SOLUZIONI DELL'ESAME DI ALGEBRA 3, 29/07/2014

Esercizio 1. Si consideri il polinomio $f(X) := X^7 - 13 \in \mathbb{Q}[X]$.

(a) Si presenti il suo campo di spezzamento E (su $\mathbb{Q}$) nella forma $E = \mathbb{Q}(\alpha, \beta)$ per opportuni $\alpha, \beta \in \overline{\mathbb{Q}}$.
(b) Si calcoli $[E : \mathbb{Q}]$.
(c) Si mostri che $G_{E/\mathbb{Q}}$ è un prodotto semidiretto.
(d) Si fornisca una presentazione di $G_{E/\mathbb{Q}}$ come prodotto semidiretto.

Soluzione: (a) Il polinomio $f(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein applicato al primo 13. Sia α una qualunque radice di $f(X)$. Se ζ è una radice primitiva settima dell'unità, le radici di $f(X)$ sono

$$R_f = \left\{\alpha\zeta^i : i = 0, ..., 6\right\}.$$

Dunque $\mathbb{Q}(R_f)$ è il campo di spezzamento e chiaramente $\mathbb{Q}(R_f) \subset \mathbb{Q}(\alpha, \zeta)$. Viceversa $\alpha, \alpha\zeta \in R_f \subset \mathbb{Q}(R_f)$, da cui $\zeta = \frac{\alpha\zeta}{\alpha} \in \mathbb{Q}(R_f)$ e, pertanto, $E := \mathbb{Q}(R_f) = \mathbb{Q}(\alpha, \zeta)$.

(b) Si ha $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 7$ e $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_7) = 6$, dove $\Phi_7(X) \in \mathbb{Q}[X]$ è il settimo polinomio ciclotomico. Segue dalla moltiplicatività dei gradi che, poichè $(7, 6) = 1$,

$$\begin{aligned} &[E : \mathbb{Q}] = 7 \cdot 6 = 42, \\ &[\mathbb{Q}(\alpha) : \mathbb{Q}] = [E : \mathbb{Q}(\zeta)] = 7 \\ &\text{e } [\mathbb{Q}(\zeta) : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)] = 6. \end{aligned}$$

In particolare notiamo che $\mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha) = \mathbb{Q}$ poichè $(7, 6) = 1$.

($c - d$) Poichè $E = F(\alpha)$ con $\mu_7 \subset F = \mathbb{Q}(\zeta)$ ed $[E : F] = 7$, dalla teoria delle estensioni cicliche sappiamo che $G_{E/\mathbb{Q}(\zeta)} \simeq \mu_7$, mediante l'applicazione $g \mapsto \zeta_g$, dove ζ_g è caratterizzato dall'equazione $\frac{g(\alpha)}{\alpha} = \zeta_g$. Sia dunque $\sigma \in G_{E/\mathbb{Q}(\zeta)}$ l'unico automorfismo tale che $\sigma(\alpha) = \alpha\zeta$: poichè ζ genera μ_7, $G_{E/\mathbb{Q}(\zeta)} = \langle\sigma\rangle \simeq \frac{\mathbb{Z}}{7\mathbb{Z}}$. Notiamo che, per induzione, si ha

$$\begin{aligned} \sigma^i(\alpha) &= \sigma\left(\sigma^{i-1}(\alpha)\right) = \sigma\left(\alpha\zeta^{i-1}\right) \\ &= \sigma(\alpha)\,\sigma(\zeta)^{i-1} = \alpha\zeta\zeta^{i-1} = \alpha\zeta^i. \end{aligned} \tag{1}$$

Poichè $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois e $\mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha) = \mathbb{Q}$, sappiamo che l'applicazione di restrizione

$$G_{E/\mathbb{Q}(\alpha)} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$$

è un isomorfismo.

