SOLUZIONI DELL'ESONERO DI ALGEBRA 3, 20/11/2012

Esercizio 1. Sia $P(X) \in \mathbb{Q}[X]$ il polinomio $P(X) = X^3 + 3X^2 + 3$. Sia K un campo di spezzamento di $P(X)$ su $\mathbb{Q}$.

i. Mostrare che esiste un'unica radice reale α di $P(X)$. Determinare il grado $[K : \mathbb{Q}]$; [*Suggerimento*: Studio di funzione]

ii. Descrivere il gruppo di Galois di K su $\mathbb{Q}$ e il reticolo dei sottocampi.

Soluzione: (i) Considero $P(X)$ come una funzione $P\colon \mathbb{R} \to \mathbb{R}$ che manda $z \mapsto P(z)$. Gli zeri della derivata $P'(z) = 3z^2 + 6z$ sono $z = 0$ in cui $P(0) = 3$ e $z = -2$ in cui $P(-2) = 7$. Quindi $P(z)$ ha massimo e minimo in cui P assume valori positivi. Deduco che $P(z) = 0$ per un unico $z = \alpha \in \mathbb{R}$. Le atre radici di $P(Z)$ in $\mathbb{C}$ sono dunque complesse, non reali, e coniugate: β e $\overline{\beta}$. Quindi $K = \mathbb{Q}(\alpha, \beta)$.

Osservo che il polinomio $P(X)$ è irriducibile su $\mathbb{Q}$ per il criterio di Esisenstein applicato al primo $p = 3$. Quindi $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ ha grado 3. Visto che $\mathbb{Q}(\alpha) \subset \mathbb{R}$ e $\beta \notin \mathbb{R}$, deduco che $\mathbb{Q}(\alpha)$ è contenuto strettamente in K. Sappiamo inoltre che K, essendo campo di spezzamente di un polinomio di grado 3, ha grado $\leq 3! = 6$. Concludo che K ha grado 6 su $\mathbb{Q}$.

(ii) L'estensione $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ non è normale visto che $\beta \notin \mathbb{Q}(\alpha)$. Quindi il gruppo di Galois G di K su $\mathbb{Q}$ non è abeliano. Visto che K ha grado 6 su $\mathbb{Q}$, concludo che $G \cong S_3$. L'isomorfismo è realizzato vedendo G come il gruppo delle permutazioni dell' insieme $\{\alpha, \beta, \overline{\beta}\}$. I sottocampi di K sono

(a) K e $\mathbb{Q}$,

(b) tre estensioni di grado 3 su $\mathbb{Q}$ associate ai tre sottogruppi di ordine 2 di G date da $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ e $\mathbb{Q}(\overline{\beta})$;

(c) un'unica estensione di grado 2 su $\mathbb{Q}$ associata al sottogruppo normale di ordine 3 di G.

Esercizio 2. Si consideri il polinomio $f(X) = X^7 - 3 \in \mathbb{Q}[X]$.

i. Calcolare il campo di spezzamento E di f su $\mathbb{Q}$ e calcolarne il grado su $\mathbb{Q}$.

ii. Mostrare che il gruppo di Galois $\mathrm{Gal}_{E/\mathbb{Q}}$ è il prodotto semidiretto non diretto di due gruppi ciclici N ed H.

iii. Dare una presentazione di $\mathrm{Gal}_{E/\mathbb{Q}}$ in termini di generatori e di relazioni.

Soluzione: (i) Poichè $f'(x) = 7x^6 \geq 0$ e $f(\pm\infty) = \pm\infty$ esiste una ed una sola radice reale $\sqrt[7]{3}$ di f. Dunque, posto $\zeta := \exp(2\pi i/7)$ le radici di f sono

$$R_f = \left\{ \sqrt[7]{3}\zeta^i : i = 0, ..., 6 \right\}$$

ed $E = \mathbb{Q}(R_f)$. Notiamo che $E = \mathbb{Q}\left(\zeta, \sqrt[7]{3}\right)$. Infatti $\subset$ è ovvia e $\zeta = \frac{\sqrt[7]{3}\zeta}{\sqrt[7]{3}} \in \mathbb{Q}(R_f)$. Si ha

