2^o COMPITINO DI ALGEBRA 1

13 gennaio 2017

1. Sia dato il campo $\mathbb{K} = \mathbb{Q}(\sqrt{3}, \sqrt[3]{7}, \zeta_3)$.

(a) Calcolare il grado di $\mathbb{K}$ su $\mathbb{Q}$.

(b) Dimostrare che $\mathbb{K}$ è un'estensione di Galois di $\mathbb{Q}$.

(c) Calcolare $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$.

(d) Dire se vale l'uguaglianza $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7}) = \mathbb{Q}(\sqrt{3} + \sqrt[3]{7})$.

Soluzione es. 1:

(a) L'estensione $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$ ha grado 3 in quanto $\sqrt[3]{7}$ è radice di $x^3 - 7$, irriducibile su $\mathbb{Q}$ per Eisenstein.

L'estensione $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7})/\mathbb{Q}(\sqrt[3]{7})$ ha grado minore o uguale a 2 in quanto $\sqrt{3}$ è radice di $x^2 - 3$. Inoltre il grado di $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7})/\mathbb{Q}$ è diviso da 3 (contiene la sottoestensione $\mathbb{Q}(\sqrt[3]{7})$ di grado 3 su $\mathbb{Q}$) e da 2 (contiene la sottoestensione $\mathbb{Q}(\sqrt{3})$, di grado 2 su $\mathbb{Q}$ perché $x^2 - 3$ è irriducibile su $\mathbb{Q}$ per Eisenstein). Dunque per le torri $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7})/\mathbb{Q}$ ha grado esattamente 6.

L'estensione $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7}, \zeta_3)/\mathbb{Q}(\sqrt{3}, \sqrt[3]{7})$ ha grado 2 in quanto ζ_3 è radice di x^2+x+1 (dunque il grado è minore o uguale a 2) e inoltre il sottocampo $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7}$ è totalmente reale, mentre $\zeta_3 \notin \mathbb{R}$ in quanto il discriminante di $x^2 + x + 1$ è $-3 < 0$. Dalle torri segue che il grado di $\mathbb{K}$ su $\mathbb{Q}$ è 12.

(b) Il campo $\mathbb{K} = \mathbb{Q}(\sqrt{3}, \sqrt[3]{7}, \zeta_3) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{7}, \zeta_3\sqrt[3]{7})$ è campo di spezzamento di $(x^2 - 3)(x^3 - 7)$ su $\mathbb{Q}$ in quanto contiene tutte le sue radici ($\pm\sqrt{3}$ e $\zeta_3^i\sqrt[3]{7}$, per $i = 0, 1, 2$) ed è generato da alcune di esse. Inoltre il polinomo non costante $(x^2 - 3)(x^3 - 7)$ è separabile in quanto $\mathbb{Q}$ ha caratteristica 0. Dunque $\mathbb{K}$ è un'estensione di Galois.

(c) Notiamo che ζ_3, in quanto radice di x^2+x+1, è data da $-1/2+\sqrt{-3}/2$ e dunque $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$.

Il campo $\mathbb{F} = \mathbb{Q}(\zeta_3, \sqrt[3]{7})$ ha grado 6 su $\mathbb{Q}$ in quanto $\mathbb{K}/\mathbb{F}$ ha grado minore o uguale a 2 ($\mathbb{K}$ è il campo di spezzamento di $x^2 - 3$ su $\mathbb{F}$) e $\mathbb{K}/\mathbb{Q}$ ha grado 12. Il campo $\mathbb{F}$ è campo di spezzamento di $x^3 - 7$ su $\mathbb{Q}$ e dunque $\mathbb{F}/\mathbb{Q}$ è di Galois e $\mathrm{Aut}(\mathbb{F}/\mathbb{Q})$ si immerge in S_3. Poiché il grado dell'estensione è 6, il gruppo $\mathrm{Aut}(\mathbb{F}/\mathbb{Q})$ ha la stessa cardinalità e dunque è necessariamente isomorfo a S_3. Gli automorfismi sono determinati da tutte le possibili permutazioni di $\{\sqrt[3]{7}, \zeta_3\sqrt[3]{7}, \zeta_3^2\sqrt[3]{7}\}$.

Il campo $\mathbb{Q}(\sqrt{3})$ è un'estensione di grado 2 su $\mathbb{Q}$ e quindi è un'estensione di Galois con gruppo $\mathbb{Z}_2$. Gli automorfismi sono tutte le permutazioni di $\{\sqrt{3}, -\sqrt{3}\}$.

