SOLUZIONI DELL'ESAME DI ALGEBRA 3, 20/06/2014

Esercizio 1. Si consideri il polinomio $f(X) := X^{13} - 17 \in \mathbb{Q}[X]$.

(*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 17. Sia α una qualunque radice di $f(X)$. Se ζ è una radice primitiva tredicesima dell'unità, le radici di $f(X)$ sono

$$R_f = \left\{\alpha\zeta^i : i = 0, ..., 12\right\}.$$

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 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 13$ e $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_{13}) = 12$, dove $\Phi_{13}(X) \in \mathbb{Q}[X]$ è il tredicesimo polinomio ciclotomico. Segue dalla moltiplicatività dei gradi che, poichè $(13, 12) = 1$,

$$\begin{aligned} &[E : \mathbb{Q}] = 13 \cdot 12 = 156, \\ &[\mathbb{Q}(\alpha) : \mathbb{Q}] = [E : \mathbb{Q}(\zeta)] = 13 \\ &\text{e } [\mathbb{Q}(\zeta) : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)] = 12. \end{aligned}$$

In particolare notiamo che $\mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha) = \mathbb{Q}$ poichè $(13, 12) = 1$.

$(c - d)$ Poichè $E = F(\alpha)$ con $\mu_{13} \subset F = \mathbb{Q}(\zeta)$ ed $[E : F] = 13$, dalla teoria delle estensioni cicliche sappiamo che $G_{E/\mathbb{Q}(\zeta)} \simeq \mu_{13}$, 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_{13}, $G_{E/\mathbb{Q}(\zeta)} = \langle\sigma\rangle \simeq \frac{\mathbb{Z}}{13\mathbb{Z}}$. 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 $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{13\mathbb{Z}}\right)^\times$ mediante l'applicazione $g \mapsto i_g$, dove i_g è caratterizzato dall'equazione $g(\zeta) = \zeta^{i_g}$. Sappiamo che $\left(\frac{\mathbb{Z}}{13\mathbb{Z}}\right)^\times$ è un gruppo ciclico ed esplitamente è generato dalla moltiplicazione per 2. Dunque $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \langle\rho\rangle$, dove ρ è caratterizzato da $\rho(\zeta) = \zeta^2$ 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

$$\begin{aligned} \rho\left(\sigma\left(\rho^{-1}(\alpha)\right)\right) &= \rho(\sigma(\alpha)) = \rho(\alpha\zeta) = \rho(\alpha)\,\rho(\zeta) \\ &= \alpha\rho(\zeta) = \alpha\zeta^2 \end{aligned}$$

a dal confronto con (1) segue $\rho\sigma\rho^{-1} = \sigma^2$. Dunque

$$G_{E/\mathbb{Q}} = G_{E/\mathbb{Q}(\zeta)} \rtimes G_{E/\mathbb{Q}(\alpha)} = \langle\sigma\rangle \rtimes \langle\rho\rangle \simeq \frac{\mathbb{Z}}{13\mathbb{Z}} \rtimes_{\varphi} \frac{\mathbb{Z}}{12\mathbb{Z}}$$

dove $\varphi : \langle\rho\rangle \to Aut(\langle\sigma\rangle)$ è caratterizzato da $\varphi(\rho)(\sigma) = \rho\sigma\rho^{-1} = \sigma^2$.

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

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

Soluzione: Mostriamo per cominciare che $f(X) := X^3 - X + 1 \in \mathbb{Q}[X]$ 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

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

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

$$D(f) = 4 - 27 = -23.$$

Segue che, detto E_f il campo di spezzamento di $f(X)$, $G_{E_f/\mathbb{Q}} \simeq S_3$ (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 $D(f) < 0$ non $D(f)$ è un quadrato in $\mathbb{Q}$ e deduciamo che la seconda possibilità è da escludersi).