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6, \ \left[\mathbb{Q}\left(\sqrt[7]{3}\right) : \mathbb{Q}\right] = 7$$

poichè il polinomio ciclotomico $\Phi_6(X) \in \mathbb{Q}[X]$ ed $f(X) \in \mathbb{Q}[X]$ sono irriducibili (criterio di Eisenstein). Dunque

$$[E : \mathbb{Q}(\zeta)]\, 6 = [E : \mathbb{Q}(\zeta)]\, [\mathbb{Q}(\zeta) : \mathbb{Q}] = [E : \mathbb{Q}] = \left[E : \mathbb{Q}\left(\sqrt[7]{3}\right)\right] \left[\mathbb{Q}\left(\sqrt[7]{3}\right) : \mathbb{Q}\right] = \left[E : \mathbb{Q}\left(\sqrt[7]{3}\right)\right] 7.$$

Deduco che $7 \mid [E:\mathbb{Q}(\zeta)]$ e $6 \mid \left[E:\mathbb{Q}\left(\sqrt[7]{3}\right)\right]$. D'altra parte $[E:\mathbb{Q}(\zeta)] \leq \deg(f) = 7$ poichè $E = \mathbb{Q}\left(\zeta, \sqrt[7]{3}\right)$ è il campo ottenuto da $\mathbb{Q}(\zeta)$ aggiungendo $\sqrt[7]{3}$, che è radice di f: dunque posso scrivere $f(X) = g(X)h(X) \in \mathbb{Q}(\zeta)[X]$ con g irriducibile in $\mathbb{Q}(\zeta)[X]$ tale che $g\left(\sqrt[7]{3}\right) = 0$ e $[E:\mathbb{Q}(\zeta)] = \deg(g) \leq \deg(f)$. Concludo che $[E:\mathbb{Q}(\zeta)] = 7$ ed $[E:\mathbb{Q}] = 6 \cdot 7 = 42$.

(ii) Abbiamo la successione esatta di gruppi di Galois

$$1 \to G_{E/\mathbb{Q}(\zeta)} \to G_{E/\mathbb{Q}} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \to 1$$

dove $\#G_{\mathbb{Q}(\zeta)/\mathbb{Q}} = 6$ e $\#G_{E/\mathbb{Q}(\zeta)} = 7$. Inoltre $\chi : G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \to \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{6\mathbb{Z}}$ data da $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ è iniettiva poichè $\mathbb{Q}(\zeta)$ è generato da ζ ed è dunque una biiezione per ragioni di cardinalità E' infatti un omomorfismo. Poichè $\#G_{E/\mathbb{Q}(\zeta)} = 7$ è primo, $G_{E/\mathbb{Q}(\zeta)} \simeq \frac{\mathbb{Z}}{7\mathbb{Z}}$. Segue dal teorema di Schur-Zassenhaus che

$$G_{E/\mathbb{Q}} \simeq G_{E/\mathbb{Q}(\zeta)} \rtimes G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{7\mathbb{Z}} \rtimes \frac{\mathbb{Z}}{6\mathbb{Z}}.$$

Poichè $\mathbb{Q}\left(\sqrt[7]{3}\right)/\mathbb{Q} \subset E/\mathbb{Q}$ non è normale $G_{E/\mathbb{Q}}$ non è abeliano e dunque non è un prodotto diretto.

