SOLUZIONI DEL COMPITINO DEL 25/02/2019

Esercizio 1. Si consideri il polinomio $f(X) = X^5 - 26 \in \mathbb{Q}[X]$ e sia E un suo campo di spezzamento su $\mathbb{Q}$.

(1) Mostrare che E è un' estensione di Galois di $\mathbb{Q}$. Determinare il grado $[E : \mathbb{Q}]$.
(2) Sia G il gruppo di Galois di E su $\mathbb{Q}$. Esibire una presentazione del gruppo G con generatori e relazioni.
(3) Determinare il numero ed esibire dei generatori delle estensioni $\mathbb{Q} \subset M \subset E$ di grado 10 su $\mathbb{Q}$.

Soluzione: 1) Sia α una radice reale di $f(X)$ e sia ζ una radice primitiva dell'unità di ordine 5. Allora $E = M \cdot L$ con $M = \mathbb{Q}(\alpha)$ e $L = \mathbb{Q}(\zeta)$. Infatti le radici di $f(X)$ sono tutte e sole: $\alpha_i := \zeta^i \alpha$ con $i = 0, \dots, 4$ e quindi $E \subset M \cdot L$. Ma $\zeta = \alpha_1/\alpha \in E$ e quindi $M \cdot L \subset E$. Abbiamo $[M : \mathbb{Q}] = 5$ in quanto α ha come plinomio minimo $f(X)$ che è irriducibile per Esisnsetin per $p = 2$. Inoltre L ha grado $\phi(5) = 4$ su $\mathbb{Q}$ essendo il 5^o campo ciclotomico. L'intersezione $M \cap L$ ha grado su $\mathbb{Q}$ che divide sia 4 che 5 per moltiplciatività dei gradi. Quindi $M \cap L = \mathbb{Q}$. Siccome $\mathbb{Q} \subset L$ è di Galois, sappiamo che $[E : \mathbb{Q}] = 5 \cdot 4 = 20$.Per il lemma di moltiplicazione dei gradi abbiamo anche che $\mathcal{Q} := \{\zeta^i \alpha^j | i = 0, \dots, 3, j = 0, \dots, 4\}$ è un $\mathbb{Q}$-base di E.

2)-3) Sia $N = \mathrm{Gal}(E/L)$. Essendo $\mathbb{Q} \subset L$ di Galois, si tratta di un sottogruppo normale di G. Consideriamo l'applicazione

$$N \to \mu_5 \cong \mathbb{Z}/5\mathbb{Z},$$

dove la prima applicazione invia $\sigma \mapsto \sigma(\alpha)/\alpha$ è un omomorfismo iniettivo di gruppi e quindi un isomorfismo per questioni di cardinalità. Quindi N è ciclico di ordine 5 con generatore l'automorfismo σ che fissa ζ e invia $\alpha \mapsto \zeta\alpha$.

Sia $H = \mathrm{Gal}(E/M)$. Consideriamo l'applicazione

$$H \subset G \to G/N = \mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Aut}(\mu_5) \cong \left(\mathbb{Z}/5\mathbb{Z}\right)^* \cong \mathbb{Z}/4\mathbb{Z},$$

dove la freccia $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Aut}(\mu_5)$ invia $\tau \mapsto \tau(\zeta)$. È un omomorfismo initettivo di gruppi e per questioni di cardinalità è un isomorfismo. Quindi H è ciclico di ordine 4 con generatore l'automorfismo τ che fissa α e invia $\zeta \mapsto \zeta^2$ vsto che 2 genera il gruppo moltiplicativo $(\mathbb{Z}/5\mathbb{Z})^*$.