Dalla teoria delle estensioni ciclotomiche, sappiamo anche che $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times$ mediante l'applicazione $g \mapsto i_g$, dove i_g è caratterizzato dall'equazione $g(\zeta) = \zeta^{i_g}$. Sappiamo che $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times$ è un gruppo ciclico ed esplitamente è generato dalla moltiplicazione per 3. Dunque $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \langle\rho\rangle$, dove ρ è caratterizzato da $\rho(\zeta) = \zeta^3$ e, poichè la restrizione $G_{E/\mathbb{Q}(\alpha)} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è un isomorfismo, si ha anche $G_{E/\mathbb{Q}(\alpha)} = \langle\rho\rangle$.

Notiamo che $\sigma^i, \rho\sigma\rho^{-1} \in G_{E/\mathbb{Q}(\zeta)} \lhd G_{E/\mathbb{Q}}$ e, poichè $E = F(\alpha)$ con $F = \mathbb{Q}(\zeta)$, entrambi questi elementi sono caratterizzato dalla loro azione su α. Abbiamo

$$\begin{aligned} \rho\left(\sigma\left(\rho^{-1}(\alpha)\right)\right) &= \rho(\sigma(\alpha)) = \rho(\alpha\zeta) = \rho(\alpha)\,\rho(\zeta) \\ &= \alpha\rho(\zeta) = \alpha\zeta^3 \end{aligned}$$

a dal confronto con (1) segue $\rho\sigma\rho^{-1} = \sigma^3$. Dunque

$$G_{E/\mathbb{Q}} = G_{E/\mathbb{Q}(\zeta)} \rtimes G_{E/\mathbb{Q}(\alpha)} = \langle\sigma\rangle \rtimes \langle\rho\rangle \simeq \frac{\mathbb{Z}}{7\mathbb{Z}} \rtimes_\varphi \frac{\mathbb{Z}}{6\mathbb{Z}}$$

dove $\varphi : \langle\rho\rangle \to Aut(\langle\sigma\rangle)$ è caratterizzato da $\varphi(\rho)(\sigma) = \rho\sigma\rho^{-1} = \sigma^3$.

Esercizio 2. Si determini il gruppo di Galois $G_{E/\mathbb{Q}}$ del campo di spezzamento $E/\mathbb{Q}$ del polinomio

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

Soluzione: Mostriamo per cominciare che $f(X) := X^3 - X^2 + 1 \in \mathbb{Q}[X]$ è irriducibile. Poichè $\mathbb{Z}$ è un UFD possiamo applicare il Lemma di Gauss: essendo $f(X) \in \mathbb{Z}[X]$ primitivo, basta verificare che è irriducibile in $\mathbb{Z}[X]$ e, per fare ciò, basta mostrare che il polinomio

$$\overline{f}(X) = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$$

ottenuto per riduzione modulo 2 è irriducibile. Infatti non ha radici ed avendo grado 3 l'irriducibilità segue. Si ha

$$f'(X) = 3X^2 - 2X = X(3X - 2),$$

da cui vediamo che i massimi ed i minimi locali di $f(X)$ si hanno in $X = 0$ o $\frac{2}{3}$. Poichè $f(0) = 1$ ed $f\left(\frac{2}{3}\right) = \frac{23}{27} > 0$ deduciamo che $f(X)$ ha due radici complesse distinte; segue che, detto E_f il campo di spezzamento di $f(X)$, il coniugio si restringe ad un automorfismo di ordine 2 di $E_f/\mathbb{Q}$. Dunque si ha $G_{E_f/\mathbb{Q}} \simeq S_3$ (infatti le sole possibilità sono $G_{E_f/\mathbb{Q}} \simeq S_3$ oppure $G_{E_f/\mathbb{Q}} \simeq A_3$, essendo $G_{E_f/\mathbb{Q}}$ un sottogruppo di S_3 che agisce transitivamente su $\{1,2,3\}$; poichè esiste un 2-ciclo in $G_{E_f/\mathbb{Q}}$ la seconda possibilità è da escludere).

