SOLUZIONI DEL COMPITINO DEL 01/02/2019

Esercizio 1. Si consideri il polinomio $f(X) = X^{11} - 5 \in \mathbb{Q}[X]$ 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 $\mathbb{Q}$. Mostrare che G è un prodotto semidiretto, ma non diretto di gruppi abeliani. Determinare un numero minimo di generatori di G ed esibire dei generatori.
(3) Descrivere gli elementi di G e la legge di gruppo, utilizzando i generatori dati.
(4) Determinare il numero ed esibire dei generatori delle estensioni $\mathbb{Q} \subset M \subset E$ di grado 11 su $\mathbb{Q}$.

Soluzione: 1) Sia α una radice reale di $f(X)$ e sia ζ una radice primitiva dell'unità di ordine 11. 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 $i = 0, \dots, 10$ e quindi $E \subset M \cdot K$. Ma $\zeta = \alpha_1/\alpha \in E$ e quindi $M \cdot L \subset E$. Abbiamo $[M : \mathbb{Q}] = 11$ in quanto α ha come plinomio minimo $f(X)$ che è irriducibile per Esisnsetin per $p = 5$. Inoltre L ha grado $\phi(11) = 10$ su $\mathbb{Q}$ essendo l'11 campo ciclotomico. L'intersezione $M \cap L$ ha grado su $\mathbb{Q}$ che divide sia 10 che 11 per moltiplciatività dei gradi. Quindi $M \cap L = \mathbb{Q}$. Siccome $\mathbb{Q} \subset L$ è di Galois, sappiamo che $[E : \mathbb{Q}] = 11 \cdot 10 = 110$.Per il lemma di moltiplicazione dei gradi abbiamo anche che $\mathcal{Q} := \{\zeta^i \alpha^j | i = 0, \dots, 9, j = 0, \dots, 10\}$ 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

$$N \to \mu_{11} \cong \mathbb{Z}/11\mathbb{Z},$$

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 11 con generatore l'automorfismo σ che fissa ζ e invia $\alpha \mapsto \zeta\alpha$.

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

$$H \subset G \to G/N = \mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Aut}(\mu_{11}) \cong \left(\mathbb{Z}/11\mathbb{Z}\right)^* \cong \mathbb{Z}/10\mathbb{Z},$$

dove la freccia $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Aut}(\mu_{11})$ 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 10 con generatore l'automorfismo τ che fissa α e invia $\zeta \mapsto \zeta^2$ vsto che 2 genera il gruppo moltiplicativo $(\mathbb{Z}/11\mathbb{Z})^*$.

Osserviamo che $H \cap N = \{1\}$. Segue allora che G è prodotto semidiretto di N ed H. Non è prodotto diretto perchè altrimenti sarebbe abeliano ed ogni sottocampo di E sarebbe di Galois su $\mathbb{Q}$; questo non è vero considerando as esempio il sottocampo M.

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 $0 \leq i \leq 10$ e $0 \leq j \leq 9$. Inoltre $(\sigma^i \circ \tau^j) \circ (\sigma^a \circ \tau^b) = \sigma^i \circ (\tau^j \sigma^a \tau^{-j}) \tau^{b+j}$ and $\tau^j \sigma^a \tau^{-j}$ 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 10. Certamente ho H e i suoi coniugati per gli elementi di G, ovvero per gli elementi di N. lI sottogruppo $\sigma^i H \sigma^{-i}$, per $i = 0, \dots, 10$, corrisponde per il teorema Fondamentale della teoria di Galois al sottocampo $\mathbb{Q}(\sigma^i(\alpha)) = \mathbb{Q}(\zeta^i \alpha)$ e utilizando la $\mathbb{Q}$-base di E vediamo che questi 11 sottocampi sono distinti fra loro. Osservo

inoltre che $\sigma^i H\sigma^{-i}$ è ciclico di ordine 10 con generatore $\sigma^i\tau\sigma^{-i}$ che per i calcoli precedenti coincide con $\sigma^{-i}\tau$. Per concludere basta mostrare che questi sono tutti e soli i sottogruppi di ordine 10 di G. Sia H' un tale sottogruppo; siccome $H' \cap N = \{0\}$ per rgioni di odine, l'applicazione composta $H' \subset G \to G/N$ è un omomorfismo iniettivo e, quindi, un isomorfismo, ovvero H' è ciclico di ordine 10 e, usando la scrittura di $G = \{\sigma^i \circ \tau^j | 0 \leq i \leq 10, 0 \leq j \leq 9\}$, ho che H' è generato da un elemento della forma $\sigma^j\tau$ per un qualche j. Ma allora $H' = \sigma^{-j} H \sigma^j$.

