SOLUZIONI DELL'APPELLO DI ALGEBRA 3, 13/07/2015

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

(1) Si mostri che è irriducibile in $\mathbb{Q}[X]$.
(2) Si calcoli $G_{E_f/\mathbb{Q}}$.

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

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

D'altra parte $f'(X) = 4X^3 + 2$, che ha una sola radice reale α (poichè $f''(X) = 12X^2$ è sempre positiva). Abbiamo $f'(-1) = -2$ e $f'(1) = 6$, da cui deduciamo che $-1 < \alpha < 1$. Pertanto $f(X)$ ha un minimo (relativo) in α, è decrescente in $(-\infty, -1]$ e crescente in $[1, +\infty)$. Deduciamo che

$$f(-4) \geq f(-2) \geq f(-1) = 3,$$
$$7 = f(1) \leq f(2) \leq f(4).$$

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 e possiamo supporlo monico. Infatti, poichè $f(X)$ è monico, $f_i(X) \in \mathbb{Z}[X]$ e, riducendo modulo 3 questa uguaglianza, otterremmo che

$$\begin{aligned} X^4 + 2X + 1 &= \left(X^2 + aX + b\right)\left(X^2 + cX + d\right) \\ &= X^4 + (a+c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd \text{ in } \mathbb{F}_3[X]. \end{aligned}$$

Ma allora dedurremmo le seguenti relazioni.

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

Se $a = 1$, dalla (2) otterremmo $b + d = 1$ e dalla (3) $d - b = 1$. Da ciò seguirebbe che $2d = 2$; dunque $d = 1$ e $b = 0$ contravvenendo a (4). Se invece $a = 2$, dalla (2) otterremmo $b + d = 1$ e dalla (3) $d - b = 2$. Da ciò seguirebbe che $2d = 0$; dunque $d = 0$ contravvenendo a (4). In ogni caso otterremmo una contraddizione e, dunque, $f(X)$ non può essere prodotto di due polinomi di grado 2.

Abbiamo pertanto mostrato che $f(X)$ è irriducibile. Il suo risolvente cubico è

$$g_f(X) = X^3 - 16X - 4.$$

Si tratta di un polinomio la cui riduzione modulo 3 non ha radici e che per questo è irriducibile in $\mathbb{Q}[X]$. Il discriminante di $f(X)$ è

$$\begin{aligned} D(f) &= D(g_f) = -\left(4 \cdot (-16)^3 + 27 \cdot (-4)^2\right) = 15952 \\ &= 2^4 \cdot 997. \end{aligned}$$

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

Esercizio 2. 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) Detto c il coniugio complesso ristretto ad E, si scriva $c = \sigma^i\rho^j$ con $i \in \frac{\mathbb{Z}}{6\mathbb{Z}}$ e $j \in \frac{\mathbb{Z}}{7\mathbb{Z}}$ e si calcoli $\mathbb{R} \cap E$ nella forma $\mathbb{R} \cap E = \mathbb{Q}(\beta, \gamma)$ per opportuni $\beta, \gamma \in E$.

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

(3) Detto c il coniugio complesso ristretto ad E, sappiamo che $c(\alpha) = \alpha \in \mathbb{R}$, mentre $c(\zeta) = \zeta^{-1} = \zeta^6$. D'altra parte $\sigma^2(\alpha) = \alpha$, mentre

$$\sigma^3(\zeta) = \sigma^2(\zeta)^3 = \sigma(\zeta)^9 = \sigma(\zeta)^2 = \zeta^6.$$

Poichè $E = \mathbb{Q}(\alpha, \zeta)$, deduciamo che $\sigma^2 = c$ in $G_{E/\mathbb{Q}(\alpha)} \subset G_{E/\mathbb{Q}}$. Abbiamo

$$\mathbb{Q}\left(\alpha, \zeta + \zeta^{-1}\right) \subset \mathbb{R} \cap E = E^{\langle c\rangle}.$$

Ma $\left[E^{\langle c\rangle} : \mathbb{Q}\right] = \left[G_{E/\mathbb{Q}} : \langle c\rangle\right] = 21$; se dunque mostriamo che il polinomio minimo $f_{\zeta+\zeta^{-1}}(X) \in \mathbb{Q}(\alpha)[X]$ ha grado ≥ 3 seguirà che

$$\left[\mathbb{Q}\left(\alpha, \zeta + \zeta^{-1}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\alpha, \zeta + \zeta^{-1}\right) : \mathbb{Q}(\alpha)\right][\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 3 \cdot 7 = 21,$$

da cui $\mathbb{Q}\left(\alpha, \zeta + \zeta^{-1}\right) = E^{\langle c\rangle}$. Notiamo che, per (2), sappiamo che

$$G_{E/\mathbb{Q}(\alpha)}\left(\zeta + \zeta^{-1}\right) = \left\{\sigma^i\left(\zeta + \zeta^6\right) : i \in \mathbb{N}\right\} = \left\{\zeta + \zeta^6, \zeta^3 + \zeta^{18} = \zeta^3 + \zeta^4, \zeta^9 + \zeta^{12} = \zeta^2 + \zeta^5\right\}$$

e questi elementi sono tutti distinti poichè $\left\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6\right\}$ è una base di E su $\mathbb{Q}(\alpha)$.

Esercizio 3. Posto

$$f_{a,b,c,d}(X) := X^4 + aX^3 + bX^2 + cX + d \in \mathbb{F}_2[X]$$

e quindi $F_{a,b,c,d} := \frac{\mathbb{F}_2[X]}{\left(f_{a,b,c,d}(X)\right)}$, si mostri che $F_{a,b,c,d} \simeq F_{1,1,1,1}$ se e solo se $(a, b, c, d) \neq (0, 1, 0, 1)$, $d \neq 0$ e $d \neq 1 + a + b + c$.

