ALGEBRA 2 - Secondo esonero

12 giugno 2012

Soluzioni

1. Sia α una radice reale dell'equazione $x^4 - 7x = 10$.

   - [4pt] Calcolare il polinomio minimo di α^2 su $\mathbb{Q}$.
   - [4pt] Calcolare $[\mathbb{Q}(\alpha^2) : \mathbb{Q}]$ e $[\mathbb{Q}(\alpha^3) : \mathbb{Q}]$.
   - [4pt] E' vero che $(\alpha + 1)^{-1}$ appartiene a $\mathbb{Q}[\alpha]$? Se sì, calcolarlo; se no, dimostrare che $\alpha + 1$ non è invertibile in $\mathbb{Q}[\alpha]$.

   Soluzione: Prima di procedere, calcoliamo il polinomio minimo di α su $\mathbb{Q}$. Sicuramente α soddisfa il polinomio $f(x) = x^4 - 7x - 10$, le cui uniche radici razionali possono essere $\pm 1, \pm 2, \pm 5, \pm 10$. Sostituendo, si vede che $f(\pm 1) = -9 \mp 7$, $f(\pm 2) = 6 \mp 14$, $f(\pm 5) = 615 \mp 35$, $f(\pm 10) = 9990 \mp 70$. Pertanto, $f(x)$ non ha radici razionali.

   Questo tuttavia non ci assicura che $f(x)$ sia irriducibile in $\mathbb{Q}[x]$, ma semplicemente che non ha fattori di primo grado. Per escludere che $f(x)$ si fattorizzi nel prodotto di due polinomi di secondo grado, procediamo per forza bruta. Se $f(x) = (x^2 + ax + b)(x^2 - ax + c)$, otteniamo

   $$\begin{cases} b + c = a^2 \\ a(b - c) = 7 \\ bc = -10 \end{cases}$$

   Poiché $f(x)$ è un polinomio primitivo a coefficienti in $\mathbb{Z}$, la sua irriducibilità in $\mathbb{Q}[x]$ è equivalente alla sua irriducibilità in $\mathbb{Z}[x]$. Cerchiamo quindi le soluzioni intere del sistema appena descritto. Sappiamo che $bc = -10$ e che $b + c$ è un quadrato perfetto. Le uniche possibilità sono $b = 10, c = -1$ oppure $b = -1, c = 10$, che conducono a $b - c = \pm 11$, che non divide $a(b - c) = 7$. Concludiamo che il sistema non ha soluzioni intere.

   Ricapitolando, $x^4 - 7x - 10$ è irriducibile in $\mathbb{Q}[x]$, ed è quindi il polinomio minimo di α. Il campo $\mathbb{Q}(\alpha)$ è pertanto un'estensione di $\mathbb{Q}$ di grado 4.

   - Poiché $\alpha^4 - 10 = 7\alpha$, quadrando si ottiene $\alpha^8 - 20\alpha^4 + 100 = 49\alpha^2$. Perciò, α^2 soddisfa il polinomio $x^4 - 20x^2 - 49x + 100$. L'irriducibilità di questo polinomio segue dal punto successivo.
   - $\alpha^2 \in \mathbb{Q}(\alpha)$ garantisce $\mathbb{Q}(\alpha^2) \subset \mathbb{Q}(\alpha)$. D'altro canto $\mathbb{Q}(\alpha^2)$ contiene sicuramente $(\alpha^2)^2 = \alpha^4 = 7\alpha + 10$ e quindi anche α. Di conseguenza, vale anche $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha^2)$ e quindi $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$. Questo mostra che $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 4$.
     Per quanto riguarda α^3, si vede che $\alpha(\alpha^3 - 7) = 10$ e quindi $\alpha = 10(\alpha^3 - 7)^{-1}$. Quindi $\alpha \in \mathbb{Q}(\alpha^3)$ e, come prima $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^3)$. In conclusione, $[\mathbb{Q}(\alpha^3) : \mathbb{Q}] = 4$.
   - α è algebrico su $\mathbb{Q}$ e quindi $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. Ma $\mathbb{Q}(\alpha)$ è un campo, e $0 \neq \alpha + 1$ è un elemento di $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. Pertanto, $\alpha + 1$ è invertibile in $\mathbb{Q}[\alpha]$.
     Per trovare esplicitamente l'inverso di $\alpha + 1$ è sufficiente eseguire la divisione con resto di $x^4 - 7x - 10$ per $x + 1$. Facendo i conti, si ottiene

