COMPITO DI ALGEBRA 3, 26/02/2013

Esercizio 1. Sia $f(X) = X^7 - 5 \in \mathbb{Q}[X]$. Sia K il campo di spezzamento di $f(X)$ su $\mathbb{Q}$.

(1) Determinare il grado $\big[K : \mathbb{Q}\big]$;
(2) Descrivere il gruppo di Galois G di K su $\mathbb{Q}$;
(3) Determinare i sottocampi di K di grado 3 su $\mathbb{Q}$ e per ciascuno trovare un generatore come estensione di $\mathbb{Q}$.

Soluzione:

(1) Sia $\alpha \in \mathbb{R}$ una radice di $f(X)$. Visto che il polinomio $f(X)$ è irriducibile per il criterio di Eisenstein applicato al primo 5, deduco che $L_1 := \mathbb{Q}(\alpha)$ è una estensione di grado 7 di $\mathbb{Q}$.

Le radici di $f(X)$ sono tutte e sole della forma $\zeta_7^j \alpha$ per $j = 0, \dots, 6$ con ζ_7 una radice primitiva di ordine 7 dell'unità. Quindi K risulta essere uguale al campo composto di L_1 e di $L_2 := \mathbb{Q}\big(\zeta_7\big)$. L'estensione $\mathbb{Q} \subset L_2$ è di Galois con gruppo G_2 isomorfo a $\big(\mathbb{Z}/7\mathbb{Z}\big)^*$. Quest'ultimo è un gruppo ciclico di ordine 6 generato dalla classe di 3 modulo 7. Deduco che G_2 è un gruppo ciclico di ordine 6 generato dall'automorfismo $\gamma \colon \zeta_7 \mapsto \zeta_7^3$.

Visto che L_1 ed L_2 hanno gradi coprimi come estensioni di $\mathbb{Q}$, deduco che K ha grado $[L_1 : \mathbb{Q}][L_2 : \mathbb{Q}] = 42$.

(2) Sia $H = \mathrm{Gal}(K/L_1) \subset G$ ed $N = \mathrm{Gal}(K/L_2) \subset G$. Allora N è un sottogruppo normale di G visto che $\mathbb{Q} \subset L_2$ è di Galois. È un gruppo ciclico generato dall'automorfismo $\sigma \colon K \to K$ che invia $\alpha \mapsto \zeta_7 \alpha$. Invece, H è un sottogruppo di G generato dall'automorfismo $\gamma \colon \zeta_7 \mapsto \zeta_7^3$ e l'applicazione $H \subset G \to G/N$ è un isomorfismo. Quindi G è prodotto semidiretto di N ed H, generato da γ e σ con relazione $\gamma \circ \sigma \circ \gamma^{-1} = \sigma^3$.

(3) I sottocampi di K di grado 3 su $\mathbb{Q}$ corrispondono ai sottogruppi di G di ordine 14. Ogni tale sottogruppo deve contenere un 7-Sylow che sarà anche un 7-Sylow di G. Ma l'unico 7-Sylow di G è N visto che è normale in G. Quindi i sottocampi di K di grado 7 su $\mathbb{Q}$ corrispondono ai sottocampi di grado 3 di L_2. Visto che G_2 è ciclico di grado 6, c'è un unico sottogruppo di ordine 2 generato, ad esempio, dal coniugio complesso. Quindi esiste un unico sottocampo di K di grado 3 su $\mathbb{Q}$ e coincide con il sottocampo reale $\mathbb{Q}\big(\zeta_7 + \overline{\zeta}_7\big)$ di L_1.

Esercizio 2. Siano $K \subset L_1$ e $K \subset L_2$ estensioni finite di campi e sia $\Omega = L_1 L_2$ il campo composto di L_1 ed L_2. Supponiamo che $K \subset L_1$ sia di Galois.

