SOLUZIONI COMPITO DI ALGEBRA 3, 25/01/2013

Esercizio 1. Sia $f(X) \in \mathbb{Q}[X]$ un polinomio irriducibile di grado 3 avente una sola radice reale $\alpha \in \mathbb{R}$, siano $\beta, \overline{\beta} \in \mathbb{C} - \mathbb{R}$ le altre due radici e $K = \mathbb{Q}(\alpha, \beta)$ il campo di spezzamento.

i. Mostrare che il gruppo di Galois di K su $\mathbb{Q}$ è isomorfo al gruppo S_3 delle permutazioni di $\{\alpha, \beta, \overline{\beta}\}$;

ii. Mostrare che $\mathbb{Q}(\gamma)$, con $\gamma := (\alpha - \beta)\left(\alpha - \overline{\beta}\right)\left(\beta - \overline{\beta}\right)$ è l'unico sottocampo di K di grado 2 su $\mathbb{Q}$.

Soluzione: L'estensione $\mathbb{Q} \subset K$ ha grado n al più 6. Visto che $\mathbb{Q}(\alpha)$ ha grado 3, essendo f irriducibile, e che $\beta \notin \mathbb{R}$ e quindi $\beta \notin \mathbb{Q}(\alpha)$ ha polinomio minimo $f(X)/(X - \alpha) \in \mathbb{Q}(\alpha)[X]$, concludo che K ha grado 6 su $\mathbb{Q}$.

Poichè $\mathbb{Q}(\alpha)/\mathbb{Q}$ non è una estensione normale, $G_{K/\mathbb{Q}}$ non è abeliano. Avendo ordine 6 devo avere $G_{K/\mathbb{Q}} \simeq S_3$ e l'isomorfismo si ottiene fissano una biiezione $\left\{\alpha, \beta, \overline{\beta}\right\} \to \{1, 2, 3\}$, per esempio $\alpha \leftrightarrow 1$, $\beta \leftrightarrow 2$ e $\overline{\beta} \leftrightarrow 3$. I sottogruppi $H \subset G_{K/\mathbb{Q}}$ ed i relativi sottocampi sono dunque i seguenti:

H	$G_{K/\mathbb{Q}}$	$\langle(123)\rangle$	$\langle(23)\rangle$	$\langle(13)\rangle$	$\langle(12)\rangle$	$\{1\}$
K^H	$\mathbb{Q}$	$\mathbb{Q}(\gamma)$	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\beta)$	$\mathbb{Q}\left(\overline{\beta}\right)$	K
$\left[K^H : \mathbb{Q}\right]$	1	2	3	3	3	6.

L'unica cosa da verificare è che $\mathbb{Q}(\gamma) = K^{\langle(123)\rangle}$. Osservo che ogni scambio manda $\gamma \mapsto -\gamma$ mentre $(123)(\gamma) = \gamma$. Quindi $\mathbb{Q}(\gamma) \subset K^{\langle(123)\rangle}$ ma $\mathbb{Q}(\gamma)$ non è contenuto in $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ o $\mathbb{Q}\left(\overline{\beta}\right)$. La conclusione segue.

Esercizio 2. Sia $P(X) \in \mathbb{Q}[X]$ il polinomio $P(X) = X^6 + 5$. Sia K un campo di spezzamento di $P(X)$ su $\mathbb{Q}$.

i. Determinare il grado $[K : \mathbb{Q}]$;

ii. Descrivere il gruppo di Galois G di K su $\mathbb{Q}$.

Soluzione: (i) Il polinomio $P(X)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisentein applicato al primo 5. Sia $\alpha = (-5)^{\frac{1}{6}}$ una radice e sia $M = \mathbb{Q}(\alpha)$. È una estensione di grado 6 di $\mathbb{Q}$.

Le altre radici di $P(X)$ sono della forma $\zeta_6^j \alpha$ con $\zeta_6 = \frac{1+\sqrt{-3}}{2}$ radice primitiva di ordine 6 dell'unità in $\mathbb{C}$. Sia $L = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$. Segue che K è il campo composto $L \cdot M$. Inoltre o $[K : M] = 2$ e quindi $[K : \mathbb{Q}] = 12$ oppure $K = M$ e $[K : \mathbb{Q}] = 6$.

Il campo L è una estensione di Galois di $\mathbb{Q}$ con gruppo di Galois H isomorfo a $\mathbb{Z}/2\mathbb{Z}$ e generato dalll'automorfismo $\gamma \colon L \to L$ che manda $\sqrt{-3} \mapsto -\sqrt{-3}$.