(iii) Poichè $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois ed $E = \mathbb{Q}\left(\zeta, \sqrt[7]{3}\right)$, l'applicazione di restrizione $G_{E/\mathbb{Q}\left(\sqrt[7]{3}\right)} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è iniettiva (alternativamente nota che $\#G_{E/\mathbb{Q}\left(\sqrt[7]{3}\right)} = 6$ è primo con la cardinalità del nucleo della restrizione, che è $\#G_{E/\mathbb{Q}(\zeta)} = 7$). Inoltre

$$\#G_{E/\mathbb{Q}\left(\sqrt[7]{3}\right)} = \left[E:\mathbb{Q}\left(\sqrt[7]{3}\right)\right] = 6 = [\mathbb{Q}(\zeta):\mathbb{Q}] = \#G_{\mathbb{Q}(\zeta)/\mathbb{Q}}.$$

Segue che si tratta di un isomorfismo. Dunque $G_{E/\mathbb{Q}} = G_{E/\mathbb{Q}(\zeta)} \rtimes G_{E/\mathbb{Q}\left(\sqrt[7]{3}\right)}$ e

$$G_{E/\mathbb{Q}\left(\sqrt[7]{3}\right)} = \left\{\sigma_i : \sigma_i(\zeta) = \zeta^i, i \in \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^{\times}\right\}.$$

Poichè $[E:\mathbb{Q}(\zeta)] = 7 = \left[\mathbb{Q}\left(\sqrt[7]{3}\right):\mathbb{Q}\right]$, l'applicazione di valutazione $\frac{\mathbb{Q}(\zeta)[X]}{(f(X))} \twoheadrightarrow E$ che manda X in $\sqrt[7]{3}$ è una applicazione suriettiva tra $\mathbb{Q}(\zeta)$-spazi vettoriali della stessa dimensione. Dunque è un isomorfismo, da cui dediciamo che $f(X) \in \mathbb{Q}(\zeta)[X]$ è irriducibile e pertanto che $G_{E/\mathbb{Q}(\zeta)}$ opera transitivamente sull'insieme R_f. Abbiamo dunque $\rho_i \in G_{E/\mathbb{Q}(\zeta)}$ tale che $\rho_i\left(\sqrt[7]{3}\right) = \sqrt[7]{3}\zeta^i$ per $i = 0, ..., 6$, questi elementi sono tutti distinti poichè $E = \mathbb{Q}\left(\zeta, \sqrt[7]{3}\right)$ ed esauriscono $G_{E/\mathbb{Q}(\zeta)}$ per ragioni di cardinalità. In altre parole

$$G_{E/\mathbb{Q}(\zeta)} = \left\{\rho_i : \rho_i\left(\sqrt[7]{3}\right) = \sqrt[7]{3}\zeta^i, i = 0, ..., 6\right\}.$$

Un generatore di $G_{E/\mathbb{Q}(\zeta)}$ è un qualunque elemento che non sia l'unità e dunque, ad esempio, $\rho_1 \in G_{E/\mathbb{Q}(\zeta)}$. Abbiamo

$i \in \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^{\times}$	1	2	3	4	5	6
$\lvert i\rvert$	1	3	6	3	6	2.

Dunque un generatore di $G_{E/\mathbb{Q}\left(\sqrt[7]{3}\right)}$ è σ_3. Inoltre $\sigma_3^{-1} = \sigma_5$, come si evince dalla tabella. Calcoliamo $\sigma_3 \circ \rho_1 \circ \sigma_3^{-1} \in G_{E/\mathbb{Q}(\zeta)}$ mediante la sua azione su $\sqrt[7]{3}$:

$$\begin{aligned}\sigma_3\left(\rho_1\left(\sigma_3^{-1}\left(\sqrt[7]{3}\right)\right)\right) &= \sigma_3\left(\rho_1\left(\sigma_5\left(\sqrt[7]{3}\right)\right)\right) = \sigma_3\left(\rho_1\left(\sqrt[7]{3}\right)\right) = \sigma_3\left(\sqrt[7]{3}\zeta\right) \\ &= \sigma_3\left(\sqrt[7]{3}\right)\sigma_3(\zeta) = \sqrt[7]{3}\zeta^3 = \rho_3\left(\sqrt[7]{3}\right).\end{aligned}$$

