ESAME DI ALGEBRA 3, 26/01/2017

Esercizio 1. Sia K il campo di spezzamento di $T^5 - 5 \in \mathbb{Q}[T]$.

i. Mostrare che $\mathbb{Q} \subset K$ è una estensione finita di Galois. Determinarne il grado.
ii. Sia G il gruppo di Galois dell'estensione $\mathbb{Q} \subset K$. Descrivere il gruppo G.
iii. Determinare i sottogruppi di G di ordine 4 e i corrispondenti sottocampi di K, esibendone dei generatori su $\mathbb{Q}$.
iv. Determinare i sottogruppi di G di ordine 2 e i corrispondenti sottocampi di K, esibendone dei generatori su $\mathbb{Q}$.

Soluzione: (i) Essendo $\mathbb{Q}$ unc ampo di caratteritica 0, esso è perfetto e quindi $f(T) = T^5 - 5$ è un polinomio separabile. Concludiamo che $\mathbb{Q} \subset E$ è una estensione di Galois. Sia $\alpha \in \mathbb{C}$ una radice di $f(T)$. Se ζ è una radice primitiva dell'unità di ordine 5, l'insieme delle radici di $f(T)$ è

$$\left\{\alpha\zeta^i : i = 0, ..., 4\right\}.$$

Dunque $K \subset \mathbb{Q}(\alpha, \zeta)$ e, poichè $\zeta = \frac{\alpha\zeta}{\alpha}$, si ha $K = \mathbb{Q}(\alpha, \zeta)$. Sappiamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, poichè $f(T) \in \mathbb{Q}[T]$ è irriducibile per il criterio di Eisenstein applicato con il prima $p = 5$, e che $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(5) = 4$ per la teoria dei campi ciclotomici. La moltiplicatività dei gradi implica che il grado di $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta)$ su $\mathbb{Q}$ divida sia 4 che 5 e, quindi, sia uguale ad 1 ovvero $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$. Poichè l'estensione $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ è una estensione di Galois, sappiamo che

$$[E : \mathbb{Q}] = 20.$$

(ii) Poichè $\mathbb{Q}(\zeta)/\mathbb{Q}$ è di Galois, la restrizione $\sigma \mapsto \sigma|_{\mathbb{Q}(\zeta)}$ induce un isomorfismo di gruppi

$$\mathrm{Gal}_{K/\mathbb{Q}(\alpha)} \xrightarrow{\sim} \mathrm{Gal}_{\mathbb{Q}(\zeta)/\mathbb{Q}}.$$

D'altra parte la teoria delle estensioni ciclotomiche garantisce che

$$\mathrm{Gal}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \cong \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}.$$

Poichè 2 genera $\left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^{\times}$, esiste uno ed un solo $\sigma \in \mathrm{Gal}_{E/\mathbb{Q}}$ tale che $\sigma(\zeta) = \zeta^2$ e $\sigma(\alpha) = \alpha$. Tale elemento ha ordine 4 e genera il sottogruppo $H = \mathrm{Gal}_{K/\mathbb{Q}(\alpha)}$ di $\mathrm{Gal}_{K/\mathbb{Q}}$.

Poichè $\mu_5 \subset \mathbb{Q}(\zeta)$, sappiamo anche dalla teoria delle estensioni cicliche che

$$\mathrm{Gal}_{K/\mathbb{Q}(\zeta)} \xrightarrow{\sim} \mu_5$$

via $g \mapsto \frac{g(\alpha)}{\alpha}$. Dunque esiste uno ed un solo $\rho \in \mathrm{Gal}_{K/\mathbb{Q}(\zeta)}$ tale che $\rho(\alpha) = \zeta\alpha$. Tale elemento ha ordine 5 e genera il sottogruppo $N = \mathrm{Gal}_{K/\mathbb{Q}(\zeta)}$ di $G := \mathrm{Gal}_{K/\mathbb{Q}}$. Osserviamo che N è un sottogruppo normale per il Teorema fondamentale della teoria di Galois, in quanto $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ è di Galois. L'applicazione indotta $H \subset G \to G/N \cong \mathrm{Gal}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è un isomorfismo per quanto visto sopra e quindi G è il prodotto semidiretto di N ed H. Quindi ogni elemento di G si scrive come $\rho^j\sigma^i$ per unici interi $0 \leq j \leq 4$ e $0 \leq i \leq 3$ e vale la legge di gruppo è determinata da $\sigma^i\rho^j\sigma^{-i} = \rho^{2^i j}$: l'uguaglianza risulta verificata in quanto entrambi gli elementi di N mandano α nello stesso elemento $\zeta^{2^i j}\alpha$.