(1) Mostrare che $L_2 \subset \Omega$ è di Galois. Descrivere il gruppo di Galois $\mathrm{Gal}(\Omega/L_2)$ in termini del gruppo di Galois $\mathrm{Gal}(L_1/K)$.
(2) Mostrare che se $K \subset L_2$ è di Galois allora $K \subset \Omega$ è di Galois. Descrivere il gruppo di Galois $\mathrm{Gal}(\Omega/K)$ in termini dei gruppi di Galois $\mathrm{Gal}(L_1/K)$ e $\mathrm{Gal}(L_2/K)$.
(3) È vero che se $K \subset \Omega$ è di Galois allora $K \subset L_2$ è di Galois?

Soluzione: Vedere la Prop. 3.18 di Milne per (1) e Prop. 3.20 di Milne per (2). La risposta a (3) è negativa. Ad esempio, sia $K = \mathbb{Q}$, $L_1 = \mathbb{Q}(\zeta_3)$ con ζ_3 radice primitiva di ordine 3

dell'unità e $K_2 = \mathbb{Q}\big(2^{\frac{1}{3}}\big)$. Allora $\Omega = \mathbb{Q}\big(\zeta_3, 2^{\frac{1}{3}}\big)$ è il campo di spezzamento del polinomio $X^3 - 2$ ed è quindi di galois su $\mathbb{Q}$. Tuttavia $\mathbb{Q} \subset L_1$ *non* è di Galois.

Esercizio 3. Sia $\zeta_{12} \in \mathbb{C}$ una radice primitiva dell' unità di ordine 12. Sia $K = \mathbb{Q}\big(\zeta_{12}, \sqrt{3}\big)$.

(1) Calcolare il grado di K su $\mathbb{Q}$;
(2) Mostrare che K è una estensione di Galois di $\mathbb{Q}$ e determinarne il gruppo di Galois;
(3) Determinare le estensioni di grado 2 di $\mathbb{Q}$ contenute in K.

Soluzione: Il campo K è il campo composto del campo ciclotomico $L_1 := \mathbb{Q}\big(\zeta_{12}\big)$ e del campo quadratico $L_2 := \mathbb{Q}\big(\sqrt{3}\big)$. Essendo entrame estensioni di Galois di $\mathbb{Q}$ anche il campo composto è una estensione di Galois di $\mathbb{Q}$.

Il gruppo di Galois $G_1 := \mathrm{Gal}(L_1/\mathbb{Q})$ è isomorfo a $\big(\mathbb{Z}/12\mathbb{Z}\big)^* = \big(\mathbb{Z}/4\mathbb{Z}\big)^* \times \big(\mathbb{Z}/3\mathbb{Z}\big)^* \cong \big(\mathbb{Z}/2\mathbb{Z}\big) \times \big(\mathbb{Z}/2\mathbb{Z}\big)$ ovvero al gruppo di Klein. In particolare, L_1 è una estensione biquadratica di $\mathbb{Q}$ ed ha grado 4 su $\mathbb{Q}$. Inoltre L_1 contiene una radice primitiva $\zeta_3 = \zeta_{12}^4$ dell' unità di ordine 3 e una radice primitiva $\zeta_4 = \zeta_{12}^3$ dell' unità di ordine 4. Siccome $\mathbb{Q}\big(\zeta_3\big) = \mathbb{Q}(\sqrt{-3})$ e $\mathbb{Q}\big(\zeta_4\big) = \mathbb{Q}(\sqrt{-1})$, segue che $L_1 = \mathbb{Q}(\sqrt{-3}, \sqrt{-1})$. In particolare $\sqrt{3} \in L_1$ e quindi $L_2 \subset L_1$ e $K = L_1$.

Esercizio 4. Si determini il valore del discriminante del p-esimo campo ciclotomico con p primo dispari.

Soluzione: Sia $\zeta = \exp(2\pi i/p)$: poiché sappiamo che $\mathcal{O}_{\mathbb{Q}[\zeta]} = \mathbb{Z}[\zeta]$ ci basta calcolare il discriminante di ζ.

