Compito di Algebra 3, 2013

18 giugno 2013

COGNOME e Nome .....

MATRICOLA .....

1. Sia $f(X) = X^3 + 3 \in \mathbb{Q}[X]$. Sia K il campo di spezzamento di $f(X)$ su $\mathbb{Q}$.
   (a) Determinare il grado $\big[K : \mathbb{Q}\big]$;
   (b) Descrivere gli elementi del gruppo di Galois G di K su $\mathbb{Q}$;
   (c) Determinare il gruppo G.

   Soluzione:
   (a) Il polinomio $f(X)$ è irriducibile per il criterio di Eisenstein applicato al primo 3. Sia α una radice. Allora $L = \mathbb{Q}[\alpha] \cong \mathbb{Q}[X]/\big(f(X)\big)$ ha grado 3 su $\mathbb{Q}$. Inoltre le altre radici sono tutte e sole della forma $\zeta_3^j\alpha$ con $0 \leq j \leq 2$ e $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ una radice primitiva dell'unità di ordine 3. Quindi $K = L(\zeta_3)$. Visto che L non contiene estensioni quadratiche e $\mathbb{Q} \subset \mathbb{Q}(\zeta_3)$ ha grado 2, concludo che $\zeta_3 \notin L$ e quindi K ha grado 6 su $\mathbb{Q}$.

   L'estensione $\mathbb{Q} \subset L$ non è normale, altrimenti conterrebbe tutte le radici di $X^3 + 3$. Segue che G non è abeliano e quindi $G \cong S_3$ il gruppo delle permutazioni delle tre radici di $f(X)$. Alternativamete gli elementi di G sono Id, σ che manda $\alpha \mapsto \alpha$ e $\zeta_3 \mapsto \zeta_3^2$, ρ che manda $\zeta_3 \mapsto \zeta_3$ e $\alpha \mapsto \zeta_3\alpha$ e i composti $\rho\sigma$, ρ^2, $\rho^2\sigma$.

2. Sia $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$. Sia $K = \mathbb{Q}(\alpha)$ e $K \subset L$ una chiusura normale di K su $\mathbb{Q}$.
   (a) Determinare i gradi di K ed L su $\mathbb{Q}$;
   (b) determinare il gruppo di Galois H di L su $\mathbb{Q}$.

   Soluzione: Sia $M = \mathbb{Q}\big(\sqrt{2}, \sqrt{3}, \sqrt{5}\big)$. Si tratta del composto di tre estensioni quadratiche, e quindi di Galois, $\mathbb{Q}\big(\sqrt{2}\big)$, $\mathbb{Q}\big(\sqrt{3}\big)$ e $\mathbb{Q}\big(\sqrt{5}\big)$ di $\mathbb{Q}$. Quindi M è di Galois su $\mathbb{Q}$. Si calcola esplicitamente che $\sqrt{3} \notin \mathbb{Q}\big(\sqrt{2}\big)$ e quindi M_1 è una estensione di Galois di $\mathbb{Q}$ di grado 4 con gruppo di Galois

