SOLUZIONI DELL'ESONERO DI ALGEBRA 3, 18/11/2013

Esercizio 1. Sia $\alpha_{a,b} := a\sqrt{3} + b\sqrt{7}$ dove $a, b \in \mathbb{Q}$ ed $\alpha := \alpha_{1,1}$.

(1) Si mostri che $\mathbb{Q}(\alpha)/\mathbb{Q}$ è una estensione di Galois.
(2) Si calcoli il reticolo dei sottocampi di $\mathbb{Q}(\alpha)/\mathbb{Q}$.
(3) Si calcoli il polinomio minimo di α su $\mathbb{Q}$.
(4∗) Si mostri che $\mathbb{Q}(\alpha_{a,b})/\mathbb{Q}$ è una estensione di Galois e che $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_{a,b})$ se e solo se $ab \neq 0$.

Soluzione: Posto $F := \mathbb{Q}\left(\sqrt{3}, \sqrt{7}\right)$, mostriamo che $[F : \mathbb{Q}] = 4$. Infatti $X^2 - 3, X^2 - 7 \in \mathbb{Q}[X]$ sono irriducibili (criterio di Eisenstein) e dunque $\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{7}\right) : \mathbb{Q}\right] = 2$. Inoltre $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{7}\right)$, perchè altrimenti si avrebbe $\sqrt{3} = x + \sqrt{7}y$ per qualche $x, y \in \mathbb{Q}$. Chiaramente non è possibile che $x = y = 0$. Se $x = 0$ (rispettivamente $y = 0$), allora $\sqrt{3}/\sqrt{7} = y \in \mathbb{Q}$ (rispettivamente $\sqrt{3} = x \in \mathbb{Q}$, il che non è possibile) e dunque $X^2 - 3/7 \in \mathbb{Q}[X]$ sarebbe riducibile, il che non è possibile poichè $7X^2 - 3 \in \mathbb{Q}[X]$ è irriducibile (criterio di Eisenstein). Dunque $xy \neq 0$; ma allora

$$3 = x^2 + 2xy\sqrt{7} + 7y^2 \Rightarrow \sqrt{7} \in \mathbb{Q},$$

il che è assurdo. Dunque $\left[F : \mathbb{Q}\left(\sqrt{7}\right)\right] = 2$ e $[F : \mathbb{Q}] = 4$ per moltiplicatività dei gradi. Notiamo che, poichè $\mathbb{Q}\left(\sqrt{3}\right)/\mathbb{Q}$ e $\mathbb{Q}\left(\sqrt{7}\right)/\mathbb{Q}$ sono di Galois e $\mathbb{Q}\left(\sqrt{3}\right) \cap \mathbb{Q}\left(\sqrt{7}\right) = \mathbb{Q}$, $F/\mathbb{Q}$ è di Galois con gruppo di Galois

$$G_{F/\mathbb{Q}} \simeq G_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}} \times G_{\mathbb{Q}(\sqrt{7})/\mathbb{Q}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Se $1 \neq \sigma_3 \in \mathbb{Q}\left(\sqrt{3}\right)$ e $1 \neq \sigma_7 \in \mathbb{Q}\left(\sqrt{7}\right)$, i sottogruppi propri di $G_{F/\mathbb{Q}}$ sono $\langle\sigma_3\rangle$, $\langle\sigma_7\rangle$ e $\langle\sigma_3\sigma_7\rangle$ che corrispondono a tutti e soli i sottocampi propri $F^{\langle\sigma_3\rangle} = \mathbb{Q}\left(\sqrt{7}\right)$ $F^{\langle\sigma_7\rangle} = \mathbb{Q}\left(\sqrt{3}\right)$ e $F^{\langle\sigma_3\sigma_7\rangle} = \mathbb{Q}\left(\sqrt{3}\sqrt{7}\right)$.

Abbiamo $\mathbb{Q}(\alpha_{a,b}) \subset F$; mostriamo che $\mathbb{Q}(\alpha_{a,b}) = F$ se e solo se $ab \neq 0$ e che, in ogni caso, $\mathbb{Q}(\alpha_{a,b})/\mathbb{Q}$ è una estensione di Galois. Se $a = b = 0$ (rispettivamente se $a = 0$ e $b \neq 0$ o se $a \neq 0$ e $b = 0$), allora $\mathbb{Q}(\alpha_{a,b}) = \mathbb{Q}$ (rispettivamente $\mathbb{Q}(\alpha_{a,b}) = \mathbb{Q}\left(\sqrt{7}\right)$ o $\mathbb{Q}(\alpha_{a,b}) = \mathbb{Q}\left(\sqrt{3}\right)$). Dunque in questo caso $\mathbb{Q}(\alpha_{a,b}) \neq F$ e $\mathbb{Q}(\alpha_{a,b})/\mathbb{Q}$ è di Galois. Se $ab \neq 0$

$$\alpha_{a,b}^2 = 3a^2 + 2ab\sqrt{3}\sqrt{7} + 7b^2 \Rightarrow \sqrt{3}\sqrt{7} \in \mathbb{Q}(\alpha_{a,b}).$$