D'altra parte $g(X) := X^2 - 2 \in \mathbb{Q}[X]$ è irriducibile (per il criterio di Eisenstein applicato al primo 2) ed ha gruppo di Galois $G_{E_g/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Poichè $E_f/\mathbb{Q}$ ed $E_g/\mathbb{Q}$ sono di Galois e poichè si ha $E = E_f E_g$ deduciamo dalla teoria generale che

$$G_{E/\mathbb{Q}} \hookrightarrow G_{E_f/\mathbb{Q}} \times G_{E_g/\mathbb{Q}}$$

ha per immagine il sottogruppo

$$H := \left\{(g_1, g_2) : g_{1|E_f \cap E_g} = g_{2|E_f \cap E_g}\right\}.$$

Mostriamo che $E_f \cap E_g = \mathbb{Q}$, da cui seguirà

$$G_{E/\mathbb{Q}} \xrightarrow{\sim} G_{E_f/\mathbb{Q}} \times G_{E_g/\mathbb{Q}} \simeq S_3 \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

Se infatti $E_f \cap E_g \neq \mathbb{Q}$ deduciamo che $E_f \cap E_g = E_g$ (essendo $E_f \cap E_g \subset E_g$ ed $[E_g : \mathbb{Q}] = 2$). Dunque si avrebbe

$$\mathbb{Q}\left(\sqrt{2}\right) = E_g = E_f \cap E_g \subset E_f.$$

Segue che $\mathbb{Q}(i)$ è l'unico sottocampo quadratico di E_f (che corrisponde all'unico sottogruppo di indice due in S_3). Siano $\{r, c, \overline{c}\}$ le radici di $f(X)$, di cui r è l'unica radice reale e $c, \overline{c}$ le due radici complesse non reali coniugate. Allora posto

$$\Delta := (r - c)(r - \overline{c})(c - \overline{c})$$

[1] Il discriminate di una cubica della forma

$$f(X) := aX^3 + bX^2 + cX + d$$

è dato dalla formula

$$D(f) := 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$$

...ma ciò non dovrebbe servire...piuttosto si utilizzi la definizione!

si ha $\overline{\Delta} = -\Delta^2$. Segue che $\mathbb{Q}(\Delta)$ è l'unico sottocampo quadratico di E_f e si deve avere $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\Delta)$; ciò non è possibile perchè a sinistra il coniugio si restringe all'indentità, mentre ciò non accade a destra.

Esercizio 3. Sia E/F una estensione di Galois finita. Si mostri che, se $p \mid [E:F]$ e p è primo, allora esiste un campo K tale che $F \subset K \subset E$ e $[E:K] = p$. Se si assume solamente che E/F sia separabile e finita ciò è vero?

Soluzione: Supponiamo per cominciare che E/F sia una estensione separabile e finita (ma non necessariamente normale). Detta $\widetilde{E}/F$ la chiusura normale di E/F e posto $G := G_{\widetilde{E}/F}$, possiamo scrivere $E = \widetilde{E}^H$ per qualche sottogruppo $H \subset G$ tale che

$$p \mid [E:F] = \left[\widetilde{E}^H : \widetilde{E}^G\right] = [G:H] \mid \#G.$$

Per il teorema di Cauchy deduciamo che esiste un sottogruppo $H_p \subset G$ tale che $\#H_p = p$ e quindi

$$\left[\widetilde{E} : \widetilde{E}^{H_p}\right] = [H_p : 1] = p.$$

Se dunque $E = \widetilde{E}$ (ovvero E/F è di Galois) deduciamo la tesi con $K = \widetilde{E}^{H_p} = E^{H_p}$.

Mostriamo che la tesi non è vera se si assume solamente che E/F è separabile e finita considerando $\widetilde{E} = E_f$ campo di spezzamento di un polinomio $f(X) \in \mathbb{Q}[X]$ di grado 4 tale che $G_{E_f/\mathbb{Q}} = S_4$ (ad esempio $f(X) = X^4 - 4X + 2$). Cerchiamo un sottocampo $E = \widetilde{E}^H \subset \widetilde{E}$ tale che

$$4 = [E:F] = [G:H]$$

ma tale che non esistano sottocampi $K = \widetilde{E}^{H_2}$ tali che $F \subset K = \widetilde{E}^{H_2} \subset E = \widetilde{E}^H$ e

