Compito di Algebra 3, 2013

17 settembre 2013

COGNOME e Nome .....

MATRICOLA .....

1. Sia $f(X) = X^6 + 3 \in \mathbb{Q}[X]$. 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 6 su $\mathbb{Q}$. Inoltre le altre radici sono tutte e sole della forma $\zeta_6^j\alpha$ con $0 \leq j \leq 5$ e $\zeta_6 = \frac{1+\sqrt{-3}}{2}$ una radice primitiva dell'unità di ordine 6. Quindi $K = L(\zeta_6)$. Visto che $\big(\alpha^3\big)^2 = -3$ concludo che $\sqrt{-3} \in L$ e quindi $\zeta_6 \in L$, ovvero $K = L$ ha grado 6 su $\mathbb{Q}$.

(b) Ogni automorfismo $\sigma \in G$ è univocamente determinato da dove invia α e inoltre $\sigma(\alpha)$ deve essere un'altra radice di $f(X)$, ovvero della forma $\zeta_6^j\alpha$ per un qualche $j = 0, \ldots, 5$. L'applicazione $\rho\colon G \to \{0, \ldots, 5\}$, che invia σ nell'unico j tale che $\sigma(\alpha) = \zeta_6^j\alpha$, è iniettiva e, visto che $|G| = [K : \mathbb{Q}] = 6$, è infatti biettiva.

(c) Osservo che σ_j invia $\alpha^3 \mapsto \zeta_6^{3j}\alpha^3$ che coincide con α^3 se j è pari e coincide con $-\alpha^3$ se j è dispari. In questo secondo caso σ_j definisce l'unico automorfismo non banale su $\mathbb{Q}\big(\sqrt{-3}\big) = \mathbb{Q}(\zeta_6)$, che manda $\zeta_6 \mapsto \overline{\zeta}_6 = \zeta_6^5$. Quindi, in particolare, $\sigma_1 \circ \sigma_2(\alpha) = \sigma_1(\zeta_6^2\alpha) = \overline{\zeta}_6^2\zeta_6\alpha = \zeta_6^5\alpha$ mentre $\sigma_2 \circ \sigma_1(\alpha) = \sigma_2(\zeta_6\alpha) = \zeta_6^2\alpha$. Visto che $\zeta_6^5 \neq \zeta_6^2$, concludo che $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$ e quindi G non è commutativo. Quindi $G \cong S_3$.

2. Sia $\alpha = \zeta_8^{-1} + \sqrt{2} + \sqrt{-2}$ dove $\zeta_8 = e^{\frac{2\pi i}{8}} \in \mathbb{C}$ è una radice primitiva di ordine 8 dell'unità. Sia $K = \mathbb{Q}(\alpha)$ e $K \subset L$ una chiusura normale di K su $\mathbb{Q}$.
   (a) Determinare il grado di K ed L su $\mathbb{Q}$;

(b) Determinare il gruppo di Galois H di L su $\mathbb{Q}$;

(c) Determinare il polinomio minimo $f(x) \in \mathbb{Q}[X]$ di α

Soluzione:

(a) (b) Osservo che $\zeta_8 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$ e dunque $\zeta_8^{-1} = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}} = \frac{1}{\sqrt{2}}(1-i)$. Segue che $K \subset N := \mathbb{Q}\big(i, \sqrt{2}\big)$. Quest'ultima è l'estensone di $\mathbb{Q}$ composta delle estensioni quadratiche $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{2})$. Osservo che $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$ in quanto $i \in \mathbb{C}\backslash\mathbb{R}$ mentre $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. Quindi N ha grado 4 su $\mathbb{Q}$ ed ha gruppo di Galois G isomorfo al gruppo di Klein con generatori σ, il coniugio complesso che invia i in $-i$ e $\sqrt{2}$ in $\sqrt{2}$, ed η, che invia i in i e $\sqrt{2}$ in $-\sqrt{2}$. I sottocampi sono $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ ed N e quindi K deve essere uno di questi. Segue che K è di Galois su $\mathbb{Q}$ e concludo che $K = L$.

Riscrivo $\alpha = \frac{(3+i)}{\sqrt{2}}$. Visto che $1/\sqrt{2}$ e $i/\sqrt{2}$ sono linermente indipendenti su $\mathbb{Q}$ segue che nessuno degli elementi non banali di G, ovvero σ, η e $\sigma \circ \eta$ fissa α (i dettagli sono lasciati al lettore). Concludo che $K = N = L$.

(c) Il polinomio minimo di α su $\mathbb{Q}$ è il polinomio $\big(X-\alpha\big)\big(X-\eta(\alpha)\big)\big(X-\sigma(\alpha)\big)\big(X-\sigma(\eta(\alpha))\big) = \big(X-\frac{(3+i)}{\sqrt{2}}\big)\big(X+\frac{(3+i)}{\sqrt{2}}\big)\big(X-\frac{(3-i)}{\sqrt{2}}\big)\big(X+\frac{(3-i)}{\sqrt{2}}\big) = \big(X^2-\frac{8+6i}{2}\big)\big(X^2-\frac{8-6i}{2}\big) = X^4-8X^2+25$.

3. Sia p un primo, n un intero positivo e sia $f(X)$ il polinomio $X^n - p \in \mathbb{Q}[X]$.

(a) Dire per quali n il polinomio $f(X)$ è risolubile per radicali.

(b) Dire per quali n le radici di $f(X)$ su $\mathbb{Q}$ sono costruibili con riga e compasso.

Soluzione:

(a) Dire che $f(X)$ è risolubile per radicali equivale a dire che il capo di spezzamento K di $f(X)$ su $\mathbb{Q}$ ha gruppo di Galois G risolubile.

