SOLUZIONI DELL'ESAME SCRITTO DEL 22/01/2018

Esercizio 1. Si consideri il polinomio $f(X) = X^5 - 5 \in \mathbb{Q}[X]$ e sia E il 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 è un prodotto semidiretto, ma non diretto di gruppi abeliani.
(3) Determinare dei generatori di G e descrivere gli elementi di G utilizzando i generatori dati.
(4) Esibire le estensioni di $\mathbb{Q}$ contenute in $E \cap \mathbb{R}$. Per ciascuno esibirne dei generatori.

Soluzione: 1) Sia $\alpha = 5^{\frac{1}{5}}$ e ζ una radice primitiva quinta dell'unità. Allora $E = M \cdot N$ con $M = \mathbb{Q}(\alpha)$ e $K = \mathbb{Q}(\zeta)$. Infatti le radici si $f(X)$ sono $\alpha_i := \zeta^i \alpha$ con $i = 0, \dots, 4$. Quindi $E \subset M \cdot K$. Ma $\zeta = \alpha_1/\alpha \in E$ e quindi $M \cdot K \subset E$. Abbiamo $[M : \mathbb{Q}] = 5$ in quanto α ha come plinomio minimo $X^5 - 5$ che è irriducibile per Esisnsetin per $p = 5$. Inoltre K ha grado $\phi(5) = 4$ su $\mathbb{Q}$ essendo il 5 campo ciclotomico. L'intersezione $M \cap K$ ha grado su $\mathbb{Q}$ che divide sia 4 che 5 per moltiplciatività dei gradi. Quindi $M \cap K = \mathbb{Q}$. Siccome $\mathbb{Q} \subset K$ è di Galois, sappiamo che $[E : \mathbb{Q}] = 4 \cdot 5 = 20$.

2)-3) Sia $N = \mathrm{Gal}(E/K)$. Essendo $\mathbb{Q} \subset K$ 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 freccia 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

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

dove la freccia $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Aut}(\mu_5)$ 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. 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 sottoampo N.

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 $0 \leq j \leq 3$.

4) L'intersezione $E \cap \mathbb{R}$ è il sottocampo di E definito dagli invarianti del coniugio complesso, che definisce un sottogruppo di ordine 2 di G. Quindi $E \cap \mathbb{R}$ ha grado 10 su $\mathbb{Q}$. Contiene M e $J = K \cap \mathbb{R} = \mathbb{Q}(\sqrt{5})$ (per la teoria dei campi ciclotomici essendo $5 \equiv 1 \bmod 4$). Siccome $J \cap M = \mathbb{Q}$, avendo grado su $\mathbb{Q}$ che divide 2 e 5 per moltiplicatità dei gradi e siccome $\mathbb{Q} \subset J$ è quadratica e quindi di Galois, segue che $[J : \mathbb{Q}] = [M : \mathbb{Q}][J : \mathbb{Q}] = 10$ e quindi $E \cap \mathbb{R} = J \cdot M = \mathbb{Q}(\alpha, \sqrt{5})$.

I sottocampi di $E \cap \mathbb{R}$ diversi da $E \cap \mathbb{R}$ e da $\mathbb{Q}$ hanno grado 2 o 5 su $\mathbb{Q}$ per moltiplicatività dei gradi. Per Sylow le estensioni di grado 5 in E sono associate ai sottogruppi $\sigma^i \circ H \circ \sigma^{-i}$ per $0 \leq i \leq 4$, cioè sono i sottocampi $\mathbb{Q}(\zeta^i\alpha)$. L'unico contenuto in $\mathbb{R}$ è M.

I sottocampi di grado 2 su $\mathbb{Q}$ sono associati a sottogruppi di cardinalità 10 di G. Ciascuno di questi contiene N, l'unico 5-Sylow di G. Quindi tali sottocampi sono contenuti in K. Concludo che l'unico sottocampo di grado 2 è J.