Osserviamo che $H \cap N = \{1\}$. Segue allora che G è prodotto semidiretto di N ed H. In particolare l'applicazione $N \times H \to G$, che invia $(n, h) \mapsto n \circ h$, è biettiva ed ogni elemento di g si scrive allora come $\sigma^i \circ \tau^j$ per unici $0 \leq i \leq 4$ e $0 \leq j \leq 3$. Inoltre $(\sigma^i \circ \tau^j) \circ (\sigma^a \circ \tau^b) = \sigma^i \circ (\tau^j \sigma^a \tau^{-j}) \tau^{b+j}$ e $\tau^j \sigma^a \tau^{-j}$ è l'automorfismo che invia $\zeta \mapsto \zeta$ e $\alpha \mapsto \tau^j \sigma^a \tau^{-j}(\alpha) = \tau^j(\zeta^a \alpha) = \zeta^{2^j a}\alpha$ ovvero $\tau^j \sigma^a \tau^{-j} = \sigma^{2^j a}$.

4) Per il Teorema Fondamentale della Teoria di Galois tali sottocampi sono in corrispondenza biunivoca con i sottogruppi di G di ordine 2. Questi sono in corrispondenza biunivoca con gli eleemnti di G di ordine 2, ovvero elementi $g = (\sigma^i \circ \tau^j)$ tali che $g^2 = 1$. Ma $g^2 = \sigma^{i(2^j+1)} \circ \tau^{2j}$ è banale se e solo se $2j = 0$ e $i(2^j + 1) = 0$. Se $j = 0$ allora $2i = 0$ che modulo 5 significa $i = 0$. Dobbiamo quindi avere $j = 2$ ed allora i è arbitrario. Ho quindi 5 sottogruppi che corrispondono a 5 estensioni di $\mathbb{Q}$ di grado 10.

Osservo inoltre che $\sigma^i \tau^2 \sigma^{-i} = \sigma^{(1-4)i} \tau^2 = \sigma^{-3i} \tau^2$, ovevro tutti gli eleemnti di ordine 2 sono della forma $\sigma^i \tau^2 \sigma^{-i}$.

Siccome L^{τ^2} è il sottocampo reale di L ovvero $\mathbb{Q}(\sqrt{5})$ (per al teoria dei campi ciclotomici, ad es. il Cor. 3.11 delle Note di teoria dei Numeri) ho che $E^{\tau^2} = \mathbb{Q}(\alpha, \sqrt{5})$. Per il teorema

fondamentale della teoria dei Galois gli altri sottocampi cercati, corrispondenti agli invarianti ripetto al sottogruppo generato da $\sigma^i\tau^2\sigma^{-i}$, sono $\sigma^i(E^{\tau^2}) = \mathbb{Q}(\zeta^i\alpha, \sqrt{5})$.

Esercizio 2. [*Esonero*] Sia K il 36^o-campo ciclotomico

(1) Si calcoli il gardo $[K : \mathbb{Q}]$ e si mostri che $\mathbb{Q} \subset K$ è di Galois.
(2) Si determini il gruppo di Galois $\mathrm{Gal}(K/\mathbb{Q})$. Si dica se è ciclico.
(3) Si determini il numero di sottocampi $\mathbb{Q} \subset L \subset K$ e dei generatori, di grado 2 su $\mathbb{Q}$.

Soluzione: (1)-(2) Osservo che K è il campo di spezzamento del polinomio $X^{36}-1$. Essendo $\mathbb{Q}$ un campo di caratteristica 0, è un campo perfetto e quindi $X^{36}-1$ è un polinomio separabile. Segue che $\mathbb{Q} \subset K$ è di Galois. Il grado su $\mathbb{Q}$ è $\varphi(36) = \varphi(4)\varphi(9) = 12$. Essendo K un campo ciclotomico, il gruppo di Galois

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Aut}(\mu_{36}) \cong \left(\mathbb{Z}/36\mathbb{Z}\right)^* \cong \left(\mathbb{Z}/4\mathbb{Z}\right)^* \times \left(\mathbb{Z}/9\mathbb{Z}\right)^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$$

In particolare non si tratta di un gruppo ciclico: non esistono elementi di ordine 12, in quato ogni elemento α soddisfa $6\alpha = 0$.

