SOLUZIONI DEL COMPITINO DEL 20/02/2018

Esercizio 1. Si consideri il polinomio $f(X) = X^7 - 3 \in \mathbb{Q}[X]$ e sia E un suo campo di spezzamento su $\mathbb{Q}$.

(1) Mostrare che E è un' estensione di Galois di $\mathbb{Q}$. Determinare il grado $[E : \mathbb{Q}]$.
(2) Sia G il gruppo di Galois di E su $\mathbb{Q}$. Mostrare che è un prodotto semidiretto, ma non diretto di gruppi abeliani.
(3) Determinare dei generatori di G e descrivere gli elementi di G utilizzando i generatori dati.
(4) Determinare il numero ed esibire dei generatori delle estensioni $\mathbb{Q} \subset M \subset E$ di grado 21 su $\mathbb{Q}$.

Soluzione: 1) Sia $\alpha = 3^{\frac{1}{7}}$ e ζ una radice primitiva settima dell'unità. Allora $E = M \cdot N$ con $M = \mathbb{Q}(\alpha)$ e $K = \mathbb{Q}(\zeta)$. Infatti le radici si $f(X)$ sono $\alpha_i := \zeta^i \alpha$ con $i = 0, \dots, 6$. Quindi $E \subset M \cdot K$. Ma $\zeta = \alpha_1/\alpha \in E$ e quindi $M \cdot K \subset E$. Abbiamo $[M : \mathbb{Q}] = 7$ in quanto α ha come plinomio minimo $X^7 - 3$ che è irriducibile per Esisnsetin per $p = 3$. Inoltre K ha grado $\phi(7) = 6$ su $\mathbb{Q}$ essendo il 6 campo ciclotomico. L'intersezione $M \cap K$ ha grado su $\mathbb{Q}$ che divide sia 6 che 7 per moltiplciatività dei gradi. Quindi $M \cap K = \mathbb{Q}$. Siccome $\mathbb{Q} \subset K$ è di Galois, sappiamo che $[E : \mathbb{Q}] = 6 \cdot 7 = 42$.

2)-3) Sia $N = \mathrm{Gal}(E/K)$. Essendo $\mathbb{Q} \subset K$ di Galois, si tratta di un sottogruppo normale di G. Consideriamo l'applicazione

$$N \to \mu_7 \cong \mathbb{Z}/7\mathbb{Z},$$

dove la prima freccia invia $\sigma \mapsto \sigma(\alpha)/\alpha$ è un omomorfismo iniettivo di gruppi e quindi un isomorfismo per questioni di cardinalità. Quindi N è ciclico di ordine 7 con generatore l'automorfismo σ che fissa ζ e invia $\alpha \mapsto \zeta\alpha$.

Sia $H = \mathrm{Gal}(E/M)$. Consideriamo l'applicazione

$$H \subset G \to G/N = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Aut}(\mu_7) \cong \left(\mathbb{Z}/7\mathbb{Z}\right)^* \cong \mathbb{Z}/6\mathbb{Z},$$

dove la freccia $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Aut}(\mu_7)$ invia $\tau \mapsto \tau(\zeta)$. È un omomorfismo initettivo di gruppi e per questioni di cardinalità è un isomorfismo. Quindi H è ciclico di ordine 6 con generatore l'automorfismo τ che fissa α e invia $\zeta \mapsto \zeta^3$ vsto che 3 genera il gruppo moltiplicativo $(\mathbb{Z}/7\mathbb{Z})^*$.

Osserviamo che $H \cap N = \{1\}$. Segue allora che G è prodotto semidiretto di N ed H. Non è prodotto diretto perchè altrimenti sarebbe abeliano ed ogni sottocampo di E sarebbe di Galois su $\mathbb{Q}$; questo non è vero considerando as esempio il sottoampo N.

In particolare l'applicazione $N \times H \to G$, che invia $(n, h) \mapsto n \circ h$, è biettiva ed ogni elemento di g si scrive allora come $\sigma^i \circ \tau^j$ per unici $0 \le i \le 6$ e $0 \le j \le 5$.