Esercizio 2. Si considerino i polinomi $f(X) = X^4 - X^3 + 2X^2 - X + 1 \in \mathbb{Q}[X]$ e $g(X) = X^3 - 2 \in \mathbb{Q}[X]$ ed i relativi campi di spezzamento $K/\mathbb{Q}$ ed $L/\mathbb{Q}$. Sia $E = K \cdot L$ il campo composto.

(1) Si mostri che $\mathbb{Q} \subset K$, $\mathbb{Q} \subset L$ e $\mathbb{Q} \subset E$ sono estensioni di Galois. Se ne calcoli il grado.
(2) Si descrivano i gruppi di Galois $\mathrm{Gal}(K/\mathbb{Q})$ e $\mathrm{Gal}(L/\mathbb{Q})$.
(3) Si calcoli $\mathrm{Gal}(E/\mathbb{Q})$.

Soluzione: I campi considerati sono campi di spezzamento di polinomi separabili in quanto $\mathbb{Q}$ è un campo perfetto. Quindi sono di Galois.

Osserviamo che $f(X) = (X^2 - X + 1)(X^2 + 1)$. Quindi K è il composto dei due campi quadratici $M = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ e di $N = \mathbb{Q}(\sqrt{-1})$. Osservo che $\sqrt{3} = \sqrt{-3}\sqrt{-1} \in K$ è un elemento di $\mathbb{R}$ ma non di $\mathbb{Q}$. Concludo allora che $M \cap N = \mathbb{Q}$. Altrimenti per questioni di gradi $M = N = K$ ma $N \cap \mathbb{R} = \mathbb{Q}$.

Essendo K il campo composto di due estensioni galoisiane, ovvero M ed N, di $\mathbb{Q}$ con intersezione $M \cap N = \mathbb{Q}$ ho $[K : \mathbb{Q}] = 4$. Inoltre il gruppo di Galois è isomorfo al prodotto

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(M/\mathbb{Q}) \times \mathrm{Gal}(N/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z});$$

il primo isomorfismo manda $\sigma \mapsto (\sigma|_M, \sigma|_N)$.

Il campo di spezzamento di $g(X)$ è $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ con $\alpha_1 = \alpha = 2^{\frac{1}{3}}$ e $\alpha_i = \zeta_3^{i-1}\alpha$. Quindi $L = M(\alpha)$. Infatti $\subset$ è chiaro mentre l'inclusione opposta segue dal fatto che $\zeta_3 = \alpha_2/\alpha_1$. Il campo $\mathbb{Q}(\alpha)$ ha grado 3 su $\mathbb{Q}$ perchè il polinomio $X^3 - 2$ è irriducibile per Eisensetin con $p = 2$. Quindi L ha grado 6 su $\mathbb{Q}$. L'applicazione

$$\rho\colon \mathrm{Gal}(L/\mathbb{Q}) \to S_3,$$

che invia $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ nella permutazione delle radici $\{\alpha_1, \alpha_2, \alpha_3\}$ di $g(X)$ data da $\alpha_i \mapsto \sigma(\alpha_i)$, è un omomorfismo iniettivo di gruppi e quindi è un isomorfismo perchè S_3 ha cardinalità 6.

L'intersezione $K \cap L$ contiene M e siccome il suo grado su $\mathbb{Q}$ deve dividere $[K : \mathbb{Q}] = 4$ e $[L : \mathbb{Q}] = 6$, concludo che $K \cap L = M$. Siccome E è il campo composto di due estensioni di Galois, concludo che $[E : \mathbb{Q}] = \frac{[K:\mathbb{Q}][L:\mathbb{Q}]}{[K\cap L:\mathbb{Q}]} = 12$. Posso scrivere E come il campo composto di N ed L e $N \cap L = \mathbb{Q}$. Allora l'applicazione

$$\mathrm{Gal}(E/\mathbb{Q}) \to \mathrm{Gal}(N/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$$

che invia $\sigma \mapsto (\sigma|_N, \sigma|_L)$ è un isomorfismo di gruppi. Quindi $\mathrm{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times S_3$.

