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

Esercizio 1. Si consideri il polinomio $f(X) := X^{11} - 3 \in \mathbb{Q}[X]$.

(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 3. Poichè $f'(X) = 11X^{10}$ esiste una ed una sola radice reale $\sqrt[11]{3} \in \mathbb{R}$ tale che $f\left(\sqrt[11]{3}\right) = 0$. Se ζ è una radice primitiva undicesima dell'unità, le radici di $f(X)$ sono

$$R_f = \left\{ \sqrt[11]{3}\zeta^i : i = 0, ..., 10 \right\}.$$

Dunque $\mathbb{Q}(R_f)$ è il campo di spezzamento e chiaramente $\mathbb{Q}(R_f) \subset \mathbb{Q}\left(\sqrt[11]{3}, \zeta\right)$. Viceversa $\sqrt[11]{3}$, $\sqrt[11]{3}\zeta \in R_f \subset \mathbb{Q}(R_f)$, da cui $\zeta = \frac{\sqrt[11]{3}\zeta}{\sqrt[11]{3}} \in \mathbb{Q}(R_f)$ e, pertanto, $E := \mathbb{Q}(R_f) = \mathbb{Q}\left(\sqrt[11]{3}, \zeta\right)$.

(b) Si ha $\left[\mathbb{Q}\left(\sqrt[11]{3}\right) : \mathbb{Q}\right] = \deg(f) = 11$ e $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_{11}) = 10$, dove $\Phi_{11}(X) \in \mathbb{Q}[X]$ è l'undicesimo polinomio ciclotomico. Segue dalla moltiplicatività dei gradi che, poichè $(11, 10) = 1$,

$$\begin{aligned} &[E : \mathbb{Q}] = 11 \cdot 10 = 110, \\ &\left[\mathbb{Q}\left(\sqrt[11]{3}\right) : \mathbb{Q}\right] = [E : \mathbb{Q}(\zeta)] = 11 \\ &\text{e } [\mathbb{Q}(\zeta) : \mathbb{Q}] = \left[E : \mathbb{Q}\left(\sqrt[11]{3}\right)\right] = 10. \end{aligned}$$

($c - d$) Poichè $E = F\left(\sqrt[11]{3}\right)$ con $\mu_{11} \subset F = \mathbb{Q}(\zeta)$ e $[E : F] = 7$, dalla teoria delle estensioni cicliche sappiamo che $G_{E/\mathbb{Q}(\zeta)} \simeq \mu_{11}$, mediante l'applicazione $g \mapsto \zeta_g$, dove ζ_g è caratterizzato dall'equazione $\frac{g\left(\sqrt[11]{3}\right)}{\sqrt[11]{3}} = \zeta_g$. Sia dunque $\sigma \in G_{E/\mathbb{Q}(\zeta)}$ l'unico automorfismo tale che $\sigma\left(\sqrt[11]{3}\right) = \sqrt[11]{3}\zeta$: poichè ζ genera μ_{11}, $G_{E/\mathbb{Q}(\zeta)} = \langle\sigma\rangle \simeq \frac{\mathbb{Z}}{11\mathbb{Z}}$. Notiamo che, per induzione, si ha

$$\begin{aligned} \sigma^i\left(\sqrt[11]{3}\right) &= \sigma\left(\sigma^{i-1}\left(\sqrt[11]{3}\right)\right) = \sigma\left(\sqrt[11]{3}\zeta^{i-1}\right) \\ &= \sigma\left(\sqrt[11]{3}\right)\sigma(\zeta)^{i-1} = \sqrt[11]{3}\zeta\zeta^{i-1} = \sqrt[11]{3}\zeta^i. \end{aligned} \tag{1}$$