     $$x^4 - 7x - 10 = (x + 1)(x^3 - x^2 + x - 8) - 2.$$

Sostituendo $x = \alpha$ si vede che $(\alpha + 1)(\alpha^3 - \alpha^2 + \alpha - 8) = 2$ e quindi

$$(\alpha + 1)^{-1} = \frac{1}{2}(\alpha^3 - \alpha^2 + \alpha - 8).$$

2. Siano $\pm\alpha, \pm\beta \in \mathbb{C}$ le quattro radici distinte di $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$.

   - [2pt] Calcolare $\alpha\beta$.
   - [4pt] Calcolare $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ e $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$.
   - [3pt] Se L è il campo di spezzamento di $f(x)$, quanto vale $[L : \mathbb{Q}]$?
   - [3pt] Determinare, utilizzando la corrispondenza di Galois, tutte le estensioni intermedie $\mathbb{Q} \subset E \subset L$ tali che $[E : \mathbb{Q}] = 2$.

   Soluzione:

   - L'equazione data si risolve esplicitamente, e le radici sono $\pm\sqrt{2+\sqrt{2}}, \pm\sqrt{2-\sqrt{2}}$. Poniamo allora $\alpha = \sqrt{2+\sqrt{2}}, \beta = \sqrt{2-\sqrt{2}}$. Allora
   $$\alpha\beta = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{2}.$$
   E' importante osservare che $\beta = \alpha^{-1}\sqrt{2}$.
   - Il polinomio $f(x)$ è irriducibile in $\mathbb{Z}[x]$ per il criterio di Eisenstein, ed è quindi irriducibile in $\mathbb{Q}[x]$ per il Lemma di Gauss. Pertanto $f(x)$ è il polinomio minimo di α su $\mathbb{Q}$, e abbiamo $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
   Per quanto riguarda la seconda domanda, notiamo che $\sqrt{2} = \alpha^2 - 2$ appartiene a $\mathbb{Q}(\alpha)$. Di conseguenza, anche $\beta = \alpha^{-1}\sqrt{2}$ appartiene a $\mathbb{Q}(\alpha)$, e quindi $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$. Possiamo concludere che $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 1$.
   - Poiché $\mathbb{Q}(\alpha)$ contiene anche $-\alpha, \pm\beta$, allora $L = \mathbb{Q}(\alpha)$. Allora $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
   - La domanda è delicata. Sappiamo che $L = \mathbb{Q}(\alpha)$ è un'estensione di Galois di $\mathbb{Q}$, poiché è il campo di spezzamento di $f(x)$, la cui separabilità è ovvia, dal momento che siamo in caratteristica 0. Allora il gruppo di Galois $G = \mathrm{Gal}(L/\mathbb{Q})$ possiede 4 elementi, ed è necessariamente abeliano. Possiamo dire di più: è ciclico di ordine 4, oppure è isomorfo a $\mathrm{C}_2 \times \mathrm{C}_2$. Nel primo caso, G possiede un solo sottogruppo di indice 2, mentre nel secondo ne ha 3. Senza informazioni ulteriori, possiamo soltanto concludere, utilizzando la corrispondenza di Galois, che le sottoestensioni di L di grado 2 su $\mathbb{Q}$ sono una oppure tre, e che una di esse è sicuramente $\mathbb{Q}(\sqrt{2})$.
   Possiamo discriminare tra tali due possibilità solo determinando la struttura di G. In effetti, G è ciclico: ogni elemento di G è determinato dalla sua azione su α, e l'immagine di α è uno dei quattro elementi $\pm\alpha, \pm\beta$. Se $\phi \in G$ soddisfa $\phi(\alpha) = \beta$, allora
   $$\phi(\sqrt{2}) = \phi(\alpha^2 - 2) = \beta^2 - 2 = -\sqrt{2},$$
   e quindi
   $$\phi(\beta) = \phi(\alpha^{-1}\sqrt{2}) = \phi(\alpha)^{-1}\phi(\sqrt{2}) = -\beta^{-1}\sqrt{2} = -\alpha.$$
   Ma allora $\phi^2(\alpha) = -\alpha$, e quindi ϕ non ha ordine 2 in G. L'unica altra possibilità è che generi G ciclicamente.