Esercizio 3. [*TeoGal*] Sia n un intero. Sia $K \subset L$ un'estensione finita di campi di grado n. Supponiamo che K contenga le radici n-esime dell'unità.

(1) Dimostrare che se n è invertibile in K e se esiste $a \in K$ tale che L è campo di spezzamento del polinomio $X^n - a$, allora $K \subset L$ è di Galois, con gruppo di Galois ciclico di ordine n.
(2) Dimostrare che se K è un campo finito di caratteristica positiva $n = p$, allora $K \subset L$ è di Galois con gruppo di Galois ciclico di ordine p.
(3) Nelle ipotesi di (2) dimostrare che non esiste $a \in K$ tale che L è campo di spezzamento del polinomio $X^p - a$.

Soluzione: 1) Milne, Prop. 5.26.

(2) Sia $\varphi\colon L \to L$ l'automorfismo di Frobenius $x \mapsto x^p$. Se K è di cardinalità $q = p^n$, allora K coincide con gli elementi di L fissati da φ^n cioè con le radici di $X^q - X$. Quindi posto $\sigma = \varphi^n$ ho che $K = L^{\sigma=1}$. Segue che $K \subset L$ è di Galois (Milne, Teorema 3.10) con gruppo di Galois ciclico di ordine p generato da σ.

(3) Siccome l'omomorfismo di Frobenius $K \to K$, $x \mapsto x^p$, è un isomorfismo per ogni $a \in K$ il polinomio $X^p - a$ ammette una radice $\alpha \in K$. Quindi $X^p - a = (X - \alpha)^p$ e ilc ampo di spezzamento di $X^p - a$ risulta essere K stesso.

Esercizio 4. Si consideri il polinomio $f(X) = X^4 + X^2 - 6 \in \mathbb{Q}[X]$ e sia K il suo campo di spezzamento su $\mathbb{Q}$.

(1) Si calcoli $\mathcal{O}_K$ e $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$.
(2) Si calcoli la decomposizione di 5 in $\mathcal{O}_{K_i}$ per ogni sottoestensione quadratica $K_i \subset K$,
(3) Detta $5\mathcal{O}_K = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ la decomposizione di 5 in $\mathcal{O}_K$, si determini r, gli indici di ramificazione e_i e gli indici di inerzia f_i definiti dalla formula $\#\frac{\mathcal{O}_K}{\mathfrak{P}_i} = 5^{f_i}$.
(4)* Si esplicitino gli ideali $\mathfrak{P}_i$.

Soluzione: (1) Notiamo che

$$f(X) = \left(X^2 - 2\right)\left(X^2 + 3\right),$$

per cui $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{-3}\right)$. Dalla teoria delle estensioni quadratiche sappiamo che

$$\begin{aligned} \mathcal{O}_{\mathbb{Q}(\sqrt{2})} &= \mathbb{Z}\left[\sqrt{2}\right], \, disc\left(\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Z}\right) = 4 \cdot 2 = 8 \text{ poichè } 2 \equiv 2 \; mod(4), \\ \mathcal{O}_{\mathbb{Q}(\sqrt{-3})} &= \mathbb{Z}\left[\frac{\sqrt{-3}+1}{2}\right], \, disc\left(\mathbb{Q}\left(\sqrt{-3}\right)/\mathbb{Z}\right) = -3 \text{ poichè } -3 \equiv 1 \; mod(4). \end{aligned}$$

Si ha $\mathbb{Q}\left(\sqrt{2}\right) \cap \mathbb{Q}\left(\sqrt{-3}\right) = \mathbb{Q}$ (per esempio poichè $\mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{R}$ e $\sqrt{-3} \notin \mathbb{R}$), da cui $[K : \mathbb{Q}] = 4$. Ma allora

$$[K : \mathbb{Q}] = \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right]\left[\mathbb{Q}\left(\sqrt{-3}\right) : \mathbb{Q}\right]$$

e, poichè $\left(disc\left(\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Z}\right), disc\left(\mathbb{Q}\left(\sqrt{-3}\right)/\mathbb{Z}\right)\right) = 1$, sappiamo dalla teoria che

