SOLUZIONI DEL COMPITINO DEL 28/01/2016

Esercizio 1. Sia E il campo di spezzamento del polinomio $X^3-4\in\mathbb{Q}[X]$ ed $F=\mathbb{Q}\left(i,\sqrt{2}\right)$.

(1) Si calcoli $[E:\mathbb{Q}]$, $[F:\mathbb{Q}]$ e $[EF:\mathbb{Q}]$.
(2) Si esibiscano $\mathbb{Q}$-basi di E, F e EF come $\mathbb{Q}$-spazi vettoriali.
(3) Si determinano i gruppi di Galois $\mathrm{Gal}_{E/\mathbb{Q}}$, $\mathrm{Gal}_{F/\mathbb{Q}}$ e $\mathrm{Gal}_{EF/\mathbb{Q}}$ come gruppi astratti.

Soluzione: (1) Il polinomio $f(X)=X^3-4\in\mathbb{Q}[X]$ è irriducibile poichè la sua riduzione modulo 7 è $f_7(X)=X^3+3$ che è irriducibile avendo grado 3 e non avendo radici (infatti $f_7(0)=3$, $f_7(1)=4$, $f_7(2)=11=4$, $f_7(3)=30=2$, $f_7(4)=67=4$, $f_7(5)=128=2$, $f_7(6)=219=2$). Posto $\zeta:=\exp\left(\frac{2\pi i}{3}\right)$ ed indicata con $\sqrt[3]{4}$ l'unica radice reale di $f(X)$, l'insieme delle radici di $f(X)$ è

$$R_f=\left\{\sqrt[3]{4},\sqrt[3]{4}\zeta,\sqrt[3]{4}\zeta^2\right\}.$$

Deduciamo che $E=\mathbb{Q}\left(\sqrt[3]{4},\zeta\right)$: infatti $\subset$ è ovvia data l'espressione di R_f e, viceversa, $\sqrt[3]{4},\zeta=\frac{\sqrt[3]{4}\zeta}{\sqrt[3]{4}}\in E$. Poichè $\left[\mathbb{Q}\left(\sqrt[3]{4}\right):\mathbb{Q}\right]=3$ e $[\mathbb{Q}(\zeta):\mathbb{Q}]=2$ (essendo $f(X)$ ed il terzo polinomio ciclotomico irriducibili su $\mathbb{Q}$), deduciamo che

$$\left[\mathbb{Q}\left(\sqrt[3]{4},\zeta\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt[3]{4}\right):\mathbb{Q}\right][\mathbb{Q}(\zeta):\mathbb{Q}]=3\cdot 2=6.$$

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 $\mathbb{Q}(i)\neq\mathbb{Q}\left(\sqrt{2}\right)$). Dunque $G_{F/\mathbb{Q}}\simeq\mathbb{F}_2\times\mathbb{F}_2$.

L'estensione $\mathbb{Q}\left(\sqrt[3]{4}\right)/\mathbb{Q}$ 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 S_3 possiede un solo sottogruppo di indice 2, che dunque corrisponde all'unica estensione quadratica $\mathbb{Q}(\zeta)/\mathbb{Q}$ in E. Le sottoestensioni proprie di $F/\mathbb{Q}$ sono tre (poichè $G_{F/\mathbb{Q}}\simeq\mathbb{F}_2\times\mathbb{F}_2$ ha tre sottogruppi propri), dunque sono $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{2}\right)$ e $\mathbb{Q}\left(\sqrt{2}i\right)$, che si verificano infatti facilmente essere tutte distinte tra loro. Notiamo che

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

Se $E\cap F/\mathbb{Q}$ fosse una estensione quadratica, dovremmo avere

$$\mathbb{Q}(\zeta)=E\cap F\in\left\{\mathbb{Q}(i),\mathbb{Q}\left(\sqrt{2}\right),\mathbb{Q}\left(\sqrt{2}i\right)\right\}.$$

Ma $\mathbb{Q}(\zeta)=\mathbb{Q}\left(\sqrt{3}i\right)$ (essendo $\zeta=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$) e da ciò si verifica facilmente che $\mathbb{Q}(\zeta)$ è distinta da $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{2}\right)$ e $\mathbb{Q}\left(\sqrt{2}i\right)$. Dunque l'unica possibilità è che si abbia $E\cap F=\mathbb{Q}$, da cui

$$[EF:\mathbb{Q}]=\frac{6\cdot 4}{1}=24.$$

(2) Una base di $\mathbb{Q}(\zeta)/\mathbb{Q}$ (risp. $\mathbb{Q}\left(\sqrt[3]{4}\right)/\mathbb{Q}$) è data da $\{1,\zeta\}$ (risp. $\left\{1,\sqrt[3]{4},\left(\sqrt[3]{4}\right)^2\right\}$). Poichè abbiamo verificato che