Consideriamo quindi $G_{E/\mathbb{Q}\left(\sqrt[11]{3}\right)} \subset G_{E/\mathbb{Q}}$ e notiamo che $G_{E/\mathbb{Q}\left(\sqrt[11]{3}\right)} \cap G_{E/\mathbb{Q}(\zeta)} = 1$ poichè $E = \mathbb{Q}\left(\sqrt[11]{3}, \zeta\right)$. Segue che l'applicazione di restrizione $G_{E/\mathbb{Q}} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$, che ha nucleo $G_{E/\mathbb{Q}(\zeta)}$, da luogo ad un omomorfismo di gruppi iniettivo

$$G_{E/\mathbb{Q}\left(\sqrt[11]{3}\right)} \hookrightarrow G_{\mathbb{Q}(\zeta)/\mathbb{Q}},$$

dove infatti notiamo che $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois (e dunque l'applicazione ben definita). Ma

$$\#G_{E/\mathbb{Q}\left(\sqrt[11]{3}\right)} = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \left[E : \mathbb{Q}\left(\sqrt[11]{3}\right)\right] = \#G_{\mathbb{Q}(\zeta)/\mathbb{Q}},$$

da cui concludiamo che tale applicazione di restrizione è un isomorfismo. Dalla teoria delle estensioni ciclotomiche, sappiamo anche che $G_{\mathbb{Q}(\zeta)/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^\times$ mediante l'applicazione $g \mapsto i_g$,

dove i_g è caratterizzato dall'equazione $g(\zeta) = \zeta^{i_g}$. Sappiamo che $\left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^{\times}$ 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 $G_{E/\mathbb{Q}(\sqrt[11]{3})} \to G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è un isomorfismo, si ha anche $G_{E/\mathbb{Q}(\sqrt[11]{3})} = \langle\rho\rangle$.

Notiamo che $\sigma^i, \rho\sigma\rho^{-1} \in G_{E/\mathbb{Q}(\zeta)} \lhd G_{E/\mathbb{Q}}$ e, poichè $E = F\left(\sqrt[11]{3}\right)$ con $F = \mathbb{Q}(\zeta)$, entrambi questi elementi sono caratterizzato dalla loro azione su $\sqrt[11]{3}$. Abbiamo

$$\begin{aligned}\rho\left(\sigma\left(\rho^{-1}\left(\sqrt[11]{3}\right)\right)\right) &= \rho\left(\sigma\left(\sqrt[11]{3}\right)\right) = \rho\left(\sqrt[11]{3}\zeta\right) = \rho\left(\sqrt[11]{3}\right)\rho(\zeta)\\ &= \sqrt[11]{3}\rho(\zeta) = \sqrt[11]{3}\zeta^2\end{aligned}$$

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

$$G_{E/\mathbb{Q}} = G_{E/\mathbb{Q}(\zeta)} \rtimes G_{E/\mathbb{Q}(\sqrt[11]{3})} = \langle\sigma\rangle \rtimes \langle\rho\rangle \simeq \frac{\mathbb{Z}}{11\mathbb{Z}} \rtimes_{\varphi} \frac{\mathbb{Z}}{10\mathbb{Z}}$$

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 se il polinomio

$$f(X) = X^5 - X^2 + 1 \in \mathbb{Q}(\zeta)[X]$$

è irriducibile, dove $\zeta = e^{\frac{2\pi i}{5}}$.

[SUGG.: (1) Mostrare che $f(X)$ è irriducibile in $\mathbb{Q}(\zeta)[X]$ se e solo se è irriducibile in $\mathbb{Q}[X]$]. (2) Mostrare l'irriducibilità di $f(X)$ in $\mathbb{Z}[X]$].]

Soluzione: Mostriamo che è irriducibile (in $\mathbb{Q}(\zeta)[X]$) e, per prima cosa, verifichiamo che basta verificare che $f(X) \in \mathbb{Q}[X]$ è irriducibile. Se infatti $f(X) \in \mathbb{Q}[X]$ è irriducibile, si ha

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 5,$$

per una qualunque radice α di $f(X)$. D'altra parte $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ e per moltiplicatività dei gradi, essendo $(5, 4) = 1$, deduciamo che $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\zeta)] = 5$. Supponiamo per assurdo che si abbia $f(X) = g(X)h(X)$ in $\mathbb{Q}(\zeta)[X]$ e che $\deg(g) < \deg(f)$; possiamo supporre che $g(X)$ sia irriducibile e che $g(\alpha) = 0$, da cui

$$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\zeta)] = \deg(g) < \deg(f) = 5.$$

Questa contraddizione mostra che ciò non è possibile.

