Esonero di Algebra II

6 Giugno 2017

Soluzioni

1) Esiste un polinomio irriducibile di grado 13 in $\mathbb{Q}[x]$ con gruppo di Galois il gruppo ciclico con 13 elementi? Motivare la risposta.

Soluzione. Si prenda ζ una radice primitiva $13^2 = 169$-esima di 1. L'estensione $E = \mathbb{Q}(\zeta) \supset \mathbb{Q}$ è di Galois con $G = G(\mathbb{Q}(\zeta)/\mathbb{Q})$ ciclico di ordine $13 \times 12 = 156$. Dato che 12 divide $|G|$, G ha un sottogruppo H di ordine 12. $F = E^H$ è un'estensione di Galois di $\mathbb{Q}$ di grado 13. Sia α tale che $F = \mathbb{Q}(\alpha)$ e sia $f(x) \in \mathbb{Q}[x]$ il polinomio minimo di α. F è il campo di spezzamento di f e $G_f = G/H$ è ciclico di ordine 13.

2) Determinare il numero dei polinomi monici irriducibili di grado 3 in $\mathbb{F}_5[x]$.

Soluzione. Consideriamo il polinomio $g(x) = x^{5^3} - x \in \mathbb{F}_5[x]$. $\mathbb{F}_{5^3}$ è il campo di spezzamento di $g(x)$ ed è isomorfo a $\mathbb{F}_5[x]/(f(x))$ per ogni $f \in \mathbb{F}_5[x]$ irriducibile e monico. Dunque ogni polinomio monico irriducibile di grado 3 divide $g(x)$.

D'altro canto $\mathbb{F}_5$ e $\mathbb{F}_{5^3}$ sono gli unici sottocampi di $\mathbb{F}_{5^3}$ e dunque se $f(x)$ è un fattore irriducibile monico di grado maggiore di 1 di $g(x)$, il campo $\mathbb{F}_5 \subsetneq \mathbb{F}_5[x]/(f(x)) \subseteq \mathbb{F}_{5^3}$ è uguale a $\mathbb{F}_{5^3}$ e f ha grado 3. Ne segue che se $h(x)$ è il prodotto di tutti i polinomi irriducibili di grado 3 in $\mathbb{F}_5[x]$. Si ha

$$h(x) = \frac{x^{5^3} - x}{x^5 - x}$$

e $h(x)$ ha grado 120. Dato che ogni fattore irriducibile di $h(x)$ ha grado 3, ci sono 40 polinomi irriducibili monici distinti di grado 3.

3) Calcolare il gruppo di Galois del polinomio

$$(x^2 + 7)(x^7 - 1) \in \mathbb{Q}[x]$$

Soluzione. Sia ζ una radice settima di 1 diversa da 1. Sia $\alpha = \zeta + \zeta^2 + \zeta^4$, $\overline{\alpha} = \zeta^3 + \zeta^5 + \zeta^6$. Si ha

$$(x - \alpha)(x - \overline{\alpha}) = x^2 + x + 2$$

e questo polinomio ha discriminante -7. Ne segue che $x^2 + 7$ si spezza in $E = \mathbb{Q}(\zeta)$ il campo di spezzamento di $x^7 - 1$. Dunque E è anche il campo di spezzamento di $f = (x^2 + 7)(x^7 - 1)$ è sappiamo che $G_f = G(E/\mathbb{Q})$ è ciclico di ordine 6.

4) Sia $f(x) \in \mathbb{Q}[x]$ irriducibile di grado 4. Dimostrare che se il gruppo di Galois di f contiene una trasposizione esso è S_4 o D_4. Qual'è in gruppo di Galois di $X^4 - 3$?

Soluzione. Abbiamo visto che un polinomio irriducibile di grado 4 ha gruppo di Galois un sottogruppo transitivo di S_4 e che tali gruppi sono $V = \{e, (12)(34), (13)(24), (14)(23)\}$, C_4, D_4, A_4 e S_4. Chiaramente dato che una trasposizione è una permutazione dispari V e A_4 non contengono trasposizioni L'unico elemento di C_4 di ordine 2 è il quadrato di un generatore e dunque è pari. Rimangono solo D_4 e S_4 ed essi contengono trasposizioni.

Per vedere chi sia il gruppo di Galois di $x^4 - 3$ notiamo che tale polinomio è irriducibile (Eisenstein) e ha due radici reali e due complesse e dunque il coniugio è una trasposizione in G_f e G_f è D_4 o S_4. Inoltre il suo campo di spezzamento è $\mathbb{Q}(\sqrt[4]{3}, i)$ che ha grado al più 8. Per la prima parte $G_f = D_8$.

5) Sia ζ una radice primitiva quarantanovesima di 1. Si consideri $E = \mathbb{Q}(\zeta) \supset \mathbb{Q}$. Quanti sono i campi F tali che $\mathbb{Q} \subseteq F \subseteq E$? Motivare la risposta.

Soluzione. Il gruppo di Galois $G = G(E/\mathbb{Q})$ è ciclico di ordine 42. I campi F tali che $\mathbb{Q} \subseteq F \subseteq E$ sono tanti quanti i divisori di 42, ovvero $1, 2, 3, 6, 7, 14, 21, 42$ ovvero 8.