SOLUZIONI DEL COMPITINO DEL 17/11/2015

Esercizio 1. Si consideri il polinomio $f(X) = X^3 - 5 \in \mathbb{Q}[X]$ e sia E il suo campo di spezzamento.

(1) Descrivere tutti gli elementi di $G_{E/\mathbb{Q}}$.
(2) Trovare una base di E come $\mathbb{Q}$-spazio vettoriale.
(3) Trovare $\eta \in E$ tale che $E = \mathbb{Q}(\eta)$.

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

$$R_f = \left\{\alpha, \alpha\zeta, \alpha\zeta^2\right\},$$

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

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

D'altra parte $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$. Poichè i gradi sono coprimi, deduciamo che

$$\#G_{E/\mathbb{Q}} = [E : \mathbb{Q}] = 2 \cdot 3 = 6.$$

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

$$\left\{1, \alpha, \alpha^2\right\} \text{ (risp. } \{1, \zeta\}\text{)}.$$

Poichè

$$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 6 = 3 \cdot 2 = [\mathbb{Q}(\alpha) : \mathbb{Q}]\,[\mathbb{Q}(\zeta) : \mathbb{Q}],$$

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

$$\left\{1, \alpha, \alpha^2, \zeta, \alpha\zeta, \alpha^2\zeta\right\}.$$

(2) Poichè $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois, ha senso considerare l'applicazione di restrizione:

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

E' iniettiva poichè $E = \mathbb{Q}(\alpha)(\zeta)$ e dunque una biiezione poichè

$$\#G_{E/\mathbb{Q}(\alpha)} = [E : \mathbb{Q}(\alpha)] = \frac{[E : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = \frac{6}{3} = 2 = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \#G_{\mathbb{Q}(\zeta)/\mathbb{Q}}.$$

Ma $G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è generato dall'automorfismo che manda ζ in ζ^2. 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

$$\varphi : G_{E/\mathbb{Q}(\zeta)} \xrightarrow{\psi} \mu_3 \xrightarrow{\sim} \frac{\mathbb{Z}}{3\mathbb{Z}}$$

definita dalla formula

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

E' un omomorfismo iniettivo, che è dunque suriettivo per ragioni d'ordine. Segue che

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

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

$$G_{E/\mathbb{Q}} = \left\{1, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\right\}.$$

(3) Mostriamo che l'orbita di $\eta := \alpha+\zeta$ ha 6 elementi, da cui segue che $E = \mathbb{Q}(\eta)$. Abbiamo che:

$$\begin{array}{lll} \sigma^i\rho^j & \sigma^i\rho^j(\eta) & \\ 1 & \alpha+\zeta, & \\ \rho & \rho(\alpha+\zeta) & = \rho(\alpha)+\rho(\zeta) = \zeta\alpha+\zeta, \\ \rho^2 & \rho^2(\alpha+\zeta) & = \rho^2(\alpha)+\rho^2(\zeta) = \rho(\zeta\alpha)+\zeta = \rho(\zeta)\rho(\alpha)+\zeta = \zeta^2\alpha+\zeta, \\ \sigma & \sigma(\alpha+\zeta) & = \alpha+\zeta^2, \\ \sigma\rho & \sigma(\rho(\alpha+\zeta)) & = \sigma(\zeta\alpha+\zeta) = \sigma(\zeta)\sigma(\alpha)+\sigma(\zeta) = \zeta^2\alpha+\zeta^2, \\ \sigma\rho^2 & \sigma\left(\rho^2(\alpha+\zeta)\right) & = \sigma\left(\zeta^2\alpha+\zeta\right) = \sigma(\zeta)^2\sigma(\alpha)+\sigma(\zeta) = \zeta^4\alpha+\zeta^2 = \zeta\alpha+\zeta^2. \end{array}$$

Avendo questi elementi differenti espressioni nella base di $E/\mathbb{Q}$ trovata in (2), sono a due a due distinti e, dunque, l'orbita di $\eta := \alpha+\zeta$ ha 6 elementi.

Esercizio 2. Sia $\zeta := \exp\left(\frac{2\pi i}{11}\right)$ una radice primitiva undicesima dell'unità e sia $f(X) = X^5 - 2 \in \mathbb{Q}[X]$.

(1) Si trovi una base $\mathcal{B}_\zeta$ di $\mathbb{Q}(\zeta)/\mathbb{Q}$.
(2) Detta α una radice di $f(X)$ si trovi una $\mathbb{Q}$-base $\mathcal{B}_\alpha$ di $\mathbb{Q}(\alpha)$ e si mostri che $\mathbb{Q}(\alpha)/\mathbb{Q}$ non è normale.
(3) Si trovi una $\mathbb{Q}$-base $\mathcal{B}$ di $\mathbb{Q}(\zeta,\alpha)$. Si scriva $\frac{\zeta}{\alpha}$ in questa base.

Soluzione: (1) Sappiamo che l'undicesimo polinomio ciclotomico $\Phi_{11}(X) \in \mathbb{Q}[X]$, che ha grado 10, è il polinomio minimo di ζ su $\mathbb{Q}$. Dunque

$$\mathcal{B}_\zeta := \left\{1, \zeta, ..., \zeta^9\right\}$$

è una base di $\mathbb{Q}(\zeta)/\mathbb{Q}$.