Esercizio 2. [*Esonero*] Sia K il 24^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 $\mathrm{Gal}(K/\mathbb{Q})$.
(3) Si determini il numero di sottocampi $\mathbb{Q} \subset L \subset K$, di grado 4 su $\mathbb{Q}$.
(4) Si esibiscano, senza dimostrazione, dei generatori dei sottocampi $\mathbb{Q} \subset L \subset K$, di grado 4 su $\mathbb{Q}$.

Soluzione: (1)-(2) Osservo che K è il campo di spezzamento del polinomio $X^{24}-1$. Essendo $\mathbb{Q}$ un campo di caratteristica 0, è un campo perfetto e quindi $X^{24}-1$ è un polinomio separabile. Segue che $\mathbb{Q} \subset K$ è di Galois. Il grado su $\mathbb{Q}$ è $\varphi(24) = \varphi(3)\varphi(8) = 8$. Essendo K un campo ciclotomico, il gruppo di Galois

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Aut}(\mu_{24}) \cong \big(\mathbb{Z}/24\mathbb{Z}\big)^* \cong \big(\mathbb{Z}/3\mathbb{Z}\big)^* \times \big(\mathbb{Z}/8\mathbb{Z}\big)^* \cong (\mathbb{Z}/2\mathbb{Z})^3$$

(3) I campi cercati sono in corrispondenza biunivoca con i sottogruppi di G di ordine 2 ovvero con gli elementi non nulli di G (ciascuno di questi ha ordine 2!), ovvero con gli elementi non nulli di $(\mathbb{Z}/2\mathbb{Z})^3$ e ne ho $2^3 - 1 = 7$.

(4) Osservo che K è il campo composto dell' 8 campo ciclotomico $E := \mathbb{Q}(i, \sqrt{2})$ (essendo $\zeta_8 := \frac{1+i}{\sqrt{2}} \in E$ una radice primitiva dell'unit à di ordine 8) e del 3 campo ciclotomico $F := \mathbb{Q}(\sqrt{-3})$ (essendo $\zeta_3 - \frac{1}{2} + \frac{\sqrt{-3}}{2}$ radice primitiva terza dell'unità). Infatti $\zeta_3\zeta_8$ è radice primitiva di ordine 24 dell'unità e $E \subset K$ e $F \subset K$. Il gruppo G è isomorfo a

$$G \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3,$$

dove la prima mappa su ciascuna componente è definita per restrizione. Dato $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3$ il sottocampo corrispondente a tale elemento, vedendo $a, b, c \in \{0, 1\}$, è

$$\mathbb{Q}\big(\sqrt{-3}^{1-a}, i^{1-b}, \sqrt{2}^{1-c}, (\sqrt{-3}i)^{ab}, (\sqrt{-3}\sqrt{2})^{ac}, (i\sqrt{2})^{bc}\big).$$

Esercizio 3. [*TeoGal*] Sia K un campo finito e sia n un intero positivo.

(1) Si mostri che ogni estensione di grado n di K è di Galois con gruppo ciclico.
(2) Si dimostri che due estensioni di grado n di K sono isomorfe.
(3) Si mostri che esiste una estensione $K \subset L$ di grado n.

Soluzione: (1) Necessariamente K ha caratteristica positiva p. Sia $[K : \mathbb{F}_p] = h$. Data una estensione di grado n di K ho che $|L| = q = p^{nh}$. In particolare L^* è un gruppo moltiplicativo, ciclico, di ordine $q-1$. Segue che L è il campo di spezzamento di $X^q - X \in \mathbb{F}_p[X]$. In particolare $\mathbb{F}_p \subset L$ è una estensione di Galois e quindi anche $K \subset L$ è di Galois. Sia $\varphi\colon L \to L$, $z \mapsto z^p$, l'automorfismo di Frobenius. Siccome $L^{\varphi=1} = \mathbb{F}_p$, segue dal Teorema Fondamentale della Teoria di Galois che φ genera il gruppo $G := \mathrm{Gal}(L/\mathbb{F}_p)$ che quindi risulta essere ciclico di ordine nh. Il sottogruppo $H = \mathrm{Gal}(L/K) \subset G$ è anch'esso ciclico di ordine n. Quindi H è generato da φ^h.

(2) L è campo di spezzamento di $X^q - X \in K[X]$. Essendo due campi di spezzamento di uno stesso polinomio isomorfi per la Proposizione 2.7, il punto (2) segue.

(3) 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. E' 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 $[L : K] = n$.

