**SOLUZIONI DELL'APPELLO DI ALGEBRA 3, 28/04/2015**

**Esercizio 1.** Si consideri il polinomio $f(X) = X^7 - 3 \in \mathbb{Q}[X]$ e sia $E$ il suo campo di spezzamento.

(1) Si mostri che $E = \mathbb{Q}(\alpha, \zeta)$ con $\alpha$ radice di $f(X)$ e $\zeta$ radice primitiva settima dell'unità e si calcoli $[E : \mathbb{Q}]$.
(2) Si mostri che $G_{E/\mathbb{Q}(\alpha)}$ è ciclico, 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, generato dall'unico elemento $\rho \in G_{E/\mathbb{Q}(\zeta)}$ tale che $\rho(\alpha) = \zeta\alpha$.
(3) Si determini $i \in \mathbb{Z}$ tale che $\sigma\rho\sigma^{-1} = \rho^i$.

*Soluzione:* (1) Poichè $f'(X) = 7X^6$, esiste una ed una sola radice reale $\alpha$ 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 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$ 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 isomorpfismo

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

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 $\sigma$ 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 $\rho$ tale che $\rho(\alpha) = \zeta\alpha$.

(3) Notiamo che $G_{E/\mathbb{Q}(\zeta)} \lhd G_{E/\mathbb{Q}}$ e dunque $\sigma\rho\sigma^{-1}, \rho^i \in G_{E/\mathbb{Q}(\zeta)}$ sono determinati dalla loro azione su $\alpha$. Si verifica facilemente per induzione che $\rho^i(\alpha) = \zeta^i\alpha$, mentre

$$\sigma\left(\rho\left(\sigma^{-1}(\alpha)\right)\right) = \sigma(\rho(\alpha)) = \sigma(\zeta\alpha) = \sigma(\zeta)\sigma(\alpha) = \zeta^3\alpha.$$

Dunque $\sigma\rho\sigma^{-1} = \rho^3$.

**Esercizio 2.** Si consideri il polinomio $f(X) = X^4 + 4X^3 + 6X^2 + 7X + 7 \in \mathbb{Q}[X]$ e sia $E_f$ is suo campo di spezzamento.

(1) Si mostri che $f(X)$ è irriducibile in $\mathbb{Q}[X]$.
(2) Si mostri che $X^4 + 3X + 3$ è irriducibile in $\mathbb{Q}\left(\sqrt{21}\right)[X]$. (Suggerimento: si utilizzi il punto (3) dell'esercizio (3) , il fatto che $5\mathcal{O}_{\mathbb{Q}\left(\sqrt{21}\right)} = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_{\mathbb{Q}\left(\sqrt{21}\right)}$ con $\mathfrak{p}_1$ e $\mathfrak{p}_2$ primi distinti, grazie all'esercizio (4), e quindi si studi la riduzione modulo $\mathfrak{p}_1$).
(3) Si calcoli $G_{E_f/\mathbb{Q}}$.
(4) Si calcoli

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

*Soluzione:* (1) Abbiamo

$$f(X-1) = X^4 + 3X + 3$$

che è irriducibile per il criterio di Eisenstein.

$(2-3)$ Il risolvente cubico di $f(X)$ è il polinomio

$$\begin{aligned} g_f(X) &= X^3 - 6X^2 + (4\cdot 7 - 4\cdot 7)X + 4\cdot 6\cdot 7 - 4^2\cdot 7 - 7^2 \\ &= X^3 - 6X^2 + 7 \\ &= (X+1)\left(X^2 - 7X + 7\right). \end{aligned}$$

Poichè le radici di $X^2 - 7X + 7$ sono $\frac{7}{2} - \frac{\sqrt{21}}{2}$ ed $\frac{\sqrt{21}}{2} + \frac{7}{2}$, il campo di spezzamento di $g_f$ è $E_{g_f} = \mathbb{Q}\left(\sqrt{21}\right)$ e $\#R_f(\mathbb{Q}) = 1$. Si ha dunque $G_{E_f/\mathbb{Q}} \simeq D_4$ (risp. $G_{E_f/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$) se $f(X) \in \mathbb{Q}\left(\sqrt{21}\right)[X]$ è irridicibile (resp. riducibile). Mostriamo che non è possibile che $f(X) \in \mathbb{Q}\left(\sqrt{21}\right)[X]$ sia riducibile e che dunque si ha dunque $G_{E_f/\mathbb{Q}} \simeq D_4$.