(iii) Per il I teorema di Sylow, essendo 4 la massima potenza di 2 che divide l'ordine di $G = \mathrm{Gal}_{K/\mathbb{Q}}$, tutti i sottogruppi di ordine 4 di G sono tutti e soli i coniugati di H e, quindi sono tutti e soli i sottogruppi di G della forma $\rho^j H \rho^{-j}$ al variare di $0 \leq j \leq 4$. Per il teorema fondamentale della teoria di Galois $\rho^j H \rho^{-j}$ corrisponde al sottocampo $\rho^j\big(\mathbb{Q}(\alpha)\big) = \mathbb{Q}(\zeta^j\alpha)$. Resta da verificare che tali sottogruppi o tali sottocampi sono tutti distinti fra loro. Osserviamo che una $\mathbb{Q}$-base di E è data da $\{\zeta^i\alpha^j | 0 \leq i \leq 3, 0 \leq j \leq 4\}$, base composta delle $\mathbb{Q}$-basi $\{1, \dots \zeta^3\}$ di $\mathbb{Q}(\zeta)$ e $\{1, \dots, \alpha^4\}$ di $\mathbb{Q}(\alpha)$. Basta quindi mostrare che $\mathbb{Q}(\zeta^j\alpha)$ sono sottospazi distinti di K, al variare di $0 \leq j \leq 4$, usando la $\mathbb{Q}$-base appena esibita. Siccome $\zeta^4 = -1 - \zeta - \zeta^2 - \zeta^3$, la conclusione segue.

(*iii*) I sottogruppi di G di ordine 2 corrispondono agli elementi $g \in G$ di ordine 2. Ciascuno di essi è un elemento di un 2-Sylow e quindi, visto che ciascun $\rho^j H \rho^{-j}$ è ciclico di ordine 4, ottengo esattamente 5-elementi $\rho^j \sigma^2 \rho^{-j} = \rho^{2j}\sigma^2$ con $0 \leq j \leq 4$. A ciascuno di essi corrsiponde una estensione quadratica del campo $\mathbb{Q}(\zeta^j \alpha)$ associato a $\rho^j H \rho^{-j}$. Essa coincide quindi con il sottocampo $\mathbb{Q}(\zeta^j\alpha, \zeta + \overline{\zeta})$ osservando che σ^2 è il coniugio complesso e quindi $\zeta + \overline{\zeta}$ è fissato da $\rho^j\sigma^2\rho^{-j}$.

Esercizio 2. (*) Sia E l'ottavo campo ciclotomico.

i. Si mostri che l'estensione $\mathbb{Q} \subset E$ è finita e di Galois. Se ne calcoli il grado e il gruppo di Galois.
ii. Si determini il reticolo dei sottocampi $\mathbb{Q} \subset E$.
iii. Sia $E \subset L$ il campo di spezzamento di $(X^2-2)(X^2-3)$. Si dimostri che l'estensione $\mathbb{Q} \subset L$ è finita e di Galois. Se ne calcoli il grado e il gruppo di Galois.
iv. Si trovi $\alpha \in L$ tale che $L = \mathbb{Q}(\alpha)$.

Soluzione:
i) La teoria delle estensioni ciclotomiche garantisce che $\mathbb{Q} \subset E$ è finita e di Galois e

$$\mathrm{Gal}_{E/\mathbb{Q}} \cong \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

In particolare $[E : \mathbb{Q}] = 4$.
(ii) Siccome $\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$ è una radice primitiva dell'unità di ordine 8 abbiamo che $E \subset \mathbb{Q}(i, \sqrt{2})$ ed infatti $E = \mathbb{Q}(i, \sqrt{2})$, un campo biquadratico, per ragioni di gradi. I sottocampi sono quindi $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2}), E$.
(iii) Siccome $X^2 - 2$ si spezza in E, abbiamo che $L = E(\sqrt{3})$. Inoltre $\sqrt{3} \notin E$ visto che $\mathbb{Q}(\sqrt{3})$ non appare nella lista dei sottocampi quadratici di E esibiti in (ii). Concludo quindi che $[L : E] = 2$ e $[L : \mathbb{Q}] = 8$ per moltiplicatività dei gradi. Siccome L è il campo composto di due estensioni di Galois di $\mathbb{Q}$, ovvero E e $\mathbb{Q}(\sqrt{3})$, la cui intersezione è $\mathbb{Q}$, sappiamo dalla teoria che

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}_{E/\mathbb{Q}} \times \mathrm{Gal}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}^3.$$

Esplicitamente $\mathrm{Gal}(E/\mathbb{Q})$ è generato da tre elementi di ordine 2, denotati σ, τ e δ che fissano due dei tre elementi $\sqrt{2}, i, \sqrt{3}$ e mandano il restante in -1 volte se stesso.
(iv) Sia $\alpha = \sqrt{2} + i + \sqrt{3}$. Usando il fatto che una $\mathbb{Q}$-base di E è $\{\sqrt{2}^a i^b \sqrt{3}^c | 0 \leq a, b, c \leq 1\}$ e il punto (ii) segue che l'orbita $\mathrm{Gal}(E/\mathbb{Q})\alpha$ ha cardinalità 8 e quindi $\mathbb{Q}(\alpha)$ ha grado 8 su $\mathbb{Q}$. Concludo che $E = \mathbb{Q}(\alpha)$.