(3) I campi cercati sono in corrispondenza biunivoca con i sottogruppi di G di ordine 6. Ciascuno di questi deve quindi contenere un 3-Sylow che è il 3-Sylow di G. I sottogruppi cercati sono quindi in corrispondenza biunivoca con i sottogruppi di ordine 2 del quoziente di G per il 3-Sylow, quoziente isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$. Ho quindi 3-sottogruppi.

I tre sottocampi cercati sono le estenssioni quadratiche contenute nel sottocampo di K fissato dal 3-Sylow. Questo è una estensione di grado 4 di $\mathbb{Q}$ e deve quindi coincidere con $\mathbb{Q}(i, \sqrt{-3})$: osservo infatti che le radici primitive $i = \sqrt{-1}$ (di ordine 4) e $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ (di ordine 3) sono in K. Concludo che i tre sottocampi cercati so $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$ e $\mathbb{Q}(\sqrt{3})$.

Esercizio 3. [*TeoGal*] Sia K un campo e sia n un intero positivo. Si mostri che esiste una estensione $K \subset L$ di grado n nei seguenti casi:

(1) $K = \mathbb{Q}$;
(2) $K = \mathbb{Q}(i)$;
(3) K un campo finito.

Soluzione: (1) Considero il polinomio X^n-2. È irriducibile su $\mathbb{Q}$ per Eisenstein per il primo $p = 2$. Allora $L = \mathbb{Q}[X]/(X^n - 2)$ è un campo, di grado n su $\mathbb{Q}$ in quanto $\{1, \ldots, X^{n-1}\}$ è una $\mathbb{Q}$-base di L.

2) Sia α una radice reale di $X^n - 2$. Allora l'applicazione $\psi_\alpha \colon \mathbb{Q}[x] \to \mathbb{Q}(\alpha)$ di valutazione in α induce un isomorfismo $L \cong \mathbb{Q}(\alpha)$ di estensioni di $\mathbb{Q}$ che hanno quindi grado n su $\mathbb{Q}$ per il punto (1). Sia $M = \mathbb{Q}(i, \alpha)$ il campo composto di $\mathbb{Q}(\alpha)$ e $\mathbb{Q}(i)$. Siccome $\mathbb{Q}(\alpha) \cap \mathbb{Q}(i) = \mathbb{Q}$, in quanto $i \in \mathbb{C}\backslash\mathbb{R}$, e $\mathbb{Q} \subset \mathbb{Q}(i)$ è di Galois, allora $[M : \mathbb{Q}] = 2n$ e $[M : \mathbb{Q}(i)] = n$. Quindi $X^n - 2$ è il polinomio minimo di α anche su $\mathbb{Q}(i)$ e, in particolare, è un polinomio irriducibile in $\mathbb{Q}(i)[X]$.

3) Essendo finito necessariamente K ha caratteristica positiva p. Sia $[K : \mathbb{F}_p] = h$. Sia L è campo di spezzamento di $X^q - X \in K[X]$. con $q = p^{nh}$. Siccome $X^q - X$ ha polinomio derivato -1, esso ha tutte radici distinte in L e quindi $|L| \geq q$. Sia S =radici di $X^q - X$ in L. È un insieme di cardinalit à q, chiuso rispetto a $+$, $\cdot$, $-$, inverso (di elementi non nulli) e contiene 0 e 1. Quindi è un sottocampo di L e per minimalità è uguale ad L. Segue quindi che $|L| = q$ e quindi $[L : K] = n$.

Il gruppo moltiplicativo L^* è ciclico di ordine $q-1$. Sia α un generatore. Allora $L = K(\alpha)$ e il polinomio minimo di α su K ha grado $[L : K] = n$

Esercizio 4. Sia $K = \mathbb{Q}(\alpha)$ con α radice del polinomio $f(X) = X^3 + X + 1$.

(1) Calcolare $\mathcal{O}_K$.
(2) Calcolare $disc(\mathcal{O}_K)$.
(3) Calcolare la decomposizione di $p\mathcal{O}_K$ con $p = 2, 3, 5$ e, per ogni primo $\mathfrak{p}$ che compare nella decomposizione, si calcoli il campo residuo $\mathbb{F}(\mathfrak{p}) := \frac{\mathcal{O}_K}{\mathfrak{p}}$.