$G_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ generato da σ_1, che invia $\sqrt{2} \mapsto -\sqrt{2}$ e $\sqrt{3} \mapsto \sqrt{3}$, e da σ_2, che invia $\sqrt{2} \mapsto \sqrt{2}$ e $\sqrt{3} \mapsto -\sqrt{3}$. Gli unici sottocampi quadratici di M_1 sono tre ovevro $\mathbb{Q}\big(\sqrt{2}\big)$, $\mathbb{Q}\big(\sqrt{3}\big)$ e $\mathbb{Q}\big(\sqrt{6}\big)$, per la teoria di Galois e si calcola che $\sqrt{5}$ non appartiene a nessuno di essi. Quindi $M_1 \cap \mathbb{Q}\big(\sqrt{5}\big) = \mathbb{Q}$ ed essendo M il composto delle estensioni Galoisiane M_1 e di $\mathbb{Q}\big(\sqrt{5}\big)$ di $\mathbb{Q}$, concludo che M ha grado $[M : \mathbb{Q}][\mathbb{Q}\big(\sqrt{5}\big) : \mathbb{Q}] = 8$ su $\mathbb{Q}$ e che G è il prodotto di G_1 e del gruppo di galois di $\mathbb{Q}\big(\sqrt{5}\big)$ su $\mathbb{Q}$. Quindi $G \cong \big(\mathbb{Z}/2\mathbb{Z}\big)^3$ con generatori σ_1, che invia $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$, $\sqrt{5} \mapsto \sqrt{5}$, da σ_2, che invia $\sqrt{2} \mapsto \sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$ e $\sqrt{5} \mapsto \sqrt{5}$ e da σ_3 che invia $\sqrt{2} \mapsto \sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$ e $\sqrt{5} \mapsto -\sqrt{5}$. Segue inoltre che $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{10}, \sqrt{6}, \sqrt{15}, \sqrt{30}\}$ è una $\mathbb{Q}$-base di M. In particolare, gli elementi $\sqrt{2}, \sqrt{3}, \sqrt{5}$ sono linearmente indipendenti su $\mathbb{Q}$. Segue da espliciti calcoli che nessun elemento di G diverso dall'identità fissa α. Ad es., $\sigma_2\sigma_3$ invia $\alpha = \sqrt{2}+\sqrt{3}+\sqrt{5} \mapsto \sqrt{2}-\sqrt{3}-\sqrt{5}$ che è diverso da α. Altrimenti $2\sqrt{3} + 2\sqrt{5} = 0$. Etc. Quindi $\mathrm{Aut}\big(M/\mathbb{Q}(\alpha)\big) = \mathrm{Id}$ e dal teorema fondamentale della teoria di Galois $M = \mathbb{Q}(\alpha)$. Concludo che $K = L$ ha grado 8 su $\mathbb{Q}$ e $H = G$.

3. Sia p un primo. Sia ζ_p una radice primitiva p-esima dell'unità. Esibire tutti i primi $p \leq 100$ tali che ζ_p sia costruibile con riga e compasso a partire da $\{0, 1\}$.

Soluzione: Sappiamo che che ζ_p è costruibile con riga e compasso a partire da $\{0, 1\}$ se e solo l'estensione Galoisiana $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ è ottenuta prendendo estensioni successive $\mathbb{Q} = K_0 \subset K_1 \subset \cdots K_{n-1} \subset K_n = \mathbb{Q}(\zeta_p)$ con K_{i+1} di grado due su K_i. Questo equivale a richiedere che il gruppo di Galois G_p di $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ ammetta una filtrazione $G^0 \subset G^1 \subset \cdots \subset G^{n-1} \subset G^n = G_p$ con $G^{i-1} \subset G^i$ di indice 2. Questo equivale a richiedere che G_p sia un 2-gruppo. la condizione è chiaramente necessaria visto che $|G_p| = [\mathbb{Q}(\zeta_p) : \mathbb{Q}]$. È anche sufficiente in quanto i 2-gruppi sono risolubili. Ma $G_p \cong (\mathbb{Z}/p\mathbb{Z})^*$ e quindi $|G_p| = p - 1$. Concludiamo che ζ_p è costruibile con riga e compasso se e solo se $p = 2^h + 1$ per qualche $h \in \mathbb{N}$. Al variare di h otteniamo allora i primi 3, 5, 17.

4. Sia $K = \mathbb{Q}[\sqrt{3} - \sqrt{7}]$.
   (a) Si determini un polinomio minimo per $\sqrt{3} - \sqrt{7}$.
   (b) Si determini l'insieme $\mathrm{Ram}(K)$ degli ideali primi di $\mathbb{Z}$ che ramificano in $\mathcal{O}_K$.

Soluzione: Le estensioni $K_1 = \mathbb{Q}[\sqrt{3}]$ e $K_2 = \mathbb{Q}[\sqrt{7}$ hanno, rispettivamente, discriminante 12 e 28; essendo di secondo grado, sono necessariamente distinte con $K_1 \cap K_2 = \mathbb{Q}$. È chiaro che $K \subseteq \mathbb{Q}[\sqrt{3}, \sqrt{7}]$. Inoltre l'unico elemento del gruppo di Galois

$$\mathrm{Gal}(\mathbb{Q}[\sqrt{3}, \sqrt{7}]/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}[\sqrt{3}/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}[\sqrt{7}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

che fissa $\sqrt{3} - \sqrt{7}$ è l'identità, per cui $K = \mathbb{Q}[\sqrt{3}, \sqrt{7}]$ e il polinomio minimo di $\sqrt{3} - \sqrt{7}$ ha grado 4.