4) Per il Teorema Fondamentale della Teoria di Galois tali sottocampi sono in corrispondenza biunivoca con i sottogruppi di G di ordine 2, ovvero con gli elementi di G di ordine 2. Dato un generico elemento $g = \sigma^i \circ \tau^j$ di G abbiamo $g^2 = \left(\sigma^i \tau^j \sigma^i \tau^{-j}\right) \circ \tau^{2j}$. Inoltre $\tau^j \sigma^i \tau^{-j} = \left(\tau^j \sigma \tau^{-j}\right)^i$ e $\tau^j \sigma \tau^{-j} = \sigma^{3^j}$ visto che entrambi sono elementi di N che agiscono nello stesso modo su α. Quindi $g^2 = 1$ se e solo se (a) $2j \equiv 0$ modulo 6, ovvero $j = 0$ oppure $j = 3$ (b) $\sigma^i \tau^j \sigma^i \tau^{-j} = \sigma^{i(3^j+1)} = 1$ ovvero $i(3^j + 1) \equiv 0$ modulo 7. Siccome cerco elementi $g \neq 1$ tali che $g^2 = 1$ devo avere $j = 3$ in (a) e quindi i arbitrario.

Quindi gli elementi di ordine due cercati sono 7 e sono tutti e soli della forma $g = \sigma^i \tau^3$ con $0 \le i \le 6$. Per ciascuno il sottocampo associato degli elementi invarianti di E è $\mathbb{Q}(\zeta + \overline{\zeta}, \zeta^i \alpha)$.

Esercizio 2. [*Esonero*] Sia $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \subset \mathbb{C}$ e sia $L \subset \mathbb{C}$ il 12^o campo ciclotomico. Sia $E := K \cdot L$ il campo composto di K ed L in $\mathbb{C}$.

(1) Si mostri che i campi K, L ed E sono estensioni di Galois di $\mathbb{Q}$. Per ciascuno se ne calcoli il grado su $\mathbb{Q}$.
(2) Si descrivano i gruppi di Galois $\mathrm{Gal}(K/\mathbb{Q})$ e $\mathrm{Gal}(L/\mathbb{Q})$.
(3) Si determini il gruppo di Galois $\mathrm{Gal}(E/\mathbb{Q})$.

Soluzione: Osservo che K è il composto dei due campi quadratici $M = \mathbb{Q}(\sqrt{2})$ e di $N = \mathbb{Q}(\sqrt{3})$. Si dimostra che $M \cap N = \mathbb{Q}$. Altrimenti per questioni di gradi $M = N = K$ e $\sqrt{3}$ si scriverebeb nelal forma $a + b\sqrt{2}$ con a e $b \in \mathbb{Q}$ (assurdo).

Essendo K il campo composto di due estensioni galoisiane, ovvero M ed N, di $\mathbb{Q}$ con intersezione $M \cap N = \mathbb{Q}$ ho $[K : \mathbb{Q}] = 4$. Inoltre il gruppo di Galois è isomorfo al prodotto

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(M/\mathbb{Q}) \times \mathrm{Gal}(N/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z});$$

il primo isomorfismo manda $\sigma \mapsto (\sigma|_M, \sigma|_N)$.

Anche L, essendo un campo ciclotomico, è di Galois su $\mathbb{Q}$ con gruppo di Galois

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Aut}(\mu_{12}) \cong \left(\mathbb{Z}/12\mathbb{Z}\right)^* \cong \left(\mathbb{Z}/3\mathbb{Z}\right)^* \times \left(\mathbb{Z}/4\mathbb{Z}\right)^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}),$$

il gruppo di Klein. Infatti L è il campo composto del 4 quarto campo ciclotomico $A := \mathbb{Q}(i)$ e del 3 campo ciclotomico $B := \mathbb{Q}(\sqrt{-3})$: li contiene entrambi e $i \cdot \zeta_3$, con $\zeta_3 = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ radice primitiva terza dell'unità, è radice primitiva di ordine 12 dell'unità. In particolare L contiene $\mathbb{Q}(\sqrt{3})$ che coincide con $\mathbb{R} \cap L = K \cap L$. In particolare $[E : \mathbb{Q}] = \frac{[K:\mathbb{Q}][L:\mathbb{Q}]}{2} = 8$

Concludo allora che E è il campo composto $\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$ e

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathrm{Gal}(M/\mathbb{Q}) \times \mathrm{Gal}(N/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

Esercizio 3. [*TeoGal*] Sia $K \subset L$ una estensione di campi finiti.

