SOLUZIONI DELL' ESAME DI METÀ SEMESTRE

1. Sia F un campo e sia $f \in F[x]$ irriducibile. Mostrare che f ha radici multiple se e solo se F ha caratteristica finita $p \neq 0$ e esiste $g \in F[x]$ tale che $f(x) = g(x^p)$.

SOLUZIONE. *Si tratta di parte dell'enunciato della Proposizione 2.12 a pagina 23 delle note di Milne.*

2. Descrivere gli elementi del gruppo di Galois del polinomio $(x^2+1)(x^4-3) \in \mathbf{Q}[x]$ determinando anche tutti i sottocampi del campo di spezzamento.

SOLUZIONE. *Le sei radici del polinomio sono* $\pm i, \pm 3^{1/4}$ *e* $\pm i3^{1/4}$*; pertanto il campo di spezzamento è* $E = \mathbf{Q}[i, 3^{1/4}]$ *che ha dimensione* 8 *su* $\mathbf{Q}$*. Gli otto elementi del gruppo di Galois* $G = \mathrm{Gal}(\mathbf{Q}[i, 3^{1/4}]/\mathbf{Q})$ *sono:*

$$\mathrm{id} : \left\{ \begin{array}{c} i \mapsto i \\ 3^{1/4} \mapsto 3^{1/4} \end{array} \right\} \quad \sigma : \left\{ \begin{array}{c} i \mapsto -i \\ 3^{1/4} \mapsto 3^{1/4} \end{array} \right\} \quad \tau : \left\{ \begin{array}{c} i \mapsto i \\ 3^{1/4} \mapsto i3^{1/4} \end{array} \right\} \quad \tau\sigma : \left\{ \begin{array}{c} i \mapsto -i \\ 3^{1/4} \mapsto i3^{1/4} \end{array} \right\}$$

$$\tau^2 : \left\{ \begin{array}{c} i \mapsto i \\ 3^{1/4} \mapsto -3^{1/4} \end{array} \right\} \quad \tau^3 : \left\{ \begin{array}{c} i \mapsto i \\ 3^{1/4} \mapsto -i3^{1/4} \end{array} \right\}$$

$$\tau^2\sigma : \left\{ \begin{array}{c} i \mapsto -i \\ 3^{1/4} \mapsto -3^{1/4} \end{array} \right\} \quad \tau^3\sigma : \left\{ \begin{array}{c} i \mapsto -i \\ 3^{1/4} \mapsto -i3^{1/4} \end{array} \right\}.$$

Denotiamo con D_4 *il gruppo delle simmetrie del quadrato di vertici* $1, 2, 3$ *e* 4 *e ne rappresentiamo gli elementi mediante permutazioni dei vertici. Pertanto*

$$D_4 = \{(1),\ (1,2,3,4),\ (1,3)(2,4),\ (1,4,3,2),\ (1,2)(3,4),\ (1,4)(2,3),\ (1,3),\ (2,4)\}.$$

L'applicazione $G \longrightarrow D_4, \sigma \mapsto (1,3), \tau \mapsto (1,2,3,4)$ *definisce un isomorfismo di gruppi. I* 9 *sottogruppi di* D_4 *sono i seguenti:*

$$D_4,$$
$$\langle (1,2,3,4) \rangle, \quad \langle (1,3),\ (2,4) \rangle, \quad \langle (1,2)(3,4),\ (1,4)(2,3) \rangle,$$
$$\langle (1,2)(3,4) \rangle, \quad \langle (1,3) \rangle, \quad \langle (2,4) \rangle, \quad \langle (1,3)(2,4) \rangle, \quad \langle (1,4)(2,3) \rangle,$$
$$\langle (1) \rangle.$$

e i 9 *sottocampi corrispondenti attraverso la corrispondenza di Galois sono:*

$$\mathbf{Q},$$
$$\mathbf{Q}[i], \quad \mathbf{Q}[\sqrt{3}], \quad \mathbf{Q}[\sqrt{-3}],$$
$$\mathbf{Q}[(1-i)3^{1/4}], \quad \mathbf{Q}[3^{1/4}], \quad \mathbf{Q}[i3^{1/4}], \quad \mathbf{Q}[i, \sqrt{3}], \quad \mathbf{Q}[(1+i)3^{1/4}],$$
$$\mathbf{Q}[i, 3^{1/4}].$$