Poiché

$$(\sqrt{3} - \sqrt{7})^2 = 10 + 2\sqrt{21}$$

$\sqrt{3} - \sqrt{7}$ soddisfa la relazione

$$(X^2 - 10)^2 = 84$$

quindi il suo polinomio minimo è

$$X^4 - 20X^2 + 16$$

I primi $2\mathbb{Z}$, $3\mathbb{Z}$ e $7\mathbb{Z}$ ramificano in K_1 o K_2, quindi ramificano anche in K. Poiché $\mathrm{disc}(K_1)$ e $\mathrm{disc}(K_2)$ non sono relativamente primi, possiamo solo concludere che

$$\mathrm{disc}(K) \mid \mathrm{disc}\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\} = \det^2 \begin{pmatrix} 1 & \sqrt{3} & \sqrt{7} & \sqrt{21} \\ 1 & -\sqrt{3} & \sqrt{7} & -\sqrt{21} \\ 1 & \sqrt{3} & -\sqrt{7} & -\sqrt{21} \\ 1 & \sqrt{3} & \sqrt{7} & \sqrt{21} \end{pmatrix} = 2^8 3^2 7^2$$

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

5. Sia K/F un'estensione di campi di numeri. Si mostri che per ogni $\alpha \in K$, $T_{K/F}(\alpha)$ e $N_{K/F}(\alpha)$ appartengono ad F e che se $\alpha \in \mathcal{O}_K$ allora $T_{K/F}(\alpha)$ e $N_{K/F}(\alpha)$ appartengono a $\mathcal{O}_F$.

   Se $K/\mathbb{Q}$ è un'estensione quadratica, vale il viceversa? cioè se $\alpha \in K$ e $T_{K/\mathbb{Q}}(\alpha)$ e $N_{K/\mathbb{Q}}(\alpha)$ appartengono a $\mathbb{Z}$ allora possiamo concludere che $\alpha \in \mathcal{O}_K$?

Soluzione: Possiamo supporre che $K = F[\alpha]$: se infatti $K/F[\alpha]$ fosse di grado d allora avremmo

$$T_{K/F}(\alpha) = d\, T_{F[\alpha]/F]}(\alpha), \qquad N_{K/F}(\alpha) = N_{F[\alpha]/F]}(\alpha)^d$$

come immediata conseguenza del fatto che ogni F-omomorfismo di $F[\alpha]$ in $\mathbb{C}$ si estende a d F-omomorfismi distinti di K in $\mathbb{C}$.

Supponiamo ora che $K = F[\alpha]$ sia un'estensione di grado n e sia

$$f(x) = x^n + \cdots + a_0 = (x - \alpha_1) \cdots (x - \alpha_n)$$

il polinomio minimo di α su F, dove $\alpha = \alpha_1, \ldots, \alpha_n$ sono le radici di f. Allora abbiamo

$$T_{K/F}(\alpha) = \alpha_1 + \cdots + \alpha_n = -a_{n-1} \in F$$
$$N_{K/F}(\alpha) = \alpha_1 \cdots \alpha_n = (-1)^n a_0 \in F$$

Supponiamo ora che $\alpha \in \mathcal{O}_K$, con $K = F[\alpha]$. Allora il polinomio minimo di α sarà a coefficienti in $\mathcal{O}_F$ da cui segue che anche $T_{K/F}(\alpha)$, $N_{K/F}(\alpha) \in \mathcal{O}_F$.

Sia ora $K = \mathbb{Q}[\sqrt{d}]$ un'estensione quadratica e sia $\alpha \in K$: se $\alpha \in \mathbb{Q}$, allora $N_{K/\mathbb{Q}}(\alpha) = \alpha^2$, ma è chiaro che se $\alpha^2 \in \mathbb{Z}$ allora $\alpha \in \mathbb{Z}$. Possiamo dunque supporre che $\alpha \in K \setminus \mathbb{Q}$: allora il suo polinomio minimo è $x^2 - T(\alpha)x + N(\alpha)$. Vediamo subito che la condizione $T(\alpha)$ e $N(\alpha)$ interi è equivalente ad avere α intero algebrico.