(1) Si mostri che $K \subset L$ è una estensione di Galois.
(2) Si dimostri che esiste $\alpha \in L$, radice dell'unità, tale che $L = K(\alpha)$.
(3) Si mostri che il gruppo $\mathrm{Gal}(L/K)$ è ciclico e se ne esibisca un generatore.

Soluzione: Necessariamente K ed L devono avere caratteristica positiva p. Sia $[K : \mathbb{F}_p] = h$ e $[L : K] = n$. Allora $|L| = q = p^{nh}$. In particolare L^* è un gruppo moltiplicativo, ciclico, di ordine $q - 1$. Segue che L è il campo di spezzamento di $X^q - X \in \mathbb{F}_p[X]$. in particolare $\mathbb{F}_p \subset L$ è una estensione di Galois e quindi anche $K \subset L$ è di Galois.

Inoltre se α è un generatore di L^* allora $L = \mathbb{F}_p(\alpha) = K(\alpha)$.

Sia $\varphi\colon L \to L$, $z \mapsto z^p$, l'automorfismo di Frobenius. Siccoem $L^{\varphi=1} = \mathbb{F}_p$, segue dal Teorema Fondamentale della Teoria di Galois che φ genera il gruppo $G := \mathrm{Gal}(L/\mathbb{F}_p)$ che quindi risulta essere ciclico di ordine nh. Il sottogruppo $H = \mathrm{Gal}(L/K) \subset G$ è anch'esso ciclico di ordine n. Quindi H è generato da φ^h.

Esercizio 4. Sia $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.

(1) Si calcoli l'anello degli interi di tutte le sottoestensioni quadratiche F di K.
(2) Si mostri che, dato $\alpha \in K$, si ha $\alpha \in \mathcal{O}_K$ se e solo se $\mathrm{Tr}_{K/F}(\alpha), \mathrm{N}_{K/F}(\alpha) \in \mathcal{O}_F$ per una o equivalentemente per tutte le sottoestensioni quadratiche di K.
(3) Si mostri che $\mathcal{O}_K \subset \frac{\mathbb{Z}+\mathbb{Z}\sqrt{2}+\mathbb{Z}\sqrt{3}+\mathbb{Z}\sqrt{6}}{4}$.
(4)* Si mostri che

$$\mathcal{O}_K = \left\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, c \in \mathbb{Z},\, b, d \in \frac{\mathbb{Z}}{2} \text{ e } b - d \in \mathbb{Z} \right\}$$

(Suggerimento. Prima si mostri che $\mathcal{O}_K \subset \frac{\mathbb{Z}+\mathbb{Z}\sqrt{2}+\mathbb{Z}\sqrt{3}+\mathbb{Z}\sqrt{6}}{2}$. Poi si scriva $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, si consideri

$$\mathrm{N}_{K/\mathbb{Q}(\sqrt{3})}(\alpha) = \left(a^2 - 2b^2 + 3c^2 - 6d^2\right) + (2ac - 4bd)\sqrt{3}$$

e si mostri che, se $\alpha \in \mathcal{O}_K$, allora $a, c \in \mathbb{Z}$ e che $b - d \in \mathbb{Z}$. Quindi si mostri che tali condizioni, insieme all'inclusione, sono anche sufficienti).

Soluzione: (1) Dalla teoria di Galois sappiamo che le sottoestensioni quadratiche di K sono 3: dunque $F \in \left\{\mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}\left(\sqrt{3}\right), \mathbb{Q}\left(\sqrt{6}\right)\right\}$, essendo queste tre distinte sottoestensioni di K. Sappiamo anche che, poichï¿½ $2 = 6$ modulo 4 e $3 = 3$ modulo 4, $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}\left[\sqrt{2}\right]$, $\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}\left[\sqrt{3}\right]$ e $\mathcal{O}_{\mathbb{Q}(\sqrt{6})} = \mathbb{Z}\left[\sqrt{6}\right]$.