Resta da mostrare che $f(X) \in \mathbb{Q}[X]$ 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

$$\overline{f}(X) = X^5 + X^2 + 1 \in \mathbb{F}_2[X]$$

ottenuto per riduzione modulo 2 è irriducibile. Certamente non possiede radici e, per tanto, se fosse riducibile si avrebbe

$$\begin{aligned}\overline{f}(X) &= \left(X^2 + aX + b\right)\left(X^3 + cX^2 + dX + e\right)\\ &= X^5 + (a+c)X^4 + (b + ac + d)X^3 + (ad + bc + e)X^2\\ &\quad + (ae + bd)X + be.\end{aligned}$$

Da ciò segue che si deve avere:

(1) $a + c = 0 \Leftrightarrow a = c$;
(2) $be = 1 \Leftrightarrow b = e = 1$;
(3) $ae + bd = 0$, ovvero per 1. e 2.: $a + d = 0 \Leftrightarrow a = d = c$;
(4) $b + ac + d = 0$, ovvero per 3.: $b + a^2 + a = 0 \Leftrightarrow b = a(a + 1) = 0$.

Poichè la conclusione $b = 0$ in 4. è incontraddizione con la conclusione $b = 1$ in 2. deduciamo che $\overline{f}(X) \in \mathbb{F}_2[X]$ è irriducibile.

Esercizio 3 (*TeoGal*)**.** Si mostri che le seguenti proprietà sono equivalenti, per una estensione di Galois E/F tale che la caratteristica di F sia diversa da 2.

(1) $[E : F] = 4$ ed esiste al più un campo $K \subset E$ tale che $[K : F] = 2$.
(2) E è campo di spezzamento di un polinomio della forma

$$f(X) = X^4 + AX^2 + B \in F[X],$$

irriducibile in $F[X]$, tale che $B \notin F^{\times 2}$ e che diventa riducibile in $F\left(\sqrt{B}\right)[X]$[1].

Soluzione: Per cominciare facciamo la seguente osservazione, relativa ad una qualunque estensione E/F di Galois di grado 4. Poichè $\#G_{E/F} = 4$ si ha $G_{E/F} \simeq \mathbb{F}_2 \times \mathbb{F}_2$ oppure $G_{E/F} \simeq \mathbb{Z}/4\mathbb{Z}$: da ciò vediamo che esiste certamente una torre $F \subset K \subset E$ con $[E : K] = [K : F] = 2$. Poichè la caratteristica di F è diversa da 2 possiamo supporre che si abbia $K = F(\sqrt{\alpha})$ (risp. $E = K\left(\sqrt{\beta}\right)$) per qualche $\alpha \in F$ (risp. $\beta \in K$). Possiamo quindi scrivere $\beta = a + b\sqrt{\alpha}$ dove $a, b \in F$. Consideriamo dunque il polinomio

$$\begin{aligned} f(X) &:= \left(X - \sqrt{a + b\sqrt{\alpha}}\right)\left(X + \sqrt{a + b\sqrt{\alpha}}\right)\left(X - \sqrt{a - b\sqrt{\alpha}}\right)\left(X + \sqrt{a - b\sqrt{\alpha}}\right) \\ &= \left(X^2 - a - b\sqrt{\alpha}\right)\left(X^2 - a + b\sqrt{\alpha}\right) \\ &= \left(X^2 - a\right)^2 - b^2\alpha = X^4 - 2aX^2 + a^2 - b^2\alpha \in F[X], \end{aligned}$$

di cui $\sqrt{\beta}$ è una radice per costruzione.

(1) $\Rightarrow$ (2) Detto $f_{\sqrt{\beta}}(X)$ il polinomio minimo di $\sqrt{\beta}$ su F, si ha

$$\left[F\left(\sqrt{\beta}\right) : F\right] = \deg(f_\beta) \mid \deg(f) = 4.$$

Ovviamente $\left[F\left(\sqrt{\beta}\right) : F\right] \neq 1$ e, se $\left[F\left(\sqrt{\beta}\right) : F\right] = 2$, deduciamo che $F\left(\sqrt{\beta}\right) = K = F(\sqrt{\alpha})$ grazie ad (1). Poichè ciò non è possibile (altrimenti $E = K\left(\sqrt{\beta}\right) = K$ avrebbe grado 2 su F), si deve avere $\deg(f_\beta) = 4$, da cui il fatto che $f(X) \in F[X]$ è irriducibile con $A = -2a$ e $B = a^2 - b^2\alpha$. Segue che E è il campo di spezzamento del polinomio irriducibile $f(X) \in F[X]$ e, poichè $G_{E/F} \simeq \mathbb{Z}/4\mathbb{Z}$, la teoria delle estensioni quartiche ci dice che $D(f) \notin F^{\times 2}$ e che, detto E_{g_f} il campo di spezzamento del risolvente cubico $g_f(X) \in F[X]$ di $f(X)$, $f(X) \in E_{g_f}(X)$ è riducibile. Poichè $D(f) = 16\left(A^2 - 4B\right)^2 B$ vediamo che $D(f) \notin F^{\times 2}$ se e solo se $B \notin F^{\times 2}$ e, poichè