Esercizio 3. Sia K il 15-esimo campo ciclotomico e sia $\mathcal{O}_K$ l'anello degli interi.

i. Dimostrare che se p è un primo di $\mathbb{Z}$ che ramifica in $\mathcal{O}_K$ allora $p \in \{3, 5\}$;
ii. Dimostrare che se $p = 3$ oppure $p = 5$ allora p ramifica in $\mathcal{O}_K$;
iii. Determinare la decomposizione di 5 in $\mathcal{O}_K$.

Soluzione:
(i) Sappiamo che $\mathcal{O}_K = \mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/\big(\Phi_{15}(X)\big)$ con ζ una radice primitiva di ordine 15 dell'unità e $\Phi_{15}(X)$ il 15^o polinomio ciclotomico. Segue allora dal Teorema 6.10 che un primo intero p ramifica se e solo se divide il discriminate Δ di $\mathcal{O}_K$ relativamente a $\mathbb{Z}$. Sappiamo che Δ divide $15^{\varphi 15}$ e quindi condizione necessaria affinchè p ramifichi è che $p \in \{3, 5\}$.
(ii) Visto che $\zeta^3 =: \zeta_5$ è una radice primitiva dell'unità di ordine 5, allora K contine il quinto campo ciclotomico L. Sappiamo che 5 ramifica in quest'ultimo perchè, per un primo p, l'unico primo che ramifica nel p-esimo campo ciclotomico è p con indice di ramificazione $p-1$ e indice di inerzia 1. Per moltiplicatività degli indici di ramificazione concludiamo che 5 ramifica anche in $\mathcal{O}_K$. Analogamente $\zeta^5 =: \zeta_3$ è una radice primitiva dell'unità di ordine 3. Quindi K contine il terzo campo ciclotomico Ne 3 ramifica in $\mathcal{O}_K$. Quindi $p \in \{3, 5\}$ è anche condizione sufficiente affinchè p ramifichi in $\mathcal{O}_K$.
(iii) Sappiamo che $5\mathcal{O}_L = Q^4$ con $Q = (\zeta_5 - 1, 5)$ e $\mathcal{O}_L/Q = \mathbb{F}_5$ visto che l'indice di inerzia di Q è 1. Inoltre sappiamo che $\mathcal{O}_K = \mathcal{O}_L \cdot \mathcal{O}_N = \mathbb{Z}[\zeta_3, \zeta_5]$ avendo $\mathcal{O}_L$ ed $\mathcal{O}_N$ discriminanti coprimi. Quindi $\mathcal{O}_K = \mathcal{O}_L[\zeta_3] \cong \mathcal{O}_L[X]/(X^2 + X + 1)$ con $X^2 + X + 1$ il 3^o poliniomio ciclotomico. Osserviamo che

$X^2 + X + 1$ non ammette radici in $\mathcal{O}_L/Q = \mathbb{F}_5$ e quindi segue dal Teorema 6.8 che $P := Q\mathcal{O}_K$ è un ideal primo. Concludiamo che $5\mathcal{O}_K = P^4$.

Esercizio 4. (*TeoGal*)$^{(*)}$ Sia K il p-esimo campo ciclotomico e sia $\zeta \in K$ una radice primitiva p-esima dell'unità. Dimostare che ζ è costruibile con riga e compasso a partire da $\mathbb{Q}$ se e solo se p è un primo di Fermat cioè della forma $p = 2^h + 1$ per un qualche $h \in \mathbb{N}$.

Esercizio 5. (*TeoNum*) Sia K un campo di numeri di grado n su $\mathbb{Q}$ e sia $\mathcal{O}_K$ l'anello degli interi.

i. Dimostrare che due basi intere $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_n\}$ di $\mathcal{O}_K$ hanno uguale discriminante $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) =: d$;

ii. Siano $\gamma_1, \ldots, \gamma_n \in \mathcal{O}_K$. Dimostrare che se $\mathrm{disc}_{K/\mathbb{Q}}(\gamma_1, \ldots, \gamma_n) = d$ allora $\{\gamma_1, \ldots, \gamma_n\}$ è una base intera di $\mathcal{O}_K$.