(2) Basta applicare l'esercizio di teoria, notando che

$$f_{\alpha,K/F}(X) = X^2 - \mathrm{Tr}_{K/F}(\alpha)\, X + \mathrm{N}_{K/F}(\alpha).$$

$(3-4)$ Dalla teoria di Galois sappiamo che

$$K = \mathbb{Q} + \mathbb{Q}\sqrt{2} + \mathbb{Q}\sqrt{3} + \mathbb{Q}\sqrt{6}$$

e dunque scriviamo $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ con $a, b, c, d \in \mathbb{Z}$. Sappiamo anche dalla teoria di Galois che, essendo $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ e $\mathbb{Q}\left(\sqrt{3}\right)/\mathbb{Q}$ due estensioni di Galois con intersezione banale, abbiamo $G_{K/\mathbb{Q}} \simeq G_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} \times G_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}$, da cui vediamo che $G_{K/\mathbb{Q}} = \{1, \sigma_2, \sigma_3, \sigma_{2,3} = \sigma_2\sigma_3\}$ dove $\sigma_2\left(\sqrt{2}\right) = -\sqrt{2}$, $\sigma_2\left(\sqrt{3}\right) = \sqrt{3}$ (dunque $\sigma_2\left(\sqrt{6}\right) = -\sqrt{6}$), $\sigma_3\left(\sqrt{2}\right) = \sqrt{2}$, $\sigma_3\left(\sqrt{3}\right) = -\sqrt{3}$ (dunque $\sigma_3\left(\sqrt{6}\right) = -\sqrt{6}$) e $\sigma_{2,3}\left(\sqrt{2}\right) = -\sqrt{2}$, $\sigma_{2,3}\left(\sqrt{3}\right) = -\sqrt{3}$ (dunque $\sigma_{2,3}\left(\sqrt{6}\right) = \sqrt{6}$). Dunque

$$\sigma_3\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

e, poichï¿½ $\langle\sigma_3\rangle = G_{K/\mathbb{Q}(\sqrt{2})}$, vediamo che

$$\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{2})}(\alpha) = 2a + 2b\sqrt{2}$$

(e

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}(\sqrt{2})}(\alpha) &= \left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right)\left(a + b\sqrt{2} - \left(c\sqrt{3} + d\sqrt{6}\right)\right) \\
&= \left(a + b\sqrt{2}\right)^2 - \left(c\sqrt{3} + d\sqrt{6}\right)^2 \\
&= \left(a^2 + 2\sqrt{2}ab + 2b^2\right) - \left(3c^2 + 6\sqrt{2}cd + 6d^2\right) \\
&= \left(a^2 + 2b^2 - 3c^2 - 6d^2\right) + (2ab - 6cd)\sqrt{2}.)
\end{aligned}$$

Similmente (abbiamo $\langle\sigma_2\rangle = G_{K/\mathbb{Q}(\sqrt{3})}$, $\langle\sigma_{2,3}\rangle = G_{K/\mathbb{Q}(\sqrt{6})}$, $\sigma_2\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$ e $\sigma_{2,3}\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$):

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{3})}(\alpha) &= 2a+2c\sqrt{3},\\
\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{6})}(\alpha) &= 2a+2d\sqrt{6},\\
\mathrm{N}_{K/\mathbb{Q}(\sqrt{3})}(\alpha) &= \left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)\left(a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}\right)\\
&= \left(a+c\sqrt{3}\right)^2-\left(b\sqrt{2}+d\sqrt{6}\right)^2\\
&= \left(a^2+2\sqrt{3}ac+3c^2\right)-\left(2b^2+4\sqrt{3}bd+6d^2\right)\\
&= \left(a^2-2b^2+3c^2-6d^2\right)+\left(2ac-4bd\right)\sqrt{3},\\
(\mathrm{N}_{K/\mathbb{Q}(\sqrt{6})}(\alpha) &= \left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)\left(a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}\right)\\
&= \left(a+d\sqrt{6}\right)^2-\left(b\sqrt{2}+c\sqrt{3}\right)^2\\
&= \left(a^2+2\sqrt{6}ad+6d^2\right)-\left(2b^2+2\sqrt{6}bc+3c^2\right)\\
&= \left(a^2-2b^2-3c^2+6d^2\right)+\left(2ad-2bc\right)\sqrt{6}.)
\end{aligned}$$

