SOLUZIONI DELL'APPELLO DI ALGEBRA 3, 14/09/2015

Esercizio 1. Si consideri il polinomio $f(X) = X^7 - 2 \in \mathbb{Q}[X]$ 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 settima dell'unità e si calcoli $[E : \mathbb{Q}]$.
(2) Si mostri che $G_{E/\mathbb{Q}(\alpha)}$ è ciclico di ordine 6, generato dall'unico elemento $\sigma \in G_{E/\mathbb{Q}(\alpha)}$ tale che $\sigma(\zeta) = \zeta^3$, mentre $G_{E/\mathbb{Q}(\zeta)}$ è ciclico di ordine 7, generato dall'unico elemento $\rho \in G_{E/\mathbb{Q}(\zeta)}$ tale che $\rho(\alpha) = \zeta\alpha$.
(3) Si scriva si calcoli $\mathbb{R} \cap E$ nella forma $\mathbb{R} \cap E = \mathbb{Q}(\beta)$ per un opportuno $\beta \in E$.

Soluzione: (1) Poichè $f'(X) = 7X^6$, esiste una ed una sola radice reale α di $f(X)$. L'insieme delle radici di $f(X)$ è

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

Dunque $E \subset \mathbb{Q}(\alpha, \zeta)$ e, poichè $\zeta = \frac{\alpha\zeta}{\alpha}$, si ha $E = \mathbb{Q}(\alpha, \zeta)$. Sappiamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$, poichè $f(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein, e che $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$. La moltiplicatività dei gradi implica che si abbia $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ e

$$[E : \mathbb{Q}] = 42.$$

(2) 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

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

Poichè 3 genera $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^{\times}$, esiste uno ed un solo σ tale che $\sigma(\zeta) = \zeta^3$. Poichè $\mu_7 \subset \mathbb{Q}(\zeta)$, sappiamo anche dalla teoria delle estensioni cicliche che

$$G_{E/\mathbb{Q}(\zeta)} \xrightarrow{\sim} \mu_7$$

via $g \mapsto \frac{g(\alpha)}{\alpha}$. Dunque esiste uno ed un solo ρ tale che $\rho(\alpha) = \zeta\alpha$.

(3) Posto $\beta := \alpha + \zeta + \zeta^{-1}$, abbiamo

$$\mathbb{Q}(\beta) \subset \mathbb{R} \cap E = E^{\langle c \rangle}.$$

Ma $\left[E^{\langle c \rangle} : \mathbb{Q}\right] = \left[G_{E/\mathbb{Q}} : \langle c \rangle\right] = 21$; se dunque mostriamo che $[\mathbb{Q}(\beta) : \mathbb{Q}] \geq 21$, seguirà che $\mathbb{Q}(\beta) = E^{\langle c \rangle}$. Infatti, per la moltiplicatività dei gradi, abbiamo

$$[\mathbb{Q}(\beta) : \mathbb{Q}] \in \{1, 3, 7, 21\}$$

e, dunque, basta mostrare che $[\mathbb{Q}(\beta) : \mathbb{Q}] > 7$. Ma abbiamo

$$\left\{\rho^i(\beta) : i = 0, ..., 6, \sigma(\beta)\right\} \subset G_{E/\mathbb{Q}}(\beta)$$

e, grazie a (2), $\rho^i(\beta) = \zeta^i\alpha + \zeta + \zeta^{-1}$ mentre $\sigma(\beta) = \alpha + \zeta^3 + \zeta^{18} = \alpha + \zeta^3 + \zeta^4$. Poichè $\left\{\zeta^i\alpha^j : i = 0, ..., 6, j = 0, ..., 5\right\}$ è una base di $E/\mathbb{Q}$, questi elementi sono distinti e, dunque, detto $f_\beta(X) \in \mathbb{Q}[X]$ il polinomio minimo di β su $\mathbb{Q}$,

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg(f_\beta) = \#G_{E/\mathbb{Q}}(\beta) \geq 8.$$

Esercizio 2. Si considerino i polinomi $f(X) := X^3+7X+1 \in \mathbb{Q}[X]$ e $g(X) = X^2-3 \in \mathbb{Q}[X]$ ed i relativi campi di spezzamento $E_f/\mathbb{Q}$ e $E_g/\mathbb{Q}$.

(1) Si calcolino $G_{E_fE_g/E_g}$ ed $G_{E_fE_g/E_f}$.
(2) Si calcoli $G_{E_fE_g/\mathbb{Q}}$.

