SOLUZIONI DELL'ESAME DEL 27/01/2015

Esercizio 1. Si calcoli il gruppo di Galois del campo di spezzamento del polinomio $f(X) = X^4 + 7X + 5 \in \mathbb{Q}[X]$.

Soluzione: Mostriamo per cominciare che il polinomio è irriducibile in $\mathbb{Q}[X]$. Per il lemma di Gauss è sufficiente verificare che è irriducibile in $\mathbb{Z}[X]$ e per farlo mostriamo che la sua riduzione modulo 2,

$$f_2(X) = X^4 + X + 1 \in \mathbb{F}_2[X],$$

è irriducibile. Non ha radici e dunque, se fosse riducibile, si avrebbe

$$\begin{aligned} f_2(X) &= \left(X^2 + aX + b\right)\left(X^2 + cX + d\right) \\ &= X^4 + (a+c)X^3 + (b+d+ac)X^2 + (ad+bc)X + bd. \end{aligned}$$

Dunque dedurremmo che $a + c = 0$, $b + d + ac = 0$, $ad + bc = 1$ e $bd = 1$. L'ultima equazione implica che $b = d = 1$; inserendo questi valori nella terza equazione deduciamo che $a + c = 1$, in contraddizione con la prima equazione.

Il risolvente cubico è

$$g_f(X) = X^3 - 20X - 49 \in \mathbb{Q}[X]$$

ed il discriminante

$$D(f) = D(g_f) = 256 \cdot 5^3 - 27 \cdot 7^4 = -32827.$$

Mostriamo che il risolvente cubico è irriducibile: poichè il discriminante non è un quadrato in $\mathbb{Q}$ seguirà che il gruppo di Galois è isomorfo ad S_4.

Se è riducibile ammette una radice x (avendo grado 3) ed in questo caso sappiamo che, se $x = \frac{r}{s}$ cone $(r, s) = 1$, $s \mid 1$ ed $r \mid 49 = 7^2$. Segue che

$$x \in \{\pm 1, \pm 7, \pm 49\}.$$

Poichè $g_f(1) = -68$, $g_f(-1) = -30$, $g_f(7) = 154$, $g_f(-7) = -252$, $g_f(49) = 116620$ and $g_f(-1) = -116718$ deduciamo l'irriducibilità.

Esercizio 2. Si considerino i seguenti polinomi in $\mathbb{Q}[X]$: $f(X) = X^3 + X + 5$ e $g(X) = X^7 - 1$. Siano E_f ed E_g i rispettivi campi di spezzamento e sia E is campo di spezzamento di $f(X)\,g(X)$.

(1) Si calcoli il grado della estensione $E_f/\mathbb{Q}$ e se ne determini il gruppo di Galois, mostrando che si tratta di un sottogruppo di S_3.
(2) Si calcoli il grado della estensione $E_g/\mathbb{Q}$ e se ne determini il gruppo di Galois, mostrando che si tratta di un sottogruppo di un gruppo ciclico C.
(3) Si calcoli il grado della estensione $E/\mathbb{Q}$ e se ne determini il gruppo di Galois, mostrando che si tratta di un sottogruppo di $S_3 \times C$.
(4) Si determini l'immagine di $G_{E/\mathbb{Q}}$ in $S_3 \times C$.

Soluzione: (1) Notiamo che $f(X) \in \mathbb{Q}[X]$ è irriducibile poichè la sua riduzione modulo 2 lo è, non ammettendo radici ed avendo grado 3. Il discriminante è

$$D(f) = -4 \cdot 1^3 - 27 \cdot 5^2 = -679 = -7 \cdot 97.$$

Non è dunque un quadrato in $\mathbb{Q}$ e da ciò deduciamo che $G_{E_f/\mathbb{Q}} \simeq S_3$ e $[E_f : \mathbb{Q}] = 6$.

