**SOLUZIONI DELL'APPELLO DI ALGEBRA 3, 24/02/2015**

**Esercizio 1.** Si consideri il polinomio $f(X) = X^4 + 2X^3 + 3X + 1 \in \mathbb{Q}[X]$ e sia $E_f$ il suo campo di spezzamento.

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

$$\{K/\mathbb{Q} \text{ estensioni di campi} : [K:\mathbb{Q}] = 2 \text{ e } K \subset E_f\}.$$

*Soluzione:* (1) Le uniche possibili radici razionali di $f(X)$ sono della forma $x = \frac{r}{s}$ con $(r,s) = 1$, $r \mid 1$ ed $s \mid 1$. Dunque

$$x \in \{\pm 1\}.$$

D'altra parte $f(1) = 7$ ed $f(-1) = -3$. Dunque $f(X)$ non ha radici razionali; se fosse riducibile si avrebbe dunque $f(X) = f_1(X) f_2(X)$ dove $f_i(X) \in \mathbb{Q}[X]$ sarebbe di grado due. Infatti, poichè $f(X)$ è monico, $f_i(X) \in \mathbb{Z}[X]$ e, riducendo modulo 2 questa uguaglianza, otterremmo che

$$\begin{aligned} X^4 + X + 1 &= \left(X^2 + aX + b\right)\left(X^2 + cX + d\right) \\ &= X^4 + (a+c)X^3 + (b+d+ac)X^2 + (ad+bc)X + bd \text{ in } \mathbb{F}_2[X]. \end{aligned}$$

Ma allora deduciamo le seguenti relazioni.

(1) $a + c = 0 \Rightarrow c = -a$.
(2) $b + d + ac = 0$ dunque, per (1), $a^2 = b + d$.
(3) $ad + bc = 1$ dunque, per (1), $a(d-b) = 1$ ed allora $(a, d-b) = (1,1)$.
(4) $bd = 1$, dunque $b = d = 1$.

Dalla (4) segue che $d - b = 1 - 1 = 0$ e ciò contraddice (3). Dunque $f(X)$ non può essere prodotto di due polinomi di grado 2. Abbiamo pertanto mostrato che $f(X)$ è irriducibile.

(2) Il suo risolvente cubico è

$$\begin{aligned} g_f(X) &= X^3 + (2 \cdot 3 - 4)X - \left(2^2 + 3^2\right) \\ &= X^3 + 2X - 13. \end{aligned}$$

Si tratta di un polinomio irriducibile in $\mathbb{Q}[X]$ poichè ha grado tre e non ha radici in $\mathbb{Q}$. Infatti, se $x = \frac{r}{s}$ con $(r,s) = 1$ fosse una radice, si avrebbe $r \mid -13$ ed $s \mid 1$. Dunque

$$x \in \{\pm 1, \pm 13\}.$$

Ma $f(1) = -10$,f(13) $= 2210$, $f(-1) = -16$ ed $f(-13) = -2236$. Inoltre

$$\begin{aligned} D(f) &= D(g_f) = -4 \cdot 2^3 - 27 \cdot (-13)^2 \\ &= -4595 = -5 \cdot 919. \end{aligned}$$

Non si tratta di un quadrato in $\mathbb{Q}$ e, poichè $g_f(X)$ è irriducibile, deduciamo che $G_{E_f/\mathbb{Q}} \simeq S_4$.

(3) Poichè $G_{E_f/\mathbb{Q}} \simeq S_4$ esiste una ed una sola estensione quadratica in $E_f$: questa corrisponde all'unico sottogruppo di $S_4$ di indice 2, ovvero $A_4$. Sappiamo dunque che tale estensione è $\mathbb{Q}\left(\sqrt{D(g)}\right) = \mathbb{Q}\left(\sqrt{-4595}\right)$.

**Esercizio 2.** Si considerino i polinomi $f(X) = X^4 + 2X + 2$ ed $g(X) = X^3 + 2X + 4$ in $\mathbb{Q}[X]$ e siano $E_f$ ed $E_g$ i rispettivi campi di spezzamento.

(1) Si calcoli il gruppo di Galois $G_{E_g/\mathbb{Q}}$.
(2) Si calcoli il gruppo di Galois $G_{E_f/\mathbb{Q}}$.
(3) Posto $E$ ilc ampo composto $E := E_f E_g$ si calcoli il gruppo di Galois $G_{E/\mathbb{Q}}$.