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

(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: (1-2) Notiamo per cominiare che $f(X)$ è irriducibile in $\mathbb{Q}[X]$ per il criterio di Eisenstein. Consideriamo la $\mathbb{Q}$-base $\mathcal{B}_\alpha = \{1, \alpha, \alpha^2\}$ e calcoliamo

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

Notiamo che $\beta := 3\alpha^2$ genera una estensione di grado 3, altrimenti per la moltiplicatività dei gradi avremmo che $\mathbb{Q}(\beta) = \mathbb{Q}$, ma allora α soddisferebbe il polinomio monico $3X^2 - 3\alpha \in \mathbb{Q}[X]$ di grado due, che non è possibile. Dunque $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, da cui $f^{\text{char}}_{3\alpha^2,K/\mathbb{Q}} = f^{\min}_{3\alpha^2,\mathbb{Q}}$ e $disc(\mathcal{B}_\alpha) = c_0\left(f^{\min}_{3\alpha^2,\mathbb{Q}}\right)$ con $f^{\min}_{\beta,\mathbb{Q}} = f^{\min}_{3\alpha^2,\mathbb{Q}}$ di grado 3. Abbiamo

$$\begin{aligned} \beta^2 &= 9\alpha^4 = 9 \cdot 3\alpha = 27\alpha, \\ \beta^3 &= \beta\beta^2 = 3\alpha^2 \cdot 27\alpha = 27 \cdot 3 \cdot 3 = 243 \end{aligned}$$

e deduciamo che

$$f^{\min}_{\beta,\mathbb{Q}} = f^{\min}_{3\alpha^2,\mathbb{Q}} = X^3 - 243$$

e

$$disc(\mathcal{B}_\alpha) = c_0\left(f^{\min}_{3\alpha^2-1,\mathbb{Q}}\right) = -243 = 3^5.$$

[Alternativamente, utilizzando la moltiplicatività della norma, notiamo che $N_{K/\mathbb{Q}}\left(3\alpha^2\right) = 3^3 N_{K/\mathbb{Q}}(\alpha)^2$ e $N_{K/\mathbb{Q}}(\alpha) = -c_0\left(f^{\text{char}}_{\alpha,K/\mathbb{Q}}\right)$; essendo $f^{\text{char}}_{\alpha,K/\mathbb{Q}} = f$, deduciamo che $N_{K/\mathbb{Q}}(\alpha) = 3$ e dunque $disc(\mathcal{B}_\alpha) = -N_{K/\mathbb{Q}}\left(3\alpha^2\right) = 3^3 N_{K/\mathbb{Q}}(\alpha)^2 = -3^5$.]

Deduciamo dalla formula

$$-3^5 = -243 = disc(\mathcal{B}_\alpha) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \, disc(\mathcal{O}_K)$$

che 3 è il solo primo che può dividere $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Ma poiché $f^{\min}_{\alpha^2,\mathbb{Q}} = f \in \mathbb{Z}[X]$ è di Eisenstein in 3, sappiamo dalla teoria che ciò non è possibile. Dunque $\mathcal{O}_K = \mathbb{Z}[\alpha]$ e $disc(\mathcal{O}_K) = -243$.

(3) Notiamo che $f = X^3 - 3$ 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

$$X^3 - 3 = X^3 - 1 = (X - 1)\left(X^2 + X + 1\right) \text{ in } \mathbb{F}_2[X],$$

da cui vediamo che la decomposizione di $2\mathcal{O}_K$ è

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

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

Decomposizione di $3\mathcal{O}_K$.
Abbiamo la decomposizione

$$X^3 - 3 = X^3 \text{ in } \mathbb{F}_3[X],$$

da cui vediamo che la decomposizione di $3\mathcal{O}_K$ è

$$3\mathcal{O}_K = \mathfrak{p}^3 \text{ con } \mathfrak{p} = \mathcal{O}_K 3 + \mathcal{O}_K \sqrt[3]{3} = \mathcal{O}_K \sqrt[3]{3}$$

ed $\mathbb{F}(\mathfrak{p}) \simeq \frac{\mathbb{F}_3[X]}{(X)} \simeq \mathbb{F}_3$.
Decomposizione di $5\mathcal{O}_K$.
Abbiamo la decomposizione

$$X^3 - 3 = (X-2)\left(X^2 + 3X + 4\right) \text{ in } \mathbb{F}_5[X],$$

(infatti $X^2 + 3X + 4$ non ha radici in $\mathbb{F}_5$) da cui vediamo che la decomposizione di $3\mathcal{O}_K$ è

$$3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \text{ con } \mathfrak{p}_1 = \mathcal{O}_K 5 + \mathcal{O}_K\left(\sqrt[3]{3} - 2\right),\ \mathfrak{p}_2 = \mathcal{O}_K 5 + \mathcal{O}_K\left(3^{\frac{2}{3}} + 3 \cdot 3^{\frac{1}{3}} + 4\right)$$

ed abbiamo $\mathbb{F}(\mathfrak{p}_1) \simeq \frac{\mathbb{F}_5[X]}{(X-2)} \simeq \mathbb{F}_5$ ed $\mathbb{F}(\mathfrak{p}_2) \simeq \frac{\mathbb{F}_5[X]}{(X^2+3X+4)} \simeq \mathbb{F}_{5^2}$.