3. Dopo aver verificato che è algebrico, calcolare il polinomio minimo di $\cos \pi/18$ su $\mathbf{Q}$.

SOLUZIONE. *Scriviamo* $\nu = \cos \frac{\pi}{18} = \frac{1}{2}(\zeta_{36} + \overline{\zeta}_{36})$ *e osserviamo che* ν *è algebrico in quanto si ottiene come il prodotto di un numero razionale e la somma di due numeri algebrici. Il fatto che* ζ_{36} *e* $\overline{\zeta}_{36}$ *sono algebrici segue subito dal fatto che soddisfano il polinomio* $X^{36}-1$. *Inoltre dalla fattorizzazione* $X^{36}-1 = (X^{18}-1)(X^6+1)(X^{12}-X^6+1)$ *segue che il polinomio minimo è* $f_{\zeta_{36}}(X) = X^{12} - X^6 + 1$ *e che* ν *soddisfa un polinomio di grado sei. Osservando che*

$$f_{\zeta_{36}}(\cos \frac{\pi}{18} + i \sin \frac{\pi}{18}) = 0,$$

che $\zeta_{36}^{12} = \zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, *otteniamo*

$$-\frac{1}{2} + i\frac{\sqrt{3}}{2} - (\cos \frac{\pi}{18} + i \sin \frac{\pi}{18})^6 + 1 = 0.$$

La parte reale dell'identità sopra è

$$-\nu^6 + 15\nu^4 \sin^2 \frac{\pi}{18} - 15\nu^2 \sin^4 \frac{\pi}{18} + \sin^6 \frac{\pi}{18} + \frac{1}{2} = 0.$$

Usando la relazione $\sin^2 \frac{\pi}{18} = 1 - \cos^2 \frac{\pi}{18} = 1 - \nu^2$, *si arriva a*

$$-\nu^6 + 15\nu^4(1-\nu^2) - 15\nu^2(1-\nu^2)^2 + (1-\nu^2)^3 + \frac{1}{2} = 0.$$

Un breve calcolo ci porta a

$$-32\nu^6 + 48\nu^4 - 18\nu^2 + \frac{3}{2} = 0.$$

Dunque si ha che $f_\nu(X) = X^6 - \frac{3}{2}X^4 + \frac{9}{16}X^2 - \frac{3}{64}$.

4. Si consideri $E = \mathbf{F}_2[\alpha]$ dove α è una radice del polinomio $X^3 + X + 1$. Determinare il polinomio minimo su $\mathbf{F}_2$ di $\alpha + 1$.

SOLUZIONE. *Basta usare la regola generale che se* E/F *è un'estensione,* $\alpha \in E$ *e* $f_\alpha(X) \in F[X]$ *è il polinomio minimo di* α *su* F, *allora* $f_{A\alpha+B}(X) = A^{\partial f_\alpha} f_\alpha\big(\frac{X-B}{A}\big)$ *è il polinomio minimo di* $A\alpha + B$ *per ogni* $A, B \in F$, $A \neq 0$. *Questa proprietà segue dal fatto chiaro che* $f_{A\alpha+B}(A\alpha+B) = 0$ *e siccome* $\mathbf{Q}(\alpha) = \mathbf{Q}(A\alpha+B)$, *risulta* $\partial f_\alpha = [\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathbf{Q}(A\alpha + B) : \mathbf{Q}] = \partial f_{A\alpha+B}$.

Nel caso in questione, $A = B = 1$ *e quindi*

$$f_{\alpha+1}(X) = f_\alpha(X+1) = (X+1)^3 + (X+1) + 1 = X^3 + X^2 + 1.$$

5. Dimostrare che $\mathbf{Q}(\zeta_m)$ possiede almeno un sottocampo quadratico e fornire un esempio in cui i sottocampi quadratici sono più di uno.

SOLUZIONE. *In effetti è necessario assumere che* $m > 3$ *altrimenti* $\mathbf{Q}(\zeta_m) = \mathbf{Q}$ *e l'enunciato è falso per ragioni ovvie. Se* $m = 2^t$ *è una potenza di due, allora* $t \geq 2$*. In questo caso* $i = \zeta_4 = \zeta_{2^t}^{2^{t-2}} \in \mathbf{Q}(\zeta_{2^t})$ *e quindi* $\mathbf{Q}(i) \subseteq \mathbf{Q}(\zeta_m)$ *è un sottocampo quadratico. Altrimenti sia* $p > 2$ *un primo tale che* $p|m$*. Allora* $\zeta_m^{m/p} = \zeta_p$ *e quindi* $\mathbf{Q}(\zeta_p) \subseteq \mathbf{Q}(\zeta_m)$*. Adesso osserviamo che per ogni* $p > 3$ *il gruppo di Galois* $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong \left(\mathbf{Z}/p\mathbf{Z}\right)^* \cong C_{p-1}$ *è ciclico e pertanto ammette un unico sottogruppo per ogni divisore del suo ordine. Siccome* $d = (p-1)/2$ *divide* $p-1$*, dall'osservazione precedente otteniamo che* $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ *ammette un sottogruppo* H *con indice* $2 = (p-1)/d$*. Per il Teorema di corrispondenza otteniamo che il sottocampo fisso* E^H *ha grado 2 su* $\mathbf{Q}$ *ed è quindi quadratico.*