*Soluzione:* (1) Per cominciare notiamo che $g(X) \in \mathbb{Q}[X]$ è irriducibile, poichè la sua riduzione modulo 3 è irriducibile avendo grado 3 e non avendo radici. Il suo discriminante è

$$D(g) = -\left(4 \cdot 2^3 + 27 \cdot 4^2\right) = -464 = -2^4 \cdot 29.$$

Non essendo un quadrato in $\mathbb{Q}$, abbiamo $G_{E_g/\mathbb{Q}} \simeq S_3$.

(2) Il polinomio $f(X)$ è irriducibile in $\mathbb{Q}[X]$ per il criterio di Eisenstein applicato al primo 2. Il suo risolvente cubico è

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

Le uniche possibili radici razionali di $g_f(X)$ sono della forma $x = \frac{r}{s}$ con $(r,s) = 1$, $r \mid -4$ ed $s \mid 1$. Dunque

$$x \in \{\pm 1, \pm 2, \pm 4\}.$$

Abbiamo $g_f(1) = -11$, $g_f(-1) = 3$, $g_f(2) = -12$, $g_f(-2) = 4$, $g_f(4) = 28$ e $g_f(-4) = -36$. Pertanto $g_f(X)$ è irrucibile in $\mathbb{Q}[X]$. Il discriminante di $f(X)$ è

$$\begin{aligned} D(f) &= D(g_f) = -\left(4 \cdot (-8)^3 + 27 \cdot (-4)^2\right) = 1616 \\ &= 2^4 \cdot 101. \end{aligned}$$

Poichè $g_f(X)$ è irriducibile in $\mathbb{Q}[X]$ e $D(f)$ non è un quadrato in $\mathbb{Q}$, abbiamo $G_{E_f/\mathbb{Q}} \simeq S_4$.

(3) Poichè $E_g/\mathbb{Q}$ ed $E_f/\mathbb{Q}$ sono estensioni di Galois, posto $K := E_g \cap E_f$ sappiamo che $K/\mathbb{Q}$ è di Galois. Abbiamo inoltre

$$[K : \mathbb{Q}] \mid \#S_3 = 6.$$

Dunque $[K : \mathbb{Q}] \in \{1, 2, 3, 6\}$ ma il caso $[K : \mathbb{Q}] = 3$ è da escludere poichè le estensioni normali in $E_g/\mathbb{Q}$, che ha gruppo di Galois isomorfo ad $S_3$, hanno grado 1, 2 oppure 6. Sappiamo inoltre che $\mathbb{Q}\left(\sqrt{D(g)}\right) = \mathbb{Q}\left(\sqrt{-29}\right)$ è l'unica estensione quadratica in $E_g/\mathbb{Q}$. Se $[K : \mathbb{Q}] = 6$ (rispettivamente $[K : \mathbb{Q}] = 2$), deduciamo che

$$\mathbb{Q}\left(\sqrt{-29}\right) \subset E_g = E_g \cap E_f \subset E_f$$

(rispettivamente $\mathbb{Q}\left(\sqrt{-29}\right) = K \subset E_f$). Ma poichè $G_{E_f/\mathbb{Q}} \simeq S_4$, l'unica estensione quadratica in $E_f/\mathbb{Q}$ è quella che corrisponde all'unico sottogruppo di indice 2, ovvero $\mathbb{Q}\left(\sqrt{D(f)}\right) = \mathbb{Q}\left(\sqrt{101}\right)$. Si otterrebbe dunque

$$\sqrt{-29} \in \mathbb{Q}\left(\sqrt{-29}\right) = \mathbb{Q}\left(\sqrt{101}\right) \subset \mathbb{R}$$

e ciò non è possibile. Dunque $K = \mathbb{Q}$ ed essendo $E_g/\mathbb{Q}$ ed $E_f/\mathbb{Q}$ di Galois

$$G_{E/\mathbb{Q}} \xrightarrow{\sim} G_{E_f/\mathbb{Q}} \times G_{E_g/\mathbb{Q}} = S_4 \times S_3.$$

**Esercizio 3.** Sia $0 \neq x \in \mathbb{F}_{p^n}$ dove $p$ è un primo dispari ed $n \geq 1$.

(1) Si mostri che $p^n - 1 \equiv 0 \ mod(2)$ e che sono equivalenti le seguenti affermazioni:
   - $\exists y \in \mathbb{F}_{p^n}$ tale che $x = y^2$;
   - $x^{\frac{p^n-1}{2}} = 1$.