Visto che $\alpha^3 = \sqrt{-5} \in M$, segue che $\mathbb{Q}(\sqrt{-5}, \sqrt{-3}) \subset K$. Ma $\mathbb{Q}(\sqrt{-5}, \sqrt{-3})$ è il composto del campo quadratico $\mathbb{Q}(\sqrt{15})$, che è contenuto in $\mathbb{R}$, e del campo quadratico L, che non è contenuto in $\mathbb{R}$. Quindi, $\mathbb{Q}(\sqrt{15}) \cap \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}$ e $\mathbb{Q}(\sqrt{-5}, \sqrt{-3})$ ha grado 4 su $\mathbb{Q}$. Concludo che 4 divide $[K : \mathbb{Q}]$ e quindi deve valere $[K : \mathbb{Q}] = 12$.

(ii) Segue da (i) che $L \cap M = \mathbb{Q}$ e $K = \mathbb{Q}(\zeta_6, \alpha)$. Sia $N = \mathrm{Gal}(K/L)$. Si tratta di un gruppo ciclico di ordine 6 generato dall'automorfismo $\delta\colon K \to K$ che invia $\alpha \mapsto \zeta_6\alpha$: so di avere esattamente 6 automorfismi di K come estensione di L ed ognuno è univocamente determinato dall'immagine di α e deve inviare α in un'altra radice di $P(X)$. Quindi $N \cong \mathbb{Z}/6\mathbb{Z}$. Visto che L è di Galois allora N è normale in G e il gruppo di Galois $\tilde{H} = \mathrm{Gal}(K/M)$ è isomorfo ad H tramite l'applicazione $\tilde{H} \subset G \to G/N \cong H$ ed è generato dall'automorfismo $\tilde{\gamma}$ che invia $\sqrt{-3} \mapsto -\sqrt{-3}$.

Concludiamo che G è il prodotto semidiretto di N per H. Quindi è generato da $\tilde{\gamma}$ e da δ. Visto che $\tilde{\gamma}(\zeta_6) = \zeta_6^{-1}$ ho la relazione $\tilde{\gamma}\delta\tilde{\gamma} = \delta^{-1}$, che insieme alle relazioni $\tilde{\gamma}^2 = 1$ e $\delta^6 = 1$ determina G. Concludo che G è infatti isomorfo al gruppo diedrale di ordine 12.

Esercizio 3. Sia $\mathbb{F}_p$ il campo finito con p elementi. Sia $\overline{\mathbb{F}}$ una chiusura algebrica di $\mathbb{F}_p$. Siano $K = \mathbb{F}_q$ ed $L = \mathbb{F}_{q'}$ estensioni finite di $\mathbb{F}_p$ contenute in $\overline{\mathbb{F}}$ con $q = p^n$ e $q' = p^m$ elementi.

i) Determinare condizioni necessarie e sufficienti affinchè $K \subset L$.

ii) Nel caso in cui $K \subset L$ dimostrare che l'estensione $K \subset L$ è di Galois con gruppo ciclico.

Soluzione: (i) Per la teoria dei campi finiti sappiamo che per ogni $\alpha \in \mathbb{N}$ esiste un unico sottocampo di $\overline{\mathbb{F}}$ di cardinalità p^α che coincide con l'insieme delle radici del polinomio $X^{p^\alpha} - X$ in $\overline{\mathbb{F}}$.

In particolare, $K \subset L$ se e solo se n divide m. Infatti, se n divide m, diciamo $m = an$, allora ogni elemento $\alpha \in K$ soddisfa $\alpha^{p^n} = \alpha$ e quindi $\alpha^{p^m} = \alpha^{p^{an}} = \alpha^{p^{(a-1)n}} = \cdots = \alpha^{p^n} = \alpha$ ovvero $\alpha \in L$. Viceversa, se $K \subset L$ sia a il grado. Allora $p^m = |L| = |K|^a = p^{an}$ e quindi $m = an$.

(ii) Sia $\varphi\colon L \to L$ l'applicazione $x \mapsto x^{p^n}$. È un omomorfismo di campi e quindi, per ragioni di cardinalità, è un isomorfismo. Sia $H = \langle\varphi\rangle$ il sottogruppo di $\mathrm{Aut}(L/K)$ generato da φ. Abbiamo $L^H = \{x \in L | x^{p^n} = x\} = K$. Segue per definizione che $K \subset L$ è di Galois e per il teorema fondamentale della teoria di Galois $H = \mathrm{Gal}(L/K)$.