Guardando alle tracce vediamo subito che $\alpha\in\mathcal{O}_K$ implica $a,b,c,d\in\frac{\mathbb{Z}}{2}$ grazie a (1), dunque vale l'inclusione in (3) grazie a (2). Imponiamo altre condizioni necessarie perchï¿½ sia $\alpha\in\mathcal{O}_K$ guardando a $\mathrm{N}_{K/\mathbb{Q}(\sqrt{3})}(\alpha)$ ed utilizzando ancora (1) e (2). Abbiamo $2ac-4bd\in\mathbb{Z}$, dunque $ac\in\frac{1}{2}\left(\mathbb{Z}+4\frac{\mathbb{Z}}{4}\right)=\frac{\mathbb{Z}}{2}$ e vediamo che $a\in\mathbb{Z}$ oppure $c\in\mathbb{Z}$, perchï¿½ altrimenti $a=\frac{a'}{2}, c=\frac{c'}{2}\in\frac{\mathbb{Z}}{2}-\mathbb{Z}$ con a',c' interi coprimi con 2, da cui $ac=\frac{a'c'}{4}\in\frac{\mathbb{Z}}{4}-\frac{\mathbb{Z}}{2}$. Supponiamo che $a\in\mathbb{Z}$ (risp. $c\in\mathbb{Z}$) e notiamo, ancora guardando a $\mathrm{N}_{K/\mathbb{Q}(\sqrt{3})}(\alpha)$, che abbiamo $c^2=2b^2+6d^2-a^2\in\frac{1}{3}\left(2\frac{\mathbb{Z}}{4}+2\frac{\mathbb{Z}}{4}+\mathbb{Z}\right)=\frac{\mathbb{Z}}{6}$ (risp. $a^2=2b^2+6d^2-3c^2\in 2\frac{\mathbb{Z}}{4}+2\frac{\mathbb{Z}}{4}+\mathbb{Z}=\frac{\mathbb{Z}}{2}$) e vediamo che $c\in\mathbb{Z}$ (risp. $a\in\mathbb{Z}$), perchï¿½ altrimenti scriviamo $c=\frac{c'}{2}$ (risp. $a=\frac{a'}{2}$) come prima e vediamo che $3c^2=\frac{3c'^2}{4}\in\frac{\mathbb{Z}}{4}-\frac{\mathbb{Z}}{2}$ (risp. $a^2=\frac{a'^2}{4}\in\frac{\mathbb{Z}}{4}-\frac{\mathbb{Z}}{2}$) mentre $\left(\frac{\mathbb{Z}}{4}-\frac{\mathbb{Z}}{2}\right)\cap\frac{\mathbb{Z}}{6}=\phi$. Dunque $a,c\in\mathbb{Z}$ e allora la relazione $a^2-2b^2+3c^2-6d^2\in\mathbb{Z}$ implica che $2b^2+6d^2\in\mathbb{Z}$. Scriviamo $b=\frac{b'}{2}$ e $d=\frac{d'}{2}$ con $b',d'\in\mathbb{Z}$. Allora

$$\frac{b'^2}{2}+3\frac{d'^2}{2}=2b^2+6d^2\in\mathbb{Z}\Leftrightarrow b'^2+3d'^2\in 2\mathbb{Z}.$$

Dunque troviamo la relazione $b'^2+d'^2=b'^2+3d'^2=0$ modulo 2 e ciï¿½ï¿½ ï¿½ï¿½ possibile se e solo se $(b',d')\in\{(0,0),(1,1)\}$, ovvero se e solo se $b'=d'$ modulo 2. Ciï¿½ï¿½ significa che $b-d\in\mathbb{Z}$. In altre parole, abbiamo mostrato che

$$\mathcal{O}_K\subset\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}: a,c\in\mathbb{Z},\ b,d\in\frac{\mathbb{Z}}{2}\text{ e }b-d\in\mathbb{Z}\right\}=:A.$$