$$\left[\mathbb{Q}\left(\sqrt[3]{4},\zeta\right):\mathbb{Q}\right]=[\mathbb{Q}(\zeta):\mathbb{Q}]\left[\mathbb{Q}\left(\sqrt[3]{4}\right):\mathbb{Q}\right]$$

sappiamo che una $\mathbb{Q}$-base di $E = \mathbb{Q}\left(\sqrt[3]{4}, \zeta\right)$ si ottiene come prodotto delle basi:

$$\left\{1, \sqrt[3]{4}, \left(\sqrt[3]{4}\right)^2, \zeta, \sqrt[3]{4}\zeta, \left(\sqrt[3]{4}\right)^2 \zeta\right\}.$$

Per gli stessi motivi, una $\mathbb{Q}$-base di $F = \mathbb{Q}\left(i, \sqrt{2}\right)$ è data da

$$\left\{1, \sqrt{2}, i, \sqrt{2}i\right\}.$$

Ancora per gli stessi motivi deduciamo che una $\mathbb{Q}$-base di EF è data da

$$\left\{\zeta^a \left(\sqrt{2}\right)^b i^c \left(\sqrt[3]{4}\right)^d : a, b, c = 0, 1; d = 0, 1, 2\right\}.$$

(3) Poichè $E/\mathbb{Q}$ ed $F/\mathbb{Q}$ sono di Galois ed $E \cap F = \mathbb{Q}$, sappiamo che

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

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

(1) Mostrare che esistono elementi α e $\beta \in E$ tali che $E = \mathbb{Q}(\alpha, \beta)$.
(2) Trovare il grado $[E : \mathbb{Q}]$ ed esibire una base di E come $\mathbb{Q}$-spazio vettoriale.
(3) Determinare dei generatori del gruppo di Galois $G_{E/\mathbb{Q}}$ e descrivere gli elementi di $G_{E/\mathbb{Q}}$.
(4) Trovare $\eta \in E$ tale che $E = \mathbb{Q}(\eta)$.

Soluzione: (1)–(3) Indicata con α una radice di $f(X)$ sua radice e con ζ una radice primitiva 7 dell'unità, si ha $E = \mathbb{Q}(\alpha, \zeta)$. Infatti

$$R_f = \left\{\alpha\zeta^i : i = 0, ..., 6\right\},$$

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

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7.$$

D'altra parte $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$. Poichè i gradi sono coprimi, deduciamo che

$$\#G_{E/\mathbb{Q}} = [E : \mathbb{Q}] = 6 \cdot 7 = 42.$$

Consideriamo l'applicazione

$$\begin{array}{ccc} G_{E/\mathbb{Q}(\alpha)} & \to & G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \xrightarrow{\sim} Aut(\mu_7) = \left(\dfrac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times \\ \sigma & \mapsto & \sigma_{|\mathbb{Q}(\zeta)} \mapsto \sigma_{|\mu_7}. \end{array}$$

E' iniettiva e dunque suriettiva per questioni di ordine. Abbiamo che $\left(\zeta \mapsto \zeta^3\right)$ genera $Aut(\mu_7)$, poichè corrisponde alla moltiplicazione per 3 in $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times = Aut\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)$, che ha ordine 6 e dunque genera $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{6\mathbb{Z}}$:

$$1 \mapsto 3 \mapsto 3 \cdot 3 = 9 \equiv 2 \mapsto 3 \cdot 2 = 6,$$

dunque $3 \cdot (-)$ ha ordine > 3, ovvero 6, dovendo dividere 6. Dunque

$$G_{E/\mathbb{Q}(\alpha)} = \left\langle \sigma : \left\{ \begin{array}{c} \alpha \mapsto \alpha \\ \zeta \mapsto \zeta^3 \end{array} \right. \right\rangle.$$

Consideriamo ora l'applicazione

$$\varphi : G_{E/\mathbb{Q}(\zeta)} \xrightarrow{\psi} \mu_7 \xrightarrow{\sim} \frac{\mathbb{Z}}{7\mathbb{Z}}$$

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

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

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

$$G_{E/\mathbb{Q}} = \left\{\sigma^i\rho^j : i = 0, ..., 5; j = 0, ..., 6\right\}$$

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

$$\{\alpha^r : r = 0, ..., 6\} \text{ (risp. } \{\zeta^s : s = 0, ..., 5\}\text{)}.$$

Poichè

$$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 42 = 7 \cdot 6 = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\zeta) : \mathbb{Q}],$$

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

$$\mathcal{B} = \{\alpha^r\zeta^s : r = 0, ..., 6; s = 0, ..., 5\}.$$

(4) Mostriamo che l'orbita di $\eta := \alpha + \zeta$ ha 42 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

$$\sigma^i\rho^j(\eta) = \eta \Rightarrow (i, j) = (0, 0) \in \{0, ..., 5\} \times \{0, ..., 6\}.$$

