal{B} = \left\{\alpha^r\zeta^s : r = 0, ..., 4; s = 0, ..., 3\right\}.$$

(2) Consideriamo l'applicazione

$$\begin{array}{ccc} G_{E/\mathbb{Q}(\alpha)} & \to & G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \xrightarrow{\sim} Aut(\mu_5) = \left(\dfrac{\mathbb{Z}}{5\mathbb{Z}}\right)^\times \\ \sigma & \mapsto & \sigma_{|\mathbb{Q}(\zeta)} \mapsto \sigma_{|\mu_5}. \end{array}$$

E' iniettiva e dunque suriettiva per questioni di ordine. Abbiamo che $\left(\zeta \mapsto \zeta^2\right)$ genera $Aut(\mu_5)$, poichè corrisponde alla moltiplicazione per 2 in $\left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^\times = Aut\left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)$, che ha ordine 4 e dunque genera $\left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$:

$$1 \mapsto 2 \mapsto 2 \cdot 2 = 4 \mapsto 2 \cdot 4 = 8 \equiv 3 \mapsto 2 \cdot 3 = 6 \equiv 1,$$

dunque $2 \cdot (-)$ ha ordine 4. Dunque

$$G_{E/\mathbb{Q}(\alpha)} = \left\langle \sigma : \left\{ \begin{array}{c} \alpha \mapsto \alpha \\ \zeta \mapsto \zeta^2 \end{array} \right. \right\rangle.$$

Consideriamo ora l'applicazione

$$\varphi : G_{E/\mathbb{Q}(\zeta)} \overset{\psi}{\to} \mu_5 \overset{\sim}{\to} \frac{\mathbb{Z}}{5\mathbb{Z}}$$

definita dalla formula

$$\rho(\alpha) = \psi(\rho)\,\alpha = \zeta^{\varphi(\rho)}\alpha.$$

E' un omoorfismo iniettivo, che è dunque suriettivo per ragioni d'ordine. Dunque

$$G_{E/\mathbb{Q}(\zeta)} = \left\langle \rho : \left\{ \begin{array}{c} \alpha \mapsto \zeta\alpha \\ \zeta \mapsto \zeta \end{array} \right. \right\rangle.$$

Consideriamo l'applicazione

$$\begin{array}{rcl} G_{E/\mathbb{Q}(\alpha)} \times G_{E/\mathbb{Q}(\zeta)} & \to & G_{E/\mathbb{Q}} \\ \left(\sigma^i, \rho^j\right) & \mapsto & \sigma^i\rho^j. \end{array}$$

Poichè $G_{E/\mathbb{Q}(\alpha)} \cap G_{E/\mathbb{Q}(\zeta)} = \{1\}$ (avendo i due gruppi ordine coprimo), l'applicazione è iniettiva. Dunque è suriettiva per ragioni d'ordine ed abbiamo

$$G_{E/\mathbb{Q}} = \left\{\sigma^i\rho^j : i = 0, ..., 3; j = 0, ..., 4\right\}$$

(3) Mostriamo che l'orbita di $\eta := \alpha + \zeta$ ha 20 elementi, da cui segue che $E = \mathbb{Q}(\eta)$. Abbiamo che $g_1(\eta) = g_2(\eta)$ con $g_1 \neq g_2$ in $G_{E/\mathbb{Q}}$ se e solo se $g(\eta) = \eta$ con $g(= g_2^{-1}g_1) \neq 1$ in $G_{E/\mathbb{Q}}$. Occorre dunque verificare che

$$\sigma^i\rho^j(\eta) = \eta \Rightarrow (i,j) = (0,0) \in \{0, ..., 3\} \times \{0, ..., 4\}.$$

Notiamo che, per induzione,

$$\begin{array}{rcl} \sigma^i(\zeta) & = & \sigma^{i-1}\left(\zeta^2\right) = \sigma^{i-1}(\zeta)^2 = \left(\zeta^{2^{i-1}}\right)^2 = \zeta^{2^i}, \\ \rho^j(\alpha) & = & \rho^{j-1}(\zeta\alpha) = \zeta\rho^{j-1}(\alpha) = \zeta\zeta^{j-1}\alpha = \zeta^j\alpha. \end{array}$$

Abbiamo dunque

$$\begin{array}{rcl} \sigma^i\rho^j(\eta) & = & \sigma^i\left(\rho^j(\alpha)\right) + \sigma^i\left(\rho^j(\zeta)\right) = \sigma^i\left(\zeta^j\alpha\right) + \sigma^i(\zeta) \\ & = & \alpha\left(\sigma^i(\zeta)\right)^j + \zeta^{2^i} = \alpha\left(\zeta^{2^i}\right)^j + \zeta^{2^i} \\ & = & \alpha\zeta^{j2^i} + \zeta^{2^i}. \end{array}$$