Esercizio 4. Sia $K = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

(1) Si determini un polinomio minimo per $\sqrt{3} + \sqrt{5}$.
(2) Si determini l'insieme $\mathrm{Ram}(K)$ degli ideali primi di $\mathbb{Z}$ che ramificano in $\mathcal{O}_K$.

Soluzione: È chiaro che $K \subseteq \mathbb{Q}[\sqrt{3}, \sqrt{5}]$. Inoltre l'unico elemento del gruppo di Galois

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

che fissa $\sqrt{3} + \sqrt{5}$ è l'identità, per cui $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ e il polinomio minimo di $\sqrt{3} + \sqrt{5}$ ha grado 4.

Poichè

$$(\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{15}$$

$\sqrt{3} + \sqrt{5}$ soddisfa la relazione

$$(X^2 - 8)^2 = 60$$

quindi un suo polinomio minimo è

$$X^4 - 16X^2 + 4$$

Poniamo $K_1 = \mathbb{Q}(\sqrt{3})$ e $K_2 = \mathbb{Q}(\sqrt{5})$, allora $\mathrm{Disc}(K_1) = 12$ mentre $\mathrm{Disc}(K_2) = 5$: segue che

$$\mathcal{O}_K = \mathcal{O}_{K_1}\mathcal{O}_{K_2} = \mathbb{Z}\left[\sqrt{3}, \frac{1+\sqrt{5}}{2}\right]$$

Quindi una base intera di K è

$$\left\{1, \sqrt{3}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{3}+\sqrt{15}}{2}\right\}$$

Possiamo cosìcalcolare

$$\mathrm{Disc}(K) = \det^2 \begin{pmatrix} 1 & \sqrt{3} & \frac{1+\sqrt{5}}{2} & \frac{\sqrt{3}+\sqrt{15}}{2} \\ 1 & -\sqrt{3} & \frac{1+\sqrt{5}}{2} & \frac{\sqrt{3}+\sqrt{15}}{2} \\ 1 & \sqrt{3} & \frac{1+\sqrt{5}}{2} & \frac{\sqrt{3}+\sqrt{15}}{2} \\ 1 & \sqrt{3} & \frac{1+\sqrt{5}}{2} & \frac{\sqrt{3}+\sqrt{15}}{2} \end{pmatrix} = 2^4 3^2 5^2$$

Quindi $\mathrm{Ram}(K) = \{2, 3, 5\}$.

Esercizio 5. Sia $\{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Q}$-base del campo di numeri K e supponiamo che $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ con $d = \mathrm{Disc}(\alpha_1, \ldots, \alpha_n)$. Si dimostri che ogni intero algebrico $\alpha \in \mathcal{O}_K$ si scrive nella forma

$$\alpha = \frac{\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n}{d}$$

con $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$.

Soluzione: Siano $\sigma_1, \ldots, \sigma_n$ gli n omomorfismi di K in $\mathbb{C}$ e sia $\alpha \in K$ un elemento fissato. Poichè $\{\alpha_1, \ldots, \alpha_n\}$ è una $\mathbb{Q}$-base, esistono $x_1, \ldots, x_n \in \mathbb{Q}$ tali che

$$\alpha = \alpha_1 x_1 + \ldots \alpha_n x_n \tag{1}$$

Applicando σ_i, con $i = 1, \ldots, n$ a (1) otteniamo il sistema di n equazioni lineari in n incognite

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_n)x_n &= \sigma_1(\alpha) \\ \quad\vdots &= \quad\vdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_n)x_n &= \sigma_n(\alpha) \end{cases}$$

Poichè $\{\alpha_1, \ldots, \alpha_n\}$ è una $\mathbb{Q}$-base, la matrice $A = \big(\sigma_i(\alpha_j)\big)$ è invertibile e quindi per la regola di Kramer, $x_j = \delta_j/\delta$ dove $\delta = \det(A)$ e δ_j è il determinante della matrice ottenuta da A sostituendo la colonna j-esima con la colonna $\big(\sigma_i(\alpha)\big)$ dei termini noti. Abbiamo che $\delta^2 = d$ e che $\delta, \delta_j \in \overline{\mathbb{Z}} \cup \mathbb{Q} = \mathbb{Z}$; quindi, posto $\lambda_j = dx_j$ in (1), segue la tesi.