Esercizio 5. Svolgere i seguenti punti.

(1) Si mostri che se R è un anello commutativo unitario sono equivalenti le seguenti affermazioni.
   (*i*) Ogni ideale di R è finitamente generato.
   (*ii*) Ogni successione crescente di ideali

$$I_1 \subset I_2 \subset ... \subset I_n \subset I_{n+1} \subset ...$$

   è definitivamente costante.
   (*iii*) Ogni insieme non vuoto $\mathcal{S}$ di ideali ammette un elemento massmale.
(2) Si ricordi la definizione di dominio di Dedekind, esplicitando il significato di tutti i termini che entrano nella definizione.
(3) Si mostri che, se R è doinio di Dedekind, si ha che R è PID se e solo se R e UFD.

Soluzione: (1) Ragioniamo in circolo.
$(i) \Rightarrow (ii)$ Posto $I = \bigcup_n I_n$, l'ideale I è finitamente generato, diciamo $I = \sum_{i=1}^r Rx_i$. Poiché $x_i \in I_{n_i}$ per qualche i, esiste un intero N tale che $x_i \in I_N$ per $i = 1, ..., r$. Ma allora

$$I = \sum\nolimits_{i=1}^r Rx_i \subset I_N,$$

ovvero $I = I_N$ e la successione di ideali è costante.
$(ii) \Rightarrow (iii)$ Dato un ideale I, indichiamo con $\mathcal{S}_I$ l'insieme degli ideali di R in $\mathcal{S}$ che contengono I propriamente: dire che $I \in \mathcal{S}$ è massimale equivale a dire che $\mathcal{S}_I = \phi$. Supponiamo per assurdo che $\mathcal{S}$ non ammetta elementi massimali, ovvero $\mathcal{S}_I \neq \phi$ per ogni $I \in \mathcal{S}$. Sia $I_1 \in \mathcal{S}$, che esiste essendo $\mathcal{S} \neq \phi$. Poiché $\mathcal{S}_{I_1} \neq \phi$, esiste $I_2 \in \mathcal{S}$ tale che $I_1 \subsetneq I_2$, poichè $\mathcal{S}_{I_2} \neq \phi$, esiste $I_3 \in \mathcal{S}$ tale che $I_1 \subsetneq I_2 \subsetneq I_3$ ed itrando tale ragionamento costruiamo una successione infinita di ideali propriamente crescente, che non è possibile per l'ipotesi (ii).
$(iii) \Rightarrow (i)$ Dato l'ideale I sia $\mathcal{S}$ l'insieme degli ideali finitamente generati di R che sono contenuti in I e sia $J \in \mathcal{S}$ un ideale massimale, la cui esistenza è garantita da (iii). Se per assurdo si avesse $J \subsetneq I$, esisterebbe $x \in I - J$ e l'ideale $J + Rx \in \mathcal{S}$ conterrebbe propriamente J, contraddicendone la massimalità. Ma allora $I = J$ è finitamente generato.
(2) Si veda la Definizione 5.3 delle note.
(3) Vale sempre l'implicazione $PID \Rightarrow UFD$, mostriamo il viceversa. Poiché ogni ideale $I \neq 0$ di un dominio di Dedekind si decompone come prodotto di ideali massimali non nulli, basterà mostrare che ogni ideale massimale non nullo è generato da un singolo elemento per dedurre che I è generato da un singolo elemento. (Se infatti $I = JK$ è prodotto di ideali,

$J = Rj$ e $K = Rk$, si ha che $I = Rjk$). Sia dunque $0 \neq x \in \mathfrak{p}$ con $\mathfrak{p}$ massimale. Essendo R un UFD possiamo scrivere $x = u\pi_1^{e_1}...\pi_g^{e_g}$ dove $u \in R^\times$, $\pi_i \in R$ è irriducibile ed $e_i \in \mathbb{N}$ per $i = 1, ..., g$. Dunque $\pi_1^{e_1}...\pi_g^{e_g} = u^{-1}x \in \mathfrak{p}$ ed essendo $\mathfrak{p}$ primo si avrà $\pi_i \in \mathfrak{p}$ per qualche i. Ma allora $R\pi_i \subset \mathfrak{p}$ e, poichè R è UFD e π_i è irriducibile, genera un ideale primo non nullo, che è pertanto massimale. Deduciamo che $\mathfrak{p} = R\pi_i$.