Otteniamo allora

$$\sigma^i\rho^j(\eta) = \eta \Leftrightarrow \alpha\zeta^{j2^i} - \alpha = \zeta - \zeta^{2^i}.$$

Poichè $\zeta^4 = -1 - \zeta - \zeta^2 - \zeta^3$, abbiamo

$$\begin{array}{rcl} \alpha\zeta^{j2^i} - \alpha & \in & \displaystyle\sum_{s=0}^{4} \mathbb{Q}\alpha\zeta^s = \bigoplus_{s=0}^{3} \mathbb{Q}\alpha\zeta^s =: V_1, \\ \zeta - \zeta^{2^i} & \in & \displaystyle\sum_{s=0}^{4} \mathbb{Q}\zeta^s = \bigoplus_{s=0}^{3} \mathbb{Q}\zeta^s =: V_2. \end{array}$$

Poichè $V_1 \cap V_2 = \{0\}$ (dalla espressione di $\mathcal{B}$), otteniamo $\alpha\zeta^{j2^i} = \alpha \Leftrightarrow \zeta^{j2^i} = 1 \Leftrightarrow j2^i \equiv 0 \mod(5)$ e $\zeta^{2^i} = \zeta \Leftrightarrow 2^i \equiv 1 \mod(5)$. Dunque

$$j \equiv j2^i \equiv 0 \bmod(5) \;\Rightarrow\; j = 0.$$

D'altra parte, poichè $\langle 2\rangle = \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$, $2^i \equiv 1 \Rightarrow i \equiv 0 \bmod(4). \Rightarrow i = 0$.

Esercizio 3. (*Teo. Gal*) Supponiamo che $F \subset K \subset L$ siano estensioni algebriche (non necessariamente finite) e che Ω sia un campo algebricamente chiuso che contiene F.

(1) Si mostri che l'applicazione
$$p = p_{L/K} : Hom_F(L, \Omega) \to Hom_F(K, \Omega)$$
definita da $\sigma \mapsto \sigma_{|K}$ è suriettiva.

(2) Sia $\delta \colon K \hookrightarrow \Omega$ un F-omomorfismo e indichiamo con Ω_δ ilc ampo Ω visto come estensione $K \subset \Omega$ tramite δ. Mostrare che
$$p^{-1}(\delta) = Hom_K(L, \Omega_\delta).$$

(3) Si mostri che $\#p^{-1}(\delta)$ non dipende dalla scelta di $\delta \in Hom_F(K, \Omega)$.

Soluzione: (1) Supponiamo per cominciare che $L = K(x) \simeq \frac{K[X]}{(f_{x,K}(X))}$ sia semplice. Se $\delta \in Hom_F(K, \Omega)$, indichiamo con $R_{\delta(f_{x,K})} \subset \Omega$ l'insieme delle radici di $\delta(f_{x,K})$ e con Ω_δ la K-algebra $\delta : K \hookrightarrow \Omega$. Se $\alpha \in R_{\delta(f_{x,K})} \subset \Omega$ è una radice di $\delta(f_{x,K})$, allora l'omomorfismo di K-algebre $\psi_\alpha : K[X] \to \Omega_\delta$ such that $\psi_\alpha(X) = \alpha$ soddisfa la relazione
$$\psi_\alpha(f_{x,K}(X)) = \psi_\alpha(f_{x,K})\,\psi_\alpha(X) = \delta(f_{x,K})(\alpha) = 0$$
e, dunque, induce un omomorfismo di K-algebre
$$\overline{\psi_\alpha} : K(x) \simeq \frac{K[X]}{(f_{x,K}(X))} \to \Omega_\sigma.$$
Allora $\overline{\psi_\alpha} \in Hom_K(L, \Omega_\delta) \subset Hom_F(L, \Omega)$ è tale che $\overline{\psi_\alpha}_{|K} = \sigma$ e $\overline{\psi_\alpha}(x) = \alpha$, mostrando che p è suriettiva.

Infine supponiamo che L/K sia algebrica e, dato $\delta \in Hom_{F-\mathrm{alg}}(K, \Omega)$, consideriamo l'insieme S_δ formato dalle coppie (K', σ') tali che $K \subset K' \subset L$ e $\sigma' \in Hom_F(K', \Omega)$ è tale che e $\sigma'_{|K} = \delta$. Scriviamo $(K', \sigma') \leq (K'', \sigma'')$ se $K' \subset K''$ e $\sigma''_{|K'} = \sigma'$: otteniamo in questo modo una relazione d'ordine in S_δ, che è non vuoto poichè $(K, \delta) \in S_\delta$. Data una catena $\{(K_i, \sigma_i)\}_{i\in I}$, posto $K' := \bigcup_{i\in I} K_i$ e $\sigma'(x) := \sigma_i(x)$ se $x \in K_i$, otteniamo $(K', \sigma') \in S_\delta$ tale che $(K_i, \sigma_i) \leq (K', \sigma')$ per ogni $i \in I$. Per il lemma di Zorn esiste un elemento massimale che indichiamo ancora con (K', σ') in S_δ. Se $K' \subsetneqq L$, possiamo considerare l'estensione semiplice $K'(x)/K'$ ed applicare quanto appena mostrato per affermare che esiste una estensione σ'' di σ' a $K'' = K'(x)$. Avremmo $(K', \sigma') < (K'', \sigma'')$ e questa contraddizione mostra che $K' = L$. Abbiamo dunque mostrato che $\exists \sigma' \in Hom_F(L, \Omega)$ tale che $\sigma'_{|K} = \delta$.

(2) Infatti, se $\delta \in Hom_F(K, \Omega)$, allora
$$p^{-1}(\delta) = \left\{\sigma \in Hom_F(L, \Omega) : \sigma_{|K} = \delta\right\} = Hom_K(L, \Omega_\delta),$$
dove la prima uguaglianza è la definizione e la seconda segue dal fatto che la F-algebra $\sigma : L \hookrightarrow \Omega = \Omega_\delta$ è una K-algebra se e solo se $\alpha \cdot_\sigma x = \alpha \cdot_\delta x$ per ogni $\alpha \in K$ ed $x \in \Omega$, ovvero
$$\sigma(\alpha)\, x = \alpha \cdot_\sigma x = \alpha \cdot_\delta x = \delta(\alpha)\, x.$$
Ma basta infatti verificare questa relazione per $x = 1_\Omega$, essendo poi
$$\sigma(\alpha)\, x = \sigma(\alpha)\, 1_\Omega x = \delta(\alpha)\, 1_\Omega x = \delta(\alpha)\, x.$$
Dunque σ è un omomorfismo di K-algebre se e solo se $\sigma_{|K} = \delta$.

(3) Se $\Omega_F \subset \Omega$ è l'insieme degli elementi di Ω che sono algebrici su F, allora Ω_F è una chiusura algebrica di F e tutti gli omomorfismi di F-algebre $\sigma : L \to \Omega$ tali che L/F è algebrica sono tali che $\sigma(L) \subset \Omega_F$. Possiamo dunque supporre che $\Omega = \Omega_F$ sia una chiusura algebrica di F.

Siano $\delta_1, \delta_2 \in Hom_F(K, \Omega)$ e consideriamo

$$\delta_{\delta_2,\delta_1^{-1}} : \delta_1(K) \overset{\delta_1^{-1}}{\to} K \overset{\delta_2}{\to} \Omega.$$

Per (1) (applicato a $F \subset \delta_1(K) \subset \Omega$) esiste $\sigma_{\delta_2,\delta_1^{-1}} \in Hom_F(\Omega, \Omega)$ tale che $\sigma_{\delta_2,\delta_1^{-1}|\delta_1(K)} = \delta_{\delta_2,\delta_1^{-1}}$. Consideriamo quindi l'associazione

$$\sigma_{\delta_2,\delta_1^{-1}*} : \left\{\sigma \in Hom_{F-\text{alg}}(L, \Omega) : \sigma_{|K} = \delta_1\right\} \to \left\{\sigma \in Hom_F(L, \Omega) : \sigma_{|K} = \delta_2\right\}$$

definita dalla regola $\sigma_{\delta_2,\delta_1^{-1}*}(\sigma) := \sigma_{\delta_2,\delta_1^{-1}} \circ \sigma$. E' ben definita poichè

$$\begin{aligned} \sigma_{\delta_2,\delta_1^{-1}} \circ \sigma_{|K} &= \sigma_{\delta_2,\delta_1^{-1}} \circ \delta_1 = \sigma_{\delta_2,\delta_1^{-1}|\delta_1(K)} \circ \delta_1 = \delta_{\delta_2,\delta_1^{-1}} \circ \delta_1 \\ &= \delta_2 \circ \delta_1^{-1} \circ \delta_1 = \delta_2. \end{aligned}$$

E' una biiezione poichè $\sigma^{-1}_{\delta_2,\delta_1^{-1}}$ è tale che $\sigma^{-1}_{\delta_2,\delta_1^{-1}|\delta_1(K)} = \delta_{\delta_1,\delta_2^{-1}}$ e, quindi, $\sigma^{-1}_{\delta_2,\delta_1^{-1}*}(\sigma) := \sigma^{-1}_{\delta_2,\delta_1^{-1}} \circ \sigma$ definisce una applicazione inversa di $\sigma_{\delta_2,\delta_1^{-1}*}$.

Esercizio 4. (*Teo. Num*) Siano $F \subset K \subset L$ estensioni di campi di numeri. Siano $\mathcal{P} \subset \mathcal{O}_F$, $\mathcal{Q} \subset \mathcal{O}_K$ e $\mathcal{T} \subset \mathcal{O}_L$ ideali primi non nulli tali che $\mathcal{P} \subset \mathcal{Q} \subset \mathcal{T}$.

(1) Definire l'indice di ramificazione $e(\mathcal{Q}/\mathcal{P})$ e l'indice di inerzia $f(\mathcal{Q}/\mathcal{P})$.
(2) Dimostrare la moltiplicatività $e(\mathcal{T}/\mathcal{P}) = e(\mathcal{T}/\mathcal{Q})e(\mathcal{Q}/\mathcal{P})$ e $f(\mathcal{T}/\mathcal{P}) = f(\mathcal{T}/\mathcal{Q})f(\mathcal{Q}/\mathcal{P})$.
(3) Dato un ideale primo non nullo $\mathcal{Q} \subset \mathcal{O}_K$ mostrare che esiste un unico ideale primo non nullo $\mathcal{P}$ di $\mathcal{O}_F$ tale che $\mathcal{P} = \mathcal{O}_F \cap \mathcal{Q}$.

Soluzione: Per (1) e (2) vedere le Definizioni 6.2 e 6.6 e il lemma 6.7 delle Note. Per (3) vedere la Proposizione 6.5.

Esercizio 5. Sia K il 20mo campi ciclotomico.

(1) Determinare tutti e soli i primi $p \in \mathbf{Z}$ che ramificano in $\mathcal{O}_K$.
(2) Determinare la decomposizione di $5\mathcal{O}_K$ come prodotto di ideali primi di $\mathcal{O}_K$.

Soluzione: Sappiamo dal Teorema 6.10 che $p \in \mathbf{Z}$ ramifica in $\mathcal{O}_K$ se e solos e divide il discriminante $\Delta_{K/\mathbf{Q}}$. Inoltre il lemma 4.16 implica che $\Delta_{K/\mathbf{Q}}$ divide $n^{\varphi(n)}$ con $n = 20$. Quindi tutti i primi $p \neq 2, 5$ non ramificano.

Sia $F = \mathbf{Q}(i)$ il 4^o campo ciclotomico e sia $L = \mathbf{Q}(\zeta)$ il 5^o campo ciclotomico (qui $i = \sqrt{-1}$ e ζ è una radice primitiva di ordine 5 dell' unitaà). Allora $K = F \cdot L$. Infatti $F \subset K$ e $L \subset K$ ed inoltre $i \cdot \zeta$ è una radice primitiva di ordine 10 dell' unitaà. Quindi $K \subset F \cdot L$.

Grazie al Corollario 6.13 abbiamo $5\mathcal{O}_L = \mathcal{P}^4$ con $\mathcal{P} = (5, \zeta - 1)$. Quindi 5 ramifica in $\mathcal{O}_L$ e quindi anche in $\mathcal{O}_K$ per moltiplicatività degli indici di ramificazione. Segue dal corollario 6.12 che $2\mathcal{O}_F = \mathcal{Q}^2$ con $\mathcal{Q} = (2, i-1)$. Quindi 2 ramifica in $\mathcal{O}_F$ ed anche in $\mathcal{O}_K$ per moltiplicatività degli indici di ramificazione.

Quindi i primi che ramificano in $\mathcal{O}_K$ sono 2 e 5.

Grazie al Corollario 6.13 sappiamo che $\mathcal{O}_L/\mathcal{P} = \mathbf{F}_5$. Segue dal Corollario 4.13 che, essendo i discriminati di F ed L relativamente a $\mathbf{Q}$ coprimi, allora $\mathcal{O}_K = \mathcal{O}_L[i] \cong \mathcal{O}_L[X]/(X^2+1)$. Osservo che $X^2+1 = (X+2)(x-2)$ in $\mathbf{F}_5$. Quindi il teorema 6.8 implica che $\mathcal{P}\mathcal{O}_K$ è il prodotto di due primi distinti $\mathcal{Q}_1\mathcal{Q}_2$ di $\mathcal{O}_K$, con $\mathcal{Q}_1 = \mathcal{P}\mathcal{O}_K + (i-2)\mathcal{O}_K$ e $\mathcal{Q}_1 = \mathcal{P}\mathcal{O}_K + (i+2)\mathcal{O}_K$.

Concludo che $5\mathcal{O}_K = \mathcal{Q}_1^4\mathcal{Q}_2^4$.