(2) Il campo di spezzamento di $g(X)$ è il campo di spezzamento di $\frac{g(X)}{X-1} = \Phi_7(X)$, il 7-esimo polinomio ciclotomico. Dunque $E_g = \mathbb{Q}(\zeta_7)$ e, per la teoria delle estensioni ciclotomiche, sappiamo che

$$G_{E_g/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{6\mathbb{Z}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$$

e che $[E_g : \mathbb{Q}] = 6$.

$(3-4)$ Notiamo che i sottocampi $K \subset E_f$ tali che $K/\mathbb{Q}$ è normale sono in biiezione con i sottogruppi normali di $G_{E_f/\mathbb{Q}} \simeq S_3$; esiste dunque una sola estensione propria di $\mathbb{Q}$ normale $K = \mathbb{Q}\left(\sqrt{-679}\right) \subset E_f$. Poichè $G_{E_g/\mathbb{Q}}$ è abeliano, ogni sottocampo di E_g è normale su $\mathbb{Q}$ e pertanto $E_f \cap E_g/\mathbb{Q}$ è normale. Segue che $E_f \cap E_g \subset \mathbb{Q}\left(\sqrt{-679}\right)$ (essendo $\mathbb{Q}$ oppure dovendo coincidere con $\mathbb{Q}\left(\sqrt{-679}\right)$). Poichè $7 \equiv 3 \mod (4)$, $\mathbb{Q}\left(\sqrt{-7}\right) \subset E_g = \mathbb{Q}(\zeta_{31})$ e questa è l'unica estensione quadratica, essendo $G_{E_g/\mathbb{Q}}$ ciclico. Non è dunque possibile che si abbia $E_f \cap E_g = \mathbb{Q}\left(\sqrt{-679}\right)$, dovendo in tal caso essere

$$\mathbb{Q}\left(\sqrt{-679}\right) = E_f \cap E_g = \mathbb{Q}\left(\sqrt{-7}\right).$$

Pertanto $E_f \cap E_g = \mathbb{Q}$ e, poichè $E_f/\mathbb{Q}$ ed $E_g/\mathbb{Q}$ sono entrambe estensioni di Galois,

$$\begin{aligned} G_{E/\mathbb{Q}} &= \left\{(\sigma_1, \sigma_2) \in G_{E_f/\mathbb{Q}} \times G_{E_g/\mathbb{Q}} : \sigma_{1|\mathbb{Q}} = \sigma_{2|\mathbb{Q}}\right\} \\ &= G_{E_f/\mathbb{Q}} \times G_{E_g/\mathbb{Q}} \simeq S_3 \times \frac{\mathbb{Z}}{6\mathbb{Z}}. \end{aligned}$$

Esercizio 3. (*TeoGal*) Sia E/F una estensione di Galois, $f(X) \in F[X]$ e sia

$$R_f(E) = \{x \in E : f(x) = 0\}.$$

(1) Si mostri che il gruppo di Galois $G_{E/F}$ della estensione E/F agisce sull'insieme $R_f(E)$.
(2) Si mostri che, se $f(X) \in F[X]$ è irriducibile, $R_f(E) \neq \phi$ se e solo se E contiene un campo di spezzamento di $f(X)$.
(3) Si supponga che E contenga un campo di spezzamento di $f(X)$, che $f(X)$ non ha radici multiple e sia $\pi : R_f(E) \to G_{E/F}\backslash R_f(E)$ l'applicazione quoziente. Si mostri che, per ogni classe $\mathbf{x} \in G_{E/F}\backslash R_f(E)$,

$$f_{\mathbf{x}}(X) := \prod_{x \in \pi^{-1}(\mathbf{x})} (X - x) \in F[X]$$

è irriducibile in $F[X]$ e che

$$f(X) = \prod_{\mathbf{x} \in G_{E/F}\backslash R_f(E)} f_{\mathbf{x}}(X)$$

è una decomposizione di $f(X) \in F[X]$ in fattori irriducibili.