(2) Il polinomio $f(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisentein ed ha grado 5. Dunque

$$\mathcal{B}_\alpha := \left\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\right\}$$

è una base di $\mathbb{Q}(\alpha)/\mathbb{Q}$. Se $\mathbb{Q}(\alpha)/\mathbb{Q}$ fosse normale, dovendo contenere tutte le radici di $f(X)$, coinciderebbe con il suo campo di spezzamento E. Ma detta ζ_5 una radice quinta primitiva dell'unità, mostrimo che $E = \mathbb{Q}(\zeta_5, \alpha)$, che ha grado 20 su $\mathbb{Q}$ e, pertanto, non può coincidere con $\mathbb{Q}(\alpha)$. Infatti l'insieme delle radici di $f(X)$ è $\left\{\alpha\zeta_5^i : i = 0, ..., 4\right\}$: dunque $\subset$ è ovvia e l'inclusione opposta segue dal fatto che $\zeta_5 = \frac{\alpha\zeta_5}{\alpha}, \alpha \in E$. Sappiamo che il quinto polinomio ciclotomico, che ha grado 4, è il polinomio minimo di ζ_5 su $\mathbb{Q}$ e, dunque, $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. Da ciò deduciamo che $[\mathbb{Q}(\zeta_5) : \mathbb{Q}]$ e $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ sono coprimi e, pertanto,

$$[\mathbb{Q}(\zeta_5, \alpha) : \mathbb{Q}] = [\mathbb{Q}(\zeta_5) : \mathbb{Q}]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 \cdot 5 = 20.$$

(3) Poichè $\mathbb{Q}(\zeta)/\mathbb{Q}$ è una estensione di Galois, vale la formula

$$[\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}(\zeta)] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha)] \mid 5.$$

Se si avesse $[\mathbb{Q}(\alpha) : \mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha)] = 1$, dedurremmo

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta).$$

Ma esiste un isomorfismo

$$G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \xrightarrow{\sim} Aut\left(\mu_{11}\right) = \left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{10\mathbb{Z}}.$$

In particolare, $G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è abeliano e, dunque, tutte le sue sottoestensioni sono normali. Dunque $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$ implica che $\mathbb{Q}(\alpha)/\mathbb{Q}$ è normale, contraddicendo a (2). Segue che necessariamente

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

Ma allora

$$[\mathbb{Q}(\zeta,\alpha) : \mathbb{Q}] = [\mathbb{Q}(\zeta,\alpha) : \mathbb{Q}(\zeta)]\,[\mathbb{Q}(\zeta) : \mathbb{Q}] = 5 \cdot 10 = [\mathbb{Q}(\alpha) : \mathbb{Q}]\,[\mathbb{Q}(\zeta) : \mathbb{Q}].$$

Da questa uguaglianza segue che

$$\mathcal{B} := \mathcal{B}_\zeta \mathcal{B}_\alpha = \left\{\alpha^i \zeta^j : i = 0, ..., 4; j = 0, ..., 9\right\}$$

è una base di $\mathbb{Q}(\zeta,\alpha)/\mathbb{Q}$. Poichè $\alpha^5 = 2$, ovvero $\frac{1}{2}\alpha^5 = 1$, si ha $\alpha^{-1} = \frac{1}{2}\alpha^4$. Dunque

$$\frac{\zeta}{\alpha} = \frac{1}{2}\alpha^4 \zeta.$$

Esercizio 3. Siano F ed Ω due campi e sia $\mathcal{F} \subset F[X]$ una famiglia di polinomi.

(1) Se $F \subset \Omega$ mostrare che sono equivalenti le seguenti affermazioni.
   (*i*) Per ogni estensione semplice $F(x)/F$ tale $f_x(X) \in \mathcal{F}$, dove $f_x(X)$ è polinomio minimo di x su F, esiste una immersione di campi $\delta : F(x) \hookrightarrow \Omega$ tale che $\delta_{|F} = 1_F$.
   (*ii*) Per ogni $f(X) \in \mathcal{F}$, esiste una radice di $f(X)$ in Ω.

(2) Se $\sigma : F \hookrightarrow \Omega$ è una immersione di campi, riformulare l'equivalenza in (1) e dimostrarla.

Soluzione: L'affermazione (1) segue da (2) con $\sigma : F \hookrightarrow \Omega$ l'inclusione $F \subset \Omega$. Possiamo pertanto riformulare l'equivalenza in (1) come segue. Sono equivalenti le seguenti affermazioni:

(*i*) Per ogni estensione semplice $F(x)/F$ tale $\sigma(f_x)(X) \in \mathcal{F}$, dove $f_x(X)$ è polinomio minimo di x su F, esiste una immersione di campi $\delta : F(x) \hookrightarrow \Omega$ tale che $\delta_{|F} = \sigma$.
(*ii*) Per ogni $f(X) \in \mathcal{F}$, esiste una radice di $\sigma(f)(X) \in \Omega[X]$ in Ω.

Detta Ω_σ la F-algebra $\sigma : F \hookrightarrow \Omega$, una immersione di campi $\delta : F(x) \hookrightarrow \Omega$ tale che $\delta_{|F} = \sigma$ è un omomorfismo di F-algebre. D'altra parte una estensione semplice come in (*i*) è isomorfa, come F-algebra, al quoziente $\frac{F[X]}{(f_x(X))}$. Dunque dare δ come in (*i*) significa dare $\delta : \frac{F[X]}{(f_x(X))} \to \Omega_\sigma$ di F-algebre, ovvero dare $\psi_\alpha : F[X] \to \Omega_\sigma$ di F-algebre tale che $\psi_\alpha(f_x(X)) = 0$, dove $\alpha \in \Omega$. Poichè

$$\psi_\alpha(f_x(X)) = \psi_\alpha(f_x)(\psi_\alpha(X)) = \sigma(f_x)(\alpha),$$

vediamo che ciò equivale a dare $\alpha \in \Omega$ radice di $\sigma(f)(X) \in \Omega[X]$, cioè (*ii*).