L'intersezione $\mathbb{Q}(\sqrt{3}) \cap \mathbb{F}$ è uguale a $\mathbb{Q}$ in quanto $\mathbb{Q}(\sqrt{3})$ avendo grado 2 non contiene sottoestensioni non banali e se fosse $\sqrt{3} \in \mathbb{F}$ avremmo che $\mathbb{F} = \mathbb{K}$ che dunque sarebbe un'estensione di $\mathbb{Q}$ di grado 6.

Avendo che le due estensioni $\mathbb{F}$ e $\mathbb{Q}(\sqrt{3})$ sono di Galois su $\mathbb{Q}$, che la loro composizione è $\mathbb{K}$ e che la loro intersezione è banale, segue che

$$G := \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \mathrm{Aut}(\mathbb{F}/\mathbb{Q}) \times \mathrm{Aut}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = S_3 \times \mathbb{Z}_2.$$

Gli automorfismi di ciascuno dei due campi ($\mathbb{F}$ e $\mathbb{Q}(\sqrt{3})$) si estendono ad automorfismi che agiscono banalmente sull'altro campo. Dunque G è generato da:

$$\sigma : \begin{cases} \sqrt[3]{7} & \mapsto & \zeta_3\sqrt[3]{7} \\ \zeta_3 & \mapsto & \zeta_3 \\ \sqrt{3} & \mapsto & \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{7} & \mapsto & \sqrt[3]{7} \\ \zeta_3 & \mapsto & \zeta_3^2 \\ \sqrt{3} & \mapsto & \sqrt{3} \end{cases} \qquad \rho : \begin{cases} \sqrt[3]{7} & \mapsto & \sqrt[3]{7} \\ \zeta_3 & \mapsto & \zeta_3 \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{cases}$$

dove σ e τ sono un 3-ciclo ed una trasposizione di S_3 e ρ genera $\mathbb{Z}_2$.

(d) L'estensione $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})$ è contenuta in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7})$. Quest'ultima ha grado 6 su $\mathbb{Q}$ perchè possiamo ottenere $\mathbb{K}$ aggiungendo ζ_3, ovvero con un'estensione di grado minore o uguale a 2.
Inoltre $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7}, \sqrt{3}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{7})$, dunque l'estensione $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7})/\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})$ ha grado ≤ 2 perché $\sqrt{3}$ è annullato da un polinomio di grado 2; quindi se i due campi sono distinti il grado dell'estensione deve essere esattamente 2. Mostriamo che questo caso non è possibile.
Ovviamente vale l'uguaglianza $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7}, \sqrt[3]{7}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{7})$ e $\sqrt[3]{7}$ è radice di x^3-7. Se questo polinomio fosse irriducibile su $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})$ allora il grado dell'estensione non potrebbe essere 2 (sarebbe 3). Se invece x^3-7 fosse riducibile su $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})$, allora il campo, che è contenuto in $\mathbb{R}$, dovrebbe contenerne una radice. Tuttavia l'unica radice reale è $\sqrt[3]{7}$, da cui otterremmo che $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{7})$.

2. Si consideri il polinomio a coefficienti interi $p(x) = x^6 - n^3$, $n \in \mathbb{Z}$.

(a) al variare di n tra gli interi descrivere il campo di spezzamento $\mathbb{F}$ di $p(x)$ su $\mathbb{Q}$ e calcolarne il grado su $\mathbb{Q}$;

(b) al variare di n tra gli interi descrivere il gruppo di Galois $\mathrm{Aut}(\mathbb{F}/\mathbb{Q})$;

(c) per $n = 7$ descrivere il campo di spezzamento $\mathbb{K}$ di $p(x)$ su $\mathbb{F}_{11}$ e calcolarne il grado su $\mathbb{F}_{11}$.

Soluzione es. 2:

(a) Il polinomio $p(x)$ si fattorizza come $(x^2-n)(x^4+nx^2+n^2) = (x^2-n)(x^2-\zeta_3^2 n)(x^2-\zeta_3 n)$. Dunque $\sqrt{n}$ e (se $n \neq 0$) ζ_3 devono appartenere al campo di spezzamento. Ovviamente se $n=0$ il campo di spezzamento è $\mathbb{Q}$ stesso e il grado è quindi 1, con gruppo di Galois banale. Nel seguito (anche per il punto (b)) supponiamo dunque $n \neq 0$.