Soluzione: (1) Poichè $f(X) \in F[X]$, si ha $\sigma(f(x)) = \sigma(f)(x) = f(x)$ per ogni $\sigma \in G_{E/F}$ ed ogni $x \in E$. Deduciamo che l'azione di $G_{E/F}$ su E manda $R_f(E)$ in se stesso e dunque $G_{E/F}$ agisce su $R_f(E)$.

(2) Poichè E/F è normale, $f(X)$ ammette una radice in E (ovvero $R_f(E) \neq \phi$) se e solo se $f(X)$ sispezza completamente in E.

(3) Possiamo scrivere

$$R_f(E) = \bigsqcup_{\mathbf{x} \in G_{E/F}\backslash R_f(E)} \pi^{-1}(\mathbf{x}),$$

da cui la decomposizione

$$f(X) = \prod_{\mathbf{x} \in G_{E/F} \backslash R_f(E)} f_{\mathbf{x}}(X) \text{ in } E[X].$$

Poichè l'azione di $G_{E/F}$ su $R_f(E)$ manda $\pi^{-1}(\mathbf{x})$ in se stesso, deduciamo che $\sigma(f_{\mathbf{x}})(X) = f_{\mathbf{x}}(X)$ per ogni $\sigma \in G_{E/F}$, ovvero

$$f_{\mathbf{x}}(X) \in E^{G_{E/F}}[X] = F[X].$$

Resta da mostrare che $f_{\mathbf{x}}(X) \in F[X]$ è irriducibile. Supponiamo che $f_{\mathbf{x}}(X) = g(X)h(X)$ dove $g(X), h(X) \in F[X]$. Poichè $g(X) \in F[X]$, $G_{E/F}$ agisce sull'insieme $R_g(E)$ e dunque $R_g(E) \subset \pi^{-1}(\mathbf{x})$ è un insieme $G_{E/F}$-saturo. Se $\deg(g) > 0$, $\exists x \in R_g(E) \subset \pi^{-1}(\mathbf{x})$ e allora, poichè $\pi^{-1}(\mathbf{x})$ è il più piccolo insieme $G_{E/F}$-saturo che contiene x (essendo l'orbita di x), deduciamo $R_g(E) = \pi^{-1}(\mathbf{x})$. Ma poichè $\pi^{-1}(\mathbf{x}) = R_g(E) \sqcup R_h(E)$ si ha $\deg(h) = 0$ e ciò mostra l'irriducibilità.

Esercizio 4. (*TeoNum)* Sia K un campo di numeri di grado n come estensione di $\mathbb{Q}$. Denotiamo con $\mathcal{O}_K$ l'anello degli interi.

(1) Dati n-elementi $\alpha_1, \ldots, \alpha_n \in K$ si ricordi la definizione di discriminate $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ e si mostri che $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$.
(2) Si mostri che se $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ allora $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$
(3) Si ricordi la definizione di base intera di $\mathcal{O}_K$ e si mostri che due basi intere $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_n\}$ hanno uguale discriminante, ovvero che

$$\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n).$$

Soluzione: vedere gli appunti di Teoria dei Numeri, in particolare le Proposizioni 3.4 e 4.4 per le prime due domande e il Lemma 4.8 per la terza.

Esercizio 5. Sia K il 20^o campo ciclotomico. Denotiamo con $\mathcal{O}_K$ il suo anello degli interi.

(1) Determinare il grado di K su $\mathbb{Q}$. Descriverne l'anello degli interi.
(2) Determinare i primi $p \in \mathbb{Z}$ che ramificano in $\mathcal{O}_K$.
(3) Trovare la decomposizione di $5 \cdot \mathcal{O}_K$ come prodotto di idelai primi di $\mathcal{O}_K$. Per ciascuno di tali primi determinare indice di inerzia e indice di ramificazione.

Soluzione: 1) Il grado $[K : \mathbb{Q}]$ è $\varphi(20) = \varphi(4)\varphi(5) = 8$ ove φ è la funzione di Eulero. L'anello degli interi è $\mathbb{Z}[\zeta]$ con ζ radice primitiva di ordine 20 dell'unità. Vedere gli appunti di Teoria dei Numeri, in particolare il Teorema 1.7 e il Teorema 4.15.