(2) Si mostri che la funzione
$$\chi : \mathbb{F}_{p^n}^{\times} \to \{\pm 1\}$$
definita dalla formula
$$\chi(x) := \begin{cases} 1 & \text{se } x \text{ è un quadrato in } \mathbb{F}_{p^n}^{\times}, \\ -1 & \text{altrimenti,} \end{cases}$$
è un omomorfismo di gruppi (moltiplicativi).

(3) Si mostri che il polinomio $f(X) := X^{\frac{p^n-1}{2}} - 1 \in \mathbb{F}_p[X]$ ha $\mathbb{F}_{p^n}$ come campo di spezzamento.

*Soluzione:* (1) Per prima cosa notiamo che
$$p^n - 1 = (p-1)\left(p^{n-1} + ... + p + 1\right) \equiv 0 mod(2)$$
poichè $p$ è dispari. Dalla teoria dei campi finiti sappiamo che is gruppo moltiplicativo $\mathbb{F}_{p^n}^{\times}$ è ciclico. Dunque $\mathbb{F}_{p^n}^{\times} \simeq \frac{\mathbb{Z}}{(p^n-1)\mathbb{Z}}$ è l'endomorfismo di $\mathbb{F}_{p^n}^{\times}$ definito da $y \mapsto y^2$ corrisponde all'omomorfismo di $\frac{\mathbb{Z}}{(p^n-1)\mathbb{Z}}$ definito da $z \mapsto 2z$. Poichè $2 \mid p^n - 1$, $(p^n-1)\mathbb{Z} \subset 2\mathbb{Z}$ e pertanto l'immagine di questo endomorfismo è $\frac{2\mathbb{Z}}{(p^n-1)\mathbb{Z}}$, ovvero l'unico sottogruppo di $\frac{\mathbb{Z}}{(p^n-1)\mathbb{Z}}$ di indice due. Se $z \in \frac{2\mathbb{Z}}{(p^n-1)\mathbb{Z}}$, allora $z = 2h$ per qualche $h \in \frac{\mathbb{Z}}{(p^n-1)\mathbb{Z}}$ e si ha
$$\frac{p^n-1}{2} z = \frac{p^n-1}{2} 2h = (p^n-1)\, h = 0.$$
Viceversa, se $\frac{p^n-1}{2} z = 0$ allora $z \in \frac{\mathbb{Z}}{(p^n-1)\mathbb{Z}}$ è rappresentato da $\widetilde{z} \in \mathbb{Z}$ tale che $\frac{p^n-1}{2}\widetilde{z} = (p^n-1)\,\widetilde{h}$ per qualche $\widetilde{h} \in \mathbb{Z}$. Deduciamo che
$$(p^n-1)\,\widetilde{z} = (p^n-1)\, 2\widetilde{h},$$
dunque $\widetilde{z} = 2\widetilde{h}$ ed infine $z = 2h$. Abbiamo mostrato che $\exists h$ tale che $z = 2h$ se e solo se $\frac{p^n-1}{2} z = 0$; passando alle notazioni moltiplicative otteniamo la tesi.

(2) Poichè $x^{p^n-1} = 1$ per ogni $x \in \mathbb{F}_{p^n}^{\times}$, necessariamente $x^{\frac{p^n-1}{2}} \in \{\pm 1\} \subset \mathbb{F}_{p^n}^{\times}$ (essendo $x^{\frac{p^n-1}{2}}$ una delle due radici del polinomio $X^2 - 1 \in \mathbb{F}_p[X]$). Segue da (1) che $\chi(x) = x^{\frac{p^n-1}{2}}$ e pertanto $\chi$ è un omomorfismo.

Alternativamente, come notato in (1), l'immagine dell'applicazione $y \mapsto y^2$ è l'unico sottogruppo $H \subset \mathbb{F}_{p^n}^{\times}$ di indice 2. Detta
$$\pi : \mathbb{F}_{p^n}^{\times} \to \frac{\mathbb{F}_{p^n}^{\times}}{H}$$
l'applicazione quoziente si ha che $x$ è un quadrato in $\mathbb{F}_{p^n}^{\times}$ se e solo se $x \in H$, ovvero $\pi(x) = 1$. Identificando $\frac{\mathbb{F}_{p^n}^{\times}}{H} \simeq \{\pm 1\}$ (come gruppi moltiplicativi nell'unico modo possibile), si ha che $\pi$ corrisponde a $\chi$, che è dunque un omomorpfismo.