D'altra parte $g(X) := X^2 + 1 \in \mathbb{Q}[X]$ è irriducibile (essendolo in $\mathbb{R}[X]$) 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

$$\mathbb{Q}(i) = E_g = E_f \cap E_g \subset E_f.$$

Segue che $\mathbb{Q}(i)$ è l'unico sottocampo quadratico di E_f (che corrisponde all'unico sottogruppo di indice due in S_3), ovvero $\mathbb{Q}(i) = \mathbb{Q}\left(\sqrt{23}i\right)$ (infatti $\left[\mathbb{Q}\left(\sqrt{D(f)}\right) : \mathbb{Q}\right]$ poichè $D(f) = -23$ è un quadrato in $\mathbb{Q}$). Ma ciò non è possibile perchè in tal caso, posto $K := \mathbb{Q}(i) = \mathbb{Q}\left(\sqrt{23}i\right)$, si avrebbe $\sqrt{23} = \frac{\sqrt{23}i}{i} \in K$ da cui $K = \mathbb{Q}\left(\sqrt{23}\right) \subset \mathbb{R}$ (essendo $[K : \mathbb{Q}] = \left[\mathbb{Q}\left(\sqrt{23}\right) : \mathbb{Q}\right]$).

Esercizio 3 (*TeoGal*)**.** Sia E/F una estensione separabile non di Galois, tale che $[E : F] = 4$ e si supponga che la caratteristica di F sia diversa da 2. Si deduca che, detta K/F la chiusura di Galois di E/F, si ha (a meno di isomorfismi)

$$G_{K/F} \in \{S_4, A_4, D_4\}.$$

Soluzione: Per il teorema dell'elemento primitivo si ha $E = F(\alpha)$ per qualche $\alpha \in E$: detto $f(X) \in F[X]$ il polinomio minimo di α su F sappiamo che $\deg(f) = [E : F]$. Sia quindi E_f/F il campo di spezzamento di f. Certamente $K \subset E_f$ poichè $E \subset E_f$ ed E_f/F è di Galois; viceversa, se β è tale che $f(\beta) = 0$, poichè $F \subset F(\alpha) \subset K$ e K/F è normale, deduciamo che $\beta \in K$, da cui $K \subset E_f$. Ma allora $G_{K/F} = G_{E_f/F} =: G$ e, dallo studio delle estensioni quartiche, sappiamo che possiamo avere le seguenti possibilità per il gruppo di Galois $G := G_{E_f/F}$:

$$G \in \left\{ S_4, A_4, D_4, \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}, \frac{\mathbb{Z}}{4\mathbb{Z}} \right\}.$$

Poichè $4 = [E : F] \mid [E_f : F] = \#G$ i casi $\#G = 4$ sono da escludersi; infatti essi implicherebbero $[E : F] = [E_f : F]$ e quindi che $E/F = E_f/F$ è di Galois.

Esercizio 4 (*TeoNum*)**.** Sia L un campo di numeri, di Galois su $\mathbb{Q}$, con gruppo di Galois G.

i. Mostrare che ogni $\sigma \in G$ definisce un automorfismo di $\mathcal{O}_L \to \mathcal{O}_L$, tramite $x \mapsto \sigma(x)$.
ii. Mostrare che ogni $\sigma \in G$ definisce un isomorfismo di gruppi sull'insieme degli ideali frazionali di L.
iii. Mostrare che ogni $\sigma \in G$ che manda ideali massimali di $\mathcal{O}_L$ in ideali masimali di $\mathcal{O}_L$ e che per ogni ideale massimale $\mathcal{P}$ di $\mathcal{O}_L$, l'automorfismo $\sigma \in G$ definisce un isomorfismo $\mathcal{O}_L/\mathcal{P} \to \mathcal{O}_L/\sigma(\mathcal{P})$.

Soluzione: (i) Se $x \in \mathcal{O}_L$ allora x è radice di un polinomio monico $P(T)$, non nullo, a coefficienti in $\mathbb{Z}$. Ma allora $0 = \sigma\big(P(x)\big) = P(\sigma(x))$ in quanto σ è un omomorfismo di anelli ed è l'identità su $\mathbb{Z}$. Quindi anche $\sigma(x)$ è radice di $P(T)$ ovvero $\sigma(x) \in \mathcal{O}_L$. Visto che σ è isomorfismo di campi, $\sigma|_{\mathcal{O}_L} : \mathcal{O}_L \to \mathcal{O}_L$ è omomorfismo di anelli. È inoltre biettivo con inversa $\sigma^{-1}|_{\mathcal{O}_L}$.