Soluzione: Notiamo per cominciare che $f(X) \in \mathbb{Q}[X]$ è irriducibile per il lemma di Gauss, essendolo in $\mathbb{Z}[X]$ poichè la sua riduzione modulo 2 non ammette radici. Consideriamo la $\mathbb{Q}$-base $\mathcal{B}_\alpha = \{1, \alpha, \alpha^2\}$ e calcoliamo

$$\begin{aligned} disc(\mathcal{B}_\alpha) &= (-1)^{\frac{3\cdot 2}{2}} N_{K/\mathbb{Q}}\left(f'(\alpha)\right) = -N_{K/\mathbb{Q}}\left(f'(\alpha)\right) \\ &= -N_{K/\mathbb{Q}}\left(3\alpha^2+1\right) = -(-1)^3 \cdot c_0\left(f^{\text{char}}_{3\alpha^2+1,K/\mathbb{Q}}\right) \\ &= c_0\left(f^{\text{char}}_{3\alpha^2+1,K/\mathbb{Q}}\right), \end{aligned}$$

con $c_0\left(f^{\text{char}}_{3\alpha^2+1,K/\mathbb{Q}}\right)$ il termine costante del polinomio caratteristico di $3\alpha^2+1$. Abbiamo

$$\begin{aligned} &\left(3\alpha^2+1\right)\cdot 1 = 3\alpha^2+1, \\ &\left(3\alpha^2+1\right)\cdot \alpha = 3\alpha^3+\alpha = -3(\alpha+1)+\alpha = -2\alpha-3 \\ &\left(3\alpha^2+1\right)\cdot \alpha^2 = 3\alpha^4+\alpha^2 = -3\alpha(\alpha+1)+\alpha^2 \\ &\quad = -2\alpha^2-3\alpha. \end{aligned}$$

Dunque vediamo che la matrice della moltiplicazione per $3\alpha^2+1$ rispetto alla $\mathbb{Q}$-base $\mathcal{B}_\alpha = \{1, \alpha, \alpha^2\}$ è

$$M_{3\alpha^2+1} = \begin{bmatrix} 1 & -3 & 0 \\ 0 & -2 & -3 \\ 3 & 0 & -2 \end{bmatrix} \Rightarrow c_0\left(f^{\text{char}}_{3\alpha^2+1,K/\mathbb{Q}}\right) = (-1)^3 \det\left(M_{3\alpha^2+1}\right) = -31.$$

Segue che $disc(\mathcal{B}_\alpha) = -31$. Notiamo che vale la formula

$$-31 = disc(\mathcal{B}_\alpha) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2\, disc(\mathcal{O}_K),$$

da cui deduciamo che, essendo 31 primo, abbiamo $\mathcal{O}_K = \mathbb{Z}[\alpha]$ e $disc(\mathcal{O}_K) = disc(\mathcal{B}_\alpha) = -31$.

Notiamo che f è il polinomio minimo di α e, poichè $\mathcal{O}_K = \mathbb{Z}[\alpha]$, possiamo utilizzare la decomposizione del polinomio minimo di α in $\mathbb{F}_p[X]$ per capire come si decompone p e come è fatto il campo residuo.

Decomposizione di $2\mathcal{O}_K$.

Abbiamo la decomposizione

$$X^3+X+1 \text{ in } \mathbb{F}_2[X],$$

(come già notato f non ha radici modulo 2) da cui vediamo che $2\mathcal{O}_K$ è primo ed il campo residuo è $\frac{\mathbb{F}_2[X]}{(X^3+X+1)} \simeq \mathbb{F}_{2^3}$.

Decomposizione di $3\mathcal{O}_K$.

