SOLUZIONI DELL'APPELLO DI ALGEBRA 3, 15/06/2015

Esercizio 1. Si consideri il polinomio $f(X) = X^4 + 2X + 2 \in \mathbb{Q}[X]$.

(1) Si mostri che è irriducibile in $\mathbb{Q}[X]$.
(2) Si calcoli il gruppo di Galois $G_{E/\mathbb{Q}}$ del campo di spezzamento E di $f(X) \in \mathbb{Q}[X]$.

Soluzione: (1) Possiamo applicare il criterio di Eisenstein al primo 2.
(2) Il risolvente cubico è il polinomio

$$g_f(X) = X^3 - 4 \cdot 2X - 2^2 = X^3 - 8X - 4$$

che ha discriminante

$$D_f = D_{g_f} = -4(-8)^3 - 27(4)^2 = 1616 = 2^4 \cdot 101.$$

Notiamo che

$$g_f(X) = X^3 + 2X + 1 \text{ in } \mathbb{F}_5[X],$$

polinomio che non ha radici. È dunque irriducibile in $\mathbb{F}_5[X]$, avendo grado 3, e pertanto $g_f(X) \in \mathbb{Z}[X]$ è irriducibile. Essendo monico il lemma di Gauss garantisce l'irriducibilità in $\mathbb{Q}[X]$ e, poichè D_f non è un quadrato in $\mathbb{Q}$, abbiamo $G_{E/\mathbb{Q}} \simeq S_4$.

Esercizio 2. Si consideri il polinomio $f(X) = X^{35} - 7 \in \mathbb{Q}[X]$ e sia E il suo campo di spezzamento.

(1) Si mostri che $E = \mathbb{Q}(\alpha, \zeta)$ con α radice di $f(X)$ e ζ radice primitiva 35-esima dell'unità e si calcoli $[E : \mathbb{Q}]$.
(2) Si mostri che $f(X) \in \mathbb{Q}(\zeta)[X]$ è irriducibile.
(3) Si mostri che $G_{E/\mathbb{Q}(\alpha)}$ è il prodotto di due gruppi ciclici, il primo generato dall'unico elemento $\sigma_7 \in G_{E/\mathbb{Q}(\alpha)}$ tale che $\sigma_7(\zeta^5) = \zeta^{15}$ e $\sigma_7(\zeta^7) = \zeta^7$, il secodno generato dall'unico elemento $\sigma_5 \in G_{E/\mathbb{Q}(\alpha)}$ tale che $\sigma_5(\zeta^7) = \zeta^{14}$ e $\sigma_5(\zeta^5) = \zeta^5$.

Soluzione: (1) Poichè $f'(X) = 35X^{34}$, esiste una ed una sola radice reale α di $f(X)$. L'insieme delle radici di $f(X)$ è

$$\left\{\alpha\zeta^i : i = 0, \ldots, 34\right\}.$$

Dunque $E \subset \mathbb{Q}(\alpha, \zeta)$ e, poichè $\zeta = \frac{\alpha\zeta}{\alpha}$, si ha $E = \mathbb{Q}(\alpha, \zeta)$. Sappiamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 35$ e che $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 24$. Poichè $(35, 24) = 1$, la moltiplicatività dei gradi implica che si abbia $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ e

$$[E : \mathbb{Q}] = 35 \cdot 24 = 840.$$

(2) Detto $f_\alpha(X) \in \mathbb{Q}(\zeta)[X]$ il polinomio minimo di α su $\mathbb{Q}(\zeta)$, possiamo scrivere $f(X) = f_\alpha(X)\, g(X)$. Abbiamo

$$\begin{aligned} \deg(f_\alpha) &= [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\zeta)] = \frac{[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}]}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} \\ &= \frac{35 \cdot 24}{24} = 35 = \deg(f) \end{aligned}$$

e dunque $f(X) = f_\alpha(X) \in \mathbb{Q}(\zeta)[X]$ è irriducibile.

(3) Poichè $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois, la restrizione induce un isomorfismo

$$G_{E/\mathbb{Q}(\alpha)} \xrightarrow{\sim} G_{\mathbb{Q}(\zeta)/\mathbb{Q}}.$$

D'altra parte la teoria delle estensioni cicliche garantisce che

$$G_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \left(\frac{\mathbb{Z}}{35\mathbb{Z}}\right)^{\times} = \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^{\times} \times \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{6\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}.$$

Siano $\zeta_7 = \zeta^5$ (rispettivamente $\zeta_5 = \zeta^7$) la radice primitiva settima (rispettivamente quinta) dell'unità. Poichè 3 genera $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^{\times}$ (rispettivamente 2 genera), esiste uno ed un solo $\sigma_7 \in G_{E/\mathbb{Q}(\alpha)}$ (rispettivamente $\sigma_5 \in G_{E/\mathbb{Q}(\alpha)}$) tale che $\sigma_7(\zeta_7) = \zeta_7^3$ mentre $\sigma_7(\zeta_5) = \zeta_5$ (rispettivamente $\sigma_5(\zeta_5) = \zeta_5^2$ mentre $\sigma_5(\zeta_7) = \zeta_7$). Dunque

$$\begin{aligned} \sigma_7\left(\zeta^5\right) &= \sigma_7(\zeta_7) = \zeta_7^3 = \zeta^{15} \text{ e } \sigma_7\left(\zeta^7\right) = \sigma_7(\zeta_5) = \zeta_5 = \zeta^7, \\ \sigma_5\left(\zeta^7\right) &= \sigma_5(\zeta_5) = \zeta_5^2 = \zeta^{14} \text{ e } \sigma_5\left(\zeta^5\right) = \sigma_5(\zeta_7) = \zeta_7 = \zeta^5. \end{aligned}$$

Esercizio 3. Siano E/F ed L/F due estensioni di campi finite.