$$g_f(X) = X^3 - AX^2 - 4BX + 4AB = (X - A)\left(X^2 - 4B\right) \text{ in } F[X],$$

si deduce che $E_{g_f} = F\left(\sqrt{B}\right)$. Dunque $B \notin F^{\times 2}$ ed $f(X) \in F\left(\sqrt{B}\right)(X)$ è riducibile.

(2) $\Rightarrow$ (1) Infatti, come notato appena sopra, si ha

$$g_f(X) = (X - A)\left(X^2 - 4B\right) \text{ in } F[X],$$

[1]Le radici di un polinomio della forma

$$f(X) = X^4 + AX^2 + B \in F[X]$$

sono

$$\left\{\sqrt{\frac{-A + \sqrt{A^2 - 4B}}{2}}, -\sqrt{\frac{-A + \sqrt{A^2 - 4B}}{2}}, \sqrt{\frac{-A - \sqrt{A^2 - 4B}}{2}}, -\sqrt{\frac{-A - \sqrt{A^2 - 4B}}{2}}\right\}$$

e, da ciò, si deduce che

$$\Delta(f) = 4\left(A^2 - 4B\right)\sqrt{B}.$$

da cui $E_{g_f} = F\left(\sqrt{B}\right)$. Deduciamo che $f(X)$ diventa riducibile in $E_{g_f}[X] = F\left(\sqrt{B}\right)[X]$ e la teoria delle estensioni quartiche ci dice che ciò accade se e solo se $G_{E/F} \simeq \mathbb{Z}/4\mathbb{Z}$, se E è il campo di spezzamento di $f(X)$.

Esercizio 4 (*TN*)**.** Sia $F \subset K$ un'estensione di campi di numeri di grado $d = [K : F]$. Sia $\alpha \in K$.

i. Supponiamo $\alpha \in F$. Mostrare che $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \mathrm{Nm}_{F/\mathbb{Q}}(\alpha)^d$ e $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = d\mathrm{Tr}_{F/\mathbb{Q}}(\alpha)$.
ii. Determinare $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$ e $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ in termini del polinomio minimo $f_\alpha(X) \in \mathbb{Q}[X]$ su $\mathbb{Q}$.

Soluzione: (i) Sia $K \subset E$ una chiusura normale su $\mathbb{Q}$. Denotiamo con $\{\sigma_1, \ldots, \sigma_n\}$ gli elementi dell'insieme degli omomorfismi di campi $\mathrm{Hom}_{\mathbb{Q}}(F, E)$. Ogni omomorfismo di campi $\sigma\colon K \to E$, ristretto ad F, definisce un elemento $\sigma|_F \in \mathrm{Hom}_{\mathbb{Q}}(F, E)$. Viceversa grazie a Milne, Proposizione 2.7, dato un omomorfismo $\sigma_i\colon F \to E$ ho esattamente d-omomorfismi distinti $\sigma_{i,1}, \ldots, \sigma_{i,d}\colon K \to E$ la cui restrizione ad F coincide con σ_i. Quindi $\mathrm{Hom}_{\mathbb{Q}}(K, E) = \{\sigma_{i,j} | 1 \le i \le n, 1 \le d \le d\}$.

Allora $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \prod_{j=1}^d \sigma_{i,j}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)^d = \mathrm{Nm}_{F/\mathbb{Q}}(\alpha)^d$. Analogamente $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sum_{j=1}^d \sigma_{i,j}(\alpha) = \sum_{i=1}^n d\sigma_i(\alpha) = d\mathrm{Tr}_{F/\mathbb{Q}}(\alpha)$.