In tal caso, segue dal punto (3) dell'esercizio di teoria di Galois applicato ad $F = \mathbb{Q}$, $K = \mathbb{Q}\left(\sqrt{21}\right)$ ed $E = E_f$ che possiamo scrivere $f(X) = f_1(X) f_2(X)$ in $\mathbb{Q}\left(\sqrt{21}\right)[X]$, dove $\deg(f_1) = \deg(f_2) = 2$ ed $f_i(X) \in \mathbb{Q}\left(\sqrt{21}\right)[X]$ è monico irriducibile. Ma poichè $X \mapsto X - 1$ induce un automorfismo di $\mathbb{Q}\left(\sqrt{21}\right)[X]$ come $\mathbb{Q}\left(\sqrt{21}\right)$-algebra, ciò equivale a dire che possiamo scrivere

$$\begin{aligned} X^4 + 3X + 3 &= f(X-1) = \left(X^2 + aX + b\right)\left(X^2 + cX + d\right) \\ &= X^4 + (a+c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd \end{aligned}$$

dove $a, b, c, d \in \mathbb{Q}\left(\sqrt{21}\right)$ ed i due polinomi di grado due sono irriducibili in $\mathbb{Q}\left(\sqrt{21}\right)[X]$. Ricaviamo le seguenti equazioni.

- $(i)$ $a + c = 0 \Leftrightarrow c = -a$;
- $(ii)$ $b + d + ac = 0 \Leftrightarrow$ (per la $(i)$) $b + d - a^2 = 0 \Leftrightarrow b + d = a^2$;
- $(iii)$ $ad + bc = 3$ (per la $(i)$) $a(d - b) = 3$;
- $(iv)$ $bd = 3$.

Notiamo che, poichè le radici di $X^4 + 3X + 3$ sono interi algebrici e la fattorizzazione che si considera è in polinomi monici, $a, b, c, d \in \mathcal{O}_{\mathbb{Q}(\sqrt{21})}$. Poichè $5\mathcal{O}_{\mathbb{Q}(\sqrt{21})}$ spezza in $\mathcal{O}_{\mathbb{Q}(\sqrt{21})}$, detto $\mathfrak{p}$ un primo che divide $5\mathcal{O}_{\mathbb{Q}(\sqrt{21})}$, si ha $\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{21})}}{\mathfrak{p}} = \mathbb{F}_5$. Possiamo ridurre modulo $\mathfrak{p}$ l'equazione che esprime la riducibilità di $X^4 + 3X + 3$ ed otteniamo le equazioni $(i)$, $(ii)$, $(iii)$ e $(iv)$ in $\mathbb{F}_5$. La tabella della moltiplicazione in $\mathbb{F}_5$ è la seguente:

| $\cdot$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

Segue da $(iv)$ che, a meno di permutare i ruoli dei polinomi $f_1(X)$ ed $f_2(X)$, possiamo avere $(b, d) = (1, 1)$, $(2, 3)$, $(4, 4)$. Trattaiamo separatamente ciascun caso. Se $(b, d) = (1, 1)$ oppure $(4, 4)$, allora si ottiene un contraddizione con $(iii)$. Se $(b, d) = (2, 3)$, allora $d - b = 1$ (mentre $b + d = 0$), dunque dalla $(iii)$ (risp. $(ii)$) otteniamo $a = 3$ (risp. $0 = a^2$): la $(iii)$ e la $(ii)$ sono incompatibili. Dunque otteniamo una contraddizione da ciò l'irriducibilità di $X^4 + 3X + 3$ in $\mathbb{Q}\left(\sqrt{21}\right)$.

(4) In generale i sottogruppi di $D_n = \langle r \rangle \rtimes \langle s \rangle$ sono i seguenti.

- I sottogruppi ciclici $\left\langle r^d \right\rangle$ di indice $2d$, uno ed uno solo per ogni $d \mid n$.

- I sottogruppi diedrali $\left\langle r^d \right\rangle \rtimes \left\langle r^i s \right\rangle$ di indice $d$, uno ed uno solo per ogni $d \mid n$ e $0 \leq i \leq d-1$.