Segue che

$$3a\sqrt{7} + 7b\sqrt{3} = \sqrt{3}\sqrt{7}\alpha_{a,b} \in \mathbb{Q}(\alpha_{a,b})$$

e quindi

$$\begin{aligned}\left(3a - \frac{7}{a}b^2\right)\sqrt{7} &= 3a\sqrt{7} + 7b\sqrt{3} - \frac{7}{a}ba\sqrt{3} - \frac{7}{a}bb\sqrt{7} \\ &= 3a\sqrt{7} + 7b\sqrt{3} - \frac{7}{a}b\alpha_{a,b} \in \mathbb{Q}(\alpha_{a,b}).\end{aligned}$$

Si ha $3a - \frac{7}{a}b^2 = 0$ se e solo se $3/7 = (b/a)^2$ se e solo se $\sqrt{3}/\sqrt{7} = \pm b/a \in \mathbb{Q}$, il che non è possibile come già notato. Dalla precedente relazione segue dunque che $\sqrt{7} \in \mathbb{Q}(\alpha_{a,b})$. Dunque, avendo già mostrato che $\sqrt{3}\sqrt{7} \in \mathbb{Q}(\alpha_{a,b})$, deduciamo che $\sqrt{3} = \sqrt{3}\sqrt{7}/\sqrt{7} \in \mathbb{Q}(\alpha_{a,b})$ e pertanto $F = \mathbb{Q}(\alpha_{a,b})$.

Con ciò si è mostrato (1), (2) e (4); mostriamo (5) (e quindi (3)). L'orbita di $\alpha_{a,b}$ sotto l'azione di $G_{F/\mathbb{Q}}$ è data da

$$\begin{aligned}&\{\alpha_{a,b}, \sigma_3(\alpha_{a,b}), \sigma_7(\alpha_{a,b}), \sigma_3\sigma_7(\alpha_{a,b})\} = \{\alpha_{a,b}, \alpha_{-a,b}, \alpha_{a,-b}, \alpha_{-a,-b}\}\\ &= \{\alpha_{a,b}, \alpha_{-a,b}, -\alpha_{-a,b}, -\alpha_{a,b}\}.\end{aligned}$$

Dunque

$$\begin{aligned}f_{a,b}(X) &:= \prod_{\sigma\in G_{F/\mathbb{Q}}} (X - \sigma(\alpha_{a,b})) = (X-\alpha_{a,b})(X+\alpha_{a,b})(X-\alpha_{-a,b})(X+\alpha_{-a,b})\\ &= \left(X^2-\alpha_{a,b}^2\right)\left(X^2-\alpha_{-a,b}^2\right) = X^4 - \left(\alpha_{a,b}^2+\alpha_{-a,b}^2\right)X^2 + \alpha_{a,b}^2\alpha_{-a,b}^2.\end{aligned}$$

Abbiamo

$$\begin{aligned}\alpha_{a,b}^2 &= 3a^2 + 2ab\sqrt{3}\sqrt{7} + 7b^2,\\ \alpha_{-a,b}^2 &= 3a^2 - 2ab\sqrt{3}\sqrt{7} + 7b^2,\\ \alpha_{a,b}^2\alpha_{-a,b}^2 &=\end{aligned}$$

da cui

$$f_{a,b}(X) = X^4 - 2\left(3a^2+7b^2\right)X^2 + \left(9a^4+49b^4-42a^2b^2\right).$$

Se $ab \neq 0$ abbiamo già verificato che $F = \mathbb{Q}(\alpha_{a,b})$ e pertanto $f_{a,b}(X)$ è il polinomio minimo di $\alpha_{a,b}$ su $\mathbb{Q}$. Se $a = b = 0$ (rispettivamente se $a = 0$ e $b \neq 0$ o se $a \neq 0$ e $b = 0$), allora $\alpha_{a,b} = 0$ (rispettivamente $\alpha_{a,b} = b\sqrt{7}$ o $\alpha_{a,b} = a\sqrt{3}$) ed il polinomio minimo di $\alpha_{a,b}$ su $\mathbb{Q}$ è X (rispettivamente $X^2 - 7b^2$ o $X^2 - 3a^2$).

Esercizio 2. Sia $f(X) := \left(X^2-2\right)\left(X^3-3X-1\right) \in \mathbb{Q}[X]$.

(1) Sia L il campo di spezzamento di $X^3 - 3X - 1$ su $\mathbb{Q}$. Si determinino il grado $[L:\mathbb{Q}]$ e il gruppo di Galois $\mathrm{Gal}_{L/\mathbb{Q}}$;
(2) Sia F il campo di spezzamento del polinomio $f(X) \in \mathbb{Q}[X]$. Si calcolino il grado $[F:\mathbb{Q}]$ e il gruppo di Galois $\mathrm{Gal}_{F/\mathbb{Q}}$.
(3) Si calcoli il reticolo dei sottocampi di F.