Notiamo che, per induzione,

$$\begin{array}{rcl} \sigma^i(\zeta) & = & \sigma^{i-1}\left(\zeta^3\right) = \sigma^{i-1}(\zeta)^3 = \left(\zeta^{3^{i-1}}\right)^3 = \zeta^{3^i}, \\ \rho^j(\alpha) & = & \rho^{j-1}(\zeta\alpha) = \zeta\rho^{j-1}(\alpha) = \zeta\zeta^{j-1}\alpha = \zeta^j\alpha. \end{array}$$

Abbiamo dunque

$$\begin{array}{rcl} \sigma^i\rho^j(\eta) & = & \sigma^i\left(\rho^j(\alpha)\right) + \sigma^i\left(\rho^j(\zeta)\right) = \sigma^i\left(\zeta^j\alpha\right) + \sigma^i(\zeta) \\ & = & \alpha\left(\sigma^i(\zeta)\right)^j + \zeta^{3^i} = \alpha\left(\zeta^{3^i}\right)^j + \zeta^{3^i} \\ & = & \alpha\zeta^{j3^i} + \zeta^{3^i}. \end{array}$$

Otteniamo allora

$$\sigma^i\rho^j(\eta) = \eta \Leftrightarrow \alpha\zeta^{j3^i} - \alpha = \zeta - \zeta^{3^i}.$$

Poichè $\zeta^6 = -1 - \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5$, abbiamo

$$\begin{array}{rcl} \alpha\zeta^{j3^i} - \alpha & \in & \displaystyle\sum_{s=0}^{6} \mathbb{Q}\alpha\zeta^s = \bigoplus_{s=0}^{5} \mathbb{Q}\alpha\zeta^s =: V_1, \\ \zeta - \zeta^{3^i} & \in & \displaystyle\sum_{s=0}^{6} \mathbb{Q}\zeta^s = \bigoplus_{s=0}^{5} \mathbb{Q}\zeta^s =: V_2. \end{array}$$

Poichè $V_1 \cap V_2 = \{0\}$ (dalla espressione di $\mathcal{B}$), otteniamo $\alpha\zeta^{j3^i} = \alpha \Leftrightarrow \zeta^{j3^i} = 1 \Leftrightarrow j3^i \equiv 0 \mod(7)$ e $\zeta^{3^i} = \zeta \Leftrightarrow 3^i \equiv 1 \mod(7)$. Dunque

$$j \equiv j3^i \equiv 0 \bmod(7) \Rightarrow j = 0.$$

D'altra parte la seguente tabella mostra che $3^i \equiv 1 \bmod(7) \Rightarrow i = 0$[1]:

$$\begin{array}{cccccc} i & 0 & 1 & 2 & 3 & 4 & 5 \\ 3^i \bmod(7) & 1 & 3 & 9 \equiv 2 & 3 \cdot 2 = 6 & 3 \cdot 61 = 8 \equiv 4 & 3 \cdot 4 = 12 \equiv 5. \end{array}$$

Esercizio 3. Sia $\mathbb{F}_q$ un campo finito con $q = p^n$ elementi e sia ℓ un primo.

(1) Si mostri che esiste un'unica estensione K di $\mathbb{F}_q$ di grado ℓ, a meno di isomorfismo.
(2) Si descriva il reticolo dei sottocampi $\mathbb{F}_q \subset K$.
(3) Si calcoli il numero dei polinomi irriducibili di grado ℓ in $\mathbb{F}_q[X]$.

Soluzione: (1) e (2) Sia $K := \mathbb{F}_{q^\ell}$ il campo finito con q^ℓ elementi: è unico a meno di isomorfismi in quanto ogni campo finito di cardinalità q^ℓ è campo di spezzamento della equazione $X^{q^\ell} - X \in \mathbf{F}_q[X]$. Essendo $\mathbf{F}_q \subset \mathbb{F}_{q^\ell}$ di grado primo ℓ gli unici campi intermedi, per la moltiplciatività dei gradi, sono $\mathbf{F}_q$ e $\mathbb{F}_{q^\ell}$.

(3) Cominciamo contando la cardinalità dell'insieme $\mathcal{M}_\ell(\mathbb{F}_q)$ dei polinomi monici irriducibili di grado ℓ in $\mathbb{F}_q[X]$ come segue.

