SOLUZIONI DELL' ESAME DI METÀ SEMESTRE

---

1. Data un estensione E/F, si dica cosa significa che $\alpha \in E$ è algebrico su F e cosa è il polinomio minimo di α su F dimostrando che è irriducibile.

   $\alpha \in E$ si dice **algebrico** *su F se l'omomorfismo di anelli $\varphi : F[x] \to E, f(x) \mapsto f(\alpha)$ non è iniettivo.*

   In tal caso, siccome $F[x]$ è un anello a ideali principali, l'ideale $Ker\varphi \subset F[x]$ è principale.

   Pertanto esiste $f_\alpha \in F[x]$ monico tale che $Ker\varphi = \langle f_\alpha \rangle$. Tale f_α si chiama **polinomio minimo** *di α su F.*

   Infine, siccome $F(\alpha) \cong F[x]/\langle f_\alpha \rangle \hookrightarrow E$ è un campo, $\langle f_\alpha \rangle$ risulta un ideale massimale e f_α irriducibile.

---

2. Descrivere gli elementi del gruppo di Galois del polinomio $(x^2-2)(x^2+3)$ determinando anche tutti i sottocampi del campo di spezzamento.

   Sia $f(x) = (x^2-2)(x^2+3)$. Allora il campo di spezzamento di f su $\mathbf{Q}$ è $\mathbf{Q}_f = \mathbf{Q}(\sqrt{2}, \sqrt{-3})$.

   Dal fatto che $[\mathbf{Q}_f : \mathbf{Q}] = 4$ deduciamo che gli elementi del gruppo di Galois $Gal(\mathbf{Q}_f/\mathbf{Q})$ sono i seguenti:

$$\left\{ \begin{matrix} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{-3} \mapsto \sqrt{-3}, \end{matrix} \begin{matrix} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{-3} \mapsto -\sqrt{-3}, \end{matrix} \begin{matrix} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{-3} \mapsto \sqrt{-3}, \end{matrix} \begin{matrix} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{-3} \mapsto -\sqrt{-3}, \end{matrix} \right\}.$$

Ciascuno degli ultimi tre elementi del gruppo di Galois genera un sottogruppo con indice 2 che corrisponde a uno dei tre sottocampi quadratici di $\mathbf{Q}_f$

$$\mathbf{Q}(\sqrt{-3}), \quad \mathbf{Q}(\sqrt{2}), \quad \mathbf{Q}(\sqrt{-6})$$

che oltre a $\mathbf{Q}$ e $\mathbf{Q}_f$ sono tutti e soli i sottocampi di $\mathbf{Q}_f$.

---

3. Dopo aver verificato che è algebrico, calcolare il polinomio minimo di $\cos\pi/12$ su $\mathbf{Q}$.

Dal fatto $\cos\pi/12 = \frac{1}{2}\left(\zeta_{24} + \overline{\zeta}_{24}\right)$ e dal fatto che ζ_{24} e $\overline{\zeta}_{24}$ entrambi soddisfano il polinomio $x^{24}-1$ deduciamo che $\cos\pi/12$ è algebrico su $\mathbf{Q}$ in quanto somma di numeri algebrici.

Si ha inoltre che

$$\partial f_{\cos\frac{\pi}{12}} = [\mathbf{Q}(\cos\pi/12) : \mathbf{Q}] = \frac{1}{2}[\mathbf{Q}(\zeta_{24}) : \mathbf{Q}] = \varphi(24)/2 = 4.$$

Quindi $\cos\pi/12$ soddisfa un polinomio di grado 4 in $\mathbf{Q}[x]$. Scriviamo $\zeta = \zeta_{24}$

$$\cos^4\frac{\pi}{12} + A\cos^3\frac{\pi}{12} + B\cos^2\frac{\pi}{12} + C\cos\frac{\pi}{12} + D = \frac{\left((\zeta+\overline{\zeta})^4 + 2A(\zeta+\overline{\zeta})^3 + 4B(\zeta+\overline{\zeta})^2 + 8C(\zeta+\overline{\zeta}) + 16D\right)}{16}.$$

Sfruttando le identità $\zeta^8 - \zeta^4 + 1 = 0$ e $\zeta^{12} = -1$ e facendo i calcoli otteniamo che $A = C = 0$, $B = -1$ e $D = 1/16$.