Abbiamo $X^p - 1 = (X-1)\Phi(X)$, dove $\Phi(X) = X^{p-1} + \cdots + X + 1$ è il p-esimo polinomio ciclotomico. Differenziando e sostituendo X con ζ si ottiene

$$p = p\zeta^p = \zeta(\zeta - 1)\Phi'(\zeta) \tag{1}$$

Ricordiamo che $\mathrm{disc}(\zeta) = \epsilon N_{K/\mathbb{Q}}\big(\Phi'(\zeta)\big)$ dove $\epsilon = 1$ se $p \equiv 1 \bmod 4$ e $\epsilon = -1$ sennò. Applicando la norma $N_{K/\mathbb{Q}}$ all'equazione (1) otteniamo

$$p^{p-1} = \epsilon \mathrm{disc}(\mathcal{O}_K) N_{K/\mathbb{Q}}(\zeta) N_{K/\mathbb{Q}}(\zeta - 1)$$

Se $L = \mathbb{Q}[z]$ con $f(X) = X^m + \cdots + a_0$ polinomio monico minimo di z, allora $N_{L/\mathbb{Q}}(z) = (-1)^m a_0 = (-1)^m f(0)$. Quindi $N_{K/\mathbb{Q}}(\zeta) = \Phi(0) = 1$ e, essendo $\Phi(X+1)$ il polinomio minimo di $\zeta - 1$, segue che $N_{K/\mathbb{Q}}(\zeta - 1) = \Phi(1) = p$.

Otteniamo così che

$$\mathrm{disc}(\mathbb{Q}[\zeta]) = (-1)^{(p-1)/2} p^{p-2}$$

Esercizio 5. Si dimostri che per ogni m intero dispari con $m > 1$, $\mathbb{Q}[\zeta_{2m}] = \mathbb{Q}[\zeta_m]$. Si ponga poi $K = \mathbb{Q}[\zeta_{10}]$, il decimo campo ciclotomico.

(1) Si determinino il grado $[K : \mathbb{Q}]$ e un polinomio minimo di ζ_{10} su $\mathbb{Q}$.
(2) Si determinino tutte le sottoestensioni quadratiche di K, cioè i campi $L \subset K$ con $[L : \mathbb{Q}] = 2$.
(3) Si determini l'insieme $\mathrm{Ram}(K)$ dei primi naturali p tali che $p\mathbb{Z}$ ramifica in K.

Soluzione: Sia $\zeta = \zeta_{2m}$: vogliamo mostrare che $\mathbb{Q}[-\zeta] = \mathbb{Q}[\zeta^2]$. Chiaramente $\zeta^m \neq 1$; d'altra parte, $(\zeta^m)^2 = 1$, quindi $\zeta^m = -1$. Pertanto $(-\zeta)^m = (-1)^m \zeta^m = 1$ e $-\zeta$ è radice m-esima dell'unità: rimane da mostrare che $-\zeta$ è una radice *primitiva*.

Supponiamo che $(-\zeta)^n = 1$ con $0 \leq n < m$: allora $1 = (-\zeta)^{2n} = \zeta^{2n}$. Essendo ζ una radice primitiva $2m$-esima di 1, avremo che $n = 0$ cioè $-\zeta$ è primitiva. Segue immediatamente che $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta^2]$.

Posto $K = \mathbb{Q}[\zeta_{10}]$, abbiamo che $[K : \mathbb{Q}] = \phi(10) = \phi(2)\phi(5) = 4$. La radice primitiva quinta dell'unità $-\zeta_{10}$ ha polinomio minimo $\Phi_5(X) = (X^5 - 1)/(X - 1) = X^4 + X^3 + X^2 + X + 1$ perciò $\Phi_5(-X) = X^4 - X^3 + X^2 - X + 1$ è un polinomio minimo per ζ_{10}.

Avendo notato che $\mathbb{Q}[\zeta_{10}] = \mathbb{Q}[\zeta_5]$ con 5 primo e $5 \equiv 1 \bmod 4$, abbiamo che l'unica sottoestensione quadratica di K è $L = \mathbb{Q}[\sqrt{5}]$.

Sappiamo che $\mathrm{disc}(\mathbb{Q}[\zeta_5])|5^{\phi(5)}$ quindi $\mathrm{Ram}(K) \subseteq \{5\}$. D'altra parte $5\mathbb{Z}$ ramifica in $L = \mathbb{Q}[\sqrt{5}]$ e, per la moltiplicatività dell'indice di ramificazione, anche in K. Quindi $\mathrm{Ram}(K) = \{5\}$.