Dunque $\sigma_3 \circ \rho_1 \circ \sigma_3^{-1} = \rho_3$. Infine notiamo che

$$\begin{aligned}\rho_1^3\left(\sqrt[7]{3}\right) &= \rho_1\left(\rho_1\left(\sqrt[7]{3}\zeta\right)\right) = \rho_1\left(\rho_1\left(\sqrt[7]{3}\right)\rho_1(\zeta)\right) = \rho_1\left(\sqrt[7]{3}\zeta^2\right) = \rho_1\left(\sqrt[7]{3}\right)\rho_1(\zeta)^2 \\ &= \sqrt[7]{3}\zeta^3 = \rho^3\left(\sqrt[7]{3}\right).\end{aligned}$$

Segue che $\sigma_3 \circ \rho_1 \circ \sigma_3^{-1} = \rho_1^3$ e

$$\left\langle \rho, \sigma \mid \rho^7, \sigma^6, \sigma\rho\sigma^{-1}\rho^{-3} \right\rangle \xrightarrow{\sim} G_{E/\mathbb{Q}}$$

che manda $\rho \mapsto \rho_1$ e $\sigma \mapsto \sigma_3$ è una presentazione di $G_{E/\mathbb{Q}}$.

Esercizio 3. Siano date estensioni finite di campi $F \subset E_1 \subset \Omega$ ed $F \subset E_2 \subset \Omega$. Sia $E = E_1 \cdot E_2$ il campo composto. Supponiamo che E_1 sia un' estensione semplice di F ovvero $E_1 = F(\alpha)$ e sia $f(X) \in F[X]$ il polinomio minimo di α.

i. Mostrare che $E_2 \subset E$ ha grado $\leq [E_1 : F]$ e che ho uguaglianza se e solo se $f(X)$ è irriducibile su E_2.

ii. Supponiamo che $F \subset E_1$ sia di Galois. Mostrare che $E_2 \subset E$ è di Galois e che $[E : E_2]$ divide $[E_1 : F]$.

iii. Nelle ipotesi di (ii) mostrare che $[E : E_2] = [E_1 : F]$ se e solo Gal_{E/E_2} agisce in modo transitivo sulle radici di $f(X)$.

Soluzione: (i) Il grado $[E_1 : F]$ coincide con il grado d di $f(X)$. Il campo E è generato da α come estensione di E_2. In particolare, ha grado su E_2 uguale al grado n del polinomio minimo $g(X) \in E_2[X]$ di α su E_2. Visto che $f(\alpha) = 0$, segue che $g(X)$ divide $f(X)$. Dunque $n \leq d$ e $n = d$ se e solo se $f(X) = g(X)$ ovvero se e solo se $f(X)$ è irriducibile su E_2.

(ii) Se $F \subset E_1$ è di Galois, allora il polinomio $f(X)$ è separabile e spezza in E_1. Quindi E è campo di spezzamento del polinomio separabile $f(X) \in E_2[X]$. Segue che $E_2 \subset E$ è di Galois. L'applicazione $\delta\colon \mathrm{Gal}(E/E_2) \to \mathrm{Gal}(E_1/F)$ che manda $\sigma \mapsto \sigma|_{E_1}$ è un omomorfismo iniettivo di gruppi. Quindi $[E : E_2] = |\mathrm{Gal}(E/E_2)|$ divide $|\mathrm{Gal}(E_1/F)| = [E_1 : F]$.

(iii) Siccome $E = E_2(\alpha)$ ogni $\sigma \in \mathrm{Gal}(E/E_2)$ è univocamente determinato da $\sigma(\alpha)$. Detto I l'insieme delle radici di $f(X)$ in E, allora l'applicazione $\mathrm{Gal}(E/E_2) \to I$ che manda σ in $\sigma(\alpha)$ è iniettiva. Sia $J = \{\sigma(\alpha) | \sigma \in \mathrm{Gal}(E/E_2)\} \subset I$ l'immagine di tale applicazione, ovvero l'orbita di α per l'azione di G sulle radici di $f(X)$. Allora $[E : E_2] = |\mathrm{Gal}(E/E_2)| = |J|$ e $[E_1 : F] = \deg f(X) = |I|$. Quindi $[E : E_2] = [E_1 : F]$ se e solo se $I = J$ cioè l'azione di $\mathrm{Gal}(E/E_2)$ su I ha un'unica orbita.