Soluzione: Il polinomio $X^3 - 3X - 1 \in \mathbb{Q}[X]$ è irriducibile (poichè ridotto modulo 2 non ha radici) ed ha discriminante $-4(-3)^3 - 27(-1)^2 = 81 = 9^2$. Dunque il gruppo di Galois del suo campo di spezzamento K è $\simeq \mathbb{Z}/3\mathbb{Z}$. Detta $r \in \overline{\mathbb{Q}}$ una radice di $X^3 - 3X - 1 \in \mathbb{Q}[X]$, si ha $\mathbb{Q}(r) \subset K$ e l'uguaglianza segue per questioni di grado. In particolare, $\mathbb{Q}(r)/\mathbb{Q}$ è di Galois, mentre $F/\mathbb{Q}(r)$ è di Galois perchè $F/\mathbb{Q}$ è di Galois.

Poichè $X^2 - 2 \in \mathbb{Q}[X]$ è irriducibile (criterio di Eisenstein), $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ è di Galois ed ha grado 2. Posto $L := \mathbb{Q}\left(\sqrt{2}\right) \cap \mathbb{Q}(r)$ si ha $[L:\mathbb{Q}] \mid \left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right] = 2$ e $[L:\mathbb{Q}] \mid [\mathbb{Q}(r):\mathbb{Q}] = 3$, da cui si deduce $\mathbb{Q}\left(\sqrt{2}\right) \cap \mathbb{Q}(r) = \mathbb{Q}$. Poichè $F = \mathbb{Q}\left(\sqrt{2}, r\right)$ e $\mathbb{Q}\left(\sqrt{2}\right) \cap \mathbb{Q}(r) = \mathbb{Q}$,

$$G_{F/\mathbb{Q}} \simeq G_{\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}} \times G_{\mathbb{Q}(r)/\mathbb{Q}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}.$$

I sottogruppi propri di un gruppo ciclico sono in biiezione con i divisori dell'ordine del gruppo. Pertanto $G_{F/\mathbb{Q}(r)} \simeq G_{\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}}$ e $G_{F/\mathbb{Q}\left(\sqrt{2}\right)} \simeq G_{\mathbb{Q}(r)/\mathbb{Q}}$ sono i sottogruppi propri di $G_{F/\mathbb{Q}}$, che corrispondono a tutti e soli i sottocampi propri $\mathbb{Q}(r)$ e $\mathbb{Q}\left(\sqrt{2}\right)$. Con ciò si è mostrato (1) e (2); mostriamo (3).

Abbiamo già notato che $F/\mathbb{Q}(r)$ e $\mathbb{Q}(r)/\mathbb{Q}$ sono estensioni di Galois e che $G_{\mathbb{Q}(r)/\mathbb{Q}} \simeq \mathbb{Z}/3\mathbb{Z}$. Come notato, poichè $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ è di Galois e $\mathbb{Q}\left(\sqrt{2}\right) \cap \mathbb{Q}(r) = \mathbb{Q}$, $F/\mathbb{Q}(r)$ è di Galois e l'applicazione di restrizione

$$G_{F/\mathbb{Q}(r)} \to G_{\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)\cap\mathbb{Q}(r)} = G_{\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}} \simeq \mathbb{Z}/2\mathbb{Z}$$

è un isomorfismo.

Esercizio 3. Sia data una estensione E/F e sia $Aut(E/F)$ il gruppo degli automorfismi di E che fissano F (elemento per elemento). Si mostri che, se $S \subset E$ è un sottoinsieme e se $H \subset Aut(E/F)$ è un sottogruppo finito tale che $E^H = F(S)$, allora

$$H = \{\sigma \in Aut(E/F) : \forall s \in S, \sigma(s) = s\}.$$

Soluzione: Abbiamo $\sigma(s) = s$ per ogni $s \in S$, se $\sigma \in Aut(E/F(S))$ e, viceversa, se $\sigma(s) = s$ per ogni $s \in S$ con $\sigma \in Aut(E/F)$, allora $\sigma(x) = x$ per ogni $x \in F(S)$ e pertanto $\sigma \in Aut(E/F(S))$. In altre parole si ha l'equivalenza $\sigma \in Aut(E/F(S)) \Leftrightarrow \forall s \in S, \sigma(s) = s$, dove $\sigma \in Aut(E/F)$, ovvero

$$Aut(E/F(S)) = \{\sigma \in Aut(E/F) : \forall s \in S, \sigma(s) = s\}$$

Poichè $E^H = F(S)$ si ha $Aut\left(E/E^H\right) = Aut(E/F(S))$; ma poichè $H \subset Aut(E/F)$ è un sottogruppo finito di $Aut(E)$, per il teorema di Artin $H = Aut\left(E/E^H\right)$. Dunque $H = Aut(E/F(S))$, da cui la tesi.