3. Sia $g(x) = x^6 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.

   - [2pt] Fattorizzare $g(x)$ nel prodotto di polinomi irriducibili[1] di $\mathbb{F}_2[x]$.
   - [3pt] Qual è il grado su $\mathbb{F}_2$ del campo di spezzamento di $g(x)$?
   - [3pt] Se $F : L \to L$ è l'automorfismo di Frobenius $x \mapsto x^2$, determinare quanti sono gli elementi di L che sono fissati da F^2.
   - [3pt] Se $1 \neq \gamma \in L$ soddisfa $\gamma^5 = 1$, descrivere gli elementi di L fissati da F^2 per mezzo di espressioni polinomiali in γ.

   Soluzione:

   - $g(0) = g(1) = 1 \neq 0$, e quindi $g(x)$ non possiede fattori lineari in $\mathbb{F}_2[x]$. Provando a dividere $g(x)$ per l'unico polinomio irriducibile di grado 2, si ottiene

     $$g(x) = (x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

     Abbiamo già visto che $g(x)$ non ha fattori lineari, e quindi nemmeno $x^4+x^3+x^2+x+1$ ne ha. Ma l'unico prodotto di polinomi irriducibili di grado 2 è $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, e quindi $x^4 + x^3 + x^2 + x + 1$ è irriducibile in $\mathbb{F}_2[x]$.
   - Il campo di spezzamento L di $g(x)$ deve contenere almeno una radice del polinomio irriducibile $x^4+x^3+x^2+x+1$, e quindi $[L : \mathbb{F}_2] \geq 4$. Ad ogni modo, in $\mathbb{F}_{2^4}$ è il campo di spezzamento di $x^{16} - x \in \mathbb{F}_2[x]$, che è il prodotto di tutti i polinomi irriducibili in $\mathbb{F}_2[x]$ di grado $1, 2, 4$. Pertanto su $\mathbb{F}_{2^4}$ si spezzano entrambi i fattori irriducibili di $g(x)$, e quindi anche $g(x)$. Possiamo quindi concludere che $L = \mathbb{F}_{2^4}$ è un campo di spezzamento di $g(x)$, e quindi $[L : \mathbb{F}_2] = 4$.
   - Il gruppo di Galois $G = \mathrm{Gal}(L/\mathbb{F}_2)$ è ciclico di ordine 4, ed è generato da F. Il sottogruppo generato da F^2 ha indice 2 in G, e quindi fissa un sottocampo di L di grado 2 su $\mathbb{F}_2$. In altre parole, fissa un sottocampo con esattamente 4 elementi.
   - Due degli elementi fissati da F^2 sono $0, 1$. Inoltre, se $\alpha \neq 0, 1$ è fissato da F^2, allora il quarto elemento fissato da F è $\alpha + 1$. Il problema si riduce a trovare quindi un elemento $\neq 0, 1$ fissato da F^2. L'elemento γ è una radice di $x^4 + x^3 + x^2 + x + 1$, e

     $$F^2(\gamma + F^2(\gamma)) = F^2(\gamma) + F^4(\gamma) = F^2(\gamma) + \gamma,$$

     dove abbiamo utilizzato $F^4 = \mathrm{Id}$. Pertanto $\gamma + \gamma^4$ è fissato da F^2, ed è sicuramente $\neq 0, 1$, poiché altrimenti γ soddisferebbe il polinomio x^4+x+1, che ha lo stesso grado del polinomio minimo di γ, ma non ne è multiplo.

[1] Gli elementi irriducibili di $\mathbb{F}_2[x]$ di grado fino a 3 dovreste conoscerli tutti.