Quindi $\qquad f_{\cos\pi/12}(x) = x^4 - x^2 + 1/16.$

---

4. Quanti elementi ha il campo di spezzamento di $(x^2+x+1)(x^3+x^2+1)$ su $\mathbf{F}_2$?

Ne ha 2^6. Infatti x^2+x+1 e x^3+x^2+1 sono entrambi irriducibili e il campo di spezzamento E ha come sottocampi $\mathbf{F}_2(\alpha), \alpha^2 = \alpha+1$ e $\mathbf{F}_2(\beta), \beta^3 = \beta^2+1$. Pertanto sia 2 che 3 dividono $[E : \mathbf{F}_2]$.

Infine $\mathbf{F}_2(\alpha,\beta)$ è il campo di spezzamento infatti $(x^2+x+1)(x^3+x^2+1) = (x+\alpha)(x+\alpha^2)(x+\beta)(x+\beta^2)(x+\beta^4)$.

Quindi $6 = [E : \mathbf{F}_2]$ e $|E| = 2^6$.

---

5. Dimostrare che se p è primo, $\cos 2\pi/p^2$ soddisfa un polinomio di grado $p(p-1)/2$ su $\mathbf{Q}$ con gruppo di Galois ciclico.

$$[\mathbf{Q}(\cos\tfrac{2\pi}{p^2}) : \mathbf{Q}] = \frac{[\mathbf{Q}(\zeta_{p^2} : \mathbf{Q}(\cos\frac{2\pi}{p^2})]}{[:\mathbf{Q}(\zeta_{p^2}) : \mathbf{Q}(\cos\frac{2\pi}{p^2})]} = \frac{\varphi(p^2)}{2} = \frac{p(p-1)}{2}.$$

Infine $\cos 2\pi/p^2$ ha un polinomio minimo con grado $\frac{p(p-1)}{2}$ il cui gruppo di Galois è ciclico in quanto sottogruppo del gruppo ciclico $U(\mathbf{Z}/p^2\mathbf{Z})$.

---

6. Mostrare che un estensione di campi è finita se e solo se è algebrica e finitamente generata spiegando le nozioni di cui si parla.

Un estensione E/F si dice **algebrica** *se ogni elemento di E soddisfa un polinomio a coefficienti in F non nullo; si dice* **finita** *se E è uno spazio vettoriale di dimensione finita e si dice finitamente generata se esistono $\alpha_1, \ldots, \alpha_h \in E$ tali che $E = F(\alpha_1, \ldots, \alpha_h)$. Se E/F è finita, allora per ogni $\alpha \in E$, se α non fosse algebrico, la famiglia $1, \alpha, \alpha^2, \ldots$ darebbe luogo ad una famiglia infinita di vettori linearmente indipendenti. Se inoltre consideriamo la catena di sottocampi:*

$$F \subset F[\alpha_1] \subset F[\alpha_1, \alpha_2] \subset \ldots \subset E$$

dove α_i è scelto in modo tale che $\alpha_i \in E \setminus F[\alpha_1, \ldots, \alpha_{i-1}]$, Allora la catena non può crescere all'infinito cioè $E = F[\alpha_1, \ldots, \alpha_h]$ è finitamente generato.

Se invece E/F è algebrica e finitamente generata, allora.

$$E = F[\alpha_1, \ldots, \alpha_h] = F(\alpha_1, \ldots, \alpha_h) \qquad \text{e} \qquad [E : F] = \prod_{j=1}^{h-1} [F[\alpha_1, \ldots, \alpha_{j-1}] : F[\alpha_1, \ldots, \alpha_j]].$$

Ciascun fattore è finito perchè si tratta di un estensione semplice con un elemento algebrico. Quindi $[E : F]$ è finito.

