Corso di Laurea in Matematica
Algebra 1 - Soluzioni del II Compitino del 08/01/2020

Esercizio 1) Dare risposte sintetiche ad ogni domanda, come indicato, utilizzando solo lo spazio subito sotto.

a) Dire se esiste un campo K tale che $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_{193})$ e che l'estensione $\mathbb{Q} \subset K$ sia di Galois con gruppo di Galois isomorfo a $\mathbb{Z}_8 \times \mathbb{Z}_{24}$. [Scrivere Esiste o Non esiste, e motivare brevemente]

Soluzione: NON ESISTE

Dovrebbe valere $[K : \mathbb{Q}] = |\mathbb{Z}/_8 \times \mathbb{Z}/_{24}| = 8 \cdot 24 = 192$

Allora, poiché $K \subseteq \mathbb{Q}(\zeta_{193})$ e $[\mathbb{Q}(\zeta_{193}) : \mathbb{Q}] = 192$ sarebbe $K = \mathbb{Q}(\zeta_{193})$. Questo è assurdo perché $\mathrm{Aut}\left(\mathbb{Q}(\zeta_{193})/\mathbb{Q}\right) \cong \mathbb{Z}/_{192}$ mentre $\mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}/_8 \times \mathbb{Z}/_{24}$ e $\mathbb{Z}/_{192} \not\cong \mathbb{Z}/_8 \times \mathbb{Z}/_{24}$ (per es. per teorema di classificazione).

b) Stessa domanda di sopra, sostituendo $\mathbb{Q}(\zeta_{193})$ con $\mathbb{Q}(\zeta_{1241})$. [Scrivere Esiste o Non esiste, e motivare brevemente]

Soluzione: ESISTE.

Dato che $1241 = 17 \cdot 73$ (con 17 e 73 primi), sappiamo che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{1241})$ è di Galois e il suo gruppo di Galois è
$$\mathrm{Aut}\left(\mathbb{Q}(\zeta_{1241})/\mathbb{Q}\right) \cong \mathbb{Z}/_{17}^* \times \mathbb{Z}/_{73}^* \cong \mathbb{Z}/_{16} \times \mathbb{Z}/_{72}.$$

Considero il s. gruppo $H = \left((8,0),(0,24)\right)$ di $\mathbb{Z}/_{16} \times \mathbb{Z}/_{72}$ che è normale perché siamo in un contesto abeliano. Allora per i teoremi di corrispondenza di Galois vale che l'estensione $\mathbb{Q} \subseteq \mathrm{Fix}(H)$ è di Galois e il suo gruppo di Galois è
$$\mathrm{Aut}\left(\mathrm{Fix}(H)/\mathbb{Q}\right) \cong \frac{\mathbb{Z}/_{16} \times \mathbb{Z}/_{72}}{((8,0),(0,24))} \cong \mathbb{Z}/_8 \times \mathbb{Z}/_{24}.$$

c) Scrivere la definizione della Ascending Chain Condition per un anello commutativo R. Scrivere in sintesi una dimostrazione del fatto che se R soddisfa la ACC allora ogni ideale di R è generato da un numero finito di elementi.

Soluzione: vedi le dispense (la Definizione 14.2.1 e la dimostrazione del Teorema 14.3.1).

Esercizio 2. Sia $\alpha = \sqrt[4]{3} + \sqrt{3} \in \mathbb{R}$.

a) Calcolare il polinomio minimo $p(x)$ di α su $\mathbb{Q}$ e il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
b) Mostrare che $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[4]{3})$ e calcolare $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}(\alpha)]$.
c) Mostrare che $\mathbb{Q}(\alpha)$ non è un'estensione di Galois di $\mathbb{Q}$
d) Dire se i campi di spezzamento di $p(x)$ e di $x^4 - 3$ coincidono o sono distinti.