Abbiamo la decomposizione

$$X^3+X+1 = (X-1)\left(X^2+X+2\right) \text{ in } \mathbb{F}_3[X],$$

(infatti X^2+X+2 è irriducibile non avendo radici) da cui vediamo che la decomposizione di $3\mathcal{O}_K$ è

$$3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \text{ con } \mathfrak{p}_1 = \mathcal{O}_K 3 + \mathcal{O}_K(\alpha-1),\ \mathfrak{p}_2 = \mathcal{O}_K 3 + \mathcal{O}_K\left(\alpha^2+\alpha+2\right)$$

ed abbiamo $\mathbb{F}(\mathfrak{p}_1) \simeq \frac{\mathbb{F}_3[X]}{(X-1)} \simeq \mathbb{F}_3$ ed $\mathbb{F}(\mathfrak{p}_2) \simeq \frac{\mathbb{F}_3[X]}{(X^2+X+2)} \simeq \mathbb{F}_{3^2}$.

Decomposizione di $5\mathcal{O}_K$.

Abbiamo la decomposizione

$$X^3+X+1 \text{ in } \mathbb{F}_5[X],$$

(infatti X^3+X+1 non ha radici in $\mathbb{F}_5$) da cui vediamo che $5\mathcal{O}_K$ è primo ed il campo residuo è $\frac{\mathbb{F}_5[X]}{(X^3+X+1)} \simeq \mathbb{F}_{5^3}$.

Esercizio 5. Sia R un dominio di Dedekind.

(1) Si enuncino i due principali risultati della teoria degli ideali dei Dedekind, ricordando le definizioni che intervengono negli enunciati.
(2) Si mostrino tali risultati nel caso in cui R sia un PID.

Soluzione: Primo teorema.

Teorema. Ogni ideale frazionario I in un dominio di Dedekind R, ovvero ogni R-sottomodulo $0 \neq I \subset Frac(R)$ tale che $Ix \subset R$ per qualche $0 \neq x \in K$, è invertibile, ovvero take che esiste un R-sottomodulo $0 \neq J \subset Frac(R)$ tale che $IJ = R$.

Dimostrazione per i PID

Poiché $Ix \subset R$ è un ideale non nullo e R è PID, esiste $y \in R$ tale che $Ix = Ry$, dunque $I = Rz$ con $z = y/x$ e $J = z^{-1}$ è tale che $IJ = R$. □

Secondo teorema.

Teorema. Ogni ideale frazionario I in un dominio di Dedekind R ammette una decomposizione unica in ideali primi non nulli (con esponenti eventualmente negativi).

Dimostrazione per i PID

Come notato nella dimostrazione precedente si ha $I = Rz$ per qualche $z \in Frac(R)$ e, poiché R è un PID e dunque un UFD, possiamo scrivere $z = u\pi_1^{e_1}...\pi_r^{e_r}$ in modo unico a meno di elementi invertibili, con $u \in R^\times$, $\pi_i \in R$ è irriducibile ed $e_i \in \mathbb{Z}$ per $i = 1, ..., r$. Ma allora $I = Rz = R\pi_1^{e_1}...R\pi_r^{e_r}$ e si ha che $R\pi_i$ è un ideale primo non nullo essendo generato da un elemento irriducibile ed essendo R un UFD. Sia $I = Rz = \mathfrak{p}_1^{f_1}...\mathfrak{p}_s^{f_s}$ è un'altra decomposizione in ideali primi non nulli. Essendo R un PID avremo $\mathfrak{p}_i = R\varpi_i$ per qualche elemento irriducibile $\varpi_i \in R$ (è sempre vero che se un ideale primo in un dominio è principale, allora ogni sui generatore è irriducibile). Ma allora vediamo che $z = v\varpi_1^{f_1}...\varpi_s^{f_s}$, con $v \in R^\times$, $\varpi_i \in R$ è irriducibile ed $f_i \in \mathbb{Z}$ per $i = 1, ..., s$. Per l'unicità della decomposizione di z a meno di elementi invertibili, si avrà $r = s$, $e_i = f_i$ e $\pi_i = t_i\varpi$ per qualche $t_i \in R^\times$. Dunque $r = s$, $e_i = f_i$ ed $R\pi_i = R\varpi_i = \mathfrak{p}_i$. □