$$2 = [K:F] = [G:H_2].$$

In altre parole troviamo il controesempio mostrando che esiste in S_4 un sottogruppo H di indice 4 tale che non esistano sottogruppi $H_2 \supset H$ di indice 2. I sottogruppi di indice 4 in S_4 sono i sottogruppi di ordine 6 in S_4, ovvero gli stabilizzanti $S(i) \simeq S_3$ dell'indice $i \in \{1,2,3,4\}$: mostricamo che $\nexists H_2 \supset S_3 =: S(4)$ tale che $[S_4 : H_2] = 2$. Si ha infatti in tal caso $\#H_2 = 12$ e quindi $H = A_4$. Ma $S_3 \nsubseteq A_4$ poichè esistono 2-cicli in S_3.

Esercizio 4. Si consideri l'estensione $K = \mathbb{Q}(\sqrt{7}, \zeta_5)$ dove $\zeta_5 = \exp^{\frac{2\pi i}{5}}$ è una radice primitiva quinta dell'unità.

(*i*) Determinare il grado di $[K:\mathbb{Q}]$.
(*ii*) Determinare l'anello degli interi di K.

Soluzione:

(i) Il campo K è ottenuto come il composto di due estensioni Galoisiane di $\mathbb{Q}$, l'una $L_1 = \mathbb{Q}(\sqrt{7})$ di grado 2 e l'altra $L_2 = \mathbb{Q}(\zeta_5)$ il quinto campo ciclotomico, di grado 4 su $\mathbb{Q}$. Concludiamo che anche K è di Galois su $\mathbb{Q}$ di grado $\frac{[L_1:\mathbb{Q}][L_2:\mathbb{Q}]}{[L_1\cap L_2:\mathbb{Q}]}$. L'estensione $L_1 \cap L_2$ di $\mathbb{Q}$ ha grado 1 o 2 essendo contenuta in L_1. Visto che il campo L_2 ha gruppo di Galois ciclico di ordine 4, L_2 contiene un unico sottocampo di grado 2 su $\mathbb{Q}$ per il teorema fondamentale della teoria di Galois, ovvero $\mathbb{Q}(\sqrt{5})$ per il Corollario 3.9. Se $[L_1 \cap L_2 : \mathbb{Q}] = 2$ allora $\mathbb{Q}(\sqrt{5}) = L_1 \cap L_2 = L_1 = \mathbb{Q}(\sqrt{7})$ il che è impossibile. Concludo allora che $L_1 \cap L_2 = \mathbb{Q}$ e quindi $[K:\mathbb{Q}] = 8$.

[2]Infatti $\Delta = \sqrt{D}$, dove D è il discriminante di $f(X)$.

(ii) Il discriminate di L_1 su $\mathbb{Q}$ è $4 \cdot 7 = 28$ per l' Esercizio 4.13. Il discriminate di L_2 su $\mathbb{Q}$ è 5^3 per il Corollario 3.7. Essendo i due discriminati coprimi segue che $\mathcal{O}_K = \mathcal{O}_{L_1}\mathcal{O}_{K_2}$ per il Teorema 4.14 ovvero $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}, \zeta_5]$ grazie alla Proposizione 2.8 e al Teorema 4.17.

Esercizio 5. Sia K una estensione finita di $\mathbb{Q}$.

(*i*) Definire la nozione di base intera di K.

(*ii*) Definire il discriminate Δ_K di K dimostrando che è indipendente dalla scelta della base intera.

(*iii*) Deteminare una base intera e discriminante nel caso in cui $K = \mathbb{Q}(\sqrt{d})$ con $d \in \mathbb{Z}$ un intero non nullo, privo di fattori quadratici.

Soluzione: (i) e (ii) Vedere la definizione 4.8 e il Lemma 4.10.

(iii) Grazie alla Proposizione 2.8, l'anello degli interi di K è $\mathbb{Z}[\sqrt{d}]$ se $d \equiv 2, 3$ modulo 4 e $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ se $d \equiv 1$ modulo 4. Segue allora che $\Delta_K = 4d$ nel primo caso e d nel secondo.