Scriviamo $\mathbb{F}_{q^\ell} = \mathbb{F}_q \sqcup \left(\mathbb{F}_{q^\ell} - \mathbb{F}_q\right)$. Se $\alpha \in \mathbb{F}_{q^\ell} - \mathbb{F}_q$, abbiamo $\mathbb{F}_q \subsetneqq \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^\ell}$ e dunque per (2) abbiamo $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^\ell}$. Deduciamo che esiste una associazione

$$f_\cdot : \mathbb{F}_{q^\ell} - \mathbb{F}_q \to \mathcal{M}_\ell(\mathbb{F}_q)$$

che associa ad $\alpha \in \mathbb{F}_{q^\ell}$ il suo polinomio minimo $f_\alpha(X)$. Si tratta di una applicazione suriettiva poichè, se $f(X) \in \mathcal{M}_\ell(\mathbb{F}_q)$, allora $\frac{\mathbb{F}_q[X]}{(f(X))} \simeq \mathbb{F}_{q^\ell}$ ed X corrisponde ad un elemento $\alpha \in \mathbb{F}_{q^\ell}$ tale che $f_\alpha(X) = f(X)$. Poichè $(f_\cdot)^{-1}(f) = \left\{\alpha \in \mathbb{F}_{q^\ell} : f(\alpha) = 0\right\} = R_f$ (dove le radici sono in $\mathbb{F}_{q^\ell}$, poichè $\mathbb{F}_{q^\ell}/\mathbb{F}_q$ è normale), possiamo scrivere

$$\mathbb{F}_{q^\ell} = \mathbb{F}_q \sqcup \left(\mathbb{F}_{q^\ell} - \mathbb{F}_q\right) = \mathbb{F}_q \sqcup \bigsqcup_{f \in \mathcal{M}_\ell(\mathbb{F}_q)} R_f.$$

Ma $\#R_f = l$ per ogni $f \in \mathcal{M}_\ell(\mathbb{F}_q)$ e deduciamo che

$$q^\ell = q + \#\mathcal{M}_\ell(\mathbb{F}_q)\, l.$$

Dunque $\#\mathcal{M}_\ell(\mathbb{F}_q) = \frac{q^\ell - q}{\ell}$ ed il numero dei polinomi irriducibili di grado l risulta essere

$$(q-1)\frac{q^\ell - q}{\ell} = \frac{q^{\ell+1} - q^\ell - q^2 + q}{\ell}.$$

Esercizio 4. Sia K un campo di numeri e sia $\mathcal{O}_K$ il suo anello degli interi.

i. Si mostri che esiste una $\mathbf{Q}$-base di K che consiste di elementi di $\mathcal{O}_K$.
ii. Si mostri che $\mathcal{O}_K$ ammette una $\mathbf{Z}$-base (usando liberamente le proprietà del discriminante).

Soluzione: Vedere il Lemma 4.3 e il Teorema 4.5 delle Note.

Esercizio 5. Sia K il 13-esimo campo ciclotomico.

i. Mostrare che esiste un'unica estensione quadratica L di $\mathbf{Q}$ contenuta in K e che $L = \mathbf{Q}(\sqrt{13})$.
ii. Determinare i primi di $\mathcal{O}_L$ che ramificano in $\mathcal{O}_K$.
iii. Dato un primo $\mathcal{P}$ come in (ii) determinare la decomposizione di $\mathcal{P}\mathcal{O}_K$ in prodotto di ideali primi di $\mathcal{O}_K$ e per ciascun fattore determinare generatori, indice di ramificazione e di inerzia.

[1]Alternativamente, poichè $\langle 3 \rangle = \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{6\mathbb{Z}}$, $3^i \equiv 1 \Rightarrow i \equiv 0 \bmod(6). \Rightarrow i = 0$.

Soluzione: La prima asserzione segue dalla Note, Corollario 3.11.

Sappiamo dal Corollario 6.12 delle Note che $(13) \subset \mathbb{Z}$ ramifica in $\mathcal{O}_L$ e $(13)\mathcal{O}_L = \mathcal{P}^2$. Inoltre $(13)\mathcal{O}_K = \mathcal{Q}^{12}$, con $\mathcal{Q} = (p, \zeta - 1)$ e ζ radice primitiva di ordine 13 dell'unità, grazie al Corollario 6.13 delle Note. Usando il lemma 6.7 otteniamo che $\mathcal{P}$ ramifica in $\mathcal{O}_K$ e $\mathcal{P}\mathcal{O}_K = \mathcal{Q}^6$. Siccome $\mathcal{O}_L = \mathcal{O}_K[\zeta]$, con ζ radice primitiva di ordine 13 dell'unità, e $[L : K] = 6$ deduco dal Teorema 6.10 che l'indice di inerzia è 1.

Infine per ogni altro numero primo $\ell \neq 13$ l'ideale (ℓ) non ramifica in $\mathcal{O}_L$ per il Corollario 6.13. Quindi nessun primo di $\mathcal{O}_K$ diverso da $\mathcal{P}$ ramifica in $\mathcal{O}_K$ per il lemma 6.7.