Soluzione: (1) Il polinomio $f(X) \in \mathbb{Q}[X]$ è irriducibile poichè la sua riduzione modulo due è $X^3+X+1 \in \mathbb{F}_2[X]$, che è irriducibile, mentre $g(X) \in \mathbb{Q}[X]$ è irriducibile per il criterio di Eisenstein. Abbiamo

$$D_f = -4 \cdot 7^3 - 27 \cdot 1^2 = -1399$$

che è primo e non è un quadrato in $\mathbb{Q}$. Dunque $G_{E_f/\mathbb{Q}} \simeq S_3$. Abbiamo $E_f \cap E_g = \mathbb{Q}$ poichè $E_g = \mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(\sqrt{-1399})$, l'unico sottoestensione quadratica in $E_f/\mathbb{Q}$ che corrisponde all'unico sottogruppo normale. Poichè sia $E_f/\mathbb{Q}$ che $E_g/\mathbb{Q}$ sono di Galois e $E_f \cap E_g = \mathbb{Q}$, deduciamo che

$$\begin{aligned} G_{E_fE_g/E_g} \xrightarrow{\sim} G_{E_f/E_f\cap E_g} &= G_{E_f/\mathbb{Q}} \simeq S_3, \\ G_{E_fE_g/E_f} \xrightarrow{\sim} G_{E_g/E_f\cap E_g} &= G_{E_g/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}. \end{aligned}$$

(2) Poichè sia $E_f/\mathbb{Q}$ che $E_g/\mathbb{Q}$ sono di Galois e $E_f \cap E_g = \mathbb{Q}$, abbiamo

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

Esercizio 3. Si mostri che, per ogni numero primo p, esiste una estensione E/F tale che $G_{E/F} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$. Mostrare che è possibile scegliere $F = \mathbb{Q}$.

Soluzione: Si consideri l'estensione ciclotomica $\mathbb{Q}(\mu_{p^2})/\mathbb{Q}$, che ha gruppo di Galois

$$G_{\mathbb{Q}(\mu_{p^2})/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

Il sottogruppo $H = \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$ corrisponde alla estensione $\mathbb{Q}(\mu_{p^2})^H/\mathbb{Q}$ che ha gruppo di Galois

$$G_{\mathbb{Q}(\mu_{p^2})^H/\mathbb{Q}} \simeq \frac{G_{\mathbb{Q}(\mu_{p^2})/\mathbb{Q}}}{G_{\mathbb{Q}(\mu_{p^2})/\mathbb{Q}(\mu_{p^2})^H}} = \frac{G_{\mathbb{Q}(\mu_{p^2})/\mathbb{Q}}}{H}$$

di ordine p.

Esercizio 4. Sia p un numero primo ed $n \geq 1$ un intero. Sia K il p^n-esimo campo ciclotomico ed sia L il p^{n+1}-esimo campo ciclotomico. Siano $\mathcal{O}_K$ e $\mathcal{O}_L$ gli anelli degli interi di K ed L rispettivamente.

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

Soluzione: (1) Sia ζ una radice primitiva della unità di ordine p^{n+1}. Allora $a := \zeta^p$ è una radice primitiva della unità di ordine p^{n+1}.

Visto che $\mathcal{O}_L = \mathbb{Z}[\zeta]$ e $\mathcal{O}_K = \mathbb{Z}[a]$ segue che $\mathcal{O}_L = \mathcal{O}_K[\zeta]$. Posso quindi prendere $\alpha = \zeta$. L'estensione $[L : K] = [L : \mathbb{Q}]/[K : \mathbb{Q}]$ ha grado p e quindi il polinomio minimo di ζ su K è $X^p - a$.

(2) Il discriminante di α su K è $\Delta_{L/K} = \mathrm{Norm}_{L/K}\big(f'(\alpha)\big)$ per la Proposizione 3.9 degli appunti. Calcoliamo $f'(X) = pX^{p-1}$ e quindi $f'(\alpha) = p\zeta^{p-1}$. Siccome $\mathrm{Norm}_{L/K}(\zeta) = a$ per la Proposizione 3.7 degli appunti segue che $\Delta_{L/K} = p^p a^{p-1}$.

(3) 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 $g(X) := X^p - \bar{a}$ con $\bar{a}$ la classe di a modulo $\mathfrak{P}$.

Supponiamo che $\mathfrak{P}$ non divida $p\mathcal{O}_K$. Allora $g'(X) = pX^{p-1} \neq 0$ 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 p allora $g(X) = (X-\beta)^p$ con $\beta^p = \bar{a}$ 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 $\mathfrak{P}\mathcal{O}_L = \mathfrak{Q}^p$.

Esercizio 5. Sia K un campo di numeri e sia $\mathcal{O}_K$ il suo anello degli interi.

(1) Definire la nozione di base intera di $\mathcal{O}_K$. Dimostrare che una base intera ha come discriminante un intero non nullo.
(2) Dimostrare che due basi interi hanno uguale discriminante.
(3) Dimostrare che esiste una base di K come $\mathbb{Q}$-spazio vettoriale che consiste di elementi di $\mathcal{O}_K$.

Soluzione: Vedere gli appunti.