$$\begin{aligned} \mathcal{O}_K &= \mathcal{O}_{\mathbb{Q}(\sqrt{2})}\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\sqrt{2}, \frac{\sqrt{-3}+1}{2}, \frac{\sqrt{-6}+\sqrt{2}}{2}\right] \\ disc(\mathcal{O}_K/\mathbb{Z}) &= disc\left(\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Z}\right)^{\left[\mathbb{Q}(\sqrt{-3}):\mathbb{Q}\right]} disc\left(\mathbb{Q}\left(\sqrt{-3}\right)/\mathbb{Z}\right)^{\left[\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right]} \\ &= 8^2 \cdot (-3)^2 = 576. \end{aligned}$$

(2) Sappiamo dalla teoria di Galois che, poichè $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ e $\mathbb{Q}\left(\sqrt{-3}\right)/\mathbb{Q}$ sono di Galois e $\mathbb{Q}\left(\sqrt{2}\right) \cap \mathbb{Q}\left(\sqrt{-3}\right) = \mathbb{Q}$, abbiamo

$$G_{K/\mathbb{Q}} \xrightarrow{\sim} G_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} \times G_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}} \simeq \mathbb{F}_2 \times \mathbb{F}_2.$$

Per il teorema fondamentale della teoria di Galois, le sottoestensioni quadratiche di K sono in biiezione con i sottogruppi propri di $\mathbb{F}_2 \times \mathbb{F}_2$, che sono tre. Dunque le sottoestensioni quadratiche di K sono i seguenti campi, che si verificano facilmente essere a due a due distinti: $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}\left(\sqrt{-3}\right)$ e $\mathbb{Q}\left(\sqrt{-6}\right)$. Per calcolare la decomposizione di 5 in $\mathbb{Q}\left(\sqrt{2}\right)$, noto che $X^2 - 2$ è irriducibile in $\mathbb{F}_5[X]$, da cui $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}5 = \mathfrak{p}_5$. Posto $\alpha := \frac{\sqrt{-3}+1}{2}$, il polinomio minimo di α su $\mathbb{Q}$ è $X^2 - X + 1$ ed in oltre, poichè $-6 \equiv 2 \; mod(4)$, abbiamo $\mathcal{O}_{\mathbb{Q}(\sqrt{-6})} = \mathbb{Z}\left[\sqrt{-6}\right]$: poichè $X^2 - X + 1$ è irriducibile in $\mathbb{F}_5[X]$ mentre $X^2 + 6 = (X - 2)(X - 3)$ in $\mathbb{F}_5[X]$, abbiamo $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}5 = \mathfrak{p}_5'$ e $\mathcal{O}_{\mathbb{Q}(\sqrt{-6})}5 = \mathfrak{p}_5''\mathfrak{p}_5'''$ dove $\mathfrak{p}_5'' = \mathcal{O}_{\mathbb{Q}(\sqrt{-6})}5 + \mathcal{O}_{\mathbb{Q}(\sqrt{-6})}\left(\sqrt{-6} - 2\right)$ e $\mathfrak{p}_5''' = \mathcal{O}_{\mathbb{Q}(\sqrt{-6})}5 + \mathcal{O}_{\mathbb{Q}(\sqrt{-6})}\left(\sqrt{-3} - 2\right)$. Notiamo che allora $\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}}{\mathfrak{p}_5'} \simeq \mathbb{F}_{25}$.

(3 − 4) Abbiamo $\mathcal{O}_K 5 = \mathcal{O}_K \mathfrak{p}_5'$, per cui occorre studiare la decomposizione di $\mathfrak{p}_5' \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ in $\mathcal{O}_K$. Osserviamo che $\mathcal{O}_K = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}\left[\sqrt{2}\right]$ grazie al conto di $\mathcal{O}_K$ in (1). Inoltre, il polinomio