Per quanto riguarda la seconda parte, basta considerare $\mathbf{Q}[\zeta_8] = \mathbf{Q}[i, \sqrt{2}]$ *in cui i sottocampi quadratici sono* 3*.*

6. Mostrare che se F è un campo e $g \in F[X]$, allora il grado del campo di spezzamento E_g di g su F soddisfa
$$[E_g : F] \leq \partial(g)!.$$

SOLUZIONE. *Si tratta della Proposizione 2.4 a pagina 20 delle note di Milne.*

7. Mostrare che se p_n denota l'n–esimo numero primo, allora
$$[\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}) : \mathbf{Q}] = 2^n.$$
Quanti sono i sottocampi quadratici?

SOLUZIONE. *Dalla formula della moltiplicatività del grado si ottiene che*
$$[\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{p_1}) : \mathbf{Q}] \cdot \prod_{j=2}^{n} [\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_j}) : \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{j-1}})].$$
Inoltre si ha che per ogni $j = 2, \ldots, n$*,* $\sqrt{p_j} \notin \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{j-1}})$ *come è possibile verificare facendo il calcolo e usando il fatto che i primi sono tutti distinti. Quindi* $[\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_j}) : \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{j-1}})] = 2$ *e l'enunciato segue immediatamente.*

Per quando riguarda la seconda parte, osserviamo che il gruppo di Galois
$$\mathrm{Gal}(\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})/\mathbf{Q}) \cong C_2 \times \cdots \times C_2$$
è il prodotto diretto di n *copie di* C_2*. Un isomorfismo è il seguente: se* $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in C_2^n$ *con* $\varepsilon_i \in \{0, 1\}$*, allora* $\sigma_\varepsilon \in \mathrm{Gal}(\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})/\mathbf{Q})$ *è l'automorfismo definito da* $\sigma_\varepsilon(\sqrt{p_j}) = (-1)^{\varepsilon_j}\sqrt{p_j}$ *per ogni* $j = 1, \ldots n$*.*

Si ha che C_2^n *ammette* $2^n - 1$ *sottogruppi di indice* 2*. Infatti per ogni* $\varepsilon \in C_2^n \setminus \{(0, \ldots, 0)\}$*, l'omomorfismo* $\varphi \mapsto \langle \varphi, \varepsilon \rangle$ *ha per nucleo un diverso sottogruppo di indice due (qui* $\langle \cdot, \cdot \rangle$ *denota il prodotto scalare). Si verifica che tutti i sottogruppi di indice due si ottengono in questo modo.*

Infine tutti e soli i sottocampi quadratici di $\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ *sono della forma*

$$\mathbf{Q}(\sqrt{p_{i_1} \cdots p_{i_k}})$$

dove $\{i_1, \ldots, i_k\}$ *è un sottoinsieme non vuoto di* $\{1, \ldots, n\}$*. È chiaro che diversi sottoinsiemi danno luogo a diversi sottocampi e in questo modo si ottengono i* $2^n - 1$ *sottocampi quadratici. Il sottocampo fissato dal nucleo dell'omomorfismo* $\langle \cdot, \varepsilon \rangle$ *è* $\mathbf{Q}(\sqrt{p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}})$*.*

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

SOLUZIONE.

Teorema. *Sia* E/F *un'estensione di Galois (cioè* E *è il campo di spezzamento di un polinomio separabile in* $F[x]$*) e sia* $G = \mathrm{Gal}(E/F)$*. Allora c'è una corrispondenza biunivoca tra i sottogruppi di* G *e i sottocampi di* E *che contengono* F*. Se* $H \leq G$ *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 $H_1 \leq H_2 \Leftrightarrow E^{H_1} \supseteq E^{H_2}$*;*
iii Se $H_1 \leq H_2$*, allora* $[H_2 : H_1] = [E^{H_1} : E^{H_2}]$*;*
iv Per ogni $\sigma \in G$*,* $E^{\sigma H \sigma^{-1}} = \sigma E^H$*;*
v $H \triangleleft G \Leftrightarrow E^H/F$ *è un'estensione normale. In tal caso inoltre* $Gal(E^H/F) \cong G/H$*.*

9. Mostrare che i polinomi irriducibili di grado 3 a coefficienti razionali che ammettono un'unica radice reale hanno S_3 come gruppo di Galois.