(ii) Considero $F = \mathbb{Q}(\alpha)$ e sia $n = [F : \mathbb{Q}]$. Allora il polinomio minimo $f_\alpha(X)$ di α è uguale a $g(X) = \prod_{i=1}^n \big(X - \sigma_i(\alpha)\big)$. Si tratta infatti di un polinomio monico, di grado n, di cui α è una radice, a coefficienti in $\mathbb{Q}$. Infatti i coefficienti sono elementi di E invarianti per il gruppo di Galois di E su $\mathbb{Q}$. Quindi $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = -a_{n-1}$ e $\mathrm{Nm}_{F/\mathbb{Q}}(\alpha) = (-1)^n a_0$ dove $f_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$. Usnado il punto precedente concludiamo che $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -da_{n-1}$ e $\mathrm{Nm}_{F/\mathbb{Q}}(\alpha) = (-1)^{nd} a_0^d$.

Esercizio 5. Sia K il 10-mo campo ciclotomico.

i. Trovare un generatore ζ dell'anello degli interi $\mathcal{O}_K$ di K.
ii. Determinare il discriminate $\Delta_{K/\mathbb{Q}}$ di $\mathcal{O}_K$.
iii. Determinare i primi $p \in \mathbb{Z}$ che ramificano in K.
iv. Determinare la decomposizione dell'ideale $2\mathcal{O}_K$ come prodotto di ideali primi.

Soluzione: (i)–(ii) Sia α una radice primitiva dell'unità di ordine 5. Allora $\zeta := -\alpha$ è una radice primitiva dell'unità di ordine 10. Quindi $K = \mathbb{Q}(\zeta) = \mathbb{Q}(\alpha)$ e $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Il polinomio minimo di α è $\Phi(X) = \frac{X^5-1}{X-1} = X^4 + X^3 + X^2 + X + 1$.

Il dicriminante coincide con la norma di $\Phi'(\alpha)$ ovvero 5^3 (vedere la Proposizione 3.7 e il Corollario 3.8 delle note del prof. Bertolini).

(iii) Per primi $p \neq 5$ il polinomio $X^5 - 1 \in \mathbb{F}_p[X]$ ha tutti zeri distinti (in un campo di spezzamento). Quindi anche la riduzione $\overline{\Phi}(X)$ di $\Phi(X)$ modulo p, che è un fattore di $X^5 - 1$, ha anch'esso tutti zeri distinti. Concludo che $\overline{\Phi}(X)$ si scrive in $\mathbb{F}_p[X]$ come prodotto di fattori irridcibili con molteplicità uguale ad 1. Segue che p non ramifica in $\mathcal{O}_K$.

(iv) Sappiamo che 2 non ramifica in $\mathcal{O}_K$ e dunque $2\mathcal{O}_K$ è prodotto di ideali primi distinti. Inoltre se scriviamo la riduzione $\overline{\Phi}(X)$ di $\Phi(X)$ modulo 2 come prodotto $\overline{\Phi}(X) = \prod_i \overline{g}_i(X)$ di fattori irriducibili, allora $2\mathcal{O}_K = \prod_i \mathcal{P}_i$ con $\mathcal{P}_i = \big(2, g_i(\alpha)\big)$ e $g_i(X) \in \mathbb{Z}[X]$ un qualsiasi polinomio la cui riduzione modulo 2 sia uguale a $\overline{g}_i(X)$.

Si tratta quindi di studiare la decomposizione di $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Osserviamo che non ha radici in $\mathbb{F}_2$. Non è neppure il prodotto di due fattori irriducibili di grado 2 in quanto esiste uno ed un solo polinomio irriducibile di grado 2 in $\mathbb{F}_2[X]$ ovvero $X^2 + X + 1$. Concludiamo che $X^4 + X^3 + X^2 + X + 1$ è irriducibile in $\mathbb{F}_2[X]$ e quindi $2\mathcal{O}_K = \mathcal{P}$ è un ideale primo di $\mathcal{O}_K$.

Infatti $\mathbb{F}_{16}$ è il campo di spezzamento di $\mathbb{F}_2$: il gruppo delle unità $\mathbb{F}_{16}^*$ è un gruppi ciclico di ordine $16-1=15$ e quindi contiene un sottogruppo μ_5 di ordine 5 i cui elementi sono tutti e sole le radici di X^5-1. Segue che $X^4+X^3+X^2+X+1$ spezza completamente in $\mathbb{F}_{16}$.