2) I primi che ramificano sono esattamente i primi che dividono il discriminante $\Delta_{K/\mathbb{Q}}$ di K su $\mathbb{Q}$ grazie al Teorema 6.10. Sappiamo che esso divide $20^{\varphi(20)}$ per il Lemma 4.16 e quindi i primi che ramificano sono al più 2 e 5.

Visto che $\alpha := \zeta^5$ è una radice primitva di ordine 4 dell'unità e $\beta = \zeta^4$ è una radice primitiva di ordine 5 dell'unità segue che il 4^o campo ciclotomico $M = \mathbb{Q}(\alpha)$ è contenuto in K e il 5^o campo ciclotomico $L = \mathbb{Q}(\beta)$ è contenuto in K. Ma 2 ramifica in M grazie al Teorema 6.8: infatti $\mathcal{O}_M = \mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$ e $X^2 + 1 = (X+1)^2$ in $\mathbb{F}_2[X]$. Analogamente 5 ramifica in L: $\mathcal{O}_L = \mathbb{Z}[\beta] \cong \mathbb{Z}[X]/(X^4 + X^3 + X^2 + X + 1)$ e $X^4 + X^3 + X^2 + X + 1 = (X+1)^4$ in $\mathbb{F}_5[X]$. Per la moltiplicatività degli indici di inerzia (Lemma 6.7) segue che 2 e 5 ramificano anche in K.

3) Segue dal calolo in (2) che $5\mathcal{O}_L = \mathcal{P}^4$ con $\mathcal{P} = (\beta + 1, 5)$ e $\mathcal{O}_L/\mathcal{P} = \mathbb{F}_5$.

Inoltre $\mathcal{O}_M = \mathcal{O}_L[\alpha]$. Infatti $\alpha \cdot \beta \in \mathcal{O}_L[\alpha]$ è una radice primitiva di ordine 20 dell'unità e quindi genera $\mathcal{O}_M$. Inoltre, visto che $[K : L] = 2$ e $\alpha^2 + 1 = 0$ segue che la valutazione in α definisce un isomorfismo $\mathcal{O}_L[\alpha] \cong \mathcal{O}_L[T]/(T^2+1)$. Osserviamo che $\mathbb{F}_5^*$ è un gruppo

ciclico di ordine 4 e quindi il polinomio T^4-1, ed in particolare il suo divisore T^2+1, spezza completamente in $\mathbb{F}_5$. Ad esempio le classi di 2 e di 3 sono zeri di $T^2+1 \in \mathbb{F}_5[T]$ ovvero $T^2+1=(T-2)(T-3) \in \mathcal{O}_L/\mathcal{P}[T]$. Concludo allora dal Teorema 6.8 che $\mathcal{P}\cdot\mathcal{O}_M = \mathcal{Q}_1\cdot\mathcal{Q}_2$ con

$$\mathcal{Q}_1 = \mathcal{P}\mathcal{O}_M + (\alpha-2)\mathcal{O}_M = (\beta+1, \alpha-2, 5)$$

e

$$\mathcal{Q}_2 = \mathcal{P}\mathcal{O}_M + (\alpha-3)\mathcal{O}_M = (\beta+1, \alpha-3, 5).$$

Deduco allora che $5\mathcal{O}_M = \mathcal{P}^4\mathcal{O}_M = \big(\mathcal{P}\mathcal{O}_M\big)^4 = \mathcal{Q}_1^4\mathcal{Q}_2^4$. Inoltre $\mathcal{O}_M/\mathcal{Q}_1 \cong \mathcal{O}_L/\mathcal{P}[T]/(X-2) = \mathbb{F}_5$ e quindi l'indice di inerzia di $\mathcal{Q}_1$ è 1 e il suo indice di ramificazione è 4. La stessa cosa vale anche per $\mathcal{Q}_2$.