(1) Mostrare che, se $F \subset E \subset L$, allora $[L:F] = [L:E][E:F]$.

(2) È vero che

$$[EL:F] = \frac{[E:F][L:F]}{[E \cap L:F]}?$$

(Dimostrare l'asserzione).

Soluzione: (1) Vedere la teoria.

(2) Non è vero. Per esempio, siano $E/F = \mathbb{Q}(\alpha)/\mathbb{Q}$ ed $L/F = \mathbb{Q}(\beta)/\mathbb{Q}$ dove $\alpha \neq \beta$ sono radici dello stesso polinomio $f(X) \in \mathbb{Q}[X]$ irriducibile di grado tre tale che il gruppo di Galois su $\mathbb{Q}$ del suo campo di spezzamento E_f sia isomorfo ad S_3 (come ad esempio il polinomio $g_f(X)$ del primo esercizio). Allora $EL = \mathbb{Q}(\alpha, \beta) = E_f$ ed $E \cap L = \mathbb{Q}$ (per questioni di moltiplicatività dei gradi, per esempio), ma allora

$$[EL:F] = 6 \neq \frac{3 \cdot 3}{1} = \frac{[E:F][L:F]}{[E \cap L:F]}.$$

Esercizio 4. Siano $K = \mathbb{Q}(\zeta_3)$ ed $L = \mathbb{Q}(\zeta_{27})$ il 3^o e il 27^o campo ciclotomico. Siano $\mathcal{O}_K$ e $\mathcal{O}_L$ i ripettivi anelli degli interi.

(1) Determinare i gradi delle estensioni $\mathbb{Q} \subset K$ e $K \subset L$.

(2) Determinare α tale che $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ e determinare il polinomio minimo di α su K.

(3) Determinare il discriminane di L su K.

(3) Determinare i primi $\mathfrak{P}$ di $\mathcal{O}_K$ che ramificano in L e studiare la decomposizione di $\mathfrak{P}\mathcal{O}_L$ come prodotto di idelai primi.

Soluzione: (1) I gradi di $\mathbb{Q} \subset K$ e $\mathbb{Q} \subset L$ sono $\varphi(3) = 2$ e $\varphi(27) = 18$ rispettivamente. In particolare per la moltiplicatività dei gardi ho $[L:K] = 9$. Inoltre $L = K(\zeta_{27})$ e $\zeta_{27}^9 = \zeta_3$. Quindi il polinomio minimo di ζ_{27} su K è $f(X) = X^9 - \zeta_3$.

(2) Visto che $\mathcal{O}_L = \mathbb{Z}[\zeta_{27}]$ segue che $\mathcal{O}_L = \mathcal{O}_K[\zeta_{27}]$. Posso quindi prendere $\alpha = \zeta_{27}$.

(3) Il discriminante di α su K è $\Delta_{L/K} = \mathrm{Norm}_{L/K}\left(f'(\alpha)\right)$ per la Proposizione 3.9 degli appunti. Calcoliamo $f'(X) = 9X^8$ e quindi $f'(\alpha) = 3^2\zeta_{27}^8$. Siccome $\mathrm{Norm}_{L/K}(\zeta_{27}) = \zeta_3$ per la Proposizione 3.7 degli appunti. Quindi $\Delta_{L/K} = 3^{18}\zeta_3^8 = 3^{18}\overline{\zeta}_3$.

(4) Sia $\mathfrak{P}$ un primo di $\mathcal{O}_K$ e sia $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$. Allora la riduzione di $f(X)$ modulo $\mathfrak{P}$ è il polinomio $g(X) := X^9 - \beta$ con $\beta \equiv \zeta_3$ modulo $\mathfrak{P}$.

Supponiamo che $\mathfrak{P}$ non divida $3\mathcal{O}_K$. Allora $g'(X) = 9X^8 \neq 0$ e quindi $\mathrm{mcd}(g'(X), g(X)) = 1$ ovvero $\mathfrak{P}$ non ramifica in L per il Teorema 6.10 degli appunti.

Se $\mathfrak{P}$ divide 3 allora $g(X) = X^9 - 1 = (X-1)^9$ e quindi per il Teorema 6.10 degli appunti esiste un unico primo $\mathfrak{Q}$ di $\mathcal{O}_L$ tale che $\mathfrak{Q} \cap \mathcal{O}_K = \mathfrak{P}$ ed inoltre $\mathfrak{P}\mathcal{O}_L = \mathfrak{Q}^9$. Osserviamo che

$\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ e ζ_3 ha T^2+T+1 come polinomio minimo su $\mathbb{Q}$. Siccome $T^2+T+1 \equiv (T-1)^2$ modulo 3 esiste un unico primo $\mathfrak{P}$ di $\mathcal{O}_K$ contenente 3 e vale $3\mathcal{O}_K = \mathfrak{P}^2$.

Esercizio 5. Sia $K \subset L$ un'estensione di campi di numeri con anelli di interi $\mathcal{O}_K \subset \mathcal{O}_L$.

(1) Dimostrare che dato un ideale massimale $\mathfrak{P}$ di $\mathcal{O}_L$ l'intersezione $\mathcal{O}_K \cap \mathfrak{P}$ è un ideale massimale di $\mathcal{O}_K$.
(1) Dimostrare che dato un ideale massimale $\mathfrak{Q}$ di $\mathcal{O}_K$ esiste un ideale massimale $\mathfrak{P}$ di $\mathcal{O}_L$ tale che $\mathcal{O}_K \cap \mathfrak{P} = \mathfrak{Q}$.

Soluzione: È la Proposizione 6.5 degli appunti.