minimo di $\sqrt{2}$ su $\mathbb{Q}$ è ancora X^2-2, perchè altrimenti si avrebbe $\sqrt{2}\in\mathbb{Q}\left(\sqrt{-3}\right)$ e dunque $[K:\mathbb{Q}]=2$, che è falso. Poichè X^2-2 è irriducibile in $\mathbb{F}_5[X]$, il suo campo di spezzamento è una estensione quadratica di $\mathbb{F}_5$, dunque isomorfa ad $\mathbb{F}_{25}$. Concludiamo che X^2-2 si spezza in $\mathbb{F}_{25}\simeq\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}}{\mathfrak{p}_5'}$ e, dunque,

$$\mathcal{O}_K 5=\mathcal{O}_K\mathfrak{p}_5'=\mathfrak{P}_5\mathfrak{P}_5'.$$

Per esplicitare $\mathfrak{P}_5$ e $\mathfrak{P}_5'$, notiamo che $\mathbb{F}_{25}\simeq\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}}{\mathfrak{p}_5}\simeq\frac{\mathbb{F}_5[T]}{(T^2-T+1)}$ dove il secondo isomorfismo fa corrispondere la classe $\left[\sqrt{-3}\right]$ a T: vogliamo determinare $[f(T)]\in\frac{\mathbb{F}_5[T]}{(T^2-T+1)}$ tale che $[f(T)]^2=2$, in modo tale che

$$X^2-2=(X-[f(T)])(X+[f(T)])\text{ in }\frac{\mathbb{F}_5[T]}{(T^2-T+1)}[X]\simeq\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}}{\mathfrak{p}_5}[X]$$

e $X-f\left(\sqrt{-3}\right)$ (risp. $X+f\left(\sqrt{-3}\right)$) sia un sollevamento di $X-[f(T)]$ (risp. $X+[f(T)]$) ad $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}[X]$. Abbiamo $\frac{\mathbb{F}_5[T]}{(T^2-T+1)}=a+b[T]$ con $a,b\in\mathbb{F}_5$ e

$$\begin{aligned}(a+b[T])^2&=a^2+2ab[T]+b^2[T]^2\\&=a^2+2ab[T]+b^2([T]-1)\\&=\left(a^2-b^2\right)+\left(2ab+b^2\right)[T].\end{aligned}$$

Dunque vogliamo $2ab+b^2=0$ ed $a^2-b^2=2$: una soluzione è data dalla coppia $(a,b)=(1,3)$. Dunque $f(T)=3T+1$, $f\left(\sqrt{-3}\right)=3\sqrt{-3}+1$, abbiamo i sollevamenti $X-3\sqrt{-3}-1$ ed $X+3\sqrt{-3}+1$ e, dunque,

$$\begin{aligned}\mathfrak{P}_5&=\mathcal{O}_K 5+\mathcal{O}_K\left(\sqrt{2}-3\sqrt{-3}-1\right),\\\mathfrak{P}_5'&=\mathcal{O}_K 5+\mathcal{O}_K\left(\sqrt{2}+3\sqrt{-3}+1\right).\end{aligned}$$

Esercizio 5. [*TeoNum*] Siano K ed L due campi di numeri tali che

$$[KL:\mathbb{Q}]=[K:\mathbb{Q}][L:\mathbb{Q}]$$

e siano $\mathcal{A}\subset K$ e $\mathcal{B}\subset L$ una $\mathbb{Q}$-base di K e, rispettivamente, L.