Dunque esiste un solo sottogruppo di $G_{E_f/\mathbb{Q}} \simeq D_4$ di indice 2 del primo tipo (per $d=1$) e due del secondo tipo (per $d=2$ ed $i=0,1$). Questi tre sottogruppi corrispondono alle tre estensioni quadratiche $K/\mathbb{Q}$ in $E_f$.

**Esercizio 3.** Supponiamo che $E/F$ sia una estensione di Galois che contiene tutte le radici $R_f$ di un polinomio $f(X) \in F[X]$ irriducibile e separabile.

(1) Si mostri che, se $H \subset G_{E/F}$ è un sottogruppo, $\pi_H : R_f \to H\backslash R_f$ è l'applicazione quoziente
$$f_{\mathbf{x}}(X) := \prod_{x \in \pi_H^{-1}(\mathbf{x})} (X - x) \in E^H[X]$$
è irriducibile e
$$f(X) = \prod_{\mathbf{x} \in H\backslash R_f} f_{\mathbf{x}}(X)$$
è la decomposizione di $f(X) \in E^H[X]$ in fattori irriducibili.

(2) Si mostri che, se $H \lhd G_{E/F}$ è un sottogruppo normale, allora $\deg(f_{\mathbf{x}_1}) = \deg(f_{\mathbf{x}_2})$ per ogni $\mathbf{x}_1, \mathbf{x}_2 \in H\backslash R_f$.

(3) Si mostri che, se $K/F \subset E/F$ è una sottoestensione quadratica, allora $f(X) \in K[X]$ è irriducibile, oppure
$$f(X) = f_1(X) f_2(X) \in K[X]$$
dove $f_i(X) \in K[X]$ è irriducibile ed ha grado $\deg(f)/2$.

*Soluzione:* (1) Possiamo scrivere
$$R_f = \bigsqcup_{\mathbf{x} \in H\backslash R_f} \pi_H^{-1}(\mathbf{x}).$$
Poichè $f(X) \in E[X]$ si spezza completamente e $f(X)$ ha radici distinte,
$$f(X) = \prod_{\mathbf{x} \in H\backslash R_f} f_{\mathbf{x}}(X) \text{ in } E[X].$$
Poichè l'azione di $H$ su $R_f$ manda $\pi_H^{-1}(\mathbf{x})$ in se stesso, deduciamo che $\sigma(f_{\mathbf{x}})(X) = f_{\mathbf{x}}(X)$ per ogni $\sigma \in H$, ovvero
$$f_{\mathbf{x}}(X) \in E^H[X].$$
Resta da mostrare che $f_{\mathbf{x}}(X) \in E^H[X]$ è irriducibile. Supponiamo che $f_{\mathbf{x}}(X) = g(X) h(X)$ dove $g(X), h(X) \in E^H[X]$. Poichè $g(X) \in E^H[X]$, $H$ agisce sull'insieme $R_g$ e dunque $R_g \subset \pi_H^{-1}(\mathbf{x})$ è un insieme $H$-saturo. Se $\deg(g) > 0$, $\exists x \in R_g \subset \pi_H^{-1}(\mathbf{x})$ e allora, poichè $\pi_H^{-1}(\mathbf{x})$ è il più piccolo insieme $H$-saturo che contiene $x$ (essendo l'orbita di $x$), deduciamo $R_g = \pi_H^{-1}(\mathbf{x})$. Ma poichè $\pi_H^{-1}(\mathbf{x}) = R_g \sqcup R_h$ si ha $\deg(h) = 0$ e ciò mostra l'irriducibilità.

(2) Notiamo che $\deg(f_{\mathbf{x}}) = \#\pi_H^{-1}(\mathbf{x})$ e dunque basta mostrare che $\#\pi_H^{-1}(\mathbf{x}_1) = \#\pi_H^{-1}(\mathbf{x}_2)$. Poichè $f(X) \in F[X]$ è irriducibile, $G_{E/F}$ agisce transitivamente sulle radici di $f$: se dunque $\mathbf{x}_i = Hx_i$ per qualche $x_i \in R_f$, sappiamo che esiste $g \in G_{E/F}$ tale che $x_2 = gx_1$. Consideriamo l'applicazione
$$g : R_f \to R_f;$$
si tratta di una biiezione con inversa l'applicazione $g^{-1}$. Poichè
$$ghx_1 = ghg^{-1}gx_1 = ghg^{-1}x_2 \in gHg^{-1}x_2 = Hx_2,$$
deduciamo che
$$g\left(\pi_H^{-1}(\mathbf{x}_1)\right) = gHx_1 \subset Hx_2 = \pi_H^{-1}(\mathbf{x}_2).$$