(3) Il polinomio $f(X)$ spezza completamente in $\mathbb{F}_{p^n}[X]$, come si deduce utilizzando $\mathbb{F}_{p^n}^{\times} \simeq \frac{\mathbb{Z}}{(p^n-1)\mathbb{Z}}$, oppure l'uguaglianza
$$f(X)\left(X^{\frac{p^n-1}{2}} + 1\right) = \left(X^{\frac{p^n-1}{2}} - 1\right)\left(X^{\frac{p^n-1}{2}} + 1\right) = X^{p^n-1} - 1$$
assieme al fatto che $X^{p^n-1} - 1$ spezza in $\mathbb{F}_p$. Dunque $\mathbb{F}_{p^n}$ contiene un campo di spezzamento $F$ di $f(X)$. D'altra parte, poichè $F \subset \mathbb{F}_{p^n}$ contiene l'insieme delle radici di $f(X)$ e 0 (che non è una radice di $f(X)$),
$$\#F \geq \frac{p^n-1}{2} + 1 = \frac{p^n+1}{2}.$$

Deduciamo dunque che

$$p^n = (\#F)^{[\mathbb{F}_{p^n}:F]} \geq \left(\frac{p^n+1}{2}\right)^{[\mathbb{F}_{p^n}:F]}.$$

Se dunque $[\mathbb{F}_{p^n} : F] \geq 2$, segue che

$$p^n \geq \left(\frac{p^n+1}{2}\right)^2 = \frac{p^{2n}+2p^n+1}{4}.$$

Ciò significa che

$$0 \geq p^{2n} - 2p^n + 1 = (p^n - 1)^2,$$

da cui $p^n = 1$ e quindi la contraddizione $n = 0$. Pertanto $[\mathbb{F}_{p^n} : F] = 1$, ovvero $F = \mathbb{F}_{p^n}$.

**Esercizio 4.** Sia $\zeta_7 \in \mathbb{C}$ una radice primitiva dell' unità di ordine 7. Sia $K = \mathbb{Q}(\zeta_7)$, $L = \mathbb{Q}(\sqrt{3})$ ed $M = K \cdot L$ il campo composto.

i. Calcolare il grado di $K$, $L$ ed $M$ su $\mathbb{Q}$;

ii. Determinare l'anello degli interi di $K$ ed $L$ e i discriminanti di $\mathcal{O}_K$ ed $\mathcal{O}_L$ relativamente a $\mathbb{Q}$;

iii. Determinare la decomposizione del primo 7 in $\mathcal{O}_M$ e per ciascuno primo che appare nella decomposizione determinare indice di inerzia e di ramificazione.

*Soluzione:* Il grado di $L$ su $\mathbf{Q}$ è 2 e l'anello degli interi è $\mathcal{O}_L = \mathbf{Z}[\sqrt{3}]$ per la Proposizione 2.9 degli Appunti. Il discriminante $\mathrm{disc}(\mathcal{O}_L)$ è 12 (esercizio 4.11).

Il grado di $K$ su $\mathbf{Q}$ è $\varphi(7) = 6$ e l'anello degli interi è $\mathcal{O}_K = \mathbf{Z}[\zeta_7]$ per il Teorema 4.15. Il discriminante $\mathrm{disc}(\mathcal{O}_K)$ è $-7$ per il Corollario 3.11. Segue dallo stesso Corollario che $K$ contiene un unico campo quadratico dato da $\mathbf{Q}(\sqrt{-7})$ e quindi $L$ non è contenuto in $K$ ovvero $K \cap L = \mathbf{Q}$. Visto che $K$ ed $L$ sono entrambe estensioni di Galois di $\mathbf{Q}$ concludiamo che il grado di $M$ su $\mathbf{Q}$ è $2 \cdot 6 = 12$. Inoltre, visto che i discriminanti di $\mathcal{O}_K$ e $\mathcal{O}_L$ sono coprimi segue dal Teorema 4.12 che $\mathcal{O}_M = \mathcal{O}_K \cdot \mathcal{O}_L = \mathbf{Z}[\zeta_7, \sqrt{3}]$.