(ii) Sia M un ideale frazionale di L ovvero un $\mathcal{O}_L$-modulo finitamente generato, non nullo. Se $m_1, \dots, m_n$ sono generatori, allora $\sigma(m_1), \dots, \sigma(m_n)$ sono generatori di $\sigma(M)$ come $\mathcal{O}_L$-modulo. Infatti se $x \in M$ e $x = \sum_{i=1}^n a_i m_i$ con $a_1, \dots, a_n \in \mathcal{O}_L$, allora $\sigma(m) = \sum_{i=1}^n \sigma(a_i)\sigma(m_i)$. Inoltre $\sigma(M)$ è non nullo in quanto σ è una applicazione iniettiva su L. Concludo che $\sigma(M)$ è un idale frazionale.

Se M ed N sono ideale frazionali, $M \cdot N$ è l'$\mathcal{O}_L$-modulo generato dagli elementi mn al variare di $m \in M$ e di $n \in \mathbb{N}$. Quindi $\sigma(M \cdot N)$ è l'$\mathcal{O}_L$-modulo generato dagli elementi $\sigma(m)\sigma(n)$ al variare di $m \in M$ e di $n \in \mathbb{N}$. Quindi $\sigma(M \cdot N) = \sigma(M) \cdot \sigma(N)$. Ovvero σ rispetta il prodotto di ideali frazionali. Per il punto (i) manda l'elemento neutro nell' elemento neutro.

Se M è un ideale frazionale, $M^{-1} = \{n \in L | nM \subset \mathcal{O}_L\}$. Quindi $\sigma(M^{-1}) \subset \{n \in L | n\sigma(M) \subset \mathcal{O}_L\} = \sigma(M)^{-1}$. Deduco anche $\sigma^{-1}\big(\sigma(M)^{-1}\big) \subset M^{-1}$ e quindi ho l'uguaglianza $\sigma(M^{-1}) = \sigma(M)^{-1}$.

(ii)-(iii) Sia $\mathcal{P}$ un ideale massimale di $\mathcal{O}_L$. Allora $\sigma(\mathcal{P}) \subset \mathcal{O}_L$ e $\sigma(\mathcal{P})$ è un ideale frazionale, e quindi è un ideale di $\mathcal{O}_L$. Passando alle classi di equivalenza ottengo un omomorfismo di anelli $\mathcal{O}_L/\mathcal{P} \to \mathcal{O}_L/\sigma(\mathcal{P})$ che risulta biettivo con inverso definito da σ^{-1}. Essendo $\mathcal{O}_L/\mathcal{P}$ un campo anche $\mathcal{O}_L/\sigma(\mathcal{P})$ è un campo, ovvero $\sigma(\mathcal{P})$ è un ideale massimale.

Esercizio 5. Sia $K = \mathbb{Q}(\zeta_8)$ l'8^o-campo ciclotomico con $\zeta_8 = e^{\frac{2\pi i}{8}}$.

i. Determinare un generatore dell'anello degli interi $\mathcal{O}_K$ di K.
ii. Determinare i primi interi p che ramificano in $\mathcal{O}_K$ e per tali p determinare la decomposizione di $p\mathcal{O}_K$ come prodotto di ideali primi.
iii. Determinare la decomposizione di $17\mathcal{O}_K$.

Soluzione: Sappiamo che $\mathcal{O}_K = \mathbb{Z}[\zeta_8]$ e che il polinomio minimo di ζ_8 è $f(X) = X^4 + 1$. In particolare modulo primi p dispari $X^4 + 1 \in \mathbb{F}_p[X]$ ha tutti zeri distinti in $\overline{\mathbb{F}}_p$ e quindi si decompone come prodotto di fattori con molteplicità 1. Infatti $f'(X) = 4X^3$ e quindi $\mathrm{mcd}(f(X), f'(X)) = 1$. Questo implica che p è non ramificato.

Modulo 2 ho invece $X^4+1=(X+1)^4$ e deduco quindi che $2\mathcal{O}_K=\mathcal{P}^4$ con $\mathcal{P}=(2,\zeta_8+1)$.

Il gruppo $\mathbb{F}_{17}^*$ è ciclico di ordine 16 ed esiste quindi il polinomio $X^{16}-1$ spezza completamente in $\mathbb{F}_{17}$. Segue che anche $f(X)$ modulo 17 spezza completamente. Concludo che $17\mathcal{O}_K$ è il prodotto di 4 primi a due a due distinti di $\mathcal{O}_K$.