Poichè $g$, come notato, induce una biiezione di $R_f$ in se stesso, da ciò segue che $g$ si restringe ad una biiezione

$$g : \pi_H^{-1}(\mathbf{x}_1) \to \pi_H^{-1}(\mathbf{x}_2).$$

Dunque $\#\pi_H^{-1}(\mathbf{x}_1) = \#\pi_H^{-1}(\mathbf{x}_2)$.

(3) Una estensione quadratica $K/F \subset E/F$ corrisponde ad un sottogruppo normale in $G_{E/F}$ e possiamo applicare (2).

**Esercizio 4.** Si studi la decomposizione di 2, 3 e 5 in $\mathbb{Q}\left(\sqrt{21}\right)$.

*Soluzione:* Ricordiamo che, in $\mathbb{Q}\left(\sqrt{d}\right)$ con $d \equiv 1 \mod 4$, si ha $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\alpha]$ dove $\alpha = \frac{1+\sqrt{21}}{2}$. Ricaviamo che

$$4\alpha^2 - 4\alpha + 1 - d = 0.$$

Poichè $d \equiv 1 \mod 4$, $\alpha$ soddisfa il polinomio monico

$$f_\alpha(X) = X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X].$$

Nel nostro caso $d = 21$,

$$f_\alpha(X) = X^2 - X - 5.$$

Tale polinomio è irriducibile in $\mathbb{F}_2$, poichè non ha radici. Dunque $2\mathcal{O}_{\mathbb{Q}(\sqrt{21})}$ è primo. Poichè $d \equiv 1 \mod 4$, il discriminante della estensione è 21, Dunque 3 ramifica in $\mathcal{O}_{\mathbb{Q}(\sqrt{21})}$: infatti $3\mathcal{O}_{\mathbb{Q}(\sqrt{21})} = \left(3, \sqrt{21}\right)^2$ poichè in generale, se $p \mid d$, si ha $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \left(p, \sqrt{d}\right)$ in un qualunque campo quadratico $\mathbb{Q}\left(\sqrt{d}\right)$. Infine

$$f_\alpha(X) = X(X-1) \text{ in } \mathbb{F}_5[X].$$

Dunque 5 spezza in $\mathcal{O}_{\mathbb{Q}(\sqrt{21})}$ e si ha

$$5\mathcal{O}_{\mathbb{Q}(\sqrt{21})} = (5, \alpha)(5, \alpha - 1)$$

con $(5, \alpha)$ e $(5, \alpha - 1)$ primi.

**Esercizio 5.** Sia $K$ un campo di numeri e sia $\mathcal{O}_K$ il suo anello degli interi. Siano $I$ e $J$ ideali di $\mathcal{O}_K$. Defniamo il massimo comun divisore $\mathrm{MCD}(I, J)$ di $I$ e $J$ come l'ideale di $\mathcal{O}_K$ tale che (i) $\mathrm{MCD}(I, J)$ divide $I$ e $J$ in $\mathcal{O}_K$ e (ii) se $\Delta$ è un ideale di $\mathcal{O}_K$ che divide sia $I$ che $J$, allora $\Delta$ divide $\mathrm{MCD}(I, J)$. Dimostrare che $\mathrm{MCD}(I, J)$ esiste, è unico ed è uguale all'ideale somma $I + J$.

*Soluzione:* Un ideale $I$ divide un ideale $J$ se e solo se $J \subseteq I$. Dunque la condizione (i) equivale a $I$ e $J \subseteq \mathrm{MCD}(I, J)$ mentre la condizione (ii) equivale a "$I$ e $J \subseteq \Delta$ implica $\mathrm{MCD}(I, J) \subseteq \Delta$". Segue che $\mathrm{MCD}(I, J)$ (se esiste) è il più piccolo ideale contenente $I$ e $J$. Ma il più piccolo ideale contenente $I$ e $J$ esiste ed è uguale all'ideale somma $I + J$. Abbiamo ottenuto che $\mathrm{MCD}(I, J)$ esiste, è unico ed è uguale a $I + J$.