---

7. Descrivere gli elementi del gruppo di Galois del campo di spezzamento di $x^n - 1$.

   Il campo di spezzamento del polinomio è il campo ciclotomico $\mathbf{Q}(\zeta_m)$. Inoltre se $\sigma_j : \mathbf{Q}(\zeta_m) \to \mathbf{Q}(\zeta_m), \zeta_m \mapsto \zeta_m^j$,

   Allora Gal$(\mathbf{Q}(\zeta_m)/\mathbf{Q}) = \{\sigma_j \mid j \in U(\mathbf{Z}/m\mathbf{Z})\}$.

---

8. Si enunci nella completa generalità il Teorema di corrispondenza di Galois.

Teorema. *Sia E/F un estensione di Galois (cioè E è il campo di spezzamento di un polinomio separabile in $F[x]$) e sia $G =$Gal(E/F). Allora c'è una corrispondenza biunivoca tra ti sottogruppi di G e i sottocampi di E che contengono F. Se $H \le G$ e $F \subseteq M \subseteq E$, allora la corrispondenza è data da:*

$$H \mapsto E^H, \quad M \mapsto \mathrm{Gal}(E/M).$$

Inoltre

i G corrisponde a F e $\{1\}$ corrisponde a E;

ii $H_1 \le H_2 \Leftrightarrow E^{H_1} \supseteq E^{H_2}$.

iii Per ogni $\sigma \in G$,

- $E^{\sigma H \sigma^{-1}} = \sigma E^H$;
- *Gal$(E/\sigma M) = \sigma$Gal$(E/M)\sigma^{-1}$.*

iv $H \triangleleft G \Leftrightarrow E^H/F$ è un estensione normale. In tal caso inoltre Gal$(E^H/F) \cong G/H$.

---

9. Calcolare la dimensione su $\mathbf{Q}$ del campo di spezzamento del seguente polinomio $x^3 + x + 10$.

   La dimensione è 2. Infatti $x^3 + x + 10 = (x + 2)(x^2 - 2x + 5)$ e quindi il campo di spezzamento è $\mathbf{Q}(\sqrt{-1})$.

---

10. Dare un esempio di polinomio non separabile, un esempio de estensione algebrica normale e non separabile e di una separabile e non normale.

    - $x^p - t \in \mathbf{F}_p(t)[x]$ *è un polinomio non separabile;*
    - $\mathbf{F}_p(t)/\mathbf{F}_p(t^p)$ *è un estensione algebrica normale non separabile;*
    - $\mathbf{Q}(2^{1/3})$ *è un estensione normale non separabile.*

---

11. Descrivere gli $\mathbf{Q}(\sqrt{-1})$–omomorfismi di $\mathbf{Q}(\sqrt{-3}, \sqrt{3})$ in $\mathbf{C}$.

    Sappiamo che

$$\mathbf{Q}(\sqrt{-3}, \sqrt{3}) = \mathbf{Q}(\sqrt{3}, \sqrt{-1}) = \mathbf{Q}(\sqrt{-1})(\sqrt{3})$$

e che gli $\mathbf{Q}(\sqrt{-1})$–omomorfismi sono in numero pari al numero di radici del polinomio minimo di $\sqrt{3}$ in $\mathbf{C}$ cioè due.

Si tratta quindi dell'identità e l'omomorfismo:

$$\sigma : \mathbf{Q}(\sqrt{-3}, \sqrt{3}) \to \mathbf{C}, \sqrt{-3} \mapsto -\sqrt{-3}, \sqrt{3} \mapsto -\sqrt{3}$$

che è un $\mathbf{Q}(\sqrt{-1})$–omomorfismo in quanto

$$\sigma(\sqrt{-1}) = \sigma(\frac{1}{3}\sqrt{3}\sqrt{-3}) = \sqrt{-1}.$$

---

12. Dimostrare che se E_1 e E_2 sono estensioni di Galois di F con $E_1 \subset L$ e $E_2 \subset L$, allora $E_1 \cap E_2$ e E_1E_2 (il campo composto) sono estensioni di Galois. (Per ulteriore punteggio mostrare che $\mathrm{Gal}(E_1E_2/F) \cong \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$ se $E_1 \cap E_2 = F$).

    La soluzione è nelle dispense di Milne a pagina 37 nella Proposizione 3.20.