Soluzione:

a) Si ha $\alpha - \sqrt{3} = \sqrt[4]{3}$. Quadrando si ottiene $\alpha^2 - 2\alpha\sqrt{3} + 3 = \sqrt{3}$ da cui $\alpha^2 + 3 = (2\alpha + 1)\sqrt{3}$. Quadrando ancora una volta si ottiene $(\alpha^2 + 3)^2 = (2\alpha + 1)^2 3$. Semplificando si ottiene che α soddisfa il polinomio a coefficienti razionali $x^4 - 6x^2 - 12x + 6$. Quest'ultimo è irriducibile per il Criterio di Eisenstein, usando il primo 2 oppure 3. Quindi è il polinomio minimo di α su $\mathbb{Q}$. Il grado di $\mathbb{Q}(\alpha)$ come estensione di $\mathbb{Q}$ è uguale al grado del polinomio minimo di α ed è quindi 4.
b) Per mostrare che $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[4]{3})$ basta mostrare che $\alpha \in \mathbb{Q}(\sqrt[4]{3})$ e questo è ovvio perché α è somma di $\sqrt{3} = (\sqrt[4]{3})^2$ e di $\sqrt[4]{3}$, che sono entrambi membri di $\mathbb{Q}(\sqrt[4]{3})$.
Per quanto riguarda il calcolo del grado, si ha $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Sappiamo già che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Inoltre $\sqrt[4]{3}$ soddisfa il polinomio $x^4 - 3$ che è irriducibile, nuovamente per il Criterio di Eisenstein; pertanto anche $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$. In conclusione $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}(\alpha)] = 4/4 = 1$.
c) Per quanto concluso al punto precedente abbiamo che $\mathbb{Q}(\sqrt[4]{3}) = \mathbb{Q}(\alpha)$. Mostriamo dunque che $\mathbb{Q}(\sqrt[4]{3})$ non è di Galois su $\mathbb{Q}$. Questo è immediato perchè il polinomio irriducibile $x^4 - 3$ possiede almeno una radice in $\mathbb{Q}(\sqrt[4]{3})$, ma non si spezza in fattori lineari dal momento che ha anche le radici non reali $\pm i\sqrt[4]{3}$.
d) Notiamo intanto che il campo di spezzamento di $x^4 - 3$ è $\mathbb{K} = \mathbb{Q}[\sqrt[4]{3}, i]$ che è dunque un'estensione di Galois di $\mathbb{Q}$. Abbiamo poi che $[\mathbb{K} : \mathbb{Q}] = 8$: infatti $[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}[\sqrt[4]{3}]][\mathbb{Q}[\sqrt[4]{3}] : \mathbb{Q}]$; inoltre $[\mathbb{K} : \mathbb{Q}[\sqrt[4]{3}]] \leq 2$, perché i è annullato da $x^2 + 1$, ma $[\mathbb{K} : \mathbb{Q}[\sqrt[4]{3}]] \neq 1$ perché il campo $\mathbb{Q}[\sqrt[4]{3}]$ è contenuto in $\mathbb{R}$. Dunque il campo di spezzamento del polinomio irriducibile $p(x) = x^4 - 6x^2 - 12x + 6$ deve contenere $\mathbb{Q}[\alpha]$ in quanto α è radice di $p(x)$ e deve essere contenuto in $\mathbb{K}$ in quanto $\mathbb{K}$ è un'estensione di Galois contenente α. Il campo di spezzamento di $p(x)$ deve dunque avere grado su $\mathbb{Q}$ che è multiplo di 4, diverso da 4 e divisore di 8, dunque necessariamente 8, ovvero tale campodi spezzamento è proprio $\mathbb{K}$, il campo di spezzamento di $x^4 - 3$.