Sappiamo dal Corollario 6.13 che $7\mathcal{O}_K = \mathcal{P}^6$ con $\mathcal{P}$ un ideale massimale di $\mathcal{O}_K$ con $\mathcal{O}_K/\mathcal{P} = \mathbf{F}_7$. Abbiamo visto che $\mathcal{O}_M = \mathcal{O}_K[\sqrt{3}] \cong \mathcal{O}_K[X]/(X^2-3)$ tramite l'applicazione che invia $X \mapsto \sqrt{3}$. Allora $\mathcal{O}_M/\mathcal{P}\mathcal{O}_M \cong \mathcal{O}_K/\mathcal{P}[X]/(X^2-3) = \mathbf{F}_7[X]/(X^2-3)$. Visto che 3 non è un quadrato modulo 7 (i quadrati sono 1, 2 e 4) allora $X^2 - 3 \in \mathbf{F}_7[X]$ risulta essere un polinomio irriducibile. Segue dal Teorema 6.8 che $\mathcal{Q} := \mathcal{P}\mathcal{O}_M$ è un ideale primo di $\mathcal{O}_M$ e quindi $7\mathcal{O}_K = \mathcal{Q}^6$ con indice di inerzia $f_{\mathcal{Q}/7} = 2$ e indice di ramificazione $e_{\mathcal{Q}/7} = 6$.

**Esercizio 5.** Dato un primo $p \geq 3$ ed un intero positivo $h$, si determini

(1) il $p^h$-esimo polinomio ciclotomico $\Phi_h(X)$;
(2) mostrare che il discriminante dell'anello degli interi del $p^h$-esimo campo ciclotomico è una potenza di $p$.
(3) * determinare il discriminante dell'anello degli interi del $p^h$-esimo campo ciclotomico a meno di segno.

*Soluzione:* Sia $\zeta = \exp(2\pi i/p^h)$. Il $p^h$-esimo campo ciclotomico $K$ coincide con $\mathbf{Q}(\zeta)$ ed ha grado $[K : \mathbf{Q}] = \varphi(p^h) = p^{h-1}(p-1)$. Sappiamo inoltre che $\mathcal{O}_{\mathbb{Q}[\zeta]} = \mathbb{Z}[\zeta]$. Inoltre $X^{p^h} - 1 = (X^{p^{h-1}} - 1)\Phi(X)$ (vedere il Lemma 4.17) e il discriminante cercato è uguale a $\epsilon N_{K/\mathbb{Q}}(\Phi'(\zeta))$ dove $\epsilon = 1$ se $\varphi(p^h) \equiv 0$ o 1 modulo 4 e $\epsilon = -1$ altrimenti (Teorema 4.15 e Proposizione 3.9).

Differenziando l'uguaglianza $X^{p^h} - 1 = (X^{p^{h-1}} - 1)\Phi(X)$ e sostituendo $X$ con $\zeta$ si ottiene

$$p^h = p^h \zeta^{p^h} = \zeta(\zeta^{p^{h-1}} - 1)\Phi'(\zeta).$$

Applicando la norma $N_{K/\mathbb{Q}}$ otteniamo

$$p^{h\varphi(p^h)} = \epsilon \mathrm{disc}(\mathcal{O}_K) N_{K/\mathbb{Q}}(\zeta) N_{K/\mathbb{Q}}(\zeta^{p^{h-1}} - 1).$$

Sappiamo dalla proposizione 3.7 che $N_{L/\mathbb{Q}}(\zeta)$ coincide con il termine costante di $\Phi(X)$, a meno di segno. Quindi $N_{K/\mathbb{Q}}(\zeta) = \pm\Phi(0) = \pm 1$. Osserviamo che $\eta := \zeta^{p^{h-1}}$ è una radice primitiva dell'unità di ordine $p$. In particolare è un intero algebrico e $N_{K/\mathbb{Q}}(\zeta^{p^{h-1}} - 1)$ risulta essere un intero grazie al lemma 3.8. Segue che $\mathrm{disc}(\mathcal{O}_K)$ divide $p^{h\varphi(p^h)}$.

Per rispondere all'ultimo quesito, sia $\Psi(X)$ il $p$-esimo polinomio ciclotomico. Allora il polinomio minimo di $\eta - 1$ è $\Psi(X+1)$. Quindi, ponendo $L = \mathbf{Q}(\eta)$ abbiamo che $N_{L/\mathbb{Q}}(\eta - 1) = \pm\Psi(1) = \pm p$. Segue dalla definizione 3.5 che $N_{K/\mathbb{Q}}(\eta - 1) = N_{L/\mathbb{Q}}(\eta - 1)^{[L:K]}$ che coincide, a meno di segno, con $p^{\frac{\varphi(p^h)}{p-1}} = p^{p^{h-1}}$.

Concludiamo che, a meno di segno, $\mathrm{disc}(\mathcal{O}_K) = \pm p^{(h(p-1)-1)p^{h-1}}$.