SOLUZIONI DEL COMPITINO DEL 22/06/2016

Esercizio 1. Si consideri il polinomio $f(X) = X^7 - 7 \in \mathbb{Q}[X]$ 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 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 ciclotomiche 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 $\rho \in G_{E/\mathbb{Q}(\zeta)}$ 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 determini il gruppo di Galois $G_{E/\mathbb{Q}}$ del campo di spezzamento $E/\mathbb{Q}$ del polinomio

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

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

$$D(f) = -4 \cdot (-1)^3 - 27 \cdot 3^2 = -239.$$

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 $g(X) := X^2 + 2 \in \mathbb{Q}[X]$ è irriducibile (per il criterio di Eisenstein) 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 $\mathbb{Q}\left(\sqrt{2}\right)$ è l'unico sottocampo quadratico di E_f (che corrisponde all'unico sottogruppo di indice due in S_3), ovvero $\mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}\left(\sqrt{239}i\right)$ (infatti $\left[\mathbb{Q}\left(\sqrt{D(f)}\right) : \mathbb{Q}\right] = 2$ poichè $D(f) = -239$ non è un quadrato in $\mathbb{Q}$). Ma ciò non è possibile perchè in tal caso $\mathbb{Q}\left(\sqrt{239}i\right) = \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{R}$.

Esercizio 3. Si mostri che, dato un campo F, sono equivalenti i fatti che seguono.

(1) F è perfetto;
(2) la caratteritica di F è zero oppure è $p \neq 0$ ed ogni elemento di F è una potenza di p.

Soluzione: Si veda la proposizione 2.15 di Milne.

Esercizio 4. Sia $n \geq 2$ un intero e sia $\mathbb{Q} \subset K$ l'n-esimo campo ciclotomico.

(1) Dimostrare che $[K : \mathbb{Q}]$ è uguale a $\phi(n)$.
(2) Dimostrare che il discriminante di K divide $n^{\phi(n)}$.

Soluzione: vedere le note.

Esercizio 5. Sia K il 12^o-campo ciclotomico.

(1) Determinare l'anello degli interi $\mathcal{O}_K$ ed il discriminante relativo a $\mathbb{Q}$.

(2) Determinare i primi $p \in \mathbb{Z}$ che ramificano in $\mathcal{O}_K$ e per ciascuno descrivere la decomposizione di $p\mathcal{O}_K$ come prodotto di ideali primi.
(3) Determinare i primi $p \in \mathbb{Z}$ che spezzano completamente come prodotto di quattro ideali primi distinti in $\mathcal{O}_K$

Soluzione: Osserviamo che $K = \mathbb{Q}(\zeta)$ con $\zeta = \frac{\sqrt{3}+i}{2}$ radice primitiva dell'unità di ordine 12. Quindi K coincide con $\mathbb{Q}(i, \sqrt{-3})$, il composto del 4^o campo ciclotomico $K_1 := \mathbb{Q}(i)$ e del 3^o campo ciclotomico $K_2 := \mathbb{Q}(\sqrt{-3})$. Sappiamo che $\mathcal{O}_{K_1} = \mathbb{Z}[i]$ con discriminante $\Delta_1 = -4$ e $\mathcal{O}_{K_2} = \mathbb{Z}[\alpha]$ con $\alpha := \frac{1+\sqrt{-3}}{2}$ con discriminate $\Delta_2 := -3$ (vedere l'esercizio 4.11 delle note). Visto che Δ_1 e Δ_2 sono coprimi, segue dal Corollario 4.13 che $\mathcal{O}_K \cong \mathcal{O}_{K_1}\mathcal{O}_{K_2}$ e il discriminate di K coincide con $\Delta_1^2\Delta_2^2 = 2^4 3^2$.

Quindi, dato un primo p, abbiamo $\mathcal{O}_K/p\mathcal{O}_K \cong \big(\mathcal{O}_{K_1}/p\mathcal{O}_{K_1}\big)\big(\mathcal{O}_{K_2}/p\mathcal{O}_{K_2}\big)$. Affinchè p spezzi completamente in $\mathcal{O}_K$ dobbiamo avere che $\mathcal{O}_K/p\mathcal{O}_K$ sia isomorfo a $\mathbb{F}_p^4$ (come anello) per il Teorema Cinese, ovvero $\big(\mathcal{O}_{K_1}/p\mathcal{O}_{K_1}\big) \cong \mathbb{F}_p^2$ e $\big(\mathcal{O}_{K_2}/p\mathcal{O}_{K_2}\big) \cong \mathbb{F}_p^2$. Condizione necessaria e sufficiente è quindi che p spezzi completamente sia in $\mathcal{O}_{K_1}$ che in $\mathcal{O}_{K_2}$ ovvero, grazie al Corollario 6.12 delle note, che $p \neq 2, 3$ e che -1 e -3 siano quadrati modulo p.

Siccome $2\mathcal{O}_{K_1} = \mathcal{Q}^2$ e $3\mathcal{O}_{K_2} = \mathcal{P}^2$ con $\mathcal{Q}$ e $\mathcal{P}$ ideali primi per il Corollario 6.12 delle note, segue dal lemma 6.7 delle note che 2 e 3 ramificano in $\mathcal{O}_K$. Questi sono gli unici primi che ramificano in $\mathcal{O}_K$ per il teorema 6.10(ii) delle note. Siccome $2\mathcal{O}_{K_2}$ è un ideale primo per il Corollario 6.12, segue che $2\mathcal{O}_K = \mathcal{T}^2$ con $\mathcal{T} = \mathcal{Q}\mathcal{O}_K$ primo. Analogamente siccome $3\mathcal{O}_{K_1}$ è un ideale primo per il Corollario 6.12, segue che $3\mathcal{O}_K = \mathcal{U}^2$ con $\mathcal{U} = \mathcal{P}\mathcal{O}_K$ primo.