Esercizio 3. Si consideri il polinomio $g(x) = x^6 - 2x^3 - 1$ e supponiamo di sapere già che è irriducibile in $\mathbb{Q}[x]$. Sia K il suo campo di spezzamento su $\mathbb{Q}$ e sia G il gruppo di Galois $\mathrm{Aut}(K/\mathbb{Q})$.

a) Mostrare che $g(x)$ ha due sole radici reali α e β (dove poniamo $\alpha > \beta$).
b) Mostrare che $[K : \mathbb{Q}] = 12$.
c) Dimostrare che esiste in G un unico elemento θ tale che $\theta(\zeta_3) = \zeta_3^2$ e $\theta(\alpha) = \zeta_3\beta$.
d) Descrivere G.

Soluzione:

a) Osserviamo che $g(x) = (x^3 - 1)^2 - 2$ e quindi $z \in \mathbb{C}$ è radice di $g(x)$ se e solo se $z^3 = 1 \pm \sqrt{2}$. Quindi le uniche radici reali sono $\alpha = \sqrt[3]{1 + \sqrt{2}} > 0$ e $\beta = \sqrt[3]{1 - \sqrt{2}} < 0$.
b) Notiamo che $\alpha\beta = \sqrt[3]{1 - 2} = \sqrt[3]{-1} = -1$. Segue che $\beta \in \mathbb{Q}(\alpha)$.
Quindi il campo di spezzamento di $g(x)$ è dato da $\mathbb{Q}(\alpha, \beta, \zeta_3) = \mathbb{Q}(\alpha, \zeta_3)$.
Poiché il polinomio $g(x)$ è irriducibile abbiamo che $\mathbb{Q}(\alpha)$ ha grado 6 come estensione di $\mathbb{Q}$. Inoltre dato che α è reale anche l'estensione $\mathbb{Q}(\alpha)$ è reale, quindi l'estensione $\mathbb{Q}(\alpha, \zeta_3)$

è una sua estensione propria di grado 2. Essa ha grado 12 su $\mathbb{Q}$ e quindi questo è il grado del campo di spezzamento cercato.

c) Abbiamo la torre di estensioni $\mathbb{Q}(\alpha, \zeta_3) \supset \mathbb{Q}(\zeta_3) \supset \mathbb{Q}$, dove entrambe le estensioni sono di Galois, con $[\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}(\zeta_3)] = 6$. Quindi il polinomio $g(x)$ è irriducibile anche su $\mathbb{Q}(\zeta_3)$ e dunque esiste un elemento $\varphi \in \mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q}(\zeta_3))$ che manda α in $\zeta_3\beta$, che è un'altra radice di $g(x)$. Ovviamente tale φ fissa ζ_3. Inoltre $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$ e dunque la restrizione $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3), \mathbb{Q}(\alpha)) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q})$ è un isomorfismo e quindi esiste un elemento $\psi \in \mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3), \mathbb{Q}(\alpha))$ che manda ζ_3 in ζ_3^2 (e fissa α). La composizione $\varphi \circ \psi$ manda dunque $\zeta_3 \mapsto \zeta_3^2$ e $\alpha \mapsto \zeta_3\beta$ come richiesto.

d) Per quanto detto al punto b) abbiamo che G ha 12 elementi. Si può verificare che l'elemento $\rho = \varphi \circ \psi \in G = \mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3), \mathbb{Q})$ ha ordine 6. Infatti $\rho^2(\alpha) = \zeta_3\alpha$, $\rho^3(\alpha) = \beta$, $\rho^4(\alpha) = \zeta_3^2\alpha$, $\rho^5(\alpha) = \zeta^2\beta$, $\rho^6(\alpha) = \alpha$ e $\rho^i(\zeta_3) = \zeta_3^{(-1)^i}$. Inoltre l'elemento $\psi \in G = \mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3), \mathbb{Q})$ ha ordine 2, non è contenuto nel sottogruppo generato da ρ e vale la relazione $\rho\psi = \psi\rho^{-1}$. Dunque i due elementi di G generano un gruppo isomorfo a D_6 e quindi $G \simeq D_6$.