(1) Si ricordi la definizione di $disc_{K/\mathbb{Q}}(\mathcal{A})\in\mathbb{Q}-\{0\}$.
(2) Si ricordi la definizione di $disc(\mathcal{O}_K/\mathbb{Z})\in\mathbb{Z}-\{0\}$, ricordando i fatti della teoria che ne permettono la definizione.
(3) Si mostri che, posto
$$\mathcal{AB}:=\{\alpha\beta:\alpha\in\mathcal{A},\beta\in\mathcal{B}\},$$
vale la formula
$$disc_{KL/\mathbb{Q}}(\mathcal{AB})=disc_{K/\mathbb{Q}}(\mathcal{A})^{[L:\mathbb{Q}]}\,disc_{L/\mathbb{Q}}(\mathcal{B})^{[K:\mathbb{Q}]}.$$
(Suggerimento: si utilizzi, senza dimostrarlo, il seguente fatto. Se $A=(a_{ik})_{\substack{1\le i\le m\\1\le k\le m}}$ e $(b_{jl})_{\substack{1\le j\le n\\1\le l\le n}}$, posto $A\otimes B:=(a_{ik}b_{jl})_{\substack{1\le i\le m;1\le j\le n\\1\le k\le m;1\le l\le n}}$ vale la formula
$$\det(A\otimes B)=\det(A)^n\det(B)^m).$$
(4) Si mostri che, se $(disc(\mathcal{O}_K/\mathbb{Z}),disc(\mathcal{O}_L/\mathbb{Z}))=1$, allora
$$disc(\mathcal{O}_{KL}/\mathbb{Z})=disc(\mathcal{O}_K/\mathbb{Z})^{[L:\mathbb{Q}]}\,disc(\mathcal{O}_L/\mathbb{Z})^{[K:\mathbb{Q}]}.$$

Soluzione: Per quanto riguarda (1) e (2), facciamo riferimento alle note di teoria: Definizione 3.2, Proposizione 3.4, Proposizione 4.4, Teorema 4.5 e Definizione 4.6.

(3) Posto $m := [K : \mathbb{Q}]$ ed $n := [L : \mathbb{Q}]$, scriviamo $\mathcal{A} := \{\alpha_k\}_{1\leq k\leq m}$ e $\mathcal{B} := \{\beta_l\}_{1\leq l\leq n}$, per cui $\mathcal{AB} := \{\alpha_k\beta_l\}_{1\leq k\leq m;1\leq l\leq n}$. Per definizione abbiamo

$$disc_{K/\mathbb{Q}}(\mathcal{A}) = \det\left(\{\sigma_i(\alpha_k)\}_{\substack{1\leq i\leq m\\1\leq k\leq m}}\right)^2 \text{ e } disc_{L/\mathbb{Q}}(\mathcal{B}) = \det\left(\{\delta_j(\beta_l)\}_{\substack{1\leq j\leq n\\1\leq l\leq n}}\right)^2$$

dove $\{\sigma_i\}_{1\leq i\leq m} = Hom_{\mathbb{Q}}(K,\mathbb{C})$ e $\{\delta_i\}_{1\leq j\leq n} = Hom_{\mathbb{Q}}(L,\mathbb{C})$. Consideriamo l'applicazione $\sigma \mapsto \left(\sigma_{|K}, \sigma_{|L}\right)$:

$$Hom_{\mathbb{Q}}(KL,\mathbb{C}) \longrightarrow Hom_{\mathbb{Q}}(K,\mathbb{C}) \times Hom_{\mathbb{Q}}(L,\mathbb{C}).$$

È iniettiva poichè $\sigma_{1|K} = \sigma_{2|K}$ e $\sigma_{1|L} = \sigma_{2|L}$ implica che $\sigma_1 = \sigma_2$, dunque biiettiva poichè il dominio ha cardinalitè $[KL : \mathbb{Q}]$, il codominio ha cardinalitè mn e per ipotesi $[KL : \mathbb{Q}] = mn$. Ma allora vediamo che, per definizione,

$$disc_{KL/\mathbb{Q}}(\mathcal{AB}) = \det\left(\{\sigma_i(\alpha_k)\,\delta_j(\beta_l)\}_{\substack{1\leq i\leq m;1\leq j\leq n\\1\leq k\leq m;1\leq l\leq n}}\right)^2.$$

Applicando il suggerimento otteniamo la tesi.

(4) Poichè $(disc(\mathcal{O}_K/\mathbb{Z}), disc(\mathcal{O}_L/\mathbb{Z})) = 1$, sappiamo dalla teoria che $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$. Ma allora la formula segue da (3), prendendo come $\mathcal{A}$ (risp. $\mathcal{B}$) una $\mathbb{Z}$-base di $\mathcal{O}_K$ (risp. $\mathcal{O}_L$).