Le radici di $p(x)$ sono date da $\pm\sqrt{n}, \pm\zeta_3\sqrt{n}, \pm\zeta_3^2\sqrt{n}$. Chiaramente $\sqrt{n}, \zeta_3$ bastano per generare il campo di spezzamento che è quindi dato da

$$\mathbb{F} = \mathbb{Q}(\zeta_3, \sqrt{n}).$$

Per determinarne il grado di $\mathbb{F}$ su $\mathbb{Q}$ notiamo che $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ e quindi ci basta stabilire se $\sqrt{n} \in \mathbb{Q}(\zeta_3)$ (in tal caso il campo di spezzamento è proprio $\mathbb{Q}(\zeta_3)$ ed ha grado 2) o $\sqrt{n} \notin \mathbb{Q}(\zeta_3)$ (in cal caso $\mathbb{F}$ avrà grado 4 su $\mathbb{Q}$ in quanto è ottenuto con un'estensione non banale di grado al più 2).

La radice ζ_3 è radice di $x^2 + x + 1$, che ha discriminante -3, quindi $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Affermiamo che $\sqrt{n} \in \mathbb{Q}(\sqrt{-3})$ se e solo se n è un quadrato a meno di multipli di -3. Ovviamente $\sqrt{n} \in \mathbb{Q}(\sqrt{-3})$ se n è un quadrato in $\mathbb{Z}$, mentre se $-3n = m^2$, $m \in \mathbb{Z}$, allora $\sqrt{n} = m/\sqrt{-3} \in \mathbb{Q}(\sqrt{-3})$. Viceversa, supponiamo che n sia il quadrato di un elemento di $\mathbb{Q}(\sqrt{-3})$. Allora possiamo scrivere $\sqrt{n} = a + b\sqrt{-3}$, con $a, b \in \mathbb{Q}$ e dunque $n = a^2 - 3b^2 + 2ab\sqrt{-3}$ e poiché $n \in \mathbb{Q}$ si deve avere che $2ab = 0$ e quindi uno tra a e b deve essere nullo. Quindi n deve essere della forma a^2 o della forma $-3b^2$, con $a, b \in \mathbb{Q}$. Essendo n intero, è necessario che lo siano anche a e b.

(b) Abbiamo già escluso il caso $n = 0$.

Supponiamo prima che n sia un quadrato in $\mathbb{Z}$. Il tal caso il grado dell'estensione è 2 e dunque il gruppo di Galois è $\mathbb{Z}_2$. L'elemento non banale agisce mandando $\zeta_3 \mapsto \zeta_3^2$.

Analogamente se $-3n$ è un quadrato in $\mathbb{Z}$, il grado dell'estensione è 2 e dunque il gruppo di Galois è $\mathbb{Z}_2$. L'elemento non banale agisce comunque mandando $\zeta_3 \mapsto \zeta_3^2$.

Supponiamo infine che $n, -3n$ non siano quadrati in $\mathbb{Z}$. In tal caso $\mathbb{Q}(\zeta_3)$ e $\mathbb{Q}(\sqrt{n})$ sono due estensioni di $\mathbb{Q}$ di grado due distinte (perché nel punto (a) si è mostrato che $\sqrt{n} \notin \mathbb{Q}(\zeta_3)$). Quindi il gruppo di Galois $\mathrm{Aut}(\mathbb{F}/\mathbb{Q})$ ha ordine 4 e contiene almeno 2 sottogruppi distinti di indice 2, quindi non può essere $\mathbb{Z}_4$ e deve essere necessariamente $\mathbb{Z}_2 \times \mathbb{Z}_2$, generato da

$$\sigma : \begin{cases} \zeta_3 & \mapsto \zeta_3^2 \\ \sqrt{n} & \mapsto \sqrt{n} \end{cases} \qquad \text{e} \qquad \tau : \begin{cases} \zeta_3 & \mapsto \zeta_3 \\ \sqrt{n} & \mapsto -\sqrt{n}. \end{cases}$$

(c) Analogamente al punto (a) possiamo fattorizzare $p(x) = (x^2 - n)(x^4 + nx^2 + n^2)$. Notiamo ora che $3 \nmid 10 = |\mathbb{F}_{11}^*|$ e dunque le radici terze dell'unità non appartengono a $\mathbb{F}_{11}$, ma alla sua estensione di grado 2, $\mathbb{F}_{11^2}$. Quindi in $\mathbb{F}_{11^2}$ possiamo fattorizzare $p(x) = (x^2 - n)(x^2 - \zeta_3^2 n)(x^2 - \zeta_3 n)$.

Chiaramente, anche se n non è un quadrato in $\mathbb{F}_{11}$, lo è sempre in $\mathbb{F}_{11^2}$ perché, se n non è un quadrato in $\mathbb{F}_{11}$, $\mathbb{F}_{11^2}$ è il campo di capo di spezzamento di $x^2 - n$. Dunque $\mathbb{F}_{11^2}$ contiene sicuramente $\sqrt{n}$ e le radici terze dell'unità ed è quindi il campo di spezzamento di $p(x)$, che ha quindi grado 2 su $\mathbb{F}_{11}$.