Soluzione: Mostriamo che abbiamo infatti $F_{a,b,c,d} \simeq \mathbb{F}_{2^4}$ se e solo se $(a,b,c,d) \neq (0,1,0,1)$, $d \neq 0$ e $d \neq 1+a+b+c$. Poichè $(1,1,1,1)$ soddisfa queste proprietà avremo mostrato la tesi. D'altra parte $F_{a,b,c,d} \simeq \mathbb{F}_{2^4}$ se e solo se $f_{a,b,c,d}(X) \in \mathbb{F}_2[X]$ è irriducibile. Siamo dunque interessati a mostrare che un polinomio di grado 4 in $\mathbb{F}_2[X]$ è irriducibile in $\mathbb{F}_2[X]$ se e solo se $(a,b,c,d) \neq (0,1,0,1)$, $d \neq 0$ e $d \neq 1+a+b+c$.

I polinomi irriducibili in $\mathbb{F}_2[X]$ di grado 2 sono tutti e soli quelli che non ammettono una radice in $\mathbb{F}_2$. Se siamo interessati a quelli monici, basta contare quelli che sono della forma

$$X^2 + aX + b \text{ con } a, b \in \mathbb{F}_2.$$

Dobbiamo imporre che $f(0) = b$ ed $f(1) = 1+a+b$ siano diversi da 0. Troviamo subito che $b = 1$ e dunque la seconda equazione diventa $f(1) = a$; dovendo essere non zero deduciamo che $a = 1$. Dunque $X^2 + X + 1$ è l'unico polinomio monico irriducibile di grado due. Esiste dunque un solo polinomio monico $f(X)$ di grado 4 che è prodotto di due irriducibili di grado 2; possiamo infatti supporre che i suoi fattori siano monici e troviamo

$$\left(X^2 + X + 1\right)^2 = X^4 + X^2 + 1.$$

Gli altri polinomi monici riducibili di grado 4 sono quelli che ammettono una radice. Abbiamo $f_{a,b,c,d}(0) = d$ ed $f_{a,b,c,d}(1) = 1+a+b+c+d$. Concludiamo dunque che i polinomi monici di grando 4 che sono riducibili sono $X^4 + X^2 + 1 = f_{0,1,0,1}(X)$ e quelli della forma $f_{a,b,c,d}(X)$ con $d = 0$ oppure $d = -(1+a+b+c) = 1+a+b+c$.

Esercizio 4. Sia ζ_3 una radice primitiva dell'unità di ordine 3 e sia $K = \mathbb{Q}(\sqrt{5}, \zeta_3)$.

(1) Determinare il grado della estensione $\mathbb{Q} \subset K$.
(2) Determinare l'anello degli interi $\mathcal{O}_K$ di K.
(3) Determinare la decomposizione dell'ideale $2\mathcal{O}_K$.

Soluzione: (1) Il campo K è il composto dei due campi quadratici $L = \mathbb{Q}(\sqrt{5})$ ed $M = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Il secondo non è contenuto in $\mathbb{R}$ mentre il primo lo è e quindi $L \cap M = \mathbb{Q}$. Concludo che K, essendo il composto di due estensioni galoisiane di $\mathbb{Q}$ di per grado 2, ha grado 4 su $\mathbb{Q}$.

(2) I discriminanti di L ed M sono 5 e -3 rispettivamente. Segue che $\mathcal{O}_L = \mathbb{Z}[\alpha]$ con $\alpha = (1+\sqrt{5})/2$ e $\mathcal{O}_M = \mathbb{Z}[\beta]$ con $\beta = (1+\sqrt{-3})/2$ (Proposizione 2.9 degli appunti). I discriminanti sono $\Delta_L = 5$ e $\Delta_M = -3$ rispettivamente (Esercizio 4.11 degli appunti). In particolare sono coprimi fra loro e $\mathcal{O}_K = \mathcal{O}_L \cdot \mathcal{O}_M = \mathbb{Z}[\alpha, \beta]$ per il Corollario 4.13 degli appunti.

(3) Il polinomio minimo di β su $\mathbb{Z}$ è $X^2 - X + 1$ che è irriducibile modulo 2. Segue allora che $\mathcal{P} = 2\mathcal{O}_M$ è un ideale primo (Corollario 6.12 degli appunti). Inoltre $\mathcal{O}_M/\mathcal{P} \cong \mathbb{F}_2[X]/(X^2+X+1) = \mathbb{F}_4$.

La decomposizione di 2 in $\mathcal{O}_K$ coincide con la decomposizione di $\mathcal{P}$ in $\mathcal{O}_K = \mathcal{O}_M[\alpha] \cong \mathcal{O}_M[T]/(T^2 - T - 1)$. Applico il Teorema 6.8 degli appunti. Il polinomio $T^2 - T - 1$ modulo $\mathcal{P}$ ovvero considerato in $\mathbb{F}_4[T]$ si decompone come prodotto di due fattori distinti di grado 1. Segue che $2\mathcal{O}_M = \mathcal{Q}_1\mathcal{Q}_2$ è il prodotto di due ideali primi di $\mathcal{O}_M$ ciascuno con campo residuo $\mathbb{F}_4$.

Esercizio 5. Sia K un campo di numeri. Dimostrare che l'anello degli interi $\mathcal{O}_K$ è un dominio di Dedekind ovvero

(1) Ogni ideale di $\mathcal{O}_K$ è finitamente generato.
(2) Ogni ideale primo non nullo di $\mathcal{O}_K$ è massimale.
(3) L'anello $\mathcal{O}_K$ è integralmente chiuso in K.

Soluzione: È il Teorema 5.4 degli appunti.