SOLUZIONE. *Assumiamo il fatto che i gruppi di ordine* 6 *sono isomorfi a* S_3 *oppure a* C_6*. Il fatto che il polinomio ammette un'unica radice reale implica che il suo campo di spezzamento ha grado* 6 *su* $\mathbf{Q}$*. Infatti se* $\alpha, \beta, \overline{\beta} \in \overline{\mathbf{Q}}$ *sono le radici del polinomio con* $\alpha \in \mathbf{R}$*, allora il campo di spezzamento è* $\mathbf{Q}(\alpha, \beta)$ *e siccome* $\beta \notin \mathbf{Q}(\alpha)$*, si ha*

$$[\mathbf{Q}(\alpha, \beta) : \mathbf{Q}] = [\mathbf{Q}(\alpha, \beta) : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] = 2 \times 3 = 6.$$

Quindi il gruppo di Galois, che ha tanti elementi quanto il grado del campo di spezzamento, ha cardinalità 6*. Infine i sottocampi* $\mathbf{Q}(\alpha)$ *e* $\mathbf{Q}(\beta)$ *hanno grado* 3 *su* $\mathbf{Q}$ *pertanto il gruppo di Galois non può essere ciclico altrimenti avrebbe un unico sottocampo per ogni divisore dell'ordine.*

10. Dopo aver definito la nozione di campo perfetto, dimostrare che i campi finiti sono perfetti.

SOLUZIONE. *La definizione è la 2.14 a pagina 23 delle note di Milne mentre la dimostrazione è una conseguenza diretta della Proposizione 2.15.*

11. Sia ζ_{16} una radice primitiva 16–esima dell'unità. Descrivere gli $\mathbf{Q}(\sqrt{-1})$–omomorfismi di $\mathbf{Q}(\zeta_{16})$ in $\mathbf{C}$.

SOLUZIONE. *Innanzi tutto osserviamo che* $\sqrt{-1} = \zeta_{16}^4$ *e che tutti gli omomorfismi di* $\mathbf{Q}(\zeta_{16})$ *in* $\mathbf{C}$ *sono della forma:*

$$\sigma_j : \mathbf{Q}(\zeta_{16}) \longrightarrow \mathbf{C}, \zeta_{16} \mapsto \zeta_{16}^j,$$

dove $j \in \{1, 3, 5, 7, 9, 11, 13, 15\}$. *Tali omomorfismi risultano* $\mathbf{Q}(\sqrt{-1})$*–omomorfismi se e solo se fissano* ζ_{16}^4.

La condizione $\sigma_j(\zeta_{16}^4) = \zeta_{16}^4$ *è equivalente a* $4j \equiv 4 \bmod 16$ *e cioè* $j \equiv 1 \bmod 4$. *Quindi* $j = 1, 5, 9, 13$. *Infine gli* $\mathbf{Q}(\sqrt{-1})$*–omomorfismi sono* $\{\sigma_1, \sigma_5, \sigma_9, \sigma_{13}\}$.

12. Sia E un'estensione finita di $\mathbf{Q}$ e siano E_1 e E_2 due sottocampi di E. Dimostrare che se E_1 e E_2 sono estensioni di Galois di $\mathbf{Q}$ allora anche il composto E_1E_2 è un'estensione di Galois di $\mathbf{Q}$.

SOLUZIONE. *È una conseguenza immediata del Teorema di corrispondenza di Galois il fatto che l'intersezione di due sottogruppi* H_1 *e* H_2 *di* $\mathrm{Gal}(E/F)$ *corrisponde al composto dei due campi che corrispondono a* H_1 *e* H_2 *(i.e.* $E^{H_1 \cap H_2} = E^{H_1}E^{H_2}$*)*

Infatti, per definizione l'intersezione di due sottogruppi è il più grande sottogruppo contenuto in entrambi mentre il composto di due campi è il più piccolo sottocampo contenente entrambi. Il fatto che la corrispondenza di Galois è antimonotona rispetto alla relazione di inclusione implica che l'intersezione corrisponde al composto.

Infine se E_1 *e* E_2 *sono di Galois (e quindi normali) su* F*, allora* $\mathrm{Gal}(E/E_1)$ *e* $\mathrm{Gal}(E/E_2)$ *sono normali in* $\mathrm{Gal}(E/F)$. *Da questo segue che* $\mathrm{Gal}(E/E_1) \cap \mathrm{Gal}(E/E_2)$ *è normale in* $\mathrm{Gal}(E/F)$ *in quanto l'intersezione di sottogruppi normali è normale. Da quanto detto sopra segue anche che*

$$E_1E_2 = E^{\mathrm{Gal}(E/E_1) \cap \mathrm{Gal}(E/E_2)}$$

e corrispondendo ad un sottogruppo normale, anche E_1E_2 *risulta normale.*