Sia ζ_n una radice primitiva n-esima dell' unità. Sia $\alpha = p^{\frac{1}{n}}$. Allora ogni radice di $f(X)$ è della forma $\zeta_n^i\alpha$ con $i = 0, \ldots, n-1$. Quindi $K = \mathbb{Q}(\zeta_n, \alpha)$. L'estensione $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ è l'n-esimo capo ciclotomio e quindi è una estensione di Galois con gruppo abeliano. L'estensione $\mathbb{Q}(\zeta_n) \subset K$ è abeliana. Ogni automorfismo σ invia $\alpha \mapsto \zeta_n^j\alpha$ per un unico $j = j(\sigma) = 0, \ldots, n-1$ e l'applicazione

$$j\colon \mathrm{Gal}\big(K/\mathbb{Q}(\zeta_n)\big) \to \mathbb{Z}/n\mathbb{Z}$$

è un omomorfismo iniettivo di gruppi e quindi $\mathrm{Gal}\big(K/\mathbb{Q}(\zeta_n)\big)$ è abeliano. Inoltre è un sottogruppo normale di G con quoziente isomorfo a $\mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big)$. In particolare G è risolubile. Quindi $f(X)$ è risolubile per radicali per ogni n.

(b) Sia γ una radice di $f(X)$. Condizione necessaria affinché γ sia costruibile con riga e compasso è che l'estensione $\mathbb{Q} \subset \mathbb{Q}(\gamma)$ abbia grado una potenza di 2. Visto che $f(X)$ è irriducibile su $\mathbb{Q}$ di grado n per il criterio di Eisenstein applicato al primo p, segue che n deve essere una potenza di 2.

La condizione è anche sufficiente. Supponiamo che $n = 2^h$. Allora $\mathbb{Q} \subset \mathbb{Q}(\gamma)$ ha grado n. Inoltre tale estensione si può scrivere come $\mathbb{Q} \subset \mathbb{Q}(\gamma^{2^{h-1}}) \subset \mathbb{Q}(\gamma^{2^{h-2}}) \cdots \subset \mathbb{Q}(\gamma^2) \subset \mathbb{Q}(\gamma)$ in cui due estensioni successive sono di grado 2. Segue che γ è costruibile con riga e compasso.

4. Si mostri che due basi intere dello stesso campo di numeri hanno lo stesso discriminante. Si esibiscano due differenti basi intere di $K = \mathbb{Q}[\sqrt{3}+\sqrt{5}]$.

Soluzione: Siano $\mathcal{A} = \{\alpha_i\}$ e $\mathcal{B} = \{\beta_i\}$ due basi intere per un campo L di grado n su $\mathbb{Q}$, allora esiste una matrice M $n \times n$ a coefficienti in $\mathbb{Z}$ tale che

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Scambiando il ruolo delle basi otteniamo che M è invertibile e quindi di determinante ± 1. Se $A = \big(\sigma_j(\alpha_i)\big)$ e $B = \big(\sigma_j(\beta_i)\big)$ allora $B = MA$ quindi $\det(B) = \pm\det(A)$. Poiché per definizione $\mathrm{disc}(\mathcal{A}) = \det^2(A)$ e $\mathrm{disc}(\mathcal{B}) = \det^2(B)$, l'ipotesi segue.

Siano $K_1 = \mathbb{Q}[\sqrt{3}]$ e $K_2 = \mathbb{Q}[\sqrt{5}]$: se $K_1 = K_2$, e quindi $K = K_1$, allora $N_{K/\mathbb{Q}}(1\sqrt{5}) = 5 = a^2+3b^2$ dove $\sqrt{5} = a + b\sqrt{3}$ con $a, b \in \mathbb{Z}$. Ma $a^2 + 3b^2 \equiv 0, 1 \not\equiv 5 \bmod 3$. Perciò $K_1 \neq K_2$ e $[K : \mathbb{Q}] = 4$.

Abbiamo che $\mathrm{disc}(K_1) = 12$ 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

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

Una differente base intera è, ad esempio,

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

5. Sia q un primo dispari e sia $K = \mathbb{Q}[\sqrt{2q}]$: si determinino tutti gli ideali primi di $\mathcal{O}_K$.

Soluzione: Sia $\mathcal{P}$ un ideale primo di $\mathcal{O}_K$ e sia $p = \mathcal{P} \cap \mathbb{Q}$.

Se $p = 2$ oppure $p = q$ allora $p\mathcal{O}_K = (p, \sqrt{2q})^2$ quindi $\mathcal{P} = (p, \sqrt{2q})$.

Se $p \nmid 2q$ e $2q$ non è un quadrato modulo p, allora $p\mathcal{O}_K$ è primo e quindi $\mathcal{P} = p\mathcal{O}_K$.

Infine, se $p \nmid 2q$ ma $2q \equiv n^2 \bmod p$, allora $p\mathcal{O}_K = (p, n+\sqrt{2q})(p, n-\sqrt{2q})$ quindi $\mathcal{P} = (p, n+\sqrt{2q})$ oppure $\mathcal{P} = (p, n-\sqrt{2q}) = (p, -n+\sqrt{2q})$.

Quindi i primi di $\mathcal{O}_K$ sono:

- $(2, \sqrt{2q})$,
- $(q, \sqrt{2q})$,
- $(p, n+\sqrt{2q})$ dove $n^2 \equiv 2q \bmod p$ con $p \nmid 2q$ primo,
- $p\mathcal{O}_K$ dove p è un primo tale che $2q$ non è un quadrato modulo p.

Notiamo infine che le prime tre condizioni possono essere riunite in: $(p, n+\sqrt{2q})$ dove $n^2 \equiv 2q \bmod p$ con p primo.