Per mostrare che si ha l'uguaglianza notiamo che, se $\alpha\in A$, allora $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{3})}(\alpha)\in\mathbb{Z}$ e $\mathrm{N}_{K/\mathbb{Q}(\sqrt{3})}(\alpha)\in\mathbb{Z}$ e quindi applichiamo (1) e (2). Ciï¿½ï¿½ chiaro per le tracce e, per quanto riguarda la norma, essendo $a,c\in\mathbb{Z}$, $b,d\in\frac{\mathbb{Z}}{2}$ vediamo che $2ac-4bd\in\mathbb{Z}$. Inoltre, poichï¿½ $a^2+3c^2\in\mathbb{Z}$, si ha $a^2-2b^2+3c^2-6d^2\in\mathbb{Z}$ se e solo se $2b^2+6d^2\in\mathbb{Z}$. Ma poichï¿½ $b,d\in\frac{\mathbb{Z}}{2}$, possiamo scrivere $b=\frac{b'}{2}$ e $d=\frac{d'}{2}$ con $b',d'\in\mathbb{Z}$ e vediamo che l'argomento precedente si inverte: abbiamo infatti mostrato che $2b^2+6d^2\in\mathbb{Z}\Leftrightarrow b'^2+3d'^2\in 2\mathbb{Z}$ e, riducendo questa equazione modulo 2, abbiamo visto che essa ï¿½ï¿½ equivalente a $b'=d'$ modulo 2, ovvero $b-d\in\mathbb{Z}$.

Esercizio 5. [*TeoNum*] Sia E/F una estensione di campi di numeri, sia $\alpha \in E$ e siano $f_{\alpha,F} \in F[X]$ ed $f_{\alpha,E/F} \in F[X]$, rispettivamente, il polinomio minimo di α su F ed il suo polinomio caratteristico relativo alla estensione E/F.

(1) Si mostri che $\alpha \in \mathcal{O}_E$ se e solo se $\exists f \in \mathcal{O}_F[X]$ monico tale che $f(\alpha) = 0$.
(2) Si mostri che $\alpha \in \mathcal{O}_E$ se e solo se $f_{\alpha,F} \in \mathcal{O}_F[X]$.
(3) Si mostri che $\alpha \in \mathcal{O}_E$ se e solo se $f_{\alpha,E/F} \in \mathcal{O}_F[X]$.

Soluzione: (1) Per definizione, se $\alpha \in \mathcal{O}_E$ allora $\exists f \in \mathbb{Z}[X] \subset \mathcal{O}_F[X]$ monico tale che $f(\alpha) = 0$ e dunque l'implicazione $\Rightarrow$ ï¿½ ovvia. Viceversa, supponiamo che $\exists f \in \mathcal{O}_F[X]$ monico tale che $f(\alpha) = 0$, diciamo di grado n. Poichï¿½ i coefficienti (non nulli) di questo polinomio sono interi algebrici e sono in numero finito, per la Proposizione 2.4 abbiamo che $f(X) \in A[X]$, dove $A \subset \mathbb{C}$ ï¿½ un anello il cui gruppo additivo ï¿½ finitemante generato (sappiamo infatti, per motivi meno elementari spiegati nel Teorema 4.5, che possiamo prendere $\mathcal{O}_F$ stesso) e vediamo che

$$\alpha^n \in A\alpha^{n-1} + ... + A\alpha.$$

Deduciamo che $\mathbb{Z}[\alpha] \subset A\alpha^{n-1} + ... + A\alpha$ ï¿½ contenuto in un gruppo finitamente generato e dunque, il suo gruppo additivo ï¿½ esso stesso finitemente generato. Segue che $\alpha \in \overline{\mathbb{Z}} \cap E =: \mathcal{O}_E$. (Alternativamente, se $\alpha = \alpha_0$,

$$f(X) = (X - \alpha_0)...(X - \alpha_n) \in \mathcal{O}_F[X]$$

e se $L/\mathbb{Q}$ ï¿½ una estensione di Galois finita che contiene E, vediamo che α soddisfa anche il polinomio monico

$$\prod_{\sigma \in G_{L/\mathbb{Q}}} (X - \sigma(\alpha_0))...(X - \sigma(\alpha_n)).$$

Essendo prodotto dei polinomi $\prod_{\sigma \in G_{L/\mathbb{Q}}} (X - \sigma(\alpha_i)) \in \mathbb{Q}[X]$ ha coefficienti in $\mathbb{Q}$ ed essendo prodotto dei polinomi $\prod_i (X - \sigma(\alpha_i)) \in \sigma(\mathcal{O}_E)[X] \subset \overline{\mathbb{Z}}[X]$ ha coefficienti in $\overline{\mathbb{Z}}$ (infatti si verifica facilmente che $\sigma(\mathcal{O}_E) \subset \overline{\mathbb{Z}}$, per esempio utilizzando la Proposizione 2.4). Dunque ha coefficienti in $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$ e vediamo che $\alpha \in \mathcal{O}_E$).

(2) Se $\alpha \in \mathcal{O}_E$, esiste $\exists f \in \mathbb{Z}[X] \subset F[X]$ monico tale che $f(\alpha) = 0$. Dunque possiamo scrivere $f = f_{\alpha,F} \cdot h$ con $f_{\alpha,F}, h \in F[X]$. Ma allora vediamo che le radici di $f_{\alpha,F}$, essendo radici di f, sono in $\overline{\mathbb{Z}}$ e, poichï¿½ $\overline{\mathbb{Z}}$ ï¿½ anello, deduciamo che i coefficienti di $f_{\alpha,F}$ sono in $\overline{\mathbb{Z}}$, dunque in $\overline{\mathbb{Z}} \cap F =: \mathcal{O}_F$ (alternativamente, la relazione $f_{\alpha,F} \cdot h = f \in \mathbb{Z}[X] \subset \mathcal{O}_F[X]$ con f ed $f_{\alpha,F}$ monici ed una opportuna generalizzazione del lemma di Gauss implica che $f_{\alpha,F} \in \mathcal{O}_F[X]$). Viceversa, se $f_{\alpha,F} \in \mathcal{O}_F[X]$ possiamo applicare (1) per dedurre che $\alpha \in \mathcal{O}_E$.

(3) Sappiamo che vale la formula (Proposizione 3.7):

$$f_{\alpha,E/F} = \prod_{\sigma} (X - \sigma(\alpha))$$

dove σ varia tra gli F-omomorfismi $\sigma : E \hookrightarrow \mathbb{C}$. Dunque vediamo che, se $\alpha \in \mathcal{O}_E$, $f_{\alpha,E/F} \in A[X] \subset \overline{\mathbb{Z}}[X]$ con A l'anello generato dagli anelli $\sigma(\mathcal{O}_E)$ (infatti si verifica facilmente che $\sigma(\mathcal{O}_E) \subset \overline{\mathbb{Z}}$, per esempio utilizzando la Proposizione 2.4 e quindi $A \subset \overline{\mathbb{Z}}$, essendo $\overline{\mathbb{Z}}$ anello).

(Alternativamente. Ricordiamo che $f_{\alpha,E/F} = f_{\alpha,F}^{[E:F(\alpha)]}$ e mostriamo che, se $f, g \in F[X]$ sono tali che $g = f^n$ con g monico, allora $g \in \mathcal{O}_F[X]$ se e solo se lo $f \in \mathcal{O}_F[X]$: allora vediamo che (2) $\Leftrightarrow$ (3) e basta mostrare una sola delle due equivalenze. Una implicazione ï¿½ ovvia e, viceversa, supponiamo che $g \in \mathcal{O}_F[X]$ ï¿½ notiamo che allora tutte le radici β di g sono in $\overline{\mathbb{Z}}$ grazie ad (1) (applicato ad $E = F(\beta)$, l'elemento β ed il polinomio g); ma le radici di g ed f sono le stesse, dunque tutte le radici di f sono in $\overline{\mathbb{Z}}$ e, poichï¿½ $\overline{\mathbb{Z}}$ ï¿½ anello, f risulta avere coefficienti in $\overline{\